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 $H^n_{\mathrm{sing}}(X)$ (defined using maps from simplices into X) and the de Rham cohomology $H^n_{\mathrm{dR}}(X)$ (defined using holomorphic differentials on X). There is an isomorphism

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

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

$$\begin{tikzcd} H^n_{\mathrm{dR}}(Y) \arrow[r, "\sim"] \arrow[d, "\sigma^*"] & H^n_{\mathrm{sing}}(Y, \mathbb{C}) \arrow[d, "\sigma^*"] \\ H^n_{\mathrm{dR}}(X) \arrow[r, "\sim"] & H^n_{\mathrm{sing}}(X, \mathbb{C}) \end{tikzcd}$$

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

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

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

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

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 $e^{2\pi ik/n}$. The collection of roots of unity $\{e^{2\pi ik/n} | n \in \mathbb{Z}_{>0}\}$ is enough to recover k.

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

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

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

$$\begin{gathered}\mathrm{Aut}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \\ (\zeta \mapsto \zeta^m) \mapsfrom m\,.\end{gathered}$$

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 $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n\}$ 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 $H \subset \operatorname{Aut} L$ 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 $H = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Let $\alpha_1, \ldots, \alpha_{n+1} \in L$. 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 $(c_1, \ldots, c_{n+1})$ 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,

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

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 $\alpha_1, \ldots, \alpha_{n+1}$ 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 $\mathrm{Pic}\colon \mathrm{Scheme} \to \mathrm{Ab}$ 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 $\mathrm{Pic}_{X/S}\colon \mathrm{Scheme}/S \to \mathrm{Ab}$ that sends a scheme T over S to $\mathrm{Pic}(X \times_S T)/\mathrm{Pic}(T)$. For any curve X over S, there is a natural transformation $X \mapsto \mathrm{Pic}_{X/S}$. If X is projective, then any invertible sheaf on X has a well-defined degree, so we can write

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

If X is an elliptic curve, then one can show that $X \mapsto \mathrm{Pic}^1_{X/S}$ is an isomorphism. The point O also determines an isomorphism $\mathrm{Pic}^1_{X/S} \cong \mathrm{Pic}^0_{X/S}$. Since $\mathrm{Pic}_{X/S}$ 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 $\mathbb{G}_a = \mathrm{Spec}\, K[t]$ 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

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

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 $\mathrm{Spec}\, A$, 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 $\hat{E} = \mathrm{Spf}\, \hat{A}$, 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 satisfy $|x| \geq |p|^{1/(p^n - p^{n-1})}$, 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 $\phi_*\colon \mathrm{Pic}^0_{E/K} \to \mathrm{Pic}^0_{E'/K}$. Since we can identify E,E' with $\mathrm{Pic}^0_{E/K}$, $\mathrm{Pic}^0_{E'/K}$, respectively, ϕ must also be a group homomorphism. □

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

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

(1) $\mathrm{End}\,E$ *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 $\operatorname{End}(E_L)$ can be larger than $\operatorname{End}(E)$. For example, if E is the elliptic curve $y^2=x^3-x$ over $\mathbb{Q}$, then $\operatorname{End}E=\mathbb{Z}$, but $\operatorname{End}E_{\mathbb{Q}(i)}=\mathbb{Z}[i]$, 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 $\operatorname{End}(E)\otimes\mathbb{Q}$ is an imaginary quadratic extension F of $\mathbb{Q}$, then the map $G_K\to\operatorname{End}T_p(E)$ factors through $(\mathbb{Z}_p\otimes\mathcal{O}_F)^\times$.
- If $\operatorname{End}(E)\otimes\mathbb{Q}$ 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

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

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_Qg denote the translation of g by Q Then T_Qg and g have the same divisor, so $T_Qg=\omega g$ 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

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

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.

Lemma 6.4. *Let K be a nonarchimedean field, and let L/K be an algebraic extension. Then there is a unique nonarchimedean absolute value on L extending the absolute value on K.*

Proof. See [Bos14, Theorem A.3]. □

Remark 6.5. If L/K is finite, and the norms on K, L are denoted by $|\cdot|_K$, $|\cdot|_L$, respectively, then

$$|x|_L = |N_{L/K}(x)|_K^{1/[L:K]}\,.$$

It takes some work to show that the right-hand side satisfies the triangle inequality.

Corollary 6.6. *Any finite extension of $\mathbb{Q}_p$ is nonarchimedean, as is the completion of any infinite algebraic extension of $\mathbb{Q}_p$.*

Definition 6.7. A field K is *perfect* if every irreducible polynomial in $K[x]$ is separable.

Proposition 6.8. *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 6.9. 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 6.10. 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 6.11. 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 6.12. 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 $\overline{k}$.

7. Elliptic curves over p-adic fields

Let K be a p-adic field.

Definition 7.1. 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 7.2. 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 7.3. *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 7.4. *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 7.5. *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 $\hat{E}(\mathfrak{m}_K)$, 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 7.6. *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 7.7 (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 7.8. *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.)

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 7.9. 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 7.10. *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 slope of the segment of the Newton polygon beginning at $x = n - i$ and ending at $x = n - i + 1$ is $-v(\alpha_i)$.

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 least 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 7.11. *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 7.12. *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 $x = 1, \dots, n-1$ 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 7.11. □

Example 7.13. 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 7.12, the polynomial is irreducible. So

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

8. Galois groups of fields of characteristic p and φ-modules

It is difficult to write down Galois groups explicitly, which in turn makes it difficult to write down Galois representations explicitly. To deal with this problem, we will introduce φ-modules and (φ, Γ)-modules, which can be described more explicitly. We will show that categories of these modules are equivalent to categories of Galois representations.

We will exploit the fact that the absolute Galois groups of p-adic fields are closely related to the absolute Galois groups of characteristic p fields. For example, we have the following result, which will be proved in a later lecture.

Theorem 8.1. *The absolute Galois groups of $\mathbb{Q}_p(\mu_{p^\infty})$ and $\mathbb{F}_p((t))$ are isomorphic (as topological groups).*

Now let E be a field of characteristic p. Let $G_E = \mathrm{Gal}(E^{\mathrm{sep}}/E)$. Let $\varphi_E \colon E \to E$ be the Frobenius map $x \mapsto x^p$.

Given an E-module M, we write $\varphi_E^*(M)$ for its Frobenius pullback $E \otimes_{\varphi_E, E} M$. Any φ_E-semilinear map $\varphi_M \colon M \to M$ determines an E-linear map $\varphi_E^*(M) \to M$ by $e \otimes m \mapsto e\varphi_M(m)$.

Definition 8.2. A *φ-module* over E is a pair (M, φ_M), where M is a finite-dimensional E-vector space and φ_M is a φ_E-semilinear endomorphism. We say that (M, φ_M) is *étale* if the E-linear map $\varphi_E^*(M) \to M$ induced by φ is an isomorphism (equivalently, the image of φ_M generates M as an E-module).

We will denote the category of étale φ-modules over E by $\varphi\text{-}\mathrm{Mod}_E^{\text{ét}}$.

Let $\mathrm{Rep}_{\mathbb{F}_p}(G_E)$ denote the category of continuous finite-dimensional $\mathbb{F}_p$-vector space representations of G_E.

Theorem 8.3. *The functor* $D_E\colon \mathrm{Rep}_{\mathbb{F}_p}(G_E) \to \varphi\text{-}\mathrm{Mod}_E^{\text{ét}}$ *defined by*

$$V \mapsto (V \otimes_{\mathbb{F}_p} E^{\mathrm{sep}})^{G_E}.$$

and the functor $V_E\colon \varphi\text{-}\mathrm{Mod}_E^{\text{ét}} \to \mathrm{Rep}_{\mathbb{F}_p}(G_E)$ *defined by*

$$M \mapsto (M \otimes_E E^{\mathrm{sep}})^{\varphi=1}.$$

determine an equivalence of categories between $\mathrm{Rep}_{\mathbb{F}_p}(G_E)$ *and* $\varphi\text{-}\mathrm{Mod}_E^{\text{ét}}$.

Remark 8.4. There are a few advantages to working with φ-modules rather than Galois representations. One is that Galois groups are difficult to describe explicitly, while a φ-module is described by a matrix with coefficients in E. Another reason is that φ-modules are better suited to working with families of Galois representations. For example, for any $\alpha \in \mathbb{F}_q^\times$, there is a representation $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathbb{F}_q^\times$ sending the Frobenius to α. We might like to combine these into a representation $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathbb{F}_p[t,t^{-1}]^\times$, but this does not work because we cannot raise t to powers in $\widehat{\mathbb{Z}}$. On the other hand, the φ-module corresponding to α is a 1-dimensional $\mathbb{F}_q$-vector space on which φ acts by α^{-1}. These combine nicely into a free $\mathbb{F}_p[t,t^{-1}]$-module of rank 1 on which φ acts by t^{-1}.

Remark 8.5. One might think of Theorem 8.3 as a characteristic p version of the Riemann-Hilbert correspondence, with the Frobenius action replacing the connection. For a more geometric analogue, see [Kat73, Proposition 4.1.1].

Lemma 8.6 (Galois descent)**.** *Let L/K be a Galois extension of fields (of any characteristic). Let V be a finite-dimensional L-vector space equipped with a semilinear* $\mathrm{Gal}(L/K)$*-action (meaning that the identites*

$$\sigma(v_1 + v_2) = \sigma(v_1) + \sigma(v_2)$$
$$\sigma(\lambda v_1) = \sigma(\lambda)\sigma(v_1)$$

hold for for each $\sigma \in \mathrm{Gal}(L/K), v_1, v_2 \in V, \lambda \in L$).

Suppose that for each $v \in V$, the stabilizer of v in $\mathrm{Gal}(L/K)$ *is open. Then the natural map*

$$L \otimes_K V^{\mathrm{Gal}(L/K)} \to V$$

is an isomorphism.

Proof. The case of L/K finite is [Sil09, Lemma II.5.8.1]. In general, we use the fact that a basis for V has open stabilizer to reduce to the finite case. □

Proof of Theorem 8.3. Let $V \in \mathrm{Rep}_{\mathbb{F}_p}(G_E)$. We will check that $D_E(V) \in \varphi\text{-}\mathrm{Mod}_E^{\text{ét}}$, and that there is a natural isomorphism $V_E(D_E(V)) \xrightarrow{\sim} V$. By Galois descent, the φ- and G_E-equivariant map

$$D_E(V) \otimes_E E^{\mathrm{sep}} \to V \otimes_{\mathbb{F}_p} E^{\mathrm{sep}} \tag{8.7}$$

is an isomorphism. Therefore, $\dim_E D_E(V) = \dim_{\mathbb{F}_p} V$; in particular, $D_E(V)$ is finite dimensional.

To show that $D_E(V)$ is étale, we just need to check that the matrix of Frobenius in some (equivalently, any) basis is invertible. By base change, the matrix of Frobenius on $D_E(V)$ is invertible iff the matrix of Frobenius on $D_E(V) \otimes_E E^{\mathrm{sep}} = V \otimes_{\mathbb{F}_p} E^{\mathrm{sep}}$ is invertible iff the matrix of Frobenius on V is invertible. The action of Frobenius on V is the identity.

Taking φ-invariants of (8.7) gives an isomorphism $V_E(D_E(V)) \xrightarrow{\sim} V$.

Now let $M \in \varphi\text{-Mod}_E^{\text{ét}}$. We want to show that the natural map

$$E^{\text{sep}} \otimes_{\mathbb{F}_p} V_E(M) \to E^{\text{sep}} \otimes_E M \tag{8.8}$$

is an isomorphism. First we will show that it is injective. It suffices to show that if some vectors in $V_E(M) = (E^{\text{sep}} \otimes_E M)^{\varphi=1}$ are linearly independent over $\mathbb{F}_p$, then they are also linearly independent over E^{sep}. Suppose that there is a minimal counterexample $v_1, \ldots, v_r \in V_E(M)$, with $\sum_{i=1}^r a_i v_i = 0$ for $a_i \in E^{\text{sep}}$. WLOG we may take $a_1 = 1$. Using $\varphi(v_i) = v_i$ and $\varphi(a_1) = a_1$, we obtain $0 = \sum_{i=2}^r (a_i - \varphi(a_i))v_i$. By minimality of the counterexample, we must have $(a_i - \varphi(a_i)) = 0$ for all i. Hence $a_i \in \mathbb{F}_p$ for all i, which is a contradiction. Note that we did not need to use the fact that M is étale to prove injectivity.

Now we show that (8.8) is surjective. Let c_{ij} be the matrix coefficients of Frobenius in some basis. Let X be the scheme over E defined by the equations

$$x_i^p = \sum_j c_{ij} x_j \,.$$

Surjectivity of (8.8) is equivalent to $|X(E^{\text{sep}})| = p^{\dim_E M}$. Since X is finite locally free over $\operatorname{Spec} E$ of degree $p^{\dim_E M}$, it suffices to show that X is étale over E, or equivalently that $\Omega_{X/E} = 0$. The module $\Omega_{X/E}$ is generated by the dx_i subject to the relations $\sum_j c_{ij} x_j = 0$. Since the c_{ij} define an invertible matrix, $\Omega_{X/E} = 0$. This concludes the proof that (8.8) is an isomorphism.

