Chabauty Notes

Niven Achenjang

Spring 2023

These are my course notes for "Foundations of non-abelian Chabauty" at Harvard. Each lecture will get its own 'chapter'. These notes are live-texed and so likely contain many mistakes. Furthermore, they reflect my understanding (or lack thereof) of the material as the lecture was happening, so they are far from mathematically perfect.[1] Despite this, I hope they are not flawed enough to distract from the underlying mathematics. With all that taken care of, enjoy and happy mathing.

The instructor for this class is Alexander Betts, and the course website can be found by clicking this link. The website includes handwritten notes and problem sets. Also, my notes during office hours aren't always the most faithful to what happened, because office hours are harder to take notes for.

Contents

[1] In particular, if things seem confused/false at any point, this is me being confused, not the speaker

List of Figures

List of Tables

1 Lecture 1 (1/24/2023) – Didn't Go

Note 1. Notes below added after the fact from looking at a combination of Alex's notes and those from a friend.

Diophantine Geometry is the study of rational points on varieties over $\mathbb{Q}$ (or any number field).

Theorem 1.1. *Let $X/\mathbb{Q}$ be a smooth, projective curve of genus g.*

- *If $g = 0$, then either $X(\mathbb{Q}) = \emptyset$ or $\#X(\mathbb{Q}) = \infty$.*
- *If $g = 1$, then either $X(\mathbb{Q}) = \emptyset$ or $X(\mathbb{Q})$ is a finitely generated abelian group (Mordell-Weil)*
- *If $g \geq 2$, then $\#X(\mathbb{Q}) < \infty$ (Faltings)*

Remark 1.2. In genus 0, whether or not $X(\mathbb{Q})$ is nonempty is controlled by *local* behavior. ◦

Theorem 1.3 (Hasse-Minkowski)**.** *Say X has genus 0. Then, $X(\mathbb{Q}) \neq \emptyset \iff X(\mathbb{R}) \neq \emptyset$ and $X(\mathbb{Q}_\ell) \neq \emptyset$ for all ℓ.*

Warning 1.4. This fails in higher genus (Lind, Reichardt, Selmer, etc.) •

However, we can still ask the following.

Question 1.5. *Where does $X(\mathbb{Q})$ lie inside*

$$X(\mathbb{A}_{\mathbb{Q}}^f) = \prod_{p \nmid \infty} X(\mathbb{Q}_p)?$$

This is the subject of *obstruction theory*.

1.1 Descent on Elliptic Curves

Let $E/\mathbb{Q}$ be an elliptic curve. Then,

$$E(\mathbb{Q}) \simeq \underbrace{E(\mathbb{Q})_{\text{tors}}}_{\text{Mazur}} \times \underbrace{\mathbb{Z}^{\text{rank}\, E(\mathbb{Q})}}_{\text{BSD}}.$$

For $n \in \mathbb{N}$, we have the Kummer sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0$$

which, upon taking Galois cohomology, gives rise to the global Kummer map

$$\kappa_n : E(\mathbb{Q}) \longrightarrow \mathrm{H}^1(G_{\mathbb{Q}}, E[n])$$

as well as the local Kummer maps

$$\kappa_{n,\ell} : E(\mathbb{Q}_\ell) \longrightarrow \mathrm{H}^1(G_\ell, E[n])$$

(for ℓ prime or ∞). Above, G_ℓ is the decomposition group at ℓ. Comparing these two gives rise to the n-descent square

$$\begin{array}{ccc} E(\mathbb{Q}) & \hookrightarrow & \prod_\ell E(\mathbb{Q}_\ell) \\ \downarrow{\scriptstyle \kappa_n} & & \downarrow{\scriptstyle \prod \kappa_{n,\ell}} \\ \mathrm{H}^1(G_\mathbb{Q}, E[n]) & \xrightarrow{\prod \mathrm{loc}_\ell} & \prod_\ell \mathrm{H}^1(G_\ell, E[n]) \end{array}$$

(Above, $\mathrm{loc}_\ell : \mathrm{H}^1(G_\mathbb{Q}, E[n]) \to \mathrm{H}^1(G_\ell, E[n])$ is the natural localization/restriction map).

The upshot is that $E(\mathbb{Q})$ lies in the "intersection" of $\mathrm{H}^1(G_\mathbb{Q}, E[n])$ with $E(\mathbb{A}_\mathbb{Q}) = \prod_\ell E(\mathbb{Q}_\ell)$.

Definition 1.6.

