MATH 6370 p-ADIC HODGE THEORY

DANIEL GULOTTA

1. Motivation: Complex Hodge theory

Cohomology is a way of measuring how many "loops" a space has.

Consider the space $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Definition 1.1. A 1-*cochain* on $\mathbb{C}^\times$ is a function on paths in $\mathbb{C}^\times$.

A 1-cochain φ is *closed* if for any continuous map f from a triangle ABC to $\mathbb{C}^\times$, $\phi(f(AC)) = \phi(f(AB)) + \phi(f(BC))$. It is *exact* if it is of the form

$$\psi(\text{ending point}) - \psi(\text{starting point})$$

for some function ψ on $\mathbb{C}^\times$.

Define

$$H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{Z}) = \{\mathbb{Z}\text{-valued closed 1-cochains}\}/\{\mathbb{Z}\text{-valued exact 1-cochains}\},$$

and define $H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{C})$ similarly.

Then $H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{Z})$ is a free abelian group of rank one, and

$$H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{C}) \cong H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$$

is a $\mathbb{C}$-vector space of dimension 1. A class in $H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{Z})$ has many representatives, but they all take on the same value on closed paths. There is a generator of $H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{Z})$ that takes any path to its winding number around the origin.

Definition 1.2. An holomorphic 1-form on $\mathbb{C}^\times$ is an expression of the form $f(z)\,dz$, where $f(z)$ is an analytic function on $\mathbb{C}^\times$. The holomorphic functions on $\mathbb{C}^\times$ are precisely the Laurent series

$$\sum_{n=-\infty}^{\infty} a_n z^n,$$

where $a_n \in \mathbb{C}$ and $|a_n| \to 0$ exponentially as $n \to \pm\infty$.

A holomorphic 1-form *exact* if it is of the form $f'(z)\,dz$, where $f(z)$ is a holomorphic function. (All holomorphic 1-forms are closed.)

Define

$$H^1_{\text{dR}}(\mathbb{C}^\times) = \{\text{holomorphic 1-forms}\}/\{\text{exact holomorphic 1-forms}\}$$

Then $H^1_{\text{dR}}(\mathbb{C}^\times)$ is a $\mathbb{C}$-vector space of dimension 1. The class of $z^{-1}\,dz$ is a generator. There is an isomorphism of vector spaces

$$H^1_{\text{dR}}(\mathbb{C}^\times) \xrightarrow{\sim} H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{C})$$

given by

$$f(z)\,dz \mapsto \left(\gamma \mapsto \int_\gamma f(z)\,dz\right). \tag{1.3}$$

For any complex manifold X, one can define the singular cohomology $H^n_{\text{sing}}(X)$ (defined using maps from simplices into X) and the de Rham cohomology $H^n_{\text{dR}}(X)$ (defined using holomorphic differentials on X). There is an isomorphism

$$H^n_{\text{dR}}(X) \cong H^n_{\text{sing}}(X, \mathbb{C})$$

given by integration.

This isomorphism is functorial: if we have a holomorphic or antiholomorphic map $\sigma\colon X \to Y$, then there is a commutative square

$$\begin{array}{ccc} H^n_{\text{dR}}(Y) & \xrightarrow{\sim} & H^n_{\text{sing}}(Y, \mathbb{C}) \\ \downarrow{\scriptstyle \sigma^*} & & \downarrow{\scriptstyle \sigma^*} \\ H^n_{\text{dR}}(X) & \xrightarrow{\sim} & H^n_{\text{sing}}(X, \mathbb{C}) \end{array}$$

If σ is holomorphic, then

$$\sigma^*(f(z)\,dz) = f(\sigma(z))\,d\sigma(z)$$
$$\sigma^*(\varphi)(\gamma) = \varphi(\sigma(\gamma))\,.$$

If σ is antiholomorphic, then

$$\sigma^*(f(z)\,dz) = \overline{f(\sigma(z))\,d\sigma(z)}$$
$$\sigma^*(\varphi)(\gamma) = \overline{\varphi(\sigma(\gamma))}\,.$$

What is the p-adic version of this story? Let K be a p-adic field. (You can assume for now that K is $\mathbb{Q}_p$ or a finite extension, but I will make a more general definition later.) A p-adic analogue of $\mathbb{C}^\times$ is the rigid analytic space $\mathbb{A}^1_K \setminus \{0\}$.

We will define rigid analytic spaces later. For now, we will just define the space of analytic functions on $\mathbb{A}^1_K \setminus \{0\}$. Motivated by the complex case, We define this space to be the set of Laurent series

$$\sum_{n=-\infty}^{\infty} a_n z^n\,,$$

where $a_n \in K$ and the $|a_n|$'s go to zero faster than exponentially as $n \to \pm\infty$. A 1-form is an analytic function multiplied by dz. Then

$$H^1_{\text{dR}}(\mathbb{A}^1_K \setminus \{0\}) = \{\text{1-forms}\}/\{\text{exact 1-forms}\}$$

is a 1-dimensional K-vector space generated by the class of $z^{-1}\,dz$.

A p-adic analogue of singular cohomology is étale cohomology. For now, we will just give a heuristic definition. Consider the map $\exp\colon \mathbb{C} \to \mathbb{C}^\times$. Any path in $\mathbb{C}^\times$ that starts and ends at 1 is the image of a path in $\mathbb{C}$ that starts at 0 and ends at $2\pi i k$, where k is the winding number of the path. So we can identify

$$H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{Z}) \cong \text{Hom}_{\mathbb{Z}}(2\pi i\mathbb{Z}, \mathbb{Z})\,.$$

Unlike the complex exponential function, the p-adic exponential has a finite radius of convergence. So it is useful instead to look at the collection of maps $z \mapsto z^n$ for each integer n. A path that starts and ends at 1 and has winding number k is the image under $z \mapsto z^n$ of a path that starts at 1 and ends at $e^{2\pi i k/n}$. The collection of roots of unity $\{e^{2\pi i k/n} | n \in \mathbb{Z}_{>0}\}$ is enough to recover k.

Let μ be the set of all roots of unity of $\mathbb{C}^\times$. Then we can identify

$$H^1_{\text{sing}}(\mathbb{C}^\times, \mathbb{Z}) \cong \text{Hom}_{\text{cts}}(\mu, \mathbb{Q}/\mathbb{Z})\,.$$

Here, μ has the topology inherited from $\mathbb{C}^\times$, and $\mathbb{Q}/\mathbb{Z}$ has the topology inherited from $\mathbb{R}/\mathbb{Z} \cong S^1$.

The isomorphism $\mathrm{Hom}_{\mathbb{Z}}(2\pi i\mathbb{Z}, \mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{cts}}(\mu, \mathbb{Q}/\mathbb{Z})$ can be described as follows. Any element of the former group is multiplication by $\frac{k}{2\pi i}$ for some integer k. Its image in the latter group the latter group is the map $e^{2\pi i m/n} \mapsto mk/n$.