From (8.8), we see that $V_E(M)$ is finite dimensional over $\mathbb{F}_p$. Then $V_E(M) = (M \otimes_E F)^{\varphi=1}$ for some finite separable extension F/E, so the G_E-action on $V_E(M)$ is continuous. Therefore $V_E(M) \in \operatorname{Rep}_{\mathbb{F}_p} G_E$. Taking Galois invariants of (8.8) gives an isomorphism $D_E(V_E(M)) \xrightarrow{\sim} M$. Hence we have shown that the functors D_E and V_E are essential inverses of each other. □

9. Generalizatons of φ-modules, perfectoid fields

As before, let E be a field of characteristic p. We will now turn our attention to $\mathbb{Z}_p$-representations of G_E. Let $\operatorname{Rep}_{\mathbb{Z}_p} G_E$ denote the category of finitely generated (not necessarily free) $\mathbb{Z}_p$-modules with continuous G_E-action.

Definition 9.1. Let E be a field of characteristic p. A *Cohen ring* for E is a complete discrete valuation ring $\mathcal{O}_{\mathcal{E}}$ such that the residue field of $\mathcal{O}_{\mathcal{E}}$ is E, and p is a uniformizer of $\mathcal{O}_{\mathcal{E}}$.

Theorem 9.2 ([Mat86, Theorems 29.1 and 29.2])**.** *Any field E of characteristic p admits a Cohen ring $\mathcal{O}_{\mathcal{E}}$. The Cohen ring is unique up to isomorphism. The Frobenius automorphism of E lifts to an automorphism of $\mathcal{O}_{\mathcal{E}}$.*

Example 9.3. If $E = \mathbb{F}_{p^n}$, then $\mathcal{O}_{\mathcal{E}}$ is the ring of integers of $\mathbb{Q}_{p^n}$, the unramified extension of $\mathbb{Q}_p$ of degree n. More generally, if E is perfect, then $\mathcal{O}_{\mathcal{E}} \cong W(E)$, the ring of p-typical Witt vectors over E. If $E = \mathbb{F}_p((T))$, then we can take

$$\mathcal{O}_{\mathcal{E}} = \left\{ \sum_{n=-\infty}^{\infty} a_n T^n \,\middle|\, a_n \in \mathbb{Z}_p, \lim_{n \to -\infty} a_n = 0 \right\}.$$

A commonly used choice of Frobenius action is $T \mapsto (1+T)^p - 1$.

Lemma 9.4. *There is an equivalence of categories between étale E-algebras and étale $\mathcal{O}_E$-algebras.*

In particular, E^{sep} is a direct limit of étale E algebras. The corresponding direct limit of étale $\mathcal{O}_E$-algebras is called $\mathcal{O}_E^{\mathrm{sh}}$, the strict Henselization of $\mathcal{O}_E$.

Definition 9.5. The category $\varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_\mathcal{E}}$ of étale φ-modules over $\mathcal{O}_\mathcal{E}$ consists of pairs (M, φ_M) where M is a finitely generated $\mathcal{O}_\mathcal{E}$-module and φ_M is a φ-semilinear endomorphism of M such that $\varphi^*_{\mathcal{O}_\mathcal{E}}(M) \to M$ is an isomorphism.

Definition 9.6.

Now let $\check{\mathcal{O}}_\mathcal{E} = \widehat{\mathcal{O}_\mathcal{E}^{\mathrm{sh}}}$ be the completion of the strict henselization of $\mathcal{O}_\mathcal{E}$. There is a unique continuous Frobenius on $\check{\mathcal{O}}_\mathcal{E}$ that extends the Frobenius on $\mathcal{O}_\mathcal{E}$ and E^{sep}.

Theorem 9.7. *The functor* $D_{\mathcal{O}_\mathcal{E}} \colon \mathrm{Rep}_{\mathbb{Z}_p} G_E \to \varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_\mathcal{E}}$ *defined by*

$$V \mapsto (V \otimes_{\mathbb{Z}_p} \check{\mathcal{O}}_\mathcal{E})^{G_E}$$

and the functor $V_{\mathcal{O}_\mathcal{E}} \colon \varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_\mathcal{E}} \to \mathrm{Rep}_{\mathbb{Z}_p} G_E$ *defined by*

$$M \mapsto (M \otimes_{\mathcal{O}_\mathcal{E}} \check{\mathcal{O}}_\mathcal{E})^{\varphi=1}$$

determine an equivalence of categories between $\mathrm{Rep}_{\mathbb{Z}_p} G_E$ *and* $\varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_\mathcal{E}}$.

Finally, we consider $\mathbb{Q}_p$-representations of G_E. Let $\mathrm{Rep}_{\mathbb{Q}_p} G_E$ denote the category of finite-dimensional $\mathbb{Q}_p$-vector space representation of G_E. Let $\mathcal{E} := \mathcal{O}_\mathcal{E}[1/p], \check{\mathcal{E}} := \check{\mathcal{O}}_\mathcal{E}[1/p]$.

Definition 9.8. The category $\varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{E}}$ of étale φ-modules over $\mathcal{E}$ consists of pairs (M, φ_M) where M is a finite-dimensional $\mathcal{E}$-vector space and φ_M is a φ-semilinear endomorphism of M such that $\varphi^*_\mathcal{E}(M) \to M$ is an isomorphism, and M admits a φ_M-stable $\mathcal{O}_\mathcal{E}$-lattice.

Theorem 9.9. *The functor* $D_\mathcal{E} \colon \mathrm{Rep}_{\mathbb{Q}_p} G_E \to \varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{E}}$ *defined by*

$$V \mapsto (V \otimes_{\mathbb{Q}_p} \check{\mathcal{E}})^{G_E}$$

and the functor $V_\mathcal{E} \colon \varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{E}} \to \mathrm{Rep}_{\mathbb{Q}_p} G_E$ *defined by*

$$M \mapsto (M \otimes_\mathcal{E} \check{\mathcal{E}})^{\varphi=1}$$

determine an equivalence of categories between $\mathrm{Rep}_{\mathbb{Q}_p} G_E$ *and* $\varphi\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{E}}$.

The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ contains the closed normal subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p(\mu_{p^\infty})) \cong \mathrm{Gal}(\mathbb{F}_p((t))^{\mathrm{sep}}/\mathbb{F}_p((t)))$. Moreover, this isomorphism can be extended to a map

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Aut}(\mathbb{F}_p((t))^{\mathrm{sep}}) .$$

This motivates us to consider the following setup.

Let G be a profinite group containing G_E as a closed normal subgroup. Let $\Gamma = G/G_E$. Suppose that we are given a continuous action of Γ on $\mathcal{O}_\mathcal{E}$ that commutes with Frobenius. There is an induced action of G on $\check{\mathcal{O}}_\mathcal{E}$ (again because compatible endomorphisms on E^{sep} and $\mathcal{O}_\mathcal{E}$ extend uniquely to $\check{\mathcal{O}}_\mathcal{E}$).

Definition 9.10. A (φ, Γ)-*module* over $\mathcal{O}_\mathcal{E}$ is a φ-module over $\mathcal{O}_\mathcal{E}$ equipped with a semilinear Γ-action commuting with the φ-action. We say that a (φ, Γ)-module is *étale* if it is étale as a φ-module.

Write $(\varphi, \Gamma)\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_\mathcal{E}}$ for the category of étale (φ, Γ)-modules over $\mathcal{O}_\mathcal{E}$, and write $\mathrm{Rep}_{\mathbb{Z}_p} G$ for the category of finitely generated $\mathbb{Z}_p$-modules with G-action.

Theorem 9.11. *The functor* $D_{\mathcal{E}}\colon \operatorname{Rep}_{\mathbb{Z}_p} G \to (\varphi,\Gamma)\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}$ *defined by*

$$V \mapsto (V \otimes_{\mathbb{Z}_p} \check{\mathcal{O}}_{\mathcal{E}})^{G_E}$$

and the functor $V_{\mathcal{E}}\colon (\varphi,\Gamma)\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}} \to \operatorname{Rep}_{\mathbb{Z}_p} G$ *defined by*

$$M \mapsto (M \otimes_{\mathcal{O}_{\mathcal{E}}} \check{\mathcal{O}}_{\mathcal{E}})^{\varphi=1}$$

determine an equivalence of categories between $\operatorname{Rep}_{\mathbb{Z}_p} G$ *and* $(\varphi,\Gamma)\text{-}\mathrm{Mod}^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}$.

A similar result holds for $\mathbb{F}_p$- and $\mathbb{Q}_p$-representations.

Example 9.12. Let $G = G_{\mathbb{Q}_p}$, $E = \mathbb{F}_p((T))$, and embed G in $\operatorname{Aut} E^{\text{sep}}$ using Theorem 8.1. We have $\Gamma = \operatorname{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$. The action of Γ on $\mathbb{F}_p((T))$ is given by

$$\gamma \cdot T = (1+T)^\gamma - 1\,.$$

The action of Γ on $\mathcal{O}_{\mathcal{E}}$ can then also be taken to be $\gamma \cdot T = (1+T)^\gamma - 1$.

We have claimed that $\mathbb{Q}_p(\mu_{p^\infty})$ and $\mathbb{F}_p((t))$ have isomorphic Galois groups. To prove the isomorphism, we will make use of the concept of perfectoid fields and the tilting correspondence.

Recall that a *nonarchimedean field* K is a field that is complete with respect to a nontrivial nonarchimedean absolute value $|\cdot|$, and that we write

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

Definition 9.13. A nonarchimedean field K of residue characteristic p is *perfectoid* if its value group is nondiscrete and the Frobenius map

$$\Phi\colon \mathcal{O}_K/p \to \mathcal{O}_K/p$$

is surjective.

Remark 9.14. Like most references but unlike [Ked15], we do not require that K have characteristic zero.

Example 9.15.

- The field $\mathbb{C}_p$ is perfectoid. More generally, any complete algebraically closed nonarchimedean field of residue characteristic p is perfectoid.
- A nonarchimedean field of characteristic p is perfectoid if and only if it is perfect.

Lemma 9.16. *The field* $\mathbb{Q}_p^{\text{cyc}} := \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ *is perfectoid.*

Proof. Let $\{\zeta_{p^n}\}_{n\ge 0}$ denote a system of p-power roots of unity. Note that

$$\mathcal{O}_{\mathbb{Q}_p^{\text{cyc}}}/p \cong \varinjlim_n \mathbb{Z}_p[\zeta_{p^n}]/p\,.$$

Since $\zeta_{p^n} = (\zeta_{p^{n+1}})^p$ for each n, the Frobenius map is surjective. □

Definition 9.17. Let K be a perfectoid field. The *tilt* of K, denoted $K^\flat$, is defined by

$$K^\flat := \varprojlim_{z \mapsto z^p} K\,.$$

Define addition on $K^\flat$ by $(a_n) + (b_n) = (c_n)$, where

$$c_n = \lim_{m\to\infty} (a_{m+n} + b_{m+n})^{p^m}$$

and define multiplication on $K^\flat$ by componentwise multiplication.

Define a homomorphism of multiplicative monoids $\sharp\colon K^\flat \to K$ by $(a_n)^\sharp = a_0$.

Lemma 9.18.

(1) *The limit in Definition 9.17 exists.*
(2) *$K^\flat$ is a field of characteristic p.*
(3) *The function $(a_n) \mapsto |(a_n)^\sharp| = |a_0|$ is a nonarchimedean norm on $K^\flat$, and $K^\flat$ is a perfectoid field.*
(4) *We have*
$$\mathcal{O}_{K^\flat} = \varprojlim_{z \mapsto z^p} \mathcal{O}_K\,,$$
and there is an isomorphism of rings
$$\mathcal{O}_{K^\flat} \cong \varprojlim_{\Phi} \mathcal{O}_K/p\,.$$
(5) $|K^\times| = |K^{\flat\times}|$.

Proof. Left as an exercise to the reader. Parts (1) and (4) use the following lemma. □

Lemma 9.19. *Let R be a ring, let $x, y \in R$, and let n be a positive integer. If $x \equiv y \pmod{p^n}$, then $x^p \equiv y^p \pmod{p^{n+1}}$.*

10. Tilting and untilting

Example 10.1. We claim that $(\mathbb{Q}_p^{\mathrm{cyc}})^\flat$ is isomorphic to the completion of the perfection of $\mathbb{F}_p((t))$. We have
$$\mathcal{O}_{\mathbb{Q}_p^{\mathrm{cyc}}}/p \cong \varinjlim_n \mathbb{Z}_p[\zeta_{p^n}]/p \cong \varinjlim_n \mathbb{Z}_p[\zeta_{p^n} - 1]/p^n\,.$$
The minimal polynomial of $\zeta_{p^n} - 1$ is
$$\frac{(1+T)^{p^n} - 1}{(1+T)^{p^{n-1}} - 1} \cong T^{p^n - p^{n-1}} \pmod{p}\,.$$
Since $\zeta_{p^n} - 1 \cong (\zeta_{p^{n+1}} - 1)^p \pmod{p}$ for each n, we can write
$$\mathcal{O}_{\mathbb{Q}_p^{\mathrm{cyc}}}/p \cong \varinjlim_n \mathbb{F}_p[t^{p^{-n}}]/(t^{1-1/p})\,.$$
Then
$$(\mathcal{O}_{\mathbb{Q}_p^{\mathrm{cyc}}})^\flat = \varprojlim_{\Phi} \varinjlim_n \mathbb{F}_p[t^{p^{-n}}]/(t^{1-1/p}) = \varprojlim_m \varinjlim_n \mathbb{F}_p[t^{p^{-n}}]/(t^{p^m - p^{m-1}})$$
$$(\mathbb{Q}_p^{\mathrm{cyc}})^\flat = (\mathcal{O}_{\mathbb{Q}_p^{\mathrm{cyc}}})^\flat[1/t]$$

Definition 10.2. Let K be a perfectoid field of characteristic p. An *untilt* of K is a perfectoid field $K^\sharp$, along with an isomorphism $(K^\sharp)^\flat \xrightarrow{\sim} K$.