(1) The n-Selmer group is

$$\mathrm{Sel}^{(n)}(E/\mathbb{Q}) := \left\{\xi \in \mathrm{H}^1(G_\mathbb{Q}, E[n]) : \mathrm{loc}_\ell(\xi) \in \mathrm{im}(\kappa_{n,\ell}) \text{ for all } \ell\right\}.$$

(2) The n-descent locus is

$$E(\mathbb{A}_\mathbb{Q})^{(n)} := \left\{(x_\ell)_\ell \in \prod_\ell E(\mathbb{Q}_\ell) : \exists \xi \in \mathrm{H}^1(G_\mathbb{Q}, E[n]) \text{ with } \mathrm{loc}_\ell(\xi) = \kappa_{n,\ell}(x_\ell) \text{ for all } \ell\right\}.$$

◇

Note that

$$E(\mathbb{Q}) \subset E(\mathbb{A}_\mathbb{Q})^{(n)} \subset E(\mathbb{A}_\mathbb{Q}),$$

so $E(\mathbb{A}_\mathbb{Q})^{(n)}$ constrains where $E(\mathbb{Q})$ can lie in $E(\mathbb{A}_\mathbb{Q})$.

Fact. $E(\mathbb{A}_\mathbb{Q})^{(n)} \subset E(\mathbb{A}_\mathbb{Q})$ is an open subgroup, so of finite index.

Theorem 1.7 (Stoll)**.** *If* $Ш(E/\mathbb{Q})$ *is finite, then* $\bigcap_n E(\mathbb{A}_\mathbb{Q})^{(n)}$ *is the intersection of all clopen subsets of* $E(\mathbb{A}_\mathbb{Q})$ *containing* $E(\mathbb{Q})$.

1.2 Chabauty's Method

In 1941, Claude Chabauty developed another method of constraining rational points, using p-adic integration on Abelian varieties.

Let $A/\mathbb{Q}_p$ be an abelian variety, $\omega \in \mathrm{H}^0(A, \Omega^1)$ a regular 1-form, and $t_1, \ldots, t_g$ local parameters at the identity $o \in A(\mathbb{Q}_p)$. Working in the complete local ring $\widehat{\mathcal{O}}_{A,o}$, one can write

$$\omega = \sum_{i=1}^{g} f_i \mathrm{d}t_i \text{ with } f_i \in \mathbb{Q}_p[\![t_1, \ldots, t_g]\!].$$

ω above is automatically closed (and translation invariant). Hence,

$$\frac{\partial f_i}{\partial t_j} = \frac{\partial f_j}{\partial t_i},$$

which implies there exists some power series $F_0 \in \mathbb{Q}_p[\![t_1, \ldots, t_g]\!]$, convergent on a neighborhood U of $o \in A(\mathbb{Q}_p)$, with $\mathrm{d}F_0 = \omega$.

Question: Why?

Answer: Every abelian variety is the quotient of a Jacobian. Given A, there's some curve C

Definition 1.8. We define *p-adic integration* of A by setting

$$\int_o^P \omega := F_0(t_1(P), \dots, t_g(P)) - F_0(o)$$

if $P \in U$. In general, we choose nonzero $n \in \mathbb{N}$ such that $nP \in U$ and then set

$$\int_o^P \omega := \frac{1}{n}[F_0(t_1(nP), \dots, t_g(nP)) - F_0(o)]\,.$$

Question: Why does such an n exist?

◇

Properties of this integral

(1) The pairing

$$\begin{array}{ccc} A(\mathbb{Q}_p) \times \mathrm{H}^0(A, \Omega^1) & \longrightarrow & \mathbb{Q}_p \\ (P, \omega) & \longmapsto & \displaystyle\int_o^P \omega \end{array}$$

is bilinear.

(2) For fixed ω, the map

$$\begin{array}{rccc} F_\omega : & A(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p \\ & F & \longmapsto & \displaystyle\int_o^P \omega \end{array}$$

is locally analytic and satisfies $\mathrm{d}F_\omega = \omega$ (as functionals $\operatorname{Lie} A \to \mathbb{Q}_p$?).

One can pull this back to an integration theory on curves.

Setup 1.9. Let $X/\mathbb{Q}_p$ be a curve, and let $J = \mathrm{Jac}(X)$. Note that

$$\mathrm{H}^1(X, \Omega^1) = \mathrm{H}^1(J, \Omega^1).$$

Definition 1.10. For $x, y \in X(\mathbb{Q}_p)$ and $\omega \in \mathrm{H}^0(X, \Omega^1)$, we set

$$\int_x^y \omega := \int_o^{[y]-[x]} \omega.$$

◇

For any fixed ω and $b \in X(\mathbb{Q}_p)$, the map

$$\begin{array}{rccc} F_\omega : & X(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p \\ & x & \longmapsto & \displaystyle\int_b^x \omega \end{array}$$

is a locally analytic antiderivative of ω.