With this in mind, we define

$$H^1_{\text{ét}}(\mathbb{A}^1_{\overline{K}} \setminus \{0\}, \mathbb{Z}_p) = \mathrm{Hom}_{\mathbb{Z}_p}(\mu_{p^\infty}, \mathbb{Q}_p/\mathbb{Z}_p)\,,$$

where μ_{p^∞} is the set of p-power roots of unity in $\overline{K}$. It is a free $\mathbb{Z}_p$-module of rank 1, and it has an action of $\mathrm{Gal}(\overline{K}/K)$. We will also denote this group by $\mathbb{Z}_p(-1)$.

We would like to compare $H^1_{\mathrm{dR}}(\mathbb{A}^1_K \setminus \{0\})$ and $H^1_{\text{ét}}(\mathbb{A}^1_{\overline{K}} \setminus \{0\}, \mathbb{Z}_p)$. More specifically, we would like to write down an $\mathrm{Gal}(\overline{K}/K)$-equivariant isomorphism

$$H^1_{\mathrm{dR}}(\mathbb{A}^1_K \setminus \{0\}) \otimes_K L \cong H^1_{\text{ét}}(\mathbb{A}^1_K \setminus \{0\}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} L$$

for some field L.

What should L be? The field $\overline{K}$ has a unique multiplicative absolute value extending the one on K. We write $C = \widehat{\overline{K}}$ for the completion of $\overline{K}$ with respect to this absolute value. The most obvious guess is that $L = C$.

However, it turns out that this guess does not work. We will show in a future lecture that there are no nonzero $\mathrm{Gal}(\overline{K}/K)$-equivariant maps

$$H^1_{\mathrm{dR}}(\mathbb{A}^1_K \setminus \{0\}) \otimes_K C \to H^1_{\text{ét}}(\mathbb{A}^1_{\overline{K}} \setminus \{0\}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} C\,.$$

Instead, we will have to define a ring B^+_{dR} that is a completion of $\overline{K}$ with respect to a more unusual topology. The ring B^+_{dR} will be a discrete valuation ring with residue field C. We will take $L = B_{\mathrm{dR}} = \mathrm{Frac}\, B^+_{\mathrm{dR}}$.

The p-adic analogues of complex manifolds are called rigid analytic spaces. If you are not familiar with rigid analytic spaces, you can just think about algebraic varieties over a p-adic field—there is an analytification functor that turns any such variety into a rigid analytic space. Given a rigid analytic space X over a p-adic field K, one can define étale cohomology groups

$$H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)$$

and de Rham cohomology groups

$$H^i_{\mathrm{dR}}(X)\,.$$

Theorem 1.4 (Scholze, [Sch13])**.** *If X is proper and smooth, then there is a Galois equivariant isomorphism*

$$H^i_{\mathrm{dR}}(X) \otimes_K B_{\mathrm{dR}} \cong H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} B_{\mathrm{dR}}\,.$$

Here, B_{dR} is the fraction field of B^+_{dR}.

If X comes from an algebraic variety, then this isomorphism was previously proved by Tsuji [Tsu99] and Faltings [Fal02]. There is also a version of the comparison theorem for certain non-proper varieties, including $\mathbb{A}^1_K \setminus \{0\}$, due to Li–Pan [LP19].

In p-adic Hodge theory, we study cohomology theories in p-adic geometry and the relations between them. Because $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)$ has a $\mathrm{Gal}(\overline{K}/K)$-action, and $\mathrm{Gal}(\overline{K}/K)$ is much more interesting than $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, the study of Galois representations is an important component of the theory.

2. Infinite Galois theory

Definition 2.1. Let L/K be extension of fields. Let $\mathrm{Aut}(L/K)$ denote the group of automorphisms of L fixing each element of K.

Give $\mathrm{Aut}(L/K)$ the weakest topology such that the stabilizer of any finite subset of L is open.

Example 2.2. The group $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ has two elements. The nontrivial element sends $\sqrt{2} \mapsto -\sqrt{2}$.

Example 2.3. The group $\mathrm{Aut}(\mathbb{Q}\sqrt[3]{2}/\mathbb{Q})$ is trivial. If ω is a nontrivial cube root of unity, then $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega))/\mathbb{Q}$ permutes $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$, and this permutation action induces an isomorphism $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$.

Example 2.4. Let p be a prime number. For each positive integer n, there is a field $\mathbb{F}_{p^n}$ with p^n elements. It is unique up to isomorphism. We have $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, where the Frobenius automorphism $x \mapsto x^p$ corresponds to the element $1 \in \mathbb{Z}/n\mathbb{Z}$. Then $\mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$.

Example 2.5. For each positive integer n, there is a field $\mathbb{Q}(\mu_{p^n})$ obtained by adjoining all p-power roots of unity to $\mathbb{Q}$. There is an isomorphism

$$\mathrm{Aut}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$$
$$(\zeta \mapsto \zeta^m) \leftarrow\!\shortmid m\,.$$

Let

$$\mathbb{Q}(\mu_{p^\infty}) = \varinjlim_n \mathbb{Q}(\mu_{p^n})\,.$$

Then

$$\mathrm{Aut}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p^\times\,.$$

Similarly,

$$\mathrm{Aut}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times\,.$$

Example 2.6. Let K be a field. Then $\mathrm{Aut}(K(t)/K) = \mathrm{PGL}_2(K)$, with the discrete topology. (We leave the proof as an exercise to the reader.)

Lemma 2.7. *If L/K is finite, then $\mathrm{Aut}(L/K)$ has the discrete topology.*

Proof. Choose a K-vector space basis for L. An automorphism of L fixing this basis must be the identity. □

Lemma 2.8. *If L/K is algebraic, then the map*

$$\mathrm{Aut}(L/K) \to \varprojlim_{K'} \mathrm{Aut}(K'/K)$$

is an isomorphism of topological groups, where K' runs over $\mathrm{Aut}(L/K)$-stable finite extensions of K.

Proof. Since L/K is algebraic, any $\alpha \in L$ has finite orbit under $\mathrm{Aut}(L/K)$. So the field obtained by adjoining the orbit of α to K is a finite $\mathrm{Aut}(L/K)$-stable extension of K. Specifying compatible automorphisms of each K' is equivalent to specifying an automorphism of L. □

Definition 2.9. A topological space is *profinite* if it is the inverse limit of a collection of finite sets having the discrete topology.

Lemma 2.10 ([Sta, Tag 08ZY])**.** *A topological space is profinite if and only if it is totally disconnected and compact.*

If H is a group acting on a field K, we denote by K^H the subfield of K fixed by H.