We would like to classify the untilts of a given characteristic p perfectoid field K. In order to do that, we will need to introduce the ring $W(\mathcal{O}_K)$.

Definition 10.3. An $\mathbb{F}_p$-algebra R is *perfect* if the Frobenius endomorphism of R is an isomorphism.

Definition 10.4. An abelian group A is p-adically complete and separated if $A \to \varprojlim_n A/p^n A$ is an isomorphism.

Definition 10.5. A *strict p-ring* is a ring A that is p-adically complete and separated, such that A/pA is a perfect $\mathbb{F}_p$-algebra, and p is not a zero divisor in A.

Example 10.6. If K is the completion of an unramified extension of $\mathbb{Q}_p$, then $\mathcal{O}_K$ is a strict p-ring. The p-adic completion of $\mathbb{Z}[x^{p^{-\infty}}]$ is also a strict p-ring.

The main goal of this section is to prove the following theorem.

Theorem 10.7. *The functor $A \mapsto A/pA$ from strict p-rings to perfect $\mathbb{F}_p$-algebras is an equivalence of categories.*

We will write W for the functor from perfect $\mathbb{F}_p$-algebras to strict p-rings determined by the above equivalence. For R a perfect $\mathbb{F}_p$-algebra, the ring $W(R)$ is called the ring of p-typical Witt vectors of R.

Lemma 10.8. *Let A be a strict p-ring.*

(1) *There is a unique section $[\cdot]$ of the reduction map $A \to A/pA$ that is a homomorphism of multiplicative monoids.*
(2) *Every element of A can be written uniquely in the form*

$$\sum_{n=0}^{\infty} p^n [a_n], \quad a_n \in A/pA\,.$$

Proof. For the first part, observe that for any $x \in R/pR$, we must have

$$[x] = \lim_{n\to\infty} (x_n)^{p^n}$$

where x_n is a lift of $x^{p^{-n}}$. The argument that the limit exists and is independent of the choice of lifts follows from Lemma 9.19.

Since A is p-adically complete and separated, the second part follows immediately from the first. □

Lemma 10.9. *Let A be a strict p-ring, and let $a, b \in A$. Suppose that $a = \sum_{n=0}^{\infty}[a_n]p^n$, $b = \sum_{n=0}^{\infty}[b_n]p^n$, $a + b = \sum_{n=0}^{\infty}[s_n]p^n$, $ab = \sum_{n=0}^{\infty}[t_n]p^n$. Then s_n and t_n are polynomials in the $a_i^{p^{i-n}}$, $b_i^{p^{i-n}}$ for $0 \le i \le n$. Furthermore, s_n is homogeneous of degree 1 (where each a_i and b_i has degree 1), and t_n is homogeneous in the a_i and b_i separately, each of degree 1.*

Proof. Repeatedly use the identity

$$[x+y] \equiv ([x^{p^{-n}}] + [y^{p^{-n}}])^{p^n} \pmod{p^{n+1}}\,,$$

which follows from Lemma 9.19. □

Proposition 10.10 ([Ked15, Lemma 1.1.6])**.** *Let A be a strict p-ring, and let B be a p-adically complete ring. Let $\sharp\colon A/pA \to B$ be a multiplicative map that induces a homomorphism of rings $A/pA \to B/pB$. Then the formula*

$$\Theta\left(\sum_{n=0}^{\infty} p^n [x_n]\right) = \sum_{n=0}^{\infty} p^n x_n^{\sharp}$$

defines a p-adically continuous homomorphism $\Theta\colon A \to B$ such that $\Theta \circ [\cdot] = \sharp$.

We are especially interested in applying this result in the case where $A = W(\mathcal{O}_{K^\flat})$ and $B = \mathcal{O}_K$ for some perfectoid field K.

Proof of Theorem 10.7. Full faithfulness follows from Proposition 10.10.

To prove essential surjectivity, let R be a perfect ring of characteristic p, and write $R = \mathbb{F}_p[X^{-p^\infty}]/\overline{I}$ for some set X and ideal $\overline{I} \subset \mathbb{F}_p[X^{-p^\infty}]$. Let A_0 be the p-adic completion of $\mathbb{Z}_p[X^{-p^\infty}]$; then one can check that A_0 is a strict p-ring and $A_0/pA_0 = \mathbb{F}_p[X^{-p^\infty}]$. Let $I \subset A_0$ be the set of elements of the form $\sum_{n=0}^\infty p^n[x_n]$ with $x_n \in \overline{I}$. Then one can check that I is an ideal of A_0 and $A := A_0/I$ is a strict p-ring with $R = A/pA$. □

Let K be a perfectoid field.

Definition 10.11. An ideal I of $W(\mathcal{O}_{K^\flat})$ is *primitive of degree* 1 if it is generated by an element of the form $p + [\pi]\alpha$ for some $\pi \in \mathfrak{m}_{K^\flat}$, $\alpha \in W(\mathcal{O}_{K^\flat})$.

Proposition 10.12. *The map*

$$\Theta\colon W(\mathcal{O}_{K^\flat}) \to \mathcal{O}_K$$

defined in Proposition 10.10 has the following properties:

(1) Θ *is surjective.*
(2) $\ker\Theta$ *is primitive of degree* 1*.*

Proof. By Lemma 9.18(4), the map $\sharp$ is surjective mod p. So by successive approximation, every element of $\mathcal{O}_K$ can be written as $\sum_{n=0}^\infty a_n^\sharp p^n$ for some $a_n \in \mathcal{O}_{K^\flat}$. Therefore, Θ is surjective.

If K has characteristic p, then $\ker\Theta = (p)$ is primitive of degree 1. Now suppose K has characteristic 0. Choose $\pi^\flat \in \mathcal{O}_{K^\flat}$ so that $\pi := (\pi^\flat)^\sharp$ satisfies $|\pi| = |p|$. Choose $x \in W(\mathcal{O}_{K^\flat})$ satisfying $\Theta(x) = -p/\pi$. Since $\Theta(x)$ is a unit of K, the constant term in the Teichmuller expansion of x must be a unit; then x is also a unit. Let $\xi = p + [\pi^\flat]x$; then $\xi \in \ker\Theta$. We claim that in fact ξ generates $\ker\Theta$. Observe that $\ker\Theta \subseteq ([\pi^\flat], p) = (\xi, p)$. So any element of $\ker\Theta$ can be written as $a\xi + bp$ with $\Theta(pb) = p\Theta(b) = 0$. Since p is not a zero divisor in $\mathcal{O}_K$, we get $\Theta(b) = 0$. By successive p-adic approximation, we see that $\ker\Theta = (\xi)$. □

Remark 10.13. If you find it dissatisfying that we used a separate argument for $p = 0$, see [BMS18, Lemma 3.2ii, Lemma 3.10] for a version of the argument that generalizes better. Essentially, the idea is to use Lemma 10.9 to prove that $W(\mathcal{O}_{K^\flat})$ is complete for the $[\pi^\flat]$-adic topology; then we can use $[\pi^\flat]$-adic approximation and we can assume $|p| \le |\pi| < 1$ instead of $|\pi| = |p|$.

Proposition 10.14 ([Ked15, Theorem 1.4.13])**.** *The category of perfectoid fields is equivalent to the category of pairs (K, I), where K is a perfectoid field of characteristic p and $I \subset W(\mathcal{O}_K)$ is an ideal that is primitive of degree* 1*.*

11. Tilting and field extensions, group cohomology

Corollary 11.1. *Let K be a perfectoid field. Then tilting induces an equivalence of categories between perfectoid extensions of K and perfectoid extensions of $K^\flat$.*

Moreover, if L/K is an extension of perfectoid fields, then L/K is finite iff $L^\flat/K^\flat$ is finite.

Lemma 11.2. *If K is a perfectoid field and $K^\flat$ is algebraically closed, then so is K.*

Proof. Let $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ be a monic irreducible polynomial. Since $K^\flat$ is algebraically closed, $|K^{\flat\times}|$ is a $\mathbb{Q}$-vector space, so $|K^\times|$ is as well. Therefore, by scaling the variable, we may assume that $a_0 \in \mathcal{O}_K^\times$. Since P is irreducible, its Newton polygon must be a straight line, so $a_i \in \mathcal{O}_K$ for all i.

Let $Q(X) \in \mathcal{O}_K^\flat[X]$ be a monic polynomial such that P and Q have the same image in $(\mathcal{O}_K/p\mathcal{O}_K)[X]$. Let $y \in \mathcal{O}_{K^\flat}$ be a root of $Q(X)$. Then $p \mid P(y^\sharp)$. If $P(y^\sharp) \neq 0$, choose $c \in \mathcal{O}_K$ so that $|c|^d = |P(y^\sharp)|$. Then replace $P(X)$ with $c^{-d}P(cX + y^\sharp)$. By repeating this process, we find a sequence of elements of $\mathcal{O}_K$ converging to a root of P. □

Lemma 11.3 (Krasner's lemma)**.** *Let K be a nonarchimedean field, and let $\alpha, \beta \in \overline{K}$, with α separable over $K(\beta)$. Suppose that for all $\sigma \in \mathrm{Gal}(K(\beta)^{\mathrm{sep}}/K(\beta))$, either $\sigma(\alpha) = \alpha$ or $|\alpha - \sigma(\alpha)| > |\alpha - \beta|$. Then $\alpha \in K(\beta)$.*

Proof. Let $\sigma \in \mathrm{Gal}(K(\beta)^{\mathrm{sep}}/K(\beta))$. Then

$$|\alpha - \sigma(\alpha)| \leq \max\left(|\alpha - \beta|, |\sigma(\alpha) - \beta|\right) = |\alpha - \beta|.$$

By assumption, we must have $\sigma(\alpha) = \alpha$. Since this holds for all σ, we must have $\alpha \in K(\beta)$. □

Proposition 11.4. *Any finite extension of a perfectoid field is perfectoid.*

Proof. Let K be a perfectoid field, and let $C^\flat$ be the completion of an algebraic closure of $K^\flat$. By Corollary 11.1, $C^\flat$ has an untilt C over K. Furthermore, C is algebraically closed by Lemma 11.2. Let C_0 be the union of the untilts of all finite extensions of $K^\flat$; then C_0 is dense in C since the union of all finite extensions of $C^\flat$ is dense in $C^\flat$. It follows from Krasner's lemma that a dense subfield of an algebraically closed nonarchimedean field is separably closed. Then C_0 must contain all finite extensions of K. So any finite extension L/K is contained in a Galois extension M/K that is an untilt of some $M^\flat/K^\flat$. By Galois theory, any subfield of M containing K must be the untilt of a subfield of $M^\flat$ containing $K^\flat$. □

Theorem 11.5. *Let K be a perfectoid field. There is an equivalence of categories between finite extensions of K and finite extensions of $K^\flat$.*

Hence there is an injection

$$\mathrm{Aut}_{\mathrm{cts}}(\overline{K}) \hookrightarrow \mathrm{Aut}_{\mathrm{cts}}(\overline{K^\flat})$$

inducing an isomorphism

$$\mathrm{Gal}(\overline{K}/K) \cong \mathrm{Gal}(\overline{K^\flat}/K^\flat).$$

Proof. Combine Corollary 11.1 and Proposition 11.4. □

Corollary 11.6. *The fields $\mathbb{Q}_p(\mu_{p^\infty})$, $\mathbb{Q}_p^{\mathrm{cyc}} = \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$, $\mathbb{F}_p((t^{p^{-\infty}}))$, and $\mathbb{F}_p((t))$ have isomorphic Galois groups.*

Proof. By the above theorem, $\mathbb{Q}_p^{\mathrm{cyc}} = \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ and $\mathbb{F}_p((t^{p^{-\infty}}))$ have isomorphic Galois groups. By Krasner's lemma, taking completions does not change the Galois group, and taking perfections also does not change the Galois group. □

Let G be a group. A G-module is an abelian group A along with a homomorphism $G \to \mathrm{Aut}\, A$.

We write A^G for the G-invariants of A. Then $(-)^G$ is a functor from the category of G-modules to the category of abelian groups. Observe that $A^G = \mathrm{Hom}_G(\mathbb{Z}, A)$, where $\mathbb{Z}$ has the trivial G-action. It is left exact, meaning that given an exact sequence

$$0 \to A \to A' \to A'' ,$$

the sequence

$$0 \to A^G \to (A')^G \to (A'')^G$$

is also exact. However, it is not right exact.

The forgetful functor from G-modules to abelian groups has a left adjoint $G \mapsto \mathbb{Z}[G]$. We have

$$\mathbb{Z}[G] = \bigoplus_{g \in G} \mathbb{Z} \cdot [g] ,$$

with

$$[g][h] = [gh] .$$

A G-module A is called *projective* if the functor $\mathrm{Hom}_G(A, -)$ is exact. A (possibly infinite) direct sum of copies of $\mathbb{Z}[G]$ is projective.