Theorem 1.11 (Chabauty '41)**.** *With notation as above, if* $\operatorname{rank} J(\mathbb{Q}) < g(X)$*, then* $X(\mathbb{Q})$ *is finite.*

Proof. By assumption, the map

$$\begin{array}{rccc} \Phi : & \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1) & \longrightarrow & \mathrm{Hom}(J(\mathbb{Q}), \mathbb{Q}_p) \\ & \omega & \longmapsto & \left(P \mapsto \displaystyle\int_0^P \omega\right) \end{array}$$

has non-trivial kernel (indeed, the domain has dimension $g(X)$ as the codomain has dimension rank $J(\mathbb{Q})$). Choose some nonzero $\omega \in \ker \Phi$ and fix some $b \in X(\mathbb{Q})$ (if no b exists, we're done). The map $F_\omega : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ satisfies

(1) $F_\omega(x) = 0$ if $x \in X(\mathbb{Q})$. Indeed

$$\omega \in \ker \Phi \implies = \int_0^{[x]-[b]} \omega =: \int_b^x \omega.$$

(2) F_ω is locally analytic

(3) F_ω does not vanish uniformly on any disc in $X(\mathbb{Q}_p)$ (because $\mathrm{d}F_\omega = \omega \neq 0$).

(2) + **(3)** above imply that F_ω has only finitely many zeros in $X(\mathbb{Q}_p)$.[2] ■

Remark 1.12. Coleman observed that Chabauty's argument can be used to try to compute $X(\mathbb{Q})$. More precisely, when $\operatorname{rank} J(\mathbb{Q}) < g(X)$, we can often compute a basis of $\ker(\Phi)$ up to any desired p-adic precision, and use this to explicitly compute

$$X(\mathbb{Q}_p)_{\mathrm{Chab}} := \left\{ x \in X(\mathbb{Q}_p) : \int_b^x \omega = 0 \text{ for all } \omega \in \ker \Phi \right\}.$$

Note that this is a finite set containing $X(\mathbb{Q})$. ∘

Theorem 1.13 (Coleman)**.** *Let $X/\mathbb{Q}$ be a curve satisfying* $\operatorname{rank} J(\mathbb{Q}) < g(X)$*. Let $p > 2g$ be a prime of good reduction. Then, $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g-2)$.*

2 Lecture 2 (1/26)

Some class stuff

- There's a mailing list everyone should sign up for.
- There will be completely optional psets (at least in the beginning). Can find on Alex's website.
- Pset 1 will be discussed in office hours
- OHs will be in SC411 on Thursday 3:00pm – 4:15pm

2.1 Stuff that was on the board ahead of time (recap of last time?)

We're interested in determining rational points on varieties (mainly curves in this course) over $\mathbb{Q}$.

Observation 2.1. $X(\mathbb{Q})$ certainly lives in adelic points $X(\mathbb{A}_\mathbb{Q}) = \prod_\ell X(\mathbb{Q}_\ell)$.

[2] By Weierstrass preparation, any convergent power series only vanishes at finitely many zeros in its disc of convergence. Use this and compactness of $X(\mathbb{Q}_p)$.

n-descent Let $E/\mathbb{Q}$ be an elliptic curve. Can form commutative square

$$\begin{array}{ccc} E(\mathbb{Q}) & \longrightarrow & \prod_\ell E(\mathbb{Q}_\ell) \\ \downarrow{\scriptstyle \kappa_n} & & \downarrow{\scriptstyle \prod \kappa_{n,\ell}} \\ \mathrm{H}^1(G_\mathbb{Q}, E[n]) & \longrightarrow & \prod_\ell \mathrm{H}^1(G_\ell, E[n]) \end{array}$$

Can form n-descent set

$$E(\mathbb{A}_\mathbb{Q})^{(n)} = \left\{ (x_\ell) \in \prod E(\mathbb{Q}_\ell) : \exists \xi \in \mathrm{H}^1(G_\mathbb{Q}, E[n]) \text{ s.t. } \xi_v \in \mathrm{im}(\kappa_{n,\ell}) \right\}.$$

Then, $E(\mathbb{Q}) \subset \bigcap_n E(\mathbb{A}_\mathbb{Q})^{(n)} \subset E(\mathbb{A}_\mathbb{Q})$.

Chabauty Say $X/\mathbb{Q}$ a curve and set $J = \mathrm{Jac}(X)$. Get map

$$\Phi : \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) = \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1) \longrightarrow \mathrm{Hom}(J(\mathbb{Q}), \mathbb{Q}_p)$$

given by

$$\Phi : \omega \mapsto \left(P \mapsto \int_0^P \omega \right).$$

Can form `Chabauty set`

$$X(\mathbb{Q}_p)_{\mathrm{Chab}} = \left\{ x \in X(\mathbb{Q}_p) : \int_b^x \omega = 0 \text{ for all } \omega \in \ker(\Phi) \right\}.$$

Then, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_{\mathrm{Chab}} \subset X(\mathbb{Q}_p)$.