Definition 2.11. We say that L/K is *Galois* if it is algebraic and $L^{\mathrm{Aut}(L/K)} = K$.

If L/K is Galois, then we will also denote $\mathrm{Aut}(L/K)$ by $\mathrm{Gal}(L/K)$.

Example 2.12. Of the extensions mentioned in Examples 2.2–2.5, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, $\overline{\mathbb{F}}_p/\mathbb{F}_p$, $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, $\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p$ are Galois. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois since the fixed field of the automorphism group is $\mathbb{Q}(\sqrt[3]{2})$. The extension $K(t)/K$ is not Galois since it is not algebraic.

There is a more concrete characterization of Galois extensions in terms of splitting fields.

Definition 2.13. Let K be a field. A polynomial $f(x) \in K[x]$ *factors completely* if it can be written in the form $f(x) = c\prod_{i=1}^{n}(x - x_i)$ with $n \in \mathbb{Z}_{\geq 0}$, $c, x_1, \ldots, x_n \in K$ and $c \neq 0$.

Definition 2.14. Let L/K be an algebraic extension, and let $P \subset K[x] \setminus \{0\}$. We say that L is a *splitting field* for P if every element of P factors completely over L, and no proper subfield of L has this property.

Lemma 2.15. *Every subset of $K[x] \setminus \{0\}$ admits a splitting field. It is unique up to isomorphism.*

Proof. First, suppose P consists of a single element $f(x)$. Then we can construct a splitting field inductively as follows. Letting $K_0 = K$, and for $i \geq 0$, let $f_i(x)$ be an irreducible factor of $f(x)$ of degree > 1 over $K_i[x]$, and let $K_{i+1} = K[x]/f_i(x)$. Eventually, $f(x)$ factors completely in some K_n, and this K_n is a splitting field for $\{f(x)\}$.

If L is any splitting field of $\{f(x)\}$, we can construct an isomorphism $K_n \xrightarrow{\sim} L$ as follows. For each i, we construct an embedding $K_{i+1} \hookrightarrow L$ by sending the generator of K_{i+1} to some root of the polynomial $f_i(x)$ in L (using the map $K_i \hookrightarrow L$ to consider $f_i(x)$ as an element of $L[x]$). Since f does not factor completely over any subfield of L, $K_n \to L$ must be surjective, hence an isomorphism.

To prove the lemma for arbitrary P, we use Zorn's lemma. □

Definition 2.16. A polynomial $f(x) \in K[x]$ is *separable* if $f(x)$ and $f'(x)$ generate the unit ideal.

Lemma 2.17. *Suppose the polynomial $f(x) \in K[x]$ factors completely. The factors are distinct if and only if f is separable.*

Proof. Suppose $f(x)$ is divisible by $(x-\alpha)^2$ for some $\alpha \in K$. Then $f'(x)$ is divisible by $x - \alpha$. So $(f(x), f'(x)) \subset (x - \alpha)$.

Conversely, suppose $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$ has no repeated factors. By the Chinese remainder theorem, $f(x)$ and $f'(x)$ generate the unit ideal if and only if $f'(\alpha_i) \neq 0$ for all i. In fact, we have

$$f'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j) \neq 0\,.$$

□

Lemma 2.18. *An extension L/K is Galois iff it is the splitting field of a set of separable polynomials.*

Proof. Suppose L/K is Galois. Let $\alpha \in L$. Then α is a zero of some polynomial over K. Any element of the $\mathrm{Gal}(L/K)$-orbit of α is also a zero of this polynomial. So the orbit is finite. Let $\{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n\}$ be the orbit. Then

$$\prod_{i=1}^{n}(x - \alpha_i)$$

is a polynomial that is $\mathrm{Gal}(L/K)$-invariant. Since L/K is Galois, the polynomial has coefficients in K. Then L is a splitting field for the set of all polynomials that can be constructed in this way.

Conversely, suppose L/K is the splitting field of a set of separable polynomials over K. WLOG we may assume that they are irreducible over K. If $\alpha, \alpha' \in L$ are two roots of the same irreducible polynomial, then the construction of Lemma 2.15 produces an automorphism of L fixing K and sending α to α'. □

Lemma 2.19. *Let L/K be a Galois extension. If K' is a subfield of L containing K, then L/K' is Galois, and $\mathrm{Gal}(L/K')$ is closed in $\mathrm{Gal}(L/K)$.*

Proof. By Lemma 2.18, L is a splitting field for some set of polynomials over K. Then L is a splitting field for the same set of polynomials over K', so L/K' is Galois.

By Lemma 2.10, $\mathrm{Gal}(L/K')$ and $\mathrm{Gal}(L/K)$ are compact Hausdorff spaces. So $\mathrm{Gal}(L/K')$ must be closed in $\mathrm{Gal}(L/K)$. □

Lemma 2.20. *If L is a field and $H \subset \mathrm{Aut}\, L$ is a finite subgroup, then the map $H \to \mathrm{Gal}(L/L^H)$ is an isomorphism.*

Proof. The map is injective, so it suffices to prove that $|H| \geq |\mathrm{Gal}(L/L^H)|$. From the construction of Lemma 2.15, we see that $|\mathrm{Gal}(L/L^H)| = [L : L^H]$. We will show that $[L : L^H] \leq |H|$.

Let $H = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$. Let $\alpha_1, \dots, \alpha_{n+1} \in L$. The system

$$\sum_{j=1}^{n+1} \sigma_i(\alpha_j) X_j = 0 \tag{2.21}$$

has $n + 1$ variables and n equations, so it has a nonzero solution. Among all solutions, choose a solution $(c_1, \dots, c_{n+1})$ with the fewest nonzero elements. After reordering the α_j and multiplying by a scalar, we may assume $c_1 \neq 0$ and $c_1 \in F$. For any i,

$$(c_1 - \sigma(c_1), \dots, c_{n+1} - \sigma(c_{n+1}))$$

is a solution to (2.21) with fewer nonzero terms, so it must be zero. So the c_j's are all in F, and $\alpha_1, \dots, \alpha_{n+1}$ are linearly dependent over F. Therefore, $[L : L^H] \leq |H|$, as desired. □

Theorem 2.22 (Fundamental theorem of infinite Galois theory)**.** *There is a bijection between closed subgroups H of $\mathrm{Gal}(L/K)$ and subfields K' of L containing K, given by*

$$H \mapsto L^H$$
$$K' \mapsto \mathrm{Gal}(L/K')\,.$$

Proof. By Lemma 2.19, for any subfield K' of L containing K, $L^{\mathrm{Gal}(L/K')} = L$.

Conversely, suppose H is a closed subgroup of $\mathrm{Gal}(L/K)$, and suppose $\sigma \in \mathrm{Gal}(L/K) \setminus H$. Since H is closed, we can find some finite Galois extension K'' of K such that the action of σ on K'' does not agree with the action of any element of H. By Lemma 2.20, σ cannot fix $(K'')^H$. So it cannot fix L^H. Therefore, $H \to \mathrm{Gal}(L/L^H)$ is an isomorphism. □

Definition 2.23. A *separable closure* of a field K is a splitting field for the set of all separable polynomials in $K[x]$.

We denote a separable closure of K by K^{sep}. We will sometimes write G_K for $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. If K has characteristic zero, then a separable closure is the same thing as an algebraic closure.

3. Elliptic curves

In p-adic Hodge theory, we consider étale cohomology groups $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_p)$. In general, it is difficult to describe these groups explicitly. In some situations, we can be more explicit. One of these is the case where X is an elliptic curve.

Definition 3.1. Let K be a field. An elliptic curve over K is pair (E, O), where E is a complete smooth geometrically irreducible curve of genus 1 over K and $O \in E(K)$.

Sometimes, we will abuse notation and call E an elliptic curve.

If K has characteristic $\neq 2$, then any elliptic curve is isomorphic to one of the form

$$y^2 = x^3 + ax^2 + bx + c\,,$$

where $x^3 + ax^2 + bx + c$ is separable. When E is written in this form, we usually take O to be the point at ∞.

The curve E has a group structure, meaning that there are morphisms

$$+\colon E \times E \to E$$
$$-\colon E \to E$$
$$O\colon \operatorname{Spec} k \to E$$

(with O being the point chosen above), satisfying the usual group axioms.

The group structure can be described as follows. Given two points P_1, P_2 on E, there is exactly one other point Q where the line through P_1, P_2 intersects E. (If $P_1 = P_2$, we use the tangent line through P_1.) Define $P_1 + P_2$ to be the reflection of Q about the x-axis.

Then the point at infinity is the identity, and the inverse of any point is its reflection about the x-axis.

To see that the group operation is associative, we consider line bundles on E. Let $dx + ey = f$ be the equation of the line through P_1, P_2, and let g be the x-coordinate of the third intersection of this line with the elliptic curve. The rational function $\frac{dx+ey-f}{x-g}$ has zeros at P_1, P_2 and poles at $P_1 + P_2$ and O. It determines an isomorphism of line bundles

$$\mathcal{O}([P_1] + [P_2] - [O]) \cong \mathcal{O}([P_1 + P_2])\,.$$

Given a third point P_3, we have

$$\mathcal{O}([P_1] + [P_2] + [P_3] - 2[O]) \cong \mathcal{O}([(P_1 + P_2) + P_3]) \cong \mathcal{O}([P_1 + (P_2 + P_3)])$$

Since E does not have genus 0, it cannot have a rational function with a single zero and pole, so we must have $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

The above proof is somewhat sketchy. A more rigorous treatment uses the Picard functor. There is a contravariant functor $\operatorname{Pic}\colon \text{Scheme} \to \text{Ab}$ that sends a scheme X to the group of isomorphism classes of line bundles on X, with the group operation being tensor product. For any map of schemes $X \to S$, there is a contravariant functor $\operatorname{Pic}_{X/S}\colon \text{Scheme}/S \to \text{Ab}$ that sends a scheme T over S to $\operatorname{Pic}(X \times_S T)/\operatorname{Pic}(T)$. For any curve X over S, there is a natural transformation $X \mapsto \operatorname{Pic}_{X/S}$. If X is projective, then any invertible sheaf on X has a well-defined degree, so we can write

$$\operatorname{Pic}_{X/S} = \bigsqcup_{d \in \mathbb{Z}} \operatorname{Pic}^d_{X/S} .$$

If X is an elliptic curve, then one can show that $X \mapsto \operatorname{Pic}^1_{X/S}$ is an isomorphism. The point O also determines an isomorphism $\operatorname{Pic}^1_{X/S} \cong \operatorname{Pic}^0_{X/S}$. Since $\operatorname{Pic}_{X/S}$ has a group structure, E does as well. For more details, see [KM85, Theorem 2.1.2].

Remark 3.2. If X is a singular curve defined by a Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$, then the nonsingular locus of X still has a group structure. (If a line passes through a singular point of X, the intersection multiplicity is at least 2. So if a line intersects the curve at two nonsingular points, then the third intersection point must also be nonsingular.)

For example, the additive group $\mathbb{G}_a = \operatorname{Spec} K[t]$ is isomorphic to the nonsingular locus of the cuspidal cubic $y^2 = x^3$ via the map $t \mapsto (t^{-3}, t^{-2})$. We leave it as an exercise to the reader to check that this map is a homomorphism of groups.

Remark 3.3. Although the focus of today's lecture was on elliptic curves over fields, one can define an elliptic curve over an arbitrary scheme S. It is a pair (E, O), where E is a smooth proper curve over S with geometrically connected fibers of genus 1, and $O\colon S \to E$ is a section of $E \to S$.

If E is a smooth degree 3 curve in $\mathbb{P}^2_S$ equipped with a section $O\colon S \to E$, then (E, O) is an elliptic curve. Even if E is not smooth, the nonsingular locus still has a group structure with identity O.

4. Formal groups

(This class was a guest lecture by Petar Bakić. I was not at the lecture, but this is my attempt at summarizing the relevant sections of Silverman's book.)

Let R be a ring. Let

$$E = \operatorname{Proj} R[X, Y, Z]/(X^3 + aX^2Z + bXZ^2 + cZ^3 - Y^2Z) .$$

As we saw in the previous class, the nonsingular locus E_{ns} of E admits a group structure. We take the identity to be the point $O = (0 : 1 : 0)$, corresponding to the ideal (X, Z).

We can consider the formal completion of E at O. The locus $Y \neq 0$ is the affine $\operatorname{Spec} A$, where

$$A = R[x, z]/(x^3 + ax^2z + bxz^2 + cz^3 - z) ,$$

where $x = X/Y$, $z = Z/Y$.

The point O corresponds to the ideal (x, z). The formal completion of E along O is $\hat{E} = \operatorname{Spf} \hat{A}$, where

$$\hat{A} = \varprojlim_n A/I^n \cong R[\![z]\!] .$$

(Don't worry if you are not familiar with formal schemes, as we will just be working with the power series ring $R[\![z]\!]$.) The group operation $E_{\mathrm{ns}} \times_R E_{\mathrm{ns}} \to E_{\mathrm{ns}}$ induces a group operation $\hat{E} \times_R \hat{E} \to \hat{E}$. This gives us a continuous map of power series rings

$$R[\![z]\!] \cong \hat{A} \to \hat{A} \hat{\otimes}_R \hat{A} \cong R[\![z_1, z_2]\!] .$$

Note that any map continuous map $R[\![z]\!] \to R[\![z_1, z_2]\!]$ is determined by the image of z Denote the image of z by $F(z_1, z_2)$. Similarly, there is an inverse map $\hat{E} \to \hat{E}$, which corresponds to a continuous map of power series rings $R[\![z]\!] \to R[\![z]\!]$. Let $i(z)$ be the image of z.

Since the group operation is commutative and associative, we will have

$$F(z_1, z_2) = F(z_2, z_1) ,$$
$$F(z_1, F(z_2, z_3)) = F(F(z_1, z_2), z_3) .$$

Similarly, since i is the inverse operation, and $z = 0$ is the identity,

$$F(z, i(z)) = 0 .$$

The above analysis leads us to consider the notion of a *formal group law.*

Definition 4.1. A *one-parameter commutative formal group* over a ring R is a power series $F(X, Y) \in R[\![X, Y]\!]$ satisfying the following conditions:

(1) $F(X, 0) = X$ and $F(0, Y) = Y$
(2) $F(X, F(Y, Z)) = F(F(X, Y), Z)$
(3) $F(X, Y) = F(Y, X)$
(4) There is a power series $i(T) \in R[\![T]\!]$ satisfying $i(0) = 0$ and $F(T, i(T)) = 0$.

Example 4.2. The formal additive group $\widehat{\mathbb{G}}_a$ is defined by

$$F(X, Y) = X + Y .$$

Example 4.3. The formal mutliplicative group $\widehat{\mathbb{G}}_m$ is defined by

$$F(X, Y) = (1 + X)(1 + Y) - 1 = X + Y + XY .$$

Definition 4.4. A homorphism of formal groups $F \to G$ is a power series $\phi \in R[\![T]\!]$ such that

$$\phi(F(X, Y)) = G(\phi(X), \phi(Y)) .$$

Example 4.5. For any integer m, we can define a multiplication-by-m homomorphism $[m] \colon F \to G$ inductively by

$$[0](T) = 0$$
$$[m + 1](T) = F([m]T, T)$$
$$[m - 1](T) = F([m]T, i(T))$$

If $F = \mathbb{G}_a$, then

$$[m](T) = mT .$$

If $F = \mathbb{G}_m$, then

$$[m](T) = (1 + T)^m - 1 .$$

Lemma 4.6. *Let*

$$F = a_1 T + a_2 T^2 + \cdots \in TR[\![T]\!] ,$$

with $a_1 \in R^\times$. Then there is a unique power series $G \in TR[\![T]\!]$ such that $F(G(T)) = G(F(T)) = T$.

Proof. See [Sil09, Lemma IV.2.4]. □

Lemma 4.7. *Let F be a formal group over R, and let m be an integer that is invertible in R. Then $[m]$ is an automorphism.*

Proof. It is clear that multiplication by m sends

$$T \mapsto mT + O(T^2)\,.$$

Any such map is an automorphism of $R[\![T]\!]$ by Lemma 4.6. □

Now let K be a complete discretely valued nonarchimedean field, and let $R = \mathcal{O}_K$. Let $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$, and let $k = \mathcal{O}_K/\mathfrak{m}_K$ be the residue field.

For every $x \in \mathfrak{m}_K$, there is a unique continuous homomorphism $\mathcal{O}_K[\![T]\!] \to \mathcal{O}_K$ sending $T \mapsto x$, and conversely, all continuous homomorphisms $\mathcal{O}_K[\![T]\!] \to \mathcal{O}_K$ are of this form. Similarly, homomorphisms $\mathcal{O}_K[\![T_1, T_2]\!] \to \mathcal{O}_K$ are in bijection with $\mathfrak{m}_K \times \mathfrak{m}_k$. If F is a formal group, we will denote by $F(\mathfrak{m}_K)$ the set $\mathfrak{m}_K$, with the group operation $+_F$ given by

$$x +_F y = F(x, y)\,.$$

Example 4.8. We can identify $\widehat{\mathbb{G}}_a(\mathfrak{m}_K)$ with the additive group $\mathfrak{m}_K$, and there is an exact sequence

$$0 \to \mathfrak{m}_K \to \mathcal{O}_K \to k \to 0\,.$$

Example 4.9. We can identify $\widehat{\mathbb{G}}_m(\mathfrak{m}_K)$ with the multiplicative group $1 + \mathfrak{m}_K$, and there is an exact sequence

$$1 \to (1 + \mathfrak{m}_K) \to \mathcal{O}_K^\times \to k^\times \to 1\,.$$

Lemma 4.10. *For each positive integer n, the operation $+_F$ induces the usual additive group structure on $\mathfrak{m}_K^n/\mathfrak{m}_K^{n+1}$.*

Lemma 4.11. *If $x \in F(\mathfrak{m}_K)$ has finite order, then its order is a power of the characteristic of k.*

Proof. This follows from Lemma 4.7. □

Definition 4.12. An *invariant differential* for F is an expression of the form $P(T)\,dT$, where $P(T) \in \mathcal{O}_K[\![T]\!]$, such that

$$P(F(X,Y))F^{(1,0)}(X,Y) = P(X) \tag{4.13}$$

as formal power series.

Theorem 4.14. *Let*

$$\omega_F = F^{(1,0)}(0,T)^{-1}\,dT\,. \tag{4.15}$$

Then the invariant differentials for F are precisely the constant multiples of ω_F.

Proof. When $X = 0$, the identity (4.13) becomes

$$P(Y)F^{(1,0)}(0,Y) = P(0)\,.$$

Since $F^{(1,0)}(0,Y)$ has constant term 1, it is invertible. So the only possible invariant differentials are multiples of ω_F. To see that these are actually invariant differentials, differentiate the associative law

$$F(X, F(Y,Z)) = F(F(X,Y), Z)\,.$$

with respect to U. We obtain

$$F^{(1,0)}(X, F(Y,Z)) = F^{(1,0)}(F(X,Y), Z)F^{(1,0)}(X,Y)\,.$$

When $X = 0$, this becomes

$$F^{(1,0)}(0, F(Y,Z)) = F^{(1,0)}(Y,Z)F^{(1,0)}(0,Z)\,.$$

□

Corollary 4.16. *If $\phi\colon F \to G$ is a homomorphism of formal group laws, then*

$$\omega_G \circ \phi = \phi'(0)\omega_F\,.$$

Corollary 4.17. *Let F be a formal group over $\mathcal{O}_K$, and suppose the multiplication-by-p map sends*

$$T \mapsto G(T)\,.$$

Then $G'(T)$ is divisible by p. Equivalently,

$$G(T) = pH(T) + I(T^p)$$

for some formal power series H, I.

Theorem 4.18. *Let F be a formal group over $\mathcal{O}_K$, and let $x \in F(\mathfrak{m}_k)$. Suppose that x has exact order p^n, meaning that $p^n x = 0$ but $p^{n-1}x \neq 0$. Then $|x| \geq |p|^{1/(p^n - p^{n-1})}$.*

Proof. We use induction on n. Suppose $n = 1$. Let $G(T)$ be as in Corollary 4.17. Then x satisfies $G(x) = 0$. The linear term of $G(x)$ is px. All other terms with exponent not divisible by p are also multiples of p, so they have strictly smaller absolute values. Among the terms with exponent divisible by p, the largest possible absolute value is $|x|^p$. So we must have $|px| \leq |x|^p$. We can rewrite this equality as $|x| \geq |p|^{1/(p-1)}$.

Now assume that all points of exact order n satisify $|x| \geq |p|^{1/(p^n - p^{n-1})}$, and let y be a point of exact order $n+1$. In order for any of the terms of $G(y)$ to have absolute value greater than or equal to $|x|$, we must have $|y| \geq |p|^{1/(p^{n+1} - p^n)}$. This completes the induction. □

5. Elliptic curves, continued

Definition 5.1. Let (E, O), (E', O') be elliptic curves over K. A morphism $(E, O) \to (E', O')$ is a morphism $E \to E'$ sending O to O'.

Lemma 5.2. *Any morphism $\phi\colon (E,O) \to (E',O')$ of elliptic curves is a group homomorphism.*

Proof. If ϕ is constant, then it is a group homomorphism. Otherwise, ϕ is a finite locally free morphism, so there is an induced homomorphism $\phi_*\colon \operatorname{Pic}^0_{E/K} \to \operatorname{Pic}^0_{E'/K}$. Since we can identify E,E' with $\operatorname{Pic}^0_{E/K}$, $\operatorname{Pic}^0_{E'/K}$, respectively, ϕ must also be a group homomorphism. □

We will write $\operatorname{Hom}(E, E')$ for the set of morphisms $(E,O) \to (E',O')$, and $\operatorname{End}(E)$ for $\operatorname{Hom}(E,E')$. Lemma 5.2 implies that $\operatorname{End}(E)$ is a (not necessarily commutative) ring.

Lemma 5.3. *Let E be an elliptic curve.*

(1) $\operatorname{End} E$ *has no zero divisors.*

(2) *For any nonzero integer n, the multiplication by n map $E \to E$ is not zero.*

Proof. For the first item, observe that any nonzero element of $\operatorname{End} E$ is surjective, and the composition of two surjections is a surjection.

For the second item, see [Sil09, Proposition III.4.2(a)]. □

Since the Picard functor is contravariant, any homomorphism $\phi\colon E \to E'$ also induces a homomorphism $\hat{\phi}\colon \operatorname{Pic}^0_{E'/K} \to \operatorname{Pic}^0_{E/K}$, or equivalently, a homomorphism $\hat{\phi}\colon E' \to E$.

Lemma 5.4.

(1) *For any $\phi \in \operatorname{Hom}(E, E')$, $\hat{\phi}\phi$ is multiplication by $\deg \phi$.*
(2) *For any $\phi \in \operatorname{Hom}(E, E')$, $\psi \in \operatorname{Hom}(E', E'')$, $\widehat{\psi\phi} = \hat{\phi}\hat{\psi}$.*
(3) *For any $\phi, \psi \in \operatorname{Hom}(E, E')$, $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$.*
(4) *For any integer n, the image of n in $\operatorname{Hom}(E, E)$ is self dual.*
(5) *For any $\phi \in \operatorname{Hom}(E, E')$, $\deg \hat{\phi} = \deg \phi$.*
(6) $\hat{\hat{\phi}} = \phi$

Proof. See [Sil09, Theorem 6.1 and 6.2]. □

Corollary 5.5. *The degree map* $\deg\colon \operatorname{Hom}(E, E') \to \mathbb{Z}$ *is a positive definite quadratic form.*

Corollary 5.6. *For any elliptic curve E, the multiplication by N map has degree N^2.*

For any positive integer N, let

$$E(K^{\text{sep}})[N] = \{P \in E(K^{\text{sep}}) | NP = 0\}.$$

Corollary 5.7.
If the characteristic of K does not divide N, then $E(K^{\text{sep}})[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$.

Note that $\operatorname{Gal}(K^{\text{sep}}/K)$ acts on $E(K^{\text{sep}})[N]$.

For any prime p, define the Tate module

$$T_p(E) = \varprojlim_n E(K^{\text{sep}})[p^n].$$

If the characteristic of K is different from p, then $T_p(E)$ is a free $\mathbb{Z}_p$-module of rank 2

Theorem 5.8. *Suppose the characteristic of K is different from p. Then the natural map*

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

is injective.

Proof. See [Sil09, Theorem III.7.4]. □

Corollary 5.9. $\operatorname{Hom}(E, E')$ *is a free $\mathbb{Z}$-module of rank at most 4.*

Corollary 5.10. $\operatorname{End}(E) \otimes \mathbb{Q}$ *is isomorphic to one of the following:*

(1) $\mathbb{Q}$*;*
(2) *An imaginary quadratic extension of $\mathbb{Q}$;*
(3) *A quaternion algebra over $\mathbb{Q}$, ramified at $p = \operatorname{char} K$ and ∞, and at no other places.*

A quaternion algebra over $\mathbb{Q}$ is a division algebra D with center $\mathbb{Q}$ satisfying $[D : \mathbb{Q}] = 4$. By "ramified at p and ∞", we mean that $D \otimes \mathbb{Q}_p$ and $D \otimes \mathbb{R}$ are division algebras, while $D \otimes \mathbb{Q}_\ell \cong M_2(\mathbb{Q}_\ell)$ is the ring of 2×2 matrices for all $\ell \neq p$.

Remark 5.11. If L is an extension of K, then $\mathrm{End}(E_L)$ can be larger than $\mathrm{End}(E)$. For example, if E is the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$, then $\mathrm{End}\, E = \mathbb{Z}$, but $\mathrm{End}\, E_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, where i acts by $(x, y) \mapsto (-x, iy)$.

Remark 5.12. The action of G_K on $T_p(E)$ commutes with endomorphisms of E. From the classification of Theorem 5.10, we deduce:

- If $\mathrm{End}(E) \otimes \mathbb{Q}$ is an imaginary quadratic extension F of $\mathbb{Q}$, then the map $G_K \to \mathrm{End}\, T_p(E)$ factors through $(\mathbb{Z}_p \otimes \mathcal{O}_F)^\times$.
- If $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra, then G_K acts by scalars on $T_p(E)$.

Remark 5.13. Tate modules are closely related to étale cohomology. If E is an elliptic curve over a field K, then

$$H^i_{\text{ét}}(E_{\overline{K}}, \mathbb{Z}_p) = \begin{cases} \mathbb{Z}_p \quad \text{(with trivial } G_K\text{-action)}, & i = 0 \\ \mathrm{Hom}_{\mathbb{Z}_p}(T_p(E), \mathbb{Z}_p), & i = 1 \\ \mathbb{Z}_p(-1), & i = 2 \\ 0, & \text{otherwise}\,. \end{cases}$$

6. Elliptic curves, continued

Étale cohomology is supposed to satisfy many of the same properties as singular cohomology. In particular, it is expected to satisfy Poincaré duality. For elliptic curves, this means that there should be an antisymmetric cup product map

$$H^1_{\text{ét}}(E_{\bar{K}}, \mathbb{Z}_p) \times H^1_{\text{ét}}(E_{\bar{K}}, \mathbb{Z}_p) \to H^2_{\text{ét}}(E_{\bar{K}}, \mathbb{Z}_p)$$

that is a perfect pairing. Since

$$H^1_{\text{ét}}(E_{\bar{K}}, \mathbb{Z}_p) = T_p(E)^*$$
$$H^2_{\text{ét}}(E_{\bar{K}}, \mathbb{Z}_p) = \mathbb{Z}_p(-1)\,,$$

specifying the cup product map is equivalent to specifying a perfect pairing

$$T_p(E) \times T_p(E) \to \mathbb{Z}_p(1)\,.$$

This map can be constructed using the Weil pairing.

For each N and each extension L of K, there is a Weil pairing

$$e_N \colon E(L)[N] \times E(L)[N] \to \mu_N(L)\,.$$

If can be defined as follows. Let $P, Q \in E(L)[N]$. Then

$$\sum_{m=0}^{N-1} ([P + mQ] - [mQ])$$

is a principal divisor. Let g be a function with this divisor. Let $T_Q g$ denote the translation of g by Q Then $T_Q g$ and g have the same divisor, so $T_Q g = \omega g$ for some constant ω. Since T_Q^N is the identity, ω is an nth root of unity. We define

$$e_N(P, Q) = \omega\,.$$

Theorem 6.1. *The Weil pairing has the following properties:*

(1) *It is bilinear:*

$$e_N(P+Q,R) = e_N(P,R) + e_N(Q,R), \quad e_N(P,Q+R) = e_N(P,Q) + e_N(P,R)$$

(2) *It is alternating:*

$$e_N(P,P) = 1$$

(3) *If N does not divide the characteristic of K, then it is a perfect pairing.*

(4) *It is $\mathrm{Aut}(L/K)$-invariant: for $\sigma \in \mathrm{Aut}(L/K)$,*

$$e_N(P^\sigma, Q^\sigma) = e_N(P,Q)^\sigma$$

(5) *The Weil pairings for various N are compatible: if $P \in E(L)[MN], Q \in E(L)[M]$,*

$$e_{MN}(P,Q) = e_M(NP,Q)\,.$$

If the characteristic of K is not p, then we can take inverse limits to get a perfect pairing

$$T_p(E) \times T_p(E) \to \mathbb{Z}_p(1)\,.$$

(Recall that $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}(K^{\mathrm{sep}})$, where $\mu_{p^n}(K^{\mathrm{sep}})$ is the group of p^nth roots of unity of K^{sep}.)

We are particularly interested in elliptic curves over p-adic fields. We still need to define what these are.

Definition 6.2. A *nonarchimedean field* is a field K that is complete with respect to a norm $|\cdot|\colon K \to \mathbb{R}^{\geq 0}$ such that:

$$|xy| = |x||y| \text{ and } |x+y| \leq \max(|x|,|y|) \text{ for all } x,y \in K$$

$$|0| = 0, \quad |1| = 1$$

$$0 < |x| < 1 \text{ for some } x \in K$$

We will write

$$\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$$

$$\mathfrak{m}_K = \{x \in K \mid |x| < 1\}\,.$$

We say that K is *discretely valued* if the image of $K^\times$ under $|\cdot|$ is a discrete subset of $\mathbb{R}^{>0}$. Equivalently,

$$\sup_{x \in \mathfrak{m}_K} |x| < 1\,.$$

Example 6.3. Let p be a prime. We can define a norm $|\cdot|$ on $\mathbb{Q}$ by $\left|p^m \frac{r}{s}\right| = p^{-m}$ for all integers r, s not divisible by p. Then $\mathbb{Q}_p$ is defined to be the completion of $\mathbb{Q}$ with respect to this norm. It is a nonarchimedean field.

The norm on $\mathbb{Q}_p$ extends uniquely to any algebraic extension of $\mathbb{Q}_p$. Any finite extension of $\mathbb{Q}_p$ is nonarchimedean, as is the completion of any infinite algebraic extension of $\mathbb{Q}_p$.

Definition 6.4. A field K is *perfect* if every irreducible polynomial in $K[x]$ is separable.

Proposition 6.5. *Every field of characteristic* 0 *is perfect. A field of characteristic $p > 0$ is perfect iff every element is a pth power.*

For the remainder of the lecture, we will fix a prime p.

Definition 6.6. A *p-adic field* is a discretely valued nonarchimedean field K of characteristic zero, such that its residue field $\mathcal{O}_K/\mathfrak{m}_K$ is perfect of characteristic p.

Example 6.7. The field $\mathbb{Q}_p$ is a p-adic field, as is any finite extension of $\mathbb{Q}_p$. The completion of an infinite algebraic extension of $\mathbb{Q}_p$ may or may not be a p-adic field.

Let K be a p-adic field, and let $k = \mathcal{O}_K/\mathfrak{m}_K$ be its residue field. There is a surjection $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{k}/k)$. The kernel is called the *inertia subgroup* of $\mathrm{Gal}(\overline{K}/K)$.

Definition 6.8. We say that a representation of $\mathrm{Gal}(\overline{K}/K)$ is *unramified* if it factors through $\mathrm{Gal}(\overline{k}/k)$. Otherwise, we say that it is ramified.

Example 6.9. For $\ell \neq p$, $\mathbb{Z}_\ell(1)$ is unramified, since all ℓ-power roots of unity in $\overline{K}$ have distict images in $\overline{k}$. But $\mathbb{Z}_p(1)$ is ramified since all p-power roots of unity in $\overline{K}$ map to 1 in $\overline{k}$.

Definition 6.10. We say that a proper smooth variety X over K has *good reduction* if it can be extended to a proper smooth scheme of finite type over $\mathcal{O}_K$.

Otherwise, we say that it has *bad reduction*.

Example 6.11. If $p \neq 2$, then the elliptic curve E over K defined by $y^2 = x(x-1)(x+1)$ has good reduction, since $y^2 = x(x-1)(x+1)$ defines a nonsingular curve over $\mathcal{O}_K$. It is possible to show that E does not have good reduction at 2.

Recall that an elliptic curve over $\mathcal{O}_K$ is a pair (E, O), where E is a proper smooth scheme over $\mathcal{O}_K$ such that E_K and E_k are geometrically connected curves of genus 1, and O is an $\mathcal{O}_K$-point of E.

Lemma 6.12. *Let X be a proper scheme over $\mathcal{O}_K$. Then the restriction map $X(\mathcal{O}_K) \to X(K)$ is a bijection. In particular, there is a natural reduction map $X(K) \to X(k)$.*

Proof. This follows from the valuative criterion of properness. □

Theorem 6.13. *If E is an elliptic curve over $\mathcal{O}_K$, then there is an exact sequence*

$$0 \to \hat{E}(\mathfrak{m}_K) \to E(K) \to E(k) \to 0\,.$$

Corollary 6.14. *If E is an elliptic curve over $\mathcal{O}_K$, and ℓ is a prime different form* $\mathrm{char}\, K$*, then the reduction maps*

$$E(K)[\ell^n] \to E(k)[\ell^n]$$

and

$$T_\ell(E_K) \to T_\ell(E_k)$$

are isomorphisms.

Proof. For each n, there is an exact sequence

$$\hat{E}(\mathfrak{m}_K)[\ell^n] \to E(K)[\ell^n] \to E(k)[\ell^n] \to \hat{E}(\mathfrak{m}_K)/\ell^n\,.$$

But multiplication by ℓ is invertible on $\hat{E}(\mathcal{O}_K)$, so the outer terms are zero. So the maps $E(K)[\ell^n] \to E(k)[\ell^n]$ are isomorphisms. Taking the direct limit over algebraic extensions of K and inverse limit over n shows that $T_\ell(E_K) \to T_\ell(E_k)$ is an isomorphism. □

Corollary 6.15. *If an elliptic curve E over K has good reduction, then $T_\ell(E)$ is unramified for every prime $\ell \neq p$.*

The converse is also true, although we will not give a proof.

Theorem 6.16 (Néron–Ogg–Shafarevich)**.** *Let ℓ be a prime different from p. An elliptic curve E over K has good reduction if and only if $T_\ell(E)$ is unramified. More generally, an abelian variety X over K has good reduction if and only if $T_\ell(X)$ is unramified.*

By contrast, $T_p(X)$ is never unramified. If X is an elliptic curve, then it follows from the Weil pairing that $\wedge^2 T_\ell(X) \cong \mathbb{Z}_\ell(1)$, and we saw that this representation is ramified if $\ell = p$.

However, it is possible to determine if X has good reduction from $T_p(X)$. The criterion uses the notion of a crystalline representation, which we will define in a later lecture.

Theorem 6.17. *An abelian variety X over K has good reduction if and only if $T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is crystalline.*

Before we move on, I want to do a little bit of p-adic analysis. Previously, we claimed that $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. We will now give a proof using the theory of Newton polygons. (It is possible to give a more elementary proof using Eisenstein's criterion, but the method of Newton polygons is more general, so it is useful to know.)

Lemma 6.18. *Let K be a nonarchimedean field, and let L/K be an algebraic extension. Then there is a unique nonarchimedean absolute value on K extending the absolute value on L.*

Proof. See [Bos14, Theorem A.3]. □

Let K be a nonarchimedean field with absolute value $|\cdot|$. Define a "valuation" $v\colon K \to \mathbb{R} \cup \{\infty\}$ by $v(x) = -\log|x|$.

Definition 6.19. Let K be a nonarchimedean field. Let $f(x) = \sum i = 0^n a_i x^i$ be a polynomial with $a_0, a_n \neq 0$. The *Newton polygon* of f is the lower envelope of the points $(i, v(a_i)) \in \mathbb{R}^2$.

Proposition 6.20. *Let*

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

with

$$v(\alpha_1) \leq v(\alpha_2) \leq \cdots \leq v(\alpha_n)$$

Then the slopes of the Newton polygon of f are precisely the $-v(\alpha_i)$ (with multiplicity).

Proof. Let $1 \leq m \leq n$. Then the coefficient of x^{n-m} is the sum of all products of m of the α_i's. Each term in the sum has valuation at least $\sum_{i=1}^m v(\alpha_i)$, so the valuation of the sum is at lesat this large. If $v(\alpha_m) < v(\alpha_{m+1})$, then only one term has this valuation, so the sum is exactly this large. □

Corollary 6.21. *If $f(x)$, $g(x)$ are any polynomials with nonzero constant term, then the Newton polygon of $f(x)g(x)$ is obtained from the Newton polygons of $f(x)$ and $g(x)$ by rearranging segments in order of slope.*

Proposition 6.22. *If a polynomial $f(x)$ is irreducible, then its Newton polygon has only one slope. Conversely, if f has degree n and the y-coordinates of the Newton polygon at $x = 1, \ldots, n-1$ are not in the image of v, then f is irreducible.*

Proof. The first claim follows from Hensel's lemma; see [Bos14, Lemma 4] for the statement and proof of the lemma. The second claim follows from Corollary 6.21. □

Example 6.23. The group $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)$ must send a p^nth root of unity to another p^nth root of unity, so there is a natural injection $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) \hookrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$. To show that this map is an isomorphism, it suffices to show that both groups have the same number of elements.

We claim that the polynomial

$$\frac{(1+T)^{p^n}-1}{(1+T)^{p^{n-1}}-1}$$

is irreducible. It has integer coefficients, and the coefficient of the constant term is p. If we normalize v so that $v(p)=1$, then the Newton polygon is the line segment from $(0,0)$ to $(p^n-p^{n-1},1)$. By Proposition 6.22, the polynomial is irreducible. So

$$|\operatorname{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)| = [\mathbb{Q}_p(\mu_{p^n}):\mathbb{Q}_p] = p^n - p^{n-1} = |(\mathbb{Z}/p^n\mathbb{Z})^\times|\,.$$

References

[Bos14] S. Bosch. *Lectures on formal and rigid geometry*, volume 2105 of *Lect. Notes Math.* Cham: Springer, 2014.

[Fal02] G. Faltings. Almost étale extensions. In *Cohomologies p-adiques et applications arithmétiques (II)*, pages 185–270. Paris: Société Mathématique de France, 2002.

[KM85] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Ann. Math. Stud.* Princeton University Press, Princeton, NJ, 1985.

[LP19] S. Li and X. Pan. Logarithmic de Rham comparison for open rigid spaces. *Forum Math. Sigma*, 7:53, 2019. Id/No e32.

[Sch13] P. Scholze. p-adic Hodge theory for rigid-analytic varieties. *Forum Math. Pi*, 1:77, 2013. Id/No e1.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 2009.

[Sta] Stacks Project Authors. Stacks Project. `http://stacks.math.columbia.edu`.

[Tsu99] T. Tsuji. p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case. *Invent. Math.*, 137(2):233–411, 1999.