Given a projective resolution

$$\cdots \to P_n \to P_{n-1} \to \cdots \to P_0 \to \mathbb{Z} \to 0 ,$$

we define a cochain complex $K^\bullet$ by $K^n = \mathrm{Hom}_G(P_n, A)$, with differentials induced by the maps $P_n \to P_{n-1}$. Define

$$H^n(G, A) = H^n(K^\bullet) .$$

A standard result in homological algebra is that this definition is independent of the resolution chosen. Then $A^G = H^0(G, A)$. Given any short exact sequence of G-modules

$$0 \to A \to B \to C \to 0 ,$$

there is a long exact sequence

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to \cdots .$$

A useful choice of projective resolution of $\mathbb{Z}$ is the following. Let $P_n = \mathbb{Z}[G^{n+1}]$. We consider P_n as a G-module via

$$g[g_0, \ldots, g_n] = [gg_0, \ldots, gg_n] .$$

The differentials are given by

$$d[g_0, \ldots, g_n] = \sum_{j=0}^{n} (-1)^j [g_0, \ldots, \hat{g}_j, \ldots, g_n] ,$$

where $\hat{g}_j$ indicates that g_j is omitted. (Most texts use the "bar resolution", which is equivalent but written slightly differently. I think the description given here is a bit more elegant, but maybe the bar resolution is more convenient for calculations?)

For example, $H^1(G, A)$ is the space of G-equivariant maps $\phi \colon G \times G \to A$ satisfying

$$\phi(y, z) - \phi(x, z) + \phi(x, y) = 0$$

for all $x, y, z \in G$, modulo the space of maps of the form

$$\phi(x, y) = \psi(y) - \psi(x)$$

for some G-equivariant $\psi \colon G \to A$.

Since ψ is homogeneous, we can write

$$\phi(x, y) = x\tilde{\phi}(x^{-1}y) ,$$

where
$$\tilde{\phi}(y) = \phi(1, y)\,.$$
Similarly
$$\psi(x) = x\tilde{\psi}\,,$$
where
$$\tilde{\psi} = \psi(1)\,.$$
So we can also think of $H^1(G, A)$ as the space of maps $\tilde{\phi}\colon G \to A$ satisfyig
$$y\tilde{\phi}(y^{-1}z) - \tilde{\phi}(z) + \tilde{\phi}(y) = 0$$
modulo the space of maps of the form
$$\tilde{\phi}(y) = y\tilde{\psi} - \tilde{\psi}\,.$$
By making the substitution $z = yw$, we can rewrite the constraint as
$$\tilde{\phi}(y) - \tilde{\phi}(yw) + y\tilde{\phi}(w) = 0\,.$$
If A has the trivial G-action, then the constraint simplifies to
$$\tilde{\phi}(y) - \tilde{\phi}(yw) + y\tilde{\phi}(w) = 0\,,$$
and $\tilde{\psi} - y\tilde{\psi}$ is always zero. So in that case,
$$H^1(G, A) = \mathrm{Hom}(G, A)\,.$$

12. Group cohomology

In the case $G = \mathbb{Z}$, there is also a projective resolution
$$0 \to \mathbb{Z}[\mathbb{Z}] \xrightarrow{[1]-[0]} \mathbb{Z}[\mathbb{Z}] \to \mathbb{Z} \to 0\,.$$
So for any $\mathbb{Z}$-module A,
$$H^1(\mathbb{Z}, A) = A/\left([1]a - a | a \in A\right)\,.$$
$$H^i(\mathbb{Z}, A) = 0 \text{ for all } i > 1\,.$$
The above resolution is related to the fact that $S^1 = \mathbb{R}/\mathbb{Z}$. In general, if there is a free action of G on $\mathbb{R}^n$ and $\mathbb{R}^n/G$ admits a triangulation, then every G-module has a projective resolution of length n, and $H^i(G, A) = 0$ for $i > n$.

The groups $H^1(G, A)$ and $H^2(G, A)$ admit concrete descriptions. The *semidirect product* $A \rtimes G$ is the group with underlying set $A \times G$, and group operation given by
$$(a_1, g_1)(a_2, g_2) = (a_1 + g_1 a_2, g_1 g_2)\,.$$
Consider the set of sections of the projection map $A \rtimes G \to G$. A section is a group homomorphism $G \to A \rtimes G$ of the form
$$g \mapsto (s(g), g)$$
for some $s\colon G \to A$. Such a map is a group homomorphism if and only if
$$s(g_1 g_2) = s(g_1) + g_1 s(g_2)$$
for all $g_1, g_2 \in G$. We have
$$(a, 1)(s(g), g)(-a, 1) = (s(g) + a - ga, g)\,,$$
Therefore, two sections are conjugate iff their difference is of the form $g \mapsto a - ga$. Therefore, $H^1(G, A)$ classifies sections of the projection $A \rtimes G \to G$ upto A-conjugacy.

An *extension of G by A* is a group E equipped with a short exact sequence $1 \to A \to E \to G \to 1$. There is a bijection between classes in $H^2(G, A)$ and extensions of G by A. We omit the details.

The groups $H^n(G, A)$ are functorial in both G and A. The functoriality in G can be described as follows. If $f \colon H \to G$ is a homomorphism of groups and A is a G-module, then we write f^*A for the H-module with underlying abelian group A and H-action determined by f. The machinery of derived functors tells us that there are homomorphisms

$$H^n(G, A) \to H^n(G', f^*A).$$

If the cohomology is calculated using the resolution $\cdots \to \mathbb{Z}[G \times G] \to \mathbb{Z}[G] \to \mathbb{Z}$ mentined above, then this map sends a homogeneous cocycle $\phi \colon G^{n+1} \to A$ to $(f \times \cdots \times f) \circ \phi$.

If $f \colon H \to G$ is an injection, then the functor f^* is called *restriction* and is denoted by Res. We sometimes also denote the corresponding $H^n(G, A) \to H^n(H, A)$ by Res.

The restriction functor Res has a right adjoint called Ind. Given an H-module B, the G-module $\operatorname{Ind} B$ is given by

$$\operatorname{Ind} B = \operatorname{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B),$$

where we view $\mathbb{Z}[G]$ as an H-module via multiplication on the left, and as a G-module via multiplication on the right. Recall that "right adjoint" means that for any G-module A and H-module B, there is a natural isomorphism

$$\operatorname{Hom}_{\mathbb{Z}[H]}(\operatorname{Res} A, B) \cong \operatorname{Hom}_{\mathbb{Z}[G]}(A, \operatorname{Ind} B).$$

We also have

$$H^n(H, B) = H^n(G, \operatorname{Ind} B).$$

Modules in the image of the functor Ind are called "coinduced modules". (There is also a functor called ind that is left adjoint to Res, and modules in the image of ind are called "induced modules". But we will not use ind.)

Given a normal subgroup H of G, the composite

$$H^n(G/H, A^H) \to H^n(G, A^H) \to H^n(G, A)$$

is called an *inflation map* and denoted Inf.

We would like to allow our groups and modules to have a topology. The right way to do this is probably to use condensed mathematics, but as far as I know, no one has worked out the details yet. So instead, we make the following ad hoc definition. Let G be a topological group, and let A be a topological G-module (i.e. a G-module such that the G-action is continuous). Define a cochain complex K_{cts} by letting K^n_{cts} be the set of continuous G-equivariant homomorphisms $G^{n+1} \to A$. Define $H^n_{\text{cts}}(G, A)$ to be the nth cohomology group of K_{cts}.

Warning: a short exact sequence of modules does not always give us a long exact sequence of cohomology groups. For example, we have a short exact sequence of abelian groups

$$0 \to \mathbb{Z} \to \mathbb{R} \to S^1 \to 0.$$

If we consider these as S^1-modules with trivial S^1-action, then

$$H^1_{\text{cts}}(S^1, \mathbb{R}) = \operatorname{Hom}_{\text{cts}}(S^1, \mathbb{R}) = 0$$
$$H^1_{\text{cts}}(S^1, S^1) = \operatorname{Hom}_{\text{cts}}(S^1, S^1) = \mathbb{Z}$$

$$H^2_{\mathrm{cts}}(S^1, \mathbb{Z}) = 0\,.$$

This is why it would probably be better to use condensed mathematics.

However, given a short exact sequence $0 \to A \to B \to C \to 0$, we do always get a long exact sequence

$$0 \to A^G \to B^G \to C^G \to H^1_{\mathrm{cts}}(G, A) \to H^1_{\mathrm{cts}}(G, B) \to H^1_{\mathrm{cts}}(G, C)\,.$$

We get the full long exact sequence if the map $B \to C$ admits a continuous section (as a map of topological spaces; the section need not be a G-module homomorphism).

Lemma 12.1. *Let G be a profinite group, and let A be a topological G-module.*

(1) *If A has the discrete topology, then every vector in A has an open stabilizer, and*

$$H^i_{\mathrm{cts}}(G, A) = \varinjlim_{H \subset G} H^i(G/H, A^H)\,,$$

where the limit runs over open normal subgroups of G.

(2) *If $H^i_{\mathrm{cts}}(G, \mathbb{F}_p)$ is finite for all i, and A is a finite free $\mathbb{Z}_p$-module, then*

$$H^i_{\mathrm{cts}}(G, A) = \varprojlim_n H^i_{\mathrm{cts}}(G, A/p^n A)$$

(3) *If $H^i_{\mathrm{cts}}(G, \mathbb{F}_p)$ is finite for all i, and A is a finite-dimensional $\mathbb{Q}_p$-vector space, then for any G-stable lattice $\Lambda \subset A$,*

$$H^i_{\mathrm{cts}}(G, A) = H^i_{\mathrm{cts}}(G, \Lambda) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

(Since G is compact, such a lattice always exists.)

Lemma 12.2.

(1) *Let K be a finite extension of $\mathbb{Q}_p$. Then $H^i_{\mathrm{cts}}(\mathrm{Gal}(\overline{K}/K), \mathbb{F}_p)$ is finite for all i.*

(2) *Let K be a finite extension of $\mathbb{Q}$, and let S be a finite set of places of K. Let K_S be the largest algebraic extension of K unramified outside S. Then $H^i_{\mathrm{cts}}(\mathrm{Gal}(K_S/K), \mathbb{F}_p)$ is finite for all i.*

13. Ax–Sen–Tate theorem

Let K be a p-adic field, and let $C := \widehat{\overline{K}}$ be the completion of its algebraic closure with respect to the norm topology. In a previous lecture, I claimed that there is no element "$2\pi i$" in C so that G_K acts on "$2\pi i$" $\cdot\, \mathbb{Q}_p$ by the cyclotomic character χ.

Theorem 13.1. *$C^{G_K} = K$.*

Let $K_\infty := K(\mu_{p^\infty})$, $K^{\mathrm{cyc}} := \widehat{K_\infty}$, $\Gamma := \mathrm{Gal}(K_\infty/K)$. If $\chi\colon \Gamma \to K^\times$ has infinite order, then $C(\chi)^{G_K} = 0$.

Remark 13.2. One can also show that $H^1(G_K, C)$ is a one-dimensional K-vector space and that $H^1(G_K, C(\chi)) = 0$. In the interest of space, we omit the proof. See [Tat67, §3].

For an elementary (but calculation-heavy) proof that $C^{G_K} = K$, see [Ax70] or [FO, Proposition 3.8].

The proof breaks down into the following steps.

Lemma 13.3. *Let k be the residue field of K, and let $K_0 = W(k)[1/p]$. Let π be a uniformizer of K, and let $e = \frac{\log|p|}{\log|\pi|}$. Then $[K : K_0] = e$.*

Proof. Every element of $\mathcal{O}_K$ can be written as $\sum_{i=0}^{\infty}[a_i]\pi^i$ with $a_i \in k$. We can write $\pi^e = [u]p+\sum_{i=e+1}^{\infty}[b_i]\pi^i$ with $u \in k^\times, b_i \in K$. Then by repeated substitution, every element of $\mathcal{O}_K$ can be written in the form $\sum_{i=0}^{\infty}\sum_{j=0}^{e-1}[c_i]p^i\pi^j$. Hence $1, \pi, \ldots, \pi^{e-1}$ form a basis for $\mathcal{O}_K$ as a $W(k)$-module. □

Lemma 13.4. *The field K^{cyc} is perfectoid.*

Proof. Let k be the residue field of K. Then $W(k)[1/p]^{\mathrm{cyc}}$ is perfectoid by the same argument as in Lemma 9.16. Since K is finite extension of $W(k)[1/p]$, the result follows from Lemma 11.4. □

Proposition 13.5. *If L is a perfectoid field, then $(\widehat{\overline{L}})^{G_L} = L$. In particular, $C^{\mathrm{Gal}(\overline{K}/K_\infty)} = K^{\mathrm{cyc}}$.*

Proposition 13.6. $(K^{\mathrm{cyc}})^\Gamma = K$.
If $\chi \colon \Gamma \to K^\times$ has infinite order, then $K^{\mathrm{cyc}}(\chi)^\Gamma = 0$.

To prove Proposition 13.5, we will need a few lemmas.

Lemma 13.7. *Let M/L be a finite extension of perfectoid fields. Then $\mathrm{tr}_{M/L}(\mathfrak{m}_M) = \mathfrak{m}_L$.*

Proof. Since $M^\flat/L^\flat$ is separable, $\mathrm{tr}_{M^\flat/L^\flat}(\mathfrak{m}_{M^\flat})$ is a nonzero ideal of $\mathcal{O}_L$. By applying the inverse of Frobenius, we see that it must be all of $\mathfrak{m}_{L^\flat}$. Since there are compatible surjective ring homomorphisms $\mathcal{O}_{M^\flat} \twoheadrightarrow \mathcal{O}_M/p\mathcal{O}_M$, $\mathcal{O}_{L^\flat} \twoheadrightarrow \mathcal{O}_L/p\mathcal{O}_L$, this implies that $\mathrm{tr}_{M/L}(\mathfrak{m}_M) = \mathfrak{m}_L$. □

Lemma 13.8. *Let L be a perfectoid field, and let $y \in \overline{L}$. Let $c > 1$ be a real number. Then there exists $z \in L$ so that*

$$|y - z| \leq c \max_{\sigma \in G_L} |\sigma y - y| .$$

Proof. Choose a finite extension M of L containing y. We will write tr for the trace from M to M. By Lemma 13.7, we can find $x \in M$ with $|x| < 1$, $|\mathrm{tr}\, x| \geq c^{-1}$. Let $z = \frac{\mathrm{tr}(xy)}{\mathrm{tr}\, x}$. Then

$$y - z = \frac{\sum_{\sigma \in \mathrm{Gal}(M/L)}(\sigma x)(y - \sigma y)}{\mathrm{tr}\, x} .$$

Hence $|y - z| \leq c \max_{\sigma \in H_K} |\sigma y - y|$, as desired. □

Proof of Proposition 13.5. Let $x \in (\widehat{\overline{L}})^{G_L}$. Then for any real $\epsilon > 0$, we can find $y \in \overline{L}$ so that $|x - y| < \epsilon$. By the strong triangle inequality, for all $\sigma \in G_L$,

$$|\sigma y - y| \leq \max(|\sigma y - z|, |y - z|) = |y - z| < \epsilon .$$

By Lemma 13.8, for any $c > 1$, we can find $z \in L$ so that $|y - z| \leq c\epsilon$. Hence $|x - z| < c\epsilon$. Since this is true for any ϵ, and L is complete, $x \in L$. □

In order to prove Proposition 13.6, there is no harm in replacing K with a finite Galois extension. So we may assume K contains a pth root of unity. This implies that $\Gamma \cong \mathbb{Z}_p$. Let γ be a topological generator of Γ.

Let $t \colon K_\infty \to K$ be the "normalized trace map" satisfying $t|_L = \frac{1}{[L:K]}\mathrm{tr}_{L/K}$ for every finite extension L/K inside K_∞.

Lemma 13.9. *For any $x \in K_\infty$,*

$$|x - t(x)| \leq |p|^{-1}|x - \gamma x| .$$

Proof. For each n, let K_n be the fixed field of $p^n\Gamma$. We will prove the inequality on each K_n by induction. The base case $n = 0$ is trivial. Since $1-\gamma$ divides $p - \left(1+\gamma^{p^{n-1}} + \cdots + \gamma^{p^{n-1}(p-1)}\right)$, we have

$$\left|px - \operatorname{tr}_{K_n/K_{n-1}} x\right| \leq |((1-\gamma)x| \,.$$

or equivalently,

$$\left|x - p^{-1}\operatorname{tr}_{K_n/K_{n-1}} x\right| \leq |p^{-1}|\,|(1-\gamma)x| \,.$$

By the induction hypothesis,

$$\left|p^{-1}\operatorname{tr}_{K_n/K_{n-1}} - t(x)\right| \leq |p^{-1}|\,\left|(1-\gamma)(p^{-1}\operatorname{tr}_{K_n/K_{n-1}} x)\right| \leq |p^{-1}||(1-\gamma)x| \,,$$

where we used the fact that $1-\gamma$ commutes with the normalized trace in the last inequality. Then the claim follows from the triangle inequality. $\square$

Corollary 13.10. *For any $x \in K_\infty$,*

$$|t(x)| \leq |p^{-1}||x| \,.$$

So the function t is continuous. Moreover, $1-\gamma$ is invertible on $\ker t$, and its inverse is continuous.

Hence t can be extended to a continuous function $\hat{t}\colon K^{\mathrm{cyc}} \to K$, and the restriction of $1-\gamma$ to $\ker \hat{t}$ has a continuous inverse.

Proof of Proposition 13.6. We have

$$K^{\mathrm{cyc}} = K \oplus \ker \hat{t}$$

$$(K^{\mathrm{cyc}})^\Gamma = K^\Gamma \oplus (\ker \hat{t})^\Gamma = K \oplus 0 = K \,.$$

Finally, suppose that $\chi\colon \Gamma \to K^\times$ is a character of infinite order. We will show that $K^{\mathrm{cyc}}(\chi^{-1})^\Gamma = 0$. For sufficiently large n, we must have $|\chi(\gamma^{p^n}) - 1| < |p|$. Since there is no harm with replacing K by a finite Galois extension, we may assume $|\chi(\gamma) - 1| < |p|$. On $\ker \hat{t}$,

$$\gamma - \chi(\gamma) = (\gamma - 1)(1 - (\chi(\gamma) - 1)(\gamma - 1)^{-1})$$

and $(1 - (\chi(\gamma) - 1)(\gamma - 1)^{-1})^{-1}$ has a convergent power series, so $\gamma - \chi(\gamma)$ is invertible. On K, $\gamma - \chi(\gamma) = 1 - \chi(\gamma)$ is invertible since χ has infinite order. $\square$

14. The ring B_{dR}

Now we define the ring B_{dR} mentioned in the first lecture.

Let K be a p-adic field, and let C be the completion of its algebraic closure with respect to the norm topology. We define the ring

$$A_{\mathrm{inf}} := W(\mathcal{O}_{C^\flat}) \,.$$

By Proposition 10.10, there is a homomorphism

$$\Theta\colon A_{\mathrm{inf}} \to \mathcal{O}_C \,.$$

We will consider the localization

$$\Theta_{\mathbb{Q}}\colon A_{\mathrm{inf}}[1/p] \to C \,.$$

Lemma 14.1. *For each positive integer n, $(\ker \Theta_{\mathbb{Q}})^n \cap A_{\inf} = (\ker \Theta)^n$, and $\bigcap_n (\ker \Theta_{\mathbb{Q}})^n = 0$.*

Let

$$B_{\mathrm{dR}}^+ := \varprojlim_n A_{\inf}[1/p]/(\ker \Theta_{\mathbb{Q}})^n \, .$$

Then B_{dR}^+ is a complete discrete valuation ring with residue field C.

Proof. Left as an exercise to the reader. □

Define

$$B_{\mathrm{dR}} := \operatorname{Frac} B_{\mathrm{dR}}^+ \, .$$

Define a decreasing filtration on B_{dR} by letting $\operatorname{Fil}^i B_{\mathrm{dR}}$ be the fractional ideal $(\ker \Theta_{\mathbb{Q}})^i$. Now we will define an element $t \in B_{\mathrm{dR}}^+$ that is the p-adic analogue of $2\pi i$. Let $\epsilon \in \mathcal{O}_{C^\flat}$ be an element with $\epsilon_0 = 1$, $\epsilon_1 \neq 1$. Then $[\epsilon] - 1 \in \ker \Theta$, so it makes sense to define

$$t := \log[\epsilon] = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{([\epsilon]-1)^n}{n} \, .$$

Lemma 14.2. *For any $a \in \mathbb{Q}_p$, $\log([\epsilon^a]) = a \log[\epsilon]$. Hence G_K acts on $t \cdot \mathbb{Q}_p$ by the cyclotomic character.*

Proof. It is formal that for $a \in \mathbb{Q}$, $\log([\epsilon^a]) = a \log[\epsilon]$.

We would like to argue that the equality holds for $a \in \mathbb{Q}_p$ by continuity. But the G_K-action on B_{dR}^+ is not jointly continuous for the $\ker \Theta_{\mathbb{Q}}$-adic topology, so we need to find a "better" topology.

Let ξ be a generator of $\ker \Theta$. Using Lemma 10.9 and the fact that the G_K-action on $\mathcal{O}_{C^\flat}$ is jointly continuous, we can verify that the G_K-action on $A_{\inf}$ is jointly continuous for the (p, ξ)-adic topology on $A_{\inf}$. Give $A_{\inf}/\xi^n$ the quotient topology. Extend this topology to $A_{\inf}[1/p]/\xi^n$ by letting $A_{\inf}/\xi^n$ be open. Finally, give $B_{\mathrm{dR}}^+ = \varprojlim_n A_{\inf}[1/p]/\xi^n$ the inverse limit topology. Then G_K acts jointly continuously for this topology, and log is continuous on the open set $1 + \mathfrak{m}_{A_{\inf}} + \xi B_{\mathrm{dR}}^+ \subset B_{\mathrm{dR}}^+$, where $\mathfrak{m}_{A_{\inf}}$ is the maximal ideal of $A_{\inf}$. □

Lemma 14.3. *t is a uniformizer of B_{dR}^+.*

Proof. It is clear that $t \in \operatorname{Fil}^1 B_{\mathrm{dR}}^+$, so we just need to check that $t \notin \operatorname{Fil}^2 B_{\mathrm{dR}}^+$. For this, it is enough to check that $[\epsilon] - 1 \notin \operatorname{Fil}^2 B_{\mathrm{dR}}^+$, or equivalently, $[\epsilon] - 1 \notin (\ker \Theta)^2$.

For simplicity, we will assume $p \neq 2$. See [BC, Proposition 4.4.8] for the case $p = 2$.

Recall from the proof of Proposition 10.12 that $\ker \Theta \subset (p, [\pi^\flat])$, where $\pi^\flat \in \mathcal{O}_{C^\flat}$ satisfies $|\pi^\flat| = |p|$. So it is enough to check that $[\epsilon] - 1 \notin (p, [\pi^\flat]^2)$, i.e. $|\epsilon - 1| > |p|^2$.

Recall that if ζ_{p^n} is a primitive nth root of unity, then $|\zeta_{p^n} - 1| = |p|^{1/p^{n-1}(p-1)}$. Therefore,

$$|\epsilon - 1| = \lim_{n \to \infty} |\zeta_{p_n} - 1|^{p^n} = |p|^{p/(p-1)} > |p|^2 \, .$$

□

Proposition 14.4. *There is a natural Galois-equivariant inclusion $\overline{K} \hookrightarrow B_{\mathrm{dR}}$.*

Proof. Let $\overline{k}$ be the residue field of $\overline{K}$. There is a natural inclusion $\overline{k} \hookrightarrow \mathcal{O}_{C^\flat}$ sending $x \mapsto [x^{p^{-n}}]$, which induces inclusions $W(\overline{k}) \hookrightarrow A_{\mathrm{inf}}$, $W(\overline{k})[1/p] \hookrightarrow B_{\mathrm{dR}}^+$. Any $x \in \overline{K}$ satisfies an irreducible monic polynomial over $W(\overline{k})[1/p]$. This polynomial splits completely in C, the residue field of B_{dR}^+, so it also splits in B_{dR}^+ by Hensel's lemma. So there is a unique inclusion $\overline{K} \hookrightarrow B_{\mathrm{dR}}^+$ that makes the following diagram commute.

$$\begin{tikzcd} W(\overline{k})[1/p] \arrow[r, hook] \arrow[d, hook] & B_{\mathrm{dR}}^+ \arrow[d, two heads] \\ \overline{K} \arrow[r, hook] \arrow[ur, hook, dashed] & C \end{tikzcd}$$

$\square$

Proposition 14.5. *The natural inclusions $K = \overline{K}^{G_K} \hookrightarrow (B_{\mathrm{dR}}^+)^{G_K} \hookrightarrow B_{\mathrm{dR}}^{G_K}$ are isomorphisms.*

Proof. For any n, by Lemma 14.2, we have an exact sequence

$$0 \to \mathrm{Fil}^{n+1} B_{\mathrm{dR}} \to \mathrm{Fil}^n B_{\mathrm{dR}} \to C(n) \to 0\,.$$

(Here, $C(n) = C \otimes_{\mathbb{Z}_p} (\mathbb{Z}_p(1)^{\otimes n})$.) It induces an exact sequence

$$0 \to (\mathrm{Fil}^{n+1} B_{\mathrm{dR}})^{G_K} \to (\mathrm{Fil}^n B_{\mathrm{dR}})^{G_K} \to C(n)^{G_K}\,.$$

By Theorem 13.1, $C^{G_K} = K$ and $C(n)^{G_K} = 0$ if $n \neq 0$. We can then show that for all $n > 1$, the inclusion

$$(\mathrm{Fil}^n B_{\mathrm{dR}}^+)^{G_K} \hookrightarrow (\mathrm{Fil}^1 B_{\mathrm{dR}}^+)^{G_K}$$

is an isomorphism. Since $\bigcap_n \mathrm{Fil}^n B_{\mathrm{dR}}^+ = 0$,

$$(\mathrm{Fil}^1 B_{\mathrm{dR}})^{G_K} = 0\,.$$

Then the map $(B_{\mathrm{dR}}^+)^{G_K} \to C^{G_K} = K$ is injective. We already know that $(B_{\mathrm{dR}}^+)^{G_K}$ contains $\overline{K}^{G_K} = K$, so it must equal K. Finally, we can show that for all $n \leq 0$,

$$(B_{\mathrm{dR}}^+)^{G_K} \hookrightarrow (\mathrm{Fil}^n B_{\mathrm{dR}})^{G_K}$$

is an isomorphism, implying that

$$(B_{\mathrm{dR}}^+)^{G_K} \hookrightarrow (B_{\mathrm{dR}})^{G_K}$$

is an isomorphism. $\square$

Definition 14.6. Let V be a finite-dimensional $\mathbb{Q}_p$-representation V of G_K. Let $D_{\mathrm{dR}}(V)$ be the filtered K-vector space $(V \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}})^{G_K}$.

Proposition 14.7. *Let V be a finite-dimensional $\mathbb{Q}_p$-representation V of G_K. Let*

$$\alpha_V : D_{\mathrm{dR}}(V) \otimes_K B_{\mathrm{dR}} \to V \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}$$

be the restriction of the map

$$V \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}} \otimes_K B_{\mathrm{dR}} \to V \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}$$

induced by multiplication on B_{dR}. Then α_V is an injection. In particular,

$$\dim_K D_{\mathrm{dR}}(V) \leq \dim_{\mathbb{Q}_p} V$$

with equality iff α_V is an isomorphism.

Proof. See [BC, Theorem 5.2.1(1)]. $\square$

Definition 14.8. We say that V is *de Rham* if $\dim_K D_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p} V$.

If V is de Rham, then the *Hodge–Tate weights* of V are the integers i such that $\mathrm{gr}^i D_{\mathrm{dR}}(V) \neq 0$.

Example 14.9. The Hodge-Tate weight of $\mathbb{Q}_p(n)$ is $-n$.

Theorem 14.10. *If X is a proper smooth variety over K, then $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is de Rham, with Hodge–Tate weights between 0 and i, inclusive.*

This is proved as part of the de Rham comparison theorem.

Lemma 14.11. *Let L be a finite extension of K. Then a representation of G_K is de Rham if and only if its restriction to G_L is de Rham.*

Proof. This follows from Galois descent. □

Lemma 14.12. *A tensor product of two de Rham representations is de Rham.*

Subrepresentations and quotients of a de Rham representation are de Rham.

Proof. Suppose V_1 and V_2 are de Rham representations. Multiplication on B_{dR} induces a map

$$D_{\mathrm{dR}}(V_1) \otimes_K D_{\mathrm{dR}}(V_2) \to D_{\mathrm{dR}}(V_1 \otimes_{\mathbb{Q}_p} V_2) \,.$$

To show that $V_1 \otimes V_2$ is de Rham, it suffices to show that the above map is injective. Then it also suffices to check injectivity of the map

$$D_{\mathrm{dR}}(V_1) \otimes_K D_{\mathrm{dR}}(V_2) \to (V_1 \otimes_{\mathbb{Q}_p} V_2) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}$$

and likewise of the map

$$D_{\mathrm{dR}}(V_1) \otimes_K D_{\mathrm{dR}}(V_2) \otimes_K B_{\mathrm{dR}} \to (V_1 \otimes_{\mathbb{Q}_p} V_2) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}} \,, \tag{14.13}$$

After rewriting the LHS as

$$(D_{\mathrm{dR}}(V_1) \otimes_K B_{\mathrm{dR}}) \otimes_{B_{\mathrm{dR}}} (D_{\mathrm{dR}}(V_2) \otimes_K B_{\mathrm{dR}})$$

and the RHS as

$$(V_1 \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}) \otimes_{B_{\mathrm{dR}}} (V_2 \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}) \,,$$

we see that Proposition 14.7 implies that (14.13) is an isomorphism.

We can check injectivity after tensoring with B_{dR}. Since V_1 and V_2 are de Rham, we can identify

$$\begin{aligned} D_{\mathrm{dR}}(V_1) \otimes_K D_{\mathrm{dR}}(V_2) \otimes_K B_{\mathrm{dR}} &\cong (D_{\mathrm{dR}}(V_1) \otimes_K B_{\mathrm{dR}}) \otimes_{B_{\mathrm{dR}}} (D_{\mathrm{dR}}(V_2) \otimes_K B_{\mathrm{dR}}) \\ &\cong (V_1 \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}) \otimes_{B_{\mathrm{dR}}} (V_2 \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}) \cong (V_1 \otimes V_2) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}} \end{aligned}$$

Therefore, we are reduced to showing that the induced map

$$(V_1 \otimes_{\mathbb{Q}_p} V_2) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}} \to D_{\mathrm{dR}}(V_1 \otimes_{\mathbb{Q}_p} V_2) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}$$

is injective.

Suppose we have an exact sequence of representations

$$0 \to V' \to V \to V'' \to 0$$

with V de Rham. Then we have a left exact sequence

$$0 \to D_{\mathrm{dR}}(V') \to D_{\mathrm{dR}}(V) \to D_{\mathrm{dR}}(V'') \,,$$

so

$$\dim_K D_{\mathrm{dR}}(V') + \dim_K D_{\mathrm{dR}}(V'') \geq \dim_K D_{\mathrm{dR}} V \,.$$

On the other hand,

$$\dim_K D_{\mathrm{dR}}(V') \leq \dim_{\mathbb{Q}_p} V'$$

$$\dim_K D_{\mathrm{dR}}(V'') \le \dim_{\mathbb{Q}_p} V''$$
$$\dim_K D_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p} V\,.$$

So all inequalities must actually be equalities. □

Example 14.14. Let $\psi\colon \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ be a character, and let $\chi\colon G_K \to \mathbb{Z}_p^\times$ be the cyclotomic character. The character $\psi \circ \chi\colon G_K \to \mathbb{Z}_p^\times$ is de Rham if and only if ψ is a product of a finite order character and a character of the form $z \mapsto z^n$ for some $n \in \mathbb{Z}$. In particular, there exist characters that are not de Rham. The "only if" direction follows from Theorem 13.1 by the same argument as in Proposition 14.5. For the "if" direction, we can use Lemma 14.11 to reduce to the case where the finite order character is trivial, and then apply Lemma 14.2.

15. B_{dR} and differentials

It is not immediately obvious from the definition of B_{dR} that it should have anything to do with integrals of differential forms. We will now give an alternate characterization of B_{dR}^+ that suggests a connection to differential forms.

Let k be the residue field of K. Let

$$A_{\mathrm{inf},K} := A_{\mathrm{inf}} \otimes_{W(k)} \mathcal{O}_K\,.$$

There is a map $\Theta_K\colon A_{\mathrm{inf},K} \to \mathcal{O}_C$, and for each positive integer n, $B_{\mathrm{dR}}^+/\operatorname{Fil}^n B_{\mathrm{dR}} \cong A_{\mathrm{inf},K}/(\ker \Theta_K)^n[1/p]$. So

$$B_{\mathrm{dR}}^+ \cong \varprojlim_n \left(A_{\mathrm{inf},K}/(\ker\Theta_K)^n[1/p]\right)\,.$$

Inductively define

$$\mathcal{O}_{\overline{K}}^{(0)} := \mathcal{O}_{\overline{K}}$$
$$\Omega^{(n)} := \mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_{\overline{K}}^{(n-1)}} \Omega_{\mathcal{O}_{\overline{K}}^{(n-1)}/\mathcal{O}_K}$$
$$\mathcal{O}_{\overline{K}}^{(n)} := \ker\left(d^{(n)}\colon \mathcal{O}_{\overline{K}}^{(n-1)} \to \Omega^{(n)}\right)$$

Theorem 15.1.

(1) *For any nonnegative integer n, the preimage of $A_{\mathrm{inf},K}/(\ker\Theta_K)^{n+1}$ under the inclusion $\overline{K} \hookrightarrow B_{\mathrm{dR}}^+/\operatorname{Fil}^{n+1} B_{\mathrm{dR}}$ is $\mathcal{O}_{\overline{K}}^{(n)}$.*

(2) *For any nonnegative integers m, n, the map $\mathcal{O}_{\overline{K}}^{(n)}/p^m \to A_{\mathrm{inf},K}/((\ker\Theta_K)^{n+1}, p^m)$ is an isomorphism.*

(3) *B_{dR}^+ is the completion of $\overline{K}$ for the topology defined by letting the sets $p^m\mathcal{O}_{\overline{K}}^{(n)}$ for nonnegative integers m, n be a basis of open neighborhoods of the identity.*

(4) *For any nonnegative integer n, $d^{(n)}$ is surjective.*

Corollary 15.2. *The inclusion $\overline{K} \hookrightarrow B_{\mathrm{dR}}^+$ cannot be extended to a continuous map $C \to B_{\mathrm{dR}}^+$.*

Proof. Any $x \in \operatorname{Fil}^1 B_{\mathrm{dR}}^+$ can be written as a limit of a sequence elements of $\overline{K}$. By continuity of the projection $B_{\mathrm{dR}}^+ \to C$, any such sequence converges to 0 in C. So there cannot be any map $C \to B_{\mathrm{dR}}^+$ extending the inclusion $\overline{K} \hookrightarrow B_{\mathrm{dR}}^+$ that preserves sequential limits. □

Lemma 15.3. *The image of $\mathcal{O}_{\overline{K}}^{(n)}$ in B_{dR}^+ is contained in $A_{\mathrm{inf},K} + \operatorname{Fil}^{n+1} B_{\mathrm{dR}}$.*

Proof. We will use induction on n. The case $n = 0$ follows from the surjectivity of Θ.

Let $x \in \mathcal{O}_{\overline{K}}^{(n-1)}$. By the induction hypothesis, the image of x in B_{dR}^{+} can be expressed as $x_0 + \epsilon$, with $x_0 \in A_{\mathrm{inf}}$ and $\epsilon \in \mathrm{Fil}^n B_{\mathrm{dR}}$. Recall that $A_{\mathrm{inf}} \cap \mathrm{Fil}^n B_{\mathrm{dR}} = (\ker \Theta_K)^n$. Consider the map

$$\mathcal{O}_{\overline{K}}^{(n-1)} \to \mathrm{Fil}^n B_{\mathrm{dR}} / \left((\ker \Theta_K)^n + \mathrm{Fil}^{n+1} B_{\mathrm{dR}}\right)$$
$$x \mapsto \epsilon$$

This map is an $\mathcal{O}_K$-linear derivation taking values in a $\mathcal{O}_{\overline{K}}$-module. By the universal property of $\Omega^{(n)}$, the map factors through $d^{(n)}$. In particular, its kernel contains $\ker d^{(n)} = \mathcal{O}_{\overline{K}}^{(n)}$. □

Lemma 15.4. *Let $x \in \mathcal{O}_{\overline{K}}$. Let $P \in \mathcal{O}_K[X]$ be a polynomial satisfying $P(x) = 0$, and let r be a nonnegative integer such that $P'(x) \mid p^r$ in $\mathcal{O}_{\overline{K}}$. For each nonnegative integer n, let $a_n = (2^n - 1)r$, $b_n = (2^{n+1} - 2n - 1)r$. Then for any positive integer m, $p^{a_n} x^m \in \mathcal{O}_{\overline{K}}^{(n)}$, and $x^{p^{b_n}} \in \mathcal{O}_{\overline{K}}^{(n)}$.*

Proof. Use induction on n. The base case $n = 0$ is trivial. Now assume that for some fixed n and all m, $p^{a_n} x^m \in \mathcal{O}_{\overline{K}}^{(n)}$, and $x^{p^{b_n}} \in \mathcal{O}_{\overline{K}}^{(n)}$. By repeated use of the product rule, we see that

$$d^{(n+1)}(p^{2a_n} x^m) = m p^{a_n} x^{m-1} d^{(n+1)}(p^{a_n} x) \tag{15.5}$$

for each m. In particular, this implies

$$0 = d^{(n+1)}(p^{2a_n} P(x)) = p^{a_n} P'(x) d^{(n+1)}(p^{a_n} x) \,.$$

Hence

$$0 = d^{(n+1)}(p^{2a_n + r} x) \,. \tag{15.6}$$

Then multiplying (15.5) by p^r and applying (15.6) yields

$$0 = d^{(n+1)}(p^{2a_n + r} x^m) = d^{(n+1)}(p^{a_{n+1}} x^m) \,.$$

In the case $m = p^{b_n}$, since $p^r \mid m$, we get the stronger result

$$0 = d^{(n+1)}\left(p^{2a_n} x^{p^{b_n}}\right) = p^{2a_n} d^{(n+1)}\left(x^{p^{b_n}}\right) \,.$$

Then

$$d^{(n+1)}\left(x^{p^{b_{n+1}}}\right) = d^{(n+1)}\left(x^{p^{b_n + 2a_n}}\right) = p^{2a_n} (x^{p^{b_n}})^{p^{2a_n} - 1} d^{(n+1)}\left(x^{p^{b_n}}\right) = 0 \,.$$

□

16. B_{dR} and differentials, continued

Let π be a uniformizer of K.

Lemma 16.1. *For any n, the map $\mathcal{O}_{\overline{K}}^{(n)} \to \mathcal{O}_C/\pi = \mathcal{O}_{\overline{K}}/\pi$ is surjective.*

Proof. Let $x \in \mathcal{O}_{\overline{K}}$, and let P be the minimal polynomial for x over k. Let x_m satisfy $x_m^{p^m} + \pi x_m = x$. Then $x_m^{p^m} \equiv x \pmod{\pi}$. We claim that for sufficiently large m, $x_m^{p^m} \in \mathcal{O}_{\overline{K}}^{(n)}$. Indeed, let $P_m(X) = P(X^{p^m} + \pi X)$; then $P_m(x_m) = 0$ and $P_m'(x_m) = (p^m x_m^{p^m - 1} + \pi) P'(x)$, so $|P_m'(x_m)| = |\pi||P'(x)|$. Then the claim follows from Lemma 15.4. □

By Lemma 15.3, the map $\mathcal{O}_{\overline{K}}^{(n)} \hookrightarrow B_{\mathrm{dR}}^+/\operatorname{Fil}^{n+1} B_{\mathrm{dR}}^+$ factors through $A_{\mathrm{inf},K}/(\ker \Theta_K)^{n+1}$.

Lemma 16.2. *For any n, m,*

$$\mathcal{O}_{\overline{K}}^{(n)} \to A_{\mathrm{inf},K}/(\pi^m, (\ker \Theta_K)^{n+1})$$

is surjective.

Proof. Observe that $A_{\mathrm{inf}}/(\pi^m, (\ker \Theta_K)^{n+1})$ is generated as an $\mathcal{O}_K$-module by the elements $[x]$ for $x \in \mathcal{O}_{K^\flat}$. By Lemma 16.1, for any r, we can find $\tilde{x}_r \in \mathcal{O}_{\overline{K}}^{(n)}$ such that $\tilde{x}_r$ and $x^{(r)}$ have the same image in $\mathcal{O}_C/p$. So the image of $\tilde{x}_r$ in $A_{\mathrm{inf},K}/(\ker \Theta_K)^{n+1}$ will be congruent to $[x^{p^{-r}}]$ modulo $(\pi, (\ker \Theta_K))$. If r is sufficiently large, then the image of $\tilde{x}_r^{p^r}$ will be congruent to $[x]$ modulo $(\pi^m, (\ker \Theta_K)^n)$. (Note that the bound on r does not depend on x, only on m and n.) □

Lemma 16.3. *Let m, n be nonnegative integers. Consider the map*

$$\theta_{m,n} \colon \mathcal{O}_{\overline{K}}^{(n)}/p^m \to \mathcal{O}_C/p^m \,.$$

We have

$$(\ker \theta_{m,n})^{n+1} = 0 \,.$$

Proof. We will use induction on n. The base case $n = 0$ is trivial. Assume $(\ker \theta_{m,n-1})^n = 0$. It suffices to show that for $x \in \ker \theta_{m,n}$, $y \in (\ker \theta_{m,n})^n$, $xy = 0$. Choose lifts $\tilde{x}, \tilde{y} \in \mathcal{O}_{\overline{K}}^{(n)}$. By the induction hypothesis, $\tilde{y} \in p^m \mathcal{O}_{\overline{K}}^{(n-1)}$. Then $\tilde{x} \cdot p^{-m}\tilde{y} \in \mathcal{O}_{\overline{K}}^{(n-1)}$ and

$$d^{(n)}(\tilde{x} \cdot p^{-m}\tilde{y}) = p^{-m}\tilde{y} \cdot d^{(n)}\tilde{x} + p^{-m}\tilde{x} \cdot d^{(n)}\tilde{y} = 0 \,.$$

So $\tilde{x}\tilde{y}$ is a multiple of p^m in $\mathcal{O}_{\overline{K}}^{(n)}$, implying $xy = 0$. □

Proof of Theorem 15.1(2). First, we prove item (2), that the map

$$\mathcal{O}_{\overline{K}}^{(n)}/p^m \to A_{\mathrm{inf},K}/(p^m, (\ker \Theta_K)^{n+1})$$

is an isomorphism. Denote this map by $f_{m,n}$. We will construct an inverse map

$$g_{m,n} \colon A_{\mathrm{inf}}/(p^m, (\ker \Theta_K)^{n+1}y) \to \mathcal{O}_{\overline{K}}^{(n)}/p^m \,.$$

By a generalization of Proposition 10.10, to construct a ring homomorphism

$$A_{\mathrm{inf},K}/p^m \to \mathcal{O}_{\overline{K}}^{(n)}/p^m \,,$$

it suffices to construct a multiplicative map

$$\mathcal{O}_{C^\flat} \to \mathcal{O}_{\overline{K}}^{(n)}/p^m$$

such that the induced map

$$\mathcal{O}_{C^\flat} \to \mathcal{O}_{\overline{K}}^{(n)}/\pi$$

is a ring homomorphism. For $x \in \mathcal{O}_{C^\flat}$ and r a nonnegative integer, let $\tilde{x}_r \in \mathcal{O}_{\overline{K}}^{(n)}/\pi^m$ such that $\tilde{x}_r$ and $x^{(r)}$ have the same image on $\mathcal{O}_C/\pi^m$. It follows from 16.3 that for sufficiently large r, $\tilde{x}_r^{p^r}$ will not depend on the choice of $\tilde{x}_r$. Then we choose the map $x \mapsto \tilde{x}_r^{p^r}$. The associated map $A_{\mathrm{inf},K}/\pi^m \to \mathcal{O}_{\overline{K}}^{(n)}$ is given by

$$\sum_i [x_i]\pi^i \mapsto \sum_i \tilde{x}_{i,r}^{p^r}\pi^i \,. \tag{16.4}$$

By Lemma 16.3, this map actually factors through $A_{\mathrm{inf},K}/(p^m, (\ker\Theta_K)^{n+1})$. So we have constructed $g_{m,n}$. It is clear that $f_{m,n}\circ g_{m,n} = 1$.

Now we prove that $g_{m,n}\circ f_{m,n} = 1$. Since $\mathcal{O}_{\overline{K}}^{(n)}$ has no p-torsion, $\widehat{\mathcal{O}_{\overline{K}}^{(n)}}$ also has no p-torsion. So it suffices to show that the induced maps

$$f_n \colon \widehat{\mathcal{O}_{\overline{K}}^{(n)}}[1/p] \to B_{\mathrm{dR}}^+/\operatorname{Fil}^{n+1} B_{\mathrm{dR}}^+$$

$$g_n \colon B_{\mathrm{dR}}^+/\operatorname{Fil}^{n+1} B_{\mathrm{dR}}^+ \to \widehat{\mathcal{O}_{\overline{K}}^{(n)}}[1/p]$$

satisfy $g_n\circ f_n = 1$. We can construct a map $\overline{K} \hookrightarrow \widehat{\mathcal{O}_{\overline{K}}}^{(n)}[1/p]$ by the same method as for $\overline{K}\to B_{\mathrm{dR}}$. It is not hard to see that $g_n\circ f_n$ fixes K, so $g_n\circ f_n$ must send $\overline{K}$ to itself. Since $g_n\circ f_n$ induces the identity on the residue field C, it must fix $\overline{K}$. But $\overline{K}$ is dense in $\widehat{\mathcal{O}_{\overline{K}}}^{(n)}[1/p]$, so $g_n\circ f_n = 1$. This concludes the proof of item (2). □

Proof of Theroem 15.1(1,3,4). Next, we prove item (1), that the preimage of $A_{\mathrm{inf},K}/(\ker\Theta_K)^{n+1}$ under the inclusion $\overline{K}\hookrightarrow B_{\mathrm{dR}}^+/\operatorname{Fil}^{n+1} B_{\mathrm{dR}}$ is $\mathcal{O}_{\overline{K}}^{(n)}$. Denote the preimage by $\mathcal{O}'$.

Let $x\in\mathcal{O}'$. Then by Lemma 15.4, there exists m so that $p^m x\in\mathcal{O}_{\overline{K}}^{(n)}$. By item (2), $\mathcal{O}_{\overline{K}}^{(n)}/p^m \to A_{\mathrm{inf}}/(p^m, (\ker\Theta_K)^{(n+1)})$ is injective, so $p^m x$ must be a multiple of p^m in $\mathcal{O}_{\overline{K}}^{(n)}$ as well. Hence $x\in\mathcal{O}_{\overline{K}}^{(n)}$.

Item (3) follows immediately from items (1) and (2).

Finally, we prove item (4). Each element of $\Omega^{(n)}$ is of the form $\sum_i x_i d^{(n)} y_i$ for $x_i\in\mathcal{O}_{\overline{K}}$ and $y_i\in\mathcal{O}_{\overline{K}}^{(n-1)}$. By Lemma 15.4, we can find m_i so that $p^{m_i} d^{(n)} y_i = 0$, and by Lemma 16.2, we can find $z_i\in\mathcal{O}_{\overline{K}}^{(n)}$ so that $x_i - z_i\in p^{m_i}\mathcal{O}_{\overline{K}}$. Then $\sum_i x_i d^{(n)} y_i = \sum_i z_i d^{(n)} y_i = \sum_i d^{(n)}(y_i z_i)$. □

Corollary 16.5. *For each positive integer n, there is a natural isomorphism*

$$\operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^{(n)}) \cong \operatorname{Fil}^n B_{\mathrm{dR}}/\operatorname{Fil}^{n+1} B_{\mathrm{dR}}\,.$$

Proof. By Theorem 15.1(4), there is an exact sequence

$$0\to\mathcal{O}_{\overline{K}}^{(n)}\to\mathcal{O}_{\overline{K}}^{(n-1)}\to\Omega^{(n)}\to 0\,.$$

Recall that the functor $\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Q}_p/\mathbb{Z}_p, -)$ is p-adic completion. So we get an exact sequence

$$0\to\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega^{(n)})\to A_{\mathrm{inf},K}/(\ker\Theta_K)^{n+1}\to A_{\mathrm{inf},K}/(\ker\Theta_K)^n\to 0\,.$$

Observe that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega^{(n)})\cong\operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega^{(n)})$, and since $\Omega^{(n)}$ is p-power torsion, $\operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega^{(n)})\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\cong\operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^{(n)})$. Then inverting p gives an exact sequence

$$0\to\operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^{(n)})\to B_{\mathrm{dR}}^+/\operatorname{Fil}^{n+1} B_{\mathrm{dR}}^+\to B_{\mathrm{dR}}^+/\operatorname{Fil}^n B_{\mathrm{dR}}^+\to 0\,.$$

□

17. Sites and cohomology

Recall that in the first lecture, we considered an isomorphism between the singular and de Rham cohomologies of a complex manifold. This isomorphism can be understood in terms of sheaf cohomology.

Let X be a complex manifold. A presheaf of sets on X is a contravariant functor $\mathcal{F}$ from the category of open subsets of X to the category of sets. We say that $\mathcal{F}$ is a sheaf if for every open $U \subset X$ and every covering $U = \bigcup_{i \in I} U_i$,

$$\mathcal{F}(U) \longrightarrow \prod_{i \in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j \in I} \mathcal{F}(U_i \cap U_j)$$

is an equalizer diagram. In other words, $\mathcal{F}(U)$ is the subset of $\prod_{i \in I} \mathcal{F}(U_i)$ such that for each $i, j \in I$, the projections to $\mathcal{F}(U_i)$ and $\mathcal{F}(U_j)$ have the same image in $\mathcal{F}(U_i \cap U_j)$. A morphism of (pre)sheaves $\mathcal{F} \to \mathcal{G}$ is a natural transformation of functors.

The categories of sheaves and presheaves of abelian groups on X are defined similarly. They are abelian categories.

A sheaf $\mathcal{I}$ of abelian groups on X is called *injective* if the functor $\mathrm{Hom}(-, \mathcal{I})$ is exact. An *injective resolution* of a sheaf $\mathcal{F}$ of abelian groups on X is a long exact sequence

$$0 \to \mathcal{F} \to \mathcal{I}_0 \to \mathcal{I}_1 \to \cdots$$

where $\mathcal{I}_0, \mathcal{I}_1, \ldots$ are injective sheaves.

It can be shown that every sheaf of abelian groups on X admits an injection into an injective sheaf. This implies that every sheaf of abelian groups on X admits an injective resolution.

The cohomology groups $H^n(X, \mathcal{F})$ are defined by the cohomology groups of the complex

$$0 \to \mathcal{I}_0(X) \to \mathcal{I}_1(X) \to \cdots .$$

This definition is independent of the injective resolution chosen.

A sheaf $\mathcal{G}$ is called *acyclic* if $H^n(X, \mathcal{G}) = 0$ for all $n > 0$. One can actually compute the cohomology groups $H^n(X, \mathcal{F})$ using any resolution of $\mathcal{F}$ by acyclic sheaves.

For any complex manifold X and any ring A, the complex of singular cochains on X is an acyclic resolution of the constant sheaf A. So

$$H^i_{\mathrm{sing}}(X, A) = H^i_{\mathrm{sheaf}}(X, A) .$$

If $C^\bullet$ is a complex of sheaves on X, then an injective (resp. acyclic) of $C^\bullet$ is a quasi-isomorphism of complexes $C^\bullet \to \mathcal{I}^\bullet$, where the objects of $\mathcal{I}^\bullet$ are injective (resp. acyclic). (A quasi-isomorphism of complexes is a morphism that induces an isomorphism on cohomology.) Then the hypercohomology of $H^*(X, C^\bullet)$ is defined to be the cohomology of the complex

$$0 \to \mathcal{I}_0(X) \to \mathcal{I}_1(X) \to \cdots .$$

The de Rham complex $\Omega^\bullet_X$ is the complex

$$0 \to \mathcal{O}_X \xrightarrow{d} \Omega^1_{X/\mathbb{C}} \xrightarrow{d} \cdots \xrightarrow{d} \Omega^n_{X/\mathbb{C}} \to 0 .$$

If X is an open subset of $\mathbb{C}^n$, then the $\Omega^i_{X/\mathbb{C}}$ are already acyclic. We implicitly used this fact in the first lecture when computing the de Rham cohomology of $\mathbb{C}^\times$.

The analytic de Rham cohomology of X is defined to be the hypercohomology of $\Omega^\bullet_X$. The Poincaré lemma states that $\mathbb{C}[0] \to \Omega^\bullet_X$ is a quasi-isomorphism. Therefore,

$$H^i_{\mathrm{dR}}(X) = H^i_{\mathrm{sheaf}}(X, \mathbb{C}) .$$

If X is a smooth algebraic variety over a field K, then we can define the algebraic de Rham cohomology similarly. If X is a proper variety over $\mathbb{C}$, then there is an isomorphism

$$H^i_{\mathrm{dR}}(X) \cong H^i_{\mathrm{dR}}(X(\mathbb{C})) ,$$

where $X(\mathbb{C})$ is considered as a complex analytic space.

However, the Poincaré lemma does not hold for the algebraic de Rham complex: $K[0] \to \Omega^\bullet_{X/K}$ is generally not a quasi-isomorphism. For example, if $X = \mathbb{A}^1_K \setminus \{0\}$, then $\frac{dz}{z}$ does not have an antiderivative locally in the Zariski topology. The cohomology $H^i(X, K)$ is not very interesting: it is zero if $i > 0$.

In practice, we usually use Čech cohomology to compute de Rham cohomology. If X is an affine algebraic variety, then the sheaves $\Omega^i_{X/K}$ are acyclic. More generally, if X is a separated algebraic variety, then we can write X as a finite union $X = \bigcup_{i \in I} X_i$, where the X_i's are affine, and the intersections of the X_i's are also affine. Define a complex $C^\bullet$ as follows. Let

$$C^n = \bigoplus_{J \subset I} \Omega^{n-|J|} \left(\bigcap_{j \in J} X_j \right) .$$

Given $\omega \in \Omega^{n-|J|}\left(\bigcap_{j\in J} X_j\right)$, the $\Omega^{n+1-|J|}\left(\bigcap_{j\in J} X_j\right)$-part of its differential is $d\omega$. Choose an ordering of I. If $i \notin J$, then the $\Omega^{n+1-|J\cup\{i\}|}\left(\bigcap_{j\in J\cup\{i\}} X_j\right)$-part of the differential of ω is $(-1)^{n+|\{j\in J | j<i\}|}$ times the restriction of ω. All other parts are zero. Then the de Rham cohomology of X is the cohomology of $C^\bullet$.

Étale cohomology is supposed to be an analogue of singular cohomology for more general kinds of spaces. To define étale cohomology, we need to use sites.

Definition 17.1. A site is a category $\mathcal{C}$ along a set $\mathrm{Cov}(\mathcal{C})$ of morphisms with fixed target $\{U_i \to U\}_{i\in I}$, satisfying the following axioms:

(1) If $V \to U$ is an isomorphism then $\{V \to U\} \in \mathrm{Cov}(\mathcal{C})$.
(2) If $\{U_i \to U\}_{i\in I} \in \mathrm{Cov}(\mathcal{C})$ and for each $i \in I$, $\{V_{ij} \to U_i\}_{j\in J_i} \in \mathrm{Cov}(\mathcal{C})$, then $\{V_{ij} \to U\}_{i\in I, j\in J_i} \in \mathrm{Cov}(\mathcal{C})$.
(3) If $\{U_i \to U\}_{i\in I} \in \mathrm{Cov}(\mathcal{C})$ and $V \to U$ is a morphism in $\mathcal{C}$, then for all $i \in I$, $U_i \times_U V$ exists, and $\{U_i \times_U V\}_{i\in I} \in \mathrm{Cov}(\mathcal{C})$

For any topological space X, we can define a site by taking $\mathcal{C}$ to be the category of open sets of X and coverings to be open coverings in the usual sense. Note that the fiber product is just intersection.

Now let X be a scheme. Recall that a morphism of schemes $Y \to Z$ is called *étale* if it is smooth of delative dimension 0. Define the *small étale site* $X_{\text{ét}}$ as follows. The underlying category is the category of étale morphisms $U \to X$. A collection $U_i \to X$ is a covering if the images of the U_i cover X. (There is also a big étale site, where the category includes all schemes over X, but morphisms are still jointly surjective collections of étale maps.)

Sheaves and cohomology can be defined on any site. One can show that if X is an algebraic variety over $\mathbb{C}$, then for any N,

$$H^i(X(\mathbb{C}), \mathbb{Z}/N\mathbb{Z}) \cong H^i(X_{\text{ét}}, \mathbb{Z}/N\mathbb{Z}) .$$

The reason that we need to use $\mathbb{Z}/N\mathbb{Z}$ coefficients is that finite covers of $X(\mathbb{C})$ are in bijection with finite covers of X, but the same is not true of infinite covers. To deal with this issue, we define

$$H^i_{\text{ét}}(X, \mathbb{Z}_p) = \varprojlim_n H^i(X, \mathbb{Z}/p^n\mathbb{Z})$$

$$H^i_{\text{ét}}(X, \mathbb{Q}_p) = H^i(X, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

for any algebraic variety X. Using this definition, if X is an algebraic variety over $\mathbb{C}$, then

$$H^i(X(\mathbb{C}), \mathbb{Z}_p) \cong H^i(X_{\text{ét}}, \mathbb{Z}_p) .$$

$$H^i(X(\mathbb{C}), \mathbb{Q}_p) \cong H^i(X_{\text{ét}}, \mathbb{Q}_p) .$$

Normally, we consider cohomology of varieties over an algebraically closed field, as the notion of cohomology most closely matches our geometric intuition in that case. For example, if k is a field, then

$$H^i((\operatorname{Spec} k)_{\text{ét}}, \Lambda) = H^i_{\text{cts}}(\operatorname{Gal}(k^{\text{sep}}/k), \Lambda) .$$

So the cohomology of the spectrum of a non-algebraically closed field can be quite complicated.

Actually, there is a way to define $H^i_{\text{ét}}(X, \mathbb{Z}_p)$ as cohomology on an actual site, called the "proétale site". A morphism of schemes $f : X \to Y$ is called *weakly étale* if f and $\Delta_f : X \to X \times_Y X$ are both flat. Coverings in the proétale site are defined to be collections of weakly étale maps $X_i \to Y$ such that for each affine open $V \subset Y$, there is a finite collection of affine opens $U_i \subset X_i$ whose images cover V. Then

$$H^i_{\text{ét}}(X, \mathbb{Z}_p) = H^i(X_{\text{proét}}, \mathbb{Z}_p) .$$

The site is called the "proétale site" because, if we have a tower

$$\cdots \to X_2 \to X_1 \to X$$

of schemes with étale and affine transition maps, then the projection

$$\varprojlim_i X_i \to X$$

is weakly étale. It turns out that the property of being proétale is not local, so it's better to use the property of being weakly étale for defining a site.

If X is an algebraic variety over a p-adic field K, we now know the definitions of the objects appearing in the de Rham comparison isomorphism

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

(However, proving the theorem requires getting much deeper in to p-adic geometry.)

18. Hodge-Tate decomposition for abelian varieties

i Let X be a proper variety over a p-adic field K. Recall the comparison isomorphism

$$H^n_{\mathrm{dR}}(X) \otimes_K B_{\mathrm{dR}} \cong H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} B_{\mathrm{dR}}\,. \tag{18.1}$$

This is an isomorphism of filtered vector spaces with G_K-action. Here, B_{dR} has the usual filtration, $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)$ has the trivial filtration, and the filtration on $H^n_{\mathrm{dR}}(X)$ is given by

$$\operatorname{Fil}^i H^n_{\mathrm{dR}}(X) = \operatorname{im}\Big((H^n(X, \sigma_{\geq i}\Omega^\bullet_{X/K}) \to H^n(X, \Omega^\bullet_{X/K})\Big)\,.$$

Here, $\sigma_{\geq i}\Omega^\bullet_{X/K}$ is the complex

$$\Omega^i_{X/K} \to \Omega^{i+1}_{X/K} \to \cdots \to \Omega^n_{X/K}\,.$$

One can show that there are isomorphisms

$$H^n_{\mathrm{dR}}(X) = \bigoplus_m H^{n-m}(X, \Omega^m_{X/K})\,.$$

$$\operatorname{Fil}^i H^n_{\mathrm{dR}}(X) = \bigoplus_{m \geq i} H^{n-m}(X, \Omega^m_{X/K})\,.$$

Taking the zeroth graded piece of (18.1) gives an isomorphism

$$\bigoplus_{i=0}^n H^{n-i}(X, \Omega^i_{X/K}) \otimes_K C(-i) \cong H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} C\,. \tag{18.2}$$

An *abelian variety* over K is proper group scheme over K that is geometrically reduced and irreducible. If X is an abelian variety, then the decomposition (18.2) can actually be made fairly explicit. In that case, all cohomology groups are wedge powers of H^1, so it suffices to consider $n = 1$. Furthermore, $H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)$ is dual to the Tate module $T_p(X) := \varprojlim_n X(\overline{K})[p^n]$. Therefore, giving a C-linear map $H^0(X, \Omega^1_{X/K}) \otimes_K C(-1) \to H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} C$ is equivalent to giving a map

$$H^0(X, \Omega^1_{X/K}) \times T_p(X) \to C(1)$$

that is K-linear in the first variable and $\mathbb{Z}_p$-linear in the second.

We will sketch the construction of the map, but we refer the reader to [Fon82] for the technical details.

Let $\mathfrak{X}$ be a proper flat model of X over $\mathcal{O}_K$. Recall that we defined

$$\Omega^{(1)} = \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}\,.$$

We can define a map

$$H^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \times \mathfrak{X}(\mathcal{O}_{\overline{K}}) \to \Omega^{(1)}$$

$$(\omega, x) \mapsto x^*(\omega)\,.$$

It is possible to use the group law on the generic fiber show that for some r, the restriction

$$p^r H^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \times \mathfrak{X}(\mathcal{O}_{\overline{K}}) \to \Omega^{(1)}$$

is bilinear.

By the valuative criterion of properness, $\mathfrak{X}(\mathcal{O}_{\overline{K}}) = X(K)$. Using $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, X(K)) \cong T_p(X)$ and $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega^{(1)}) \cong \ker\Theta_K/(\ker\Theta_K)^2$, we obtain a map

$$p^r H^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \times T_p(X) \to (\ker\Theta_K)/(\ker\Theta_K)^2 \,.$$

Finally, we invert p to get a bilinear map

$$H^0(X, \Omega^1_{X/K}) \times T_p(X) \to C(1) \,.$$

Now we have a constructed map (which can be shown to be injective)

$$H^0(X, \Omega^1_{X/K}) \otimes_K C(-1) \hookrightarrow H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} C \,. \tag{18.3}$$

If $X^\vee$ is the dual abelian variety, then we get a map

$$H^0(X^\vee, \Omega^1_{X^\vee/K}) \otimes_K C(-1) \hookrightarrow H^1_{\text{ét}}(X^\vee_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} C \,.$$

The Weil pairing determines a perfect pairing

$$H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \times H^1_{\text{ét}}(X^\vee_{\overline{K}}, \mathbb{Z}_p) \to \mathbb{Z}_p(-1)$$

and there is also a perfect pairing

$$H^1(X, \mathcal{O}_X) \times H^0(X^\vee, \Omega^1_{X^\vee/K}) \to K \,.$$

So we get a map

$$H^1(X, \mathcal{O}_X)^* \otimes_K C(-1) \hookrightarrow H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)^* \otimes_{\mathbb{Z}_p} C(-1) \,.$$

Taking the dual and twisting, we get a map

$$H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} C \twoheadrightarrow H^1(X, \mathcal{O}_X) \otimes_K C \,. \tag{18.4}$$

The composite of (18.3) and (18.4) must be zero since $C(1)^{G_K} = 0$. Then, by dimension counting, the sequence

(18.5)

$$0 \to H^0(X, \Omega^1_{X/K}) \otimes_K C(-1) \to H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} C \to H^1(X, \mathcal{O}_X) \otimes_K C \to 0$$

must be exact. Since $H^1(G_K, C(-1)) = 0$ (see Remark 13.2), this sequence has a G_K-equivariant splitting. Since $C(-1)^{G_K} = 0$, this splitting is unique.

References

[Ax70] J. Ax. Zeros of polynomials over local fields—The Galois action. *J. Algebra*, 15:417–428, 1970.

[BC] O. Brinon and B. Conrad. CMI summer school notes on p-adic Hodge theory. `http://math.stanford.edu/~conrad/papers/notes.pdf`.

[BMS18] B. Bhatt, M. Morrow, and P. Scholze. Integral p-adic Hodge theory. *Publ. Math. Inst. Hautes Études Sci.*, 128:219–397, 2018.

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

[Dia17] H. Diao. Period rings and period sheaves. 2017. `http://swc.math.arizona.edu/aws/2017/2017DiaoProblems.pdf`.

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

[Far08] L. Fargues. L'isomorphisme entre les tours de Lubin-Tate et de Drinfeld et applications cohomologiques. In *L'isomorphisme entre les tours de Lubin-Tate et de D rinfeld*, volume 262 of *Progr. Math.*, pages 1–325. Birkhäuser, Basel, 2008.

[FF18] L. Fargues and J.-M. Fontaine. Courbes et fibrés vectoriels en théorie de Hodge p -adique. *Astérisque*, (406):xiii+382, 2018. With a preface by Pierre Colmez.

[FO] J.-M. Fontaine and Y. Ouyang. Theory of p-adic Galois representations. `http://staff.ustc.edu.cn/~yiouyang/galoisrep.pdf`.

[Fon82] J.-M. Fontaine. Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de B arsotti-Tate. *Ann. of Math. (2)*, 115(3):529–577, 1982.

[Fon82] J.-M. Fontaine. Formes différentielles et modules de Tate des variété s abéliennes sur les corps locaux. *Invent. Math.*, 65(3):379–409, 1981/82.

[Kat73] N. M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, Berlin, 1973.

[Ked15] K. S. Kedlaya. New methods for (Γ, φ)-modules. *Res. Math. Sci.*, 2:Art. 20, 31, 2015.

[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.

[Mat86] H. Matsumura. *Commutative ring theory. Transl. from the Japanese by M. Reid*, volume 8 of *Camb. Stud. Adv. Math.* Cambridge University Press, Cambridge, 1986.

[Mes72] W. Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Lecture Notes in Mathematics, Vol. 264. Springer-Verlag, Berlin-New York, 1972.

[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`.

[SW13] P. Scholze and J. Weinstein. Moduli of p-divisible groups. *Camb. J. Math.*, 1(2):145–237, 2013.

[Tat67] J. T. Tate. p-divisible groups. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.

[Tat97] J. Tate. Finite flat group schemes. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 121–154. Springer, New York, 1997.

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