2.2 Today's stuff: Chabauty-Coleman as $\mathbb{Q}_p$-linear descent

Goal. Convince ourselves these two approaches are kind of the same.

Let $A/\mathbb{Q}$ be an abelian variety, and let p be a prime.

Definition 2.2. The $\mathbb{Z}_p$`-linear Tate module` of A is

$$T_p(A) := \varprojlim_n A[p^n],$$

where the implicit transition maps in the above system are multiplication by $[p] : A[p^{n+1}] \to A[p^n]$. ◇

Note because we have a system of finite étale group schemes, we can think of T_pA as a $\mathbb{Z}_p$-linear Galois representation w/ underlying module $T_pA \cong \mathbb{Z}_p^{2\dim A}$.

Definition 2.3. The $\mathbb{Q}_p$`-linear Tate module` of A is

$$V_p(A) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_pA,$$

a $2\dim(A)$-dimensional $\mathbb{Q}_p$-linear Galois representation. ◇

The Kummer maps

$$\kappa_{p^n} : A(\mathbb{Q}) \longrightarrow \mathrm{H}^1(G_\mathbb{Q}, A[p^n]),$$

upon taking a limit, induces a map

$$A(\mathbb{Q}) \longrightarrow \mathrm{H}^1(G_{\mathbb{Q}}, T_pA) \longrightarrow \mathrm{H}^1(G_{\mathbb{Q}}, V_pA).$$

We'll denote the composition by $\kappa_1 : A(\mathbb{Q}) \to \mathrm{H}^1(G_{\mathbb{Q}}, V_pA)$, and call it the $\mathbb{Q}_p$-linear Kummer map.

Question 2.4 (Audience)**.** *Is it obvious that* H^1 *commutes with projective limits?*

Answer. That's not obvious. Alex wrote up a careful proof of it a bit ago. Sounds like, at least, showing that the Galois cohomology of the Tate module is the inverse limit of the Galois cohomology of the $A[p^n]$'s is not so hard, but there is something one has to check. ⋆

Also have local $\mathbb{Q}_p$-linear Kummer maps

$$\kappa_{1,\ell} : A(\mathbb{Q}_p) \longrightarrow \mathrm{H}^1(G_\ell, V_pA)$$

via the same construction.

Definition 2.5. The $\mathbb{Q}_p$-linear Selmer group is

$$\mathrm{Sel}_1(A/\mathbb{Q}) = \left\{\xi \in \mathrm{H}^1(G_{\mathbb{Q}}, V_pA) : \xi_\ell \in \mathbb{Q}_p\text{-span of } \mathrm{im}(\kappa_{1,\ell}) \text{ for all } \ell\right\} \qquad \diamond$$

Notation 2.6. Alex has been writing $\mathrm{loc}_\ell(\xi) = \xi|_{G_\ell}$ for what I've been calling ξ_ℓ. Maybe I'll switch to his notation.

Theorem 2.7 (Bloch-Kato)**.**

(1) *If* $\ell \neq p$*, then* $\mathrm{im}(\kappa_{1,\ell}) = 0$*. In fact,* $\mathrm{H}^1(G_\ell, V_pA) = 0$*.*
(Can prove this using the Euler-Poincaré characteristic formula)

(2) *If* $\ell = p$*, the* $\mathbb{Q}_p$*-span of* $\mathrm{im}(\kappa_{1,p})$ *is equal to*

$$\mathrm{H}^1_f(G_p, V_pA) := \ker\left(\mathrm{H}^1(G_p, V_pA) \to \mathrm{H}^1(G_p, B_{cris} \otimes_{\mathbb{Q}_p} V_pA)\right).$$

Above, B_{cris} *is Fontaine's crystalline period ring; we'll talk more about this in a future lecture. Furthermore, one has*

$$\mathrm{H}^1_f(G_p, V_pA) \cong \mathrm{H}^0(A_{\mathbb{Q}_p}, \Omega^1)^\vee$$

and this isomorphism is known as the Bloch-Kato exponential (note RHS is $\mathrm{Lie}\, A_{Q_p}$*). The map*

$$A(\mathbb{Q}_p) \xrightarrow{\kappa_{1,p}} \mathrm{H}^1(G_p, V_pA) \cong \mathrm{H}^0(A_{\mathbb{Q}_p}, \Omega^1)^\vee$$

turns out to exactly be

$$P \longmapsto \left(\omega \mapsto \int_0^P \omega\right).$$

(3) *There is an exact sequence*

$$0 \longrightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}} A(\mathbb{Q}) \xrightarrow{\kappa_1} \mathrm{Sel}_1(A/\mathbb{Q}) \longrightarrow V_p Ш(A/\mathbb{Q}) \longrightarrow 0,$$

where $V_p Ш(A/\mathbb{Q}) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n Ш(A/\mathbb{Q})[p^n]$.

The theorem (in particular, **(1) + (2)**) tells us exactly what the local conditions defining this $\mathbb{Q}_p$-linear Selmer group look like.

Conjecture 2.8. *$V_p Ш(A/\mathbb{Q}) = 0$ always. Note this would be implied by $\#Ш(A/\mathbb{Q})[p^\infty] < \infty$.*

Let's use this stuff to say something about rational points on curves. Let $X/\mathbb{Q}$ be a curve, and fix a rational basepoint $b \in X(\mathbb{Q})$. Let $J = \mathrm{Jac}(X)$. Let $\mathrm{AJ} : X(\mathbb{Q}) \to J(\mathbb{Q})$ denote the Abel-Jacobi map.

Notation 2.9. Write $\mathrm{Sel}_1(X/\mathbb{Q}) := \mathrm{Sel}_1(J/\mathbb{Q})$ and let j_1 be the composition

$$j_1 : X(\mathbb{Q}) \xrightarrow{\mathrm{AJ}} J(\mathbb{Q}) \xrightarrow{\kappa_1} \mathrm{Sel}_1(X/\mathbb{Q}).$$

Similarly denote

$$j_{1,p} : X(\mathbb{Q}_p) \longrightarrow \mathrm{H}^1_f(G_p, V_p J).$$

With these in mind, we get a $\mathbb{Q}_p$-linear descent square

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ {\scriptstyle j_1}\downarrow & & \downarrow{\scriptstyle j_{1,p}} \\ \mathrm{Sel}_1(X/\mathbb{Q}) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, V_p J). \end{array}$$

We can use this to define an obstruction set

$$X(\mathbb{Q}_p)_1 := \{x \in X(\mathbb{Q}_p) : j_{1,p}(x) \in \mathrm{im}(\mathrm{loc}_p)\}.$$

Note that

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_1 \subset X(\mathbb{Q}_p).$$

Note that the definition of $X(\mathbb{Q}_p)_1$ is reminiscent of n-descent of elliptic curves. Be warned that we haven't actually just defined a new descent set; this $X(\mathbb{Q}_p)_1$ is in fact the Chabauty set by another name.

Theorem 2.10.

$$X(\mathbb{Q}_p)_{Chab} \subset X(\mathbb{Q}_p)_1$$

with equality if $Ш(J/\mathbb{Q})[p^\infty]$ is finite (as conjectured).

Slogan. Chabauty's method is $\mathbb{Q}_p$-linear descent.

Proof. We first slightly recast our definition of $X(\mathbb{Q}_p)_1$. Write Φ' for the composition

$$\Phi' : \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1) \simeq \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1) \cong \mathrm{H}^1_f(G_p, V_p J)^\vee \xrightarrow{\mathrm{loc}_p^\vee} \mathrm{Sel}_1(J/\mathbb{Q})^\vee.$$

If you unwind definitions (and appeal to Theorem 2.7), then you will see that

$$X(\mathbb{Q}_p)_1 = \left\{ x \in X(\mathbb{Q}_p) : \int_b^x \omega = 0 \text{ for all } \omega \in \ker(\Phi') \right\}.$$

The composition

$$\mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1) \xrightarrow{\Phi'} \mathrm{Sel}_1(J/\mathbb{Q})^\vee \xrightarrow{\kappa_1^\vee} \mathrm{Hom}(J(\mathbb{Q}), \mathbb{Q}_p)$$

is simply the map Φ defined in the context of Chabauty (i.e. $\Phi(\omega)(P) = \int_0^P \omega$). Thus, $\ker(\Phi') \subset \ker(\Phi)$ and so $X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q}_p)_{\mathrm{Chab}}$. If $Ш(J/\mathbb{Q})[p^\infty]$ is finite, then κ_1 (and so also $\kappa_1^\vee$) is an isomorphism, so we would get an equality between these two sets. ∎

We can now say a bit about what we're after in this course.

2.3 Sketch of non-abelian Chabauty

Slogan. Non-abelian Chabauty is a descent obstruction which is simultaneously $\mathbb{Q}_p$-linear, but also non-abelian.

It starts with the following observation of Minhyong (spelling?) Kim.

Observation 2.11 (Kim). Classical Chabauty-Coleman has the $\mathbb{Q}_p$-linear Tate module of the Jacobian as its star player. One way to describe this is to say that

$$V_pJ = \mathrm{H}_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) := \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^\vee.$$

In topology, one has $\mathrm{H}_1 = \pi_1^{\mathrm{ab}}$. These led Kim to ask, "Is there a non-abelian lift of Chabauty's method where we replace V_pJ with some larger part of $\pi_1^{\text{ét}}$?"

Spoiler: the answer is yes.

Take $X/\mathbb{Q}$ a curve, and let p be a prime of good reduction. Assume we're given a rational basepoint $b \in X(\mathbb{Q})$. The main player in non-abelian Chabauty is

$$U_n := \text{"}n\text{-step } \mathbb{Q}_p\text{-unipotent étale fundamental group of } (X_{\overline{\mathbb{Q}}}, b)\text{"}$$

(We'll define this rigorously later in the course).

Remark 2.12. $U_1 = V_pJ$. ∘

Using these U_n and some non-abelian cohomology, we'll end up defining "Selmer schemes"

$$\mathrm{Sel}_n(X/\mathbb{Q}) \text{ and } \mathrm{H}^1_f(G_p, U_n)$$

(the first is "global" and the second "local"). These are affine $\mathbb{Q}_p$-schemes of finite type. Think of them as affine varieties over $\mathbb{Q}_p$.[3] There will also be an algebraic localization map

$$\mathrm{loc}_p : \mathrm{Sel}_n(X/\mathbb{Q}) \longrightarrow \mathrm{H}^1_f(G_p, U_n)$$

(morphisms of $\mathbb{Q}_p$-schemes). We will also need the unipotent Kummer maps

$$\begin{aligned} j_n &\colon X(\mathbb{Q}) \longrightarrow \mathrm{Sel}_n(X/\mathbb{Q})(\mathbb{Q}_p) \\ j_{n,p} &\colon X(\mathbb{Q}_p) \longrightarrow \mathrm{H}^1_f(G_p, U_n)(\mathbb{Q}_p). \end{aligned}$$

This will give rise to a unipotent descent square

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ {\scriptstyle j_n}\downarrow & & \downarrow{\scriptstyle j_{n,p}} \\ \mathrm{Sel}_n(X/\mathbb{Q}) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, U_n) \end{array}$$

We can therefore define the *n*th non-abelian Chabauty locus

$$X(\mathbb{Q}_p)_n := \{x \in X(\mathbb{Q}_p) : j_{n,p}(x) \in \mathrm{im}(\mathrm{loc}_p)\}$$

[3] Strictly speaking, it is unknown whether or not $\mathrm{Sel}_n(X/\mathbb{Q})$ is reduced. I guess we want varieties to be reduced in this class.

(Above im="scheme-theoretic image"). One gets inclusions

$$X(\mathbb{Q}) \subset \cdots \subset X(\mathbb{Q}_p)_n \subset \cdots \subset X(\mathbb{Q}_p)_2 \subset X(\mathbb{Q}_p)_1 \subset X(\mathbb{Q}_p).$$

Remark 2.13. For all n, $X(\mathbb{Q}_p)_n = X(\mathbb{Q}_p)$ or is finite. In particular, $X(\mathbb{Q}_p)_n$ is always closed. ∘

Theorem 2.14 (Kim)**.** *If* $\dim_{\mathbb{Q}_p} \mathrm{Sel}_n(X/\mathbb{Q}) < \dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_p, U_n)$ *(*$\star_n$*), then* $X(\mathbb{Q}_p)_n$ *is finite (*$\implies$ $X(\mathbb{Q})$ *is finite).*

(The case $n = 1$ is basically the same statement as classical Chabauty)

Remark 2.15 (response to audience question). With this dimension assumption, the map $\mathrm{loc}_p : \mathrm{Sel}_n(X/\mathbb{Q}) \to \mathrm{H}^1_f(G_p, U_n)$ must be non-dominant, so some elements of the affine coordinate ring of the codomain cut out the image. These pullback to $\mathbb{Q}_p$-analytic functions cutting out $X(\mathbb{Q}_p)_n$. This is how you prove finiteness. If this localization map is dominant, then $X(\mathbb{Q}_p)_n$ will be all of $X(\mathbb{Q}_p)$. ∘

Remark 2.16.

(1) Bloch-Kato Conjecture or Fontaine-Mazur Conjecture would imply that $(\star_n)$ holds for all $n \gg 0$ if $g(X) \geq 2$.

(This would give a new proof of Mordell)

(2) Kim conjectured that $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$ if $g(X) \geq 2$.

(3) Non-abelian Chabauty can often be made explicit, especially for small n. ∘

Warning 2.17 (Responses to audience questions)**.**

- Sounds like the non-abelian story gets much more complicated over number fields. The issue is that you get $\mathbb{Q}_p$-analytic functions cutting out some set of K_v-points.
- Elliptic curves have abelian fundamental groups, so $U_n = U_1$, so **(2)** in the previous remark should fail even for rank 0 curves of genus 1. •

Let's see a couple example applications of this stuff.

Example 2.18.

Theorem 2.19 (Balakrishnan-Dogra-Müller-Tuitmin-Vonk)**.** *Suppose* $E/\mathbb{Q}$ *is an elliptic curve with* $E[13](\overline{\mathbb{Q}}) \simeq \mathbb{F}_{13}^2$ *in such a way that the image of*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(E[13]) \simeq \mathrm{GL}_2(\mathbb{F}_{13})$$

is contained in the subgroup

$$\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}.$$

Then, there are 6 possibilites for E*, all with CM.*

They proved this by using quadratic ($n = 2$) Chabauty to compute the rational points of the "cursed curve" $X_s(13)$. △

Example 2.20.

Theorem 2.21 (Evertse, B.). *Let $\mathcal{X} := \mathbb{P}^1_{\mathbb{Z}} \setminus \{0, 1, \infty\}$. Then, for all $s \geq 0$, there exists a bound $B(s)$ s.t.*

$$\#\mathcal{X}(\mathbb{Z}_S) \leq B(s)$$

for all finite sets S of primes w/ $\#S = s$.

That is, one can obtain a uniform bound on the number of solutions to the S-unit equation $x + y = 1$ (with $x, y \in \mathbb{Z}_S^\times$). If I heard correctly, sounds like this was first done (by Evertse?) using analytic techniques before Alex gave a new proof using Chabauty-Coleman-Kim. △

3 Lecture 3 (1/31): The profinite étale fundamental groupoid

Course stuff

- Lectures will start being recorded.
- Discuss problems from pset1 on Thursday.

Today is the proper start of the course. Our first topic is the *pro-unipotent étale fundamental groupoid*. We'll begin with the more familiar profinite étale fundamental groupoid.

History. Story begins with Grothendieck in the 1960's. When developing the foundations of scheme theory, Grothendieck was interested in using tools from algebraic topology to study schemes. For example, can one make sense of a sort of "singular homology for schemes"? This line of thinking led to, among other things, étale cohomology and étale fundamental groupoids. These are analogues of singular cohomology and topological fundamental groupoids. ⊖

3.1 Fundamental Groupoids in Topology

Let X be a nice topological space. By 'nice' here, we mean locally path-connected and semilocally simply connected. For example, X could be a manifold.

Definition 3.1. Choose $x, y \in X$. We set

$$\pi_1(X; x, y) = \{\text{continuous paths } \gamma : x \rightsquigarrow y \text{ in } X\} / \text{homotopy relative to endpoints.} \qquad \diamond$$

(Alex drew a picture of three paths on a genus 2 orientable surface, two of which were homotopic)
Let's write down some properties of these path sets.

- Given $x, y, z \in X$, there is a composition map

  $$\pi_1(X; y, z) \times \pi_1(X; x, y) \longrightarrow \pi_1(X; x, z)$$

  which we'll write as $(\gamma_2, \gamma_1) \mapsto \gamma_2\gamma_1$ (this is "do γ_1 and then do γ_2").

  Warning 3.2. Topologists often like to write composition in the other order, e.g. they'd write "do γ_1 then γ_2" as $\gamma_1\gamma_2$. •

- For any $x \in X$, there is an identiy path $1_x \in \pi_1(X; x, x)$ which "does nothing"
- For $\gamma \in \pi_1(X; x, y)$, there is always an inverse path $\gamma^{-1} \in \pi_1(X; y, x)$ which "traces γ in reverse."

If you squint at these properties, they look kind of like a spread out version of a group law. We make this precise by introducing the notion of groupoids.

Definition 3.3. A groupoid Π consists of the following data

- A "vertex set" V.
- For every $x, y \in V$, a "path set" $\Pi(x, y)$.
- For all $x, y, z \in V$, a composition map

$$\Pi(y, z) \times \Pi(x, y) \longrightarrow \Pi(x, z).$$

  We'll denote this as $(\gamma_2, \gamma_1) \mapsto \gamma_2\gamma_1$.
- For all $x \in V$, an identity $1_x \in \Pi(x, x)$.
- For all $x, y \in V$, an inverse map $\Pi(x, y) \to \Pi(y, x)$. We'll denote this as $\gamma \mapsto \gamma^{-1}$.

This data is required to satisfy all of the following

- (associativity)
$$\gamma_3(\gamma_2\gamma_1) = (\gamma_3\gamma_2)\gamma_1$$
  whenever either (and so both) side is defined.
- (identity) If $\gamma \in \Pi(x, y)$, then
$$1_y \cdot \gamma = \gamma = \gamma \cdot 1_x.$$
- (inverses)
$$\gamma^{-1}\gamma = 1_x \text{ and } \gamma\gamma^{-1} = 1_y$$ ◇

(Equivalently, a groupoid is a category where every morphism is an isomorphism)

Remark 3.4.

(1) If $V = \{*\}$ is a singleton, then $\Pi(*, *)$ is a group. More generally, for any $x \in V$,

$$\Pi(x) := \Pi(x, x)$$

is a group.

(2) For $x, y \in V$, then either $\Pi(x, y) = \emptyset$ or $\Pi(x, y)$ carries a simply transitive action of $\Pi(x)$ on the right and a simply transitive action of $\Pi(y)$ on the left. These are both given by the composition law. In other words, $\Pi(x, y)$ is a $(\Pi(y), \Pi(x))$-bitorsor when it is nonempty. Because of this a nonempty path set $\Pi(x, y)$ is also called a path torsor.

(3) If $\Pi(x, y) \neq \emptyset$, then $\Pi(x)$ and $\Pi(y)$ are (abstractly) isomorphic as groups. Indeed, after choosing any $\gamma_0 \in \Pi(x, y)$, one gets an isomorphism $\Pi(x) \xrightarrow{\sim} \Pi(y)$ via $\gamma \mapsto \gamma_0\gamma\gamma_0^{-1}$.

Warning 3.5. We don't want to pretend that these are equal (essentially because there's no canonical isomorphism between them). •

(4) For X a nice topological space, the sets $\pi_1(X; x, y)$ form a groupoid whose vertex set is $V = X$. This is called the fundamental groupoid $\pi_1(X)$ of X. ◦

We would like a "fundamental groupoid" in the world of schemes. It is non-obvious how to get this. What would one mean by a continuous path on a scheme? Instead of trying to answer this, one sidesteps this issue via the theory of covering spaces.

3.2 Covering Spaces

Continue to let X denote a nice topological space.

Definition 3.6. A `covering space` of X is a continuous map $p : X' \to X$ which is locally on X isomorphic to the projection $X \times (\text{discrete set}) \to X$. ◇

Example 3.7. $\mathbb{C}^\times \to \mathbb{C}^\times, z \mapsto z^2$. △

Example 3.8. $\mathbb{C} \to \mathbb{C}^\times, z \mapsto \exp(z)$. △

Fact (Homotopy lifting property)**.** Given a covering space $p : X' \to X$, a path $\gamma : x \rightsquigarrow y$ in X, and a lift $x' \in X'_x$ of x, there exists a unique lift γ' of γ to a path $\gamma' : x' \rightsquigarrow y'$ for some $y' \in X'_y$.

This fact gives a `monodromy action`

$$\begin{array}{ccc} \pi_1(X; x, y) \times X'_x & \longrightarrow & X'_y \\ (\gamma, x') & \longmapsto & y' =: \gamma \cdot x'. \end{array}$$

These actions are natural in the covering X'.

Definition 3.9. A `morphism of covering spaces` $(X' \xrightarrow{p} X) \to (X'' \xrightarrow{q} X)$ is a continuous map $f : X' \to X''$ making

$$\begin{array}{ccc} X' & \xrightarrow{\quad f \quad} & X'' \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle q} & \\ & X & \end{array}$$

commute. We write $\mathrm{Cov}(X)$ for the category of covering spaces. ◇

If $x \in X$, the assignment $(p : X' \to X) \mapsto X'_x$ is functorial, i.e. gives a `fiber functor`

$$\omega_x : \mathrm{Cov}(X) \to \mathrm{Set}.$$

Naturality of the monodromy actions means we have an action map

$$\pi_1(X; x, y) \longrightarrow \mathrm{Isom}(\omega_x, \omega_y) \tag{3.1}$$

(the RHS above is the set of natural isomorphisms from ω_x to ω_y). This map sends a path $\gamma : x \rightsquigarrow y$ to the natural transformation $\gamma : \omega_x \to \omega_y$ with

$$\begin{array}{rccc} \gamma_{X'} : & X'_x & \longrightarrow & X'_y \\ & x' & \longmapsto & \gamma \cdot x'. \end{array}$$

Theorem 3.10. *The map (3.1) is bijective. In fact, it is also compatible with composition, identities, and inverses.*[4]

[4] i.e. one has an equivalence of groupoids

Fact (Existence of universal coverings)**.** For X as above and $x \in X$, there is a covering space $\widetilde{p} : \widetilde{X} \to X$ with $\widetilde{X}$ simply connected and $x \in \mathrm{im}(\widetilde{p})$. This is called a `universal cover`. If one choose $\widetilde{x} \in \widetilde{X}_x$, then for any covering space $p : X' \to X$ and any $x' \in X'_x$, there exists a unique morphