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

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

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

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

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

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. $\square$

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. $\square$

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. $\square$

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

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

$\square$

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'. $\square$

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 $\mathrm{Gal}(L/K)$. $\square$

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

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

Let $H = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. 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. $\square$

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.

References

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

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

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

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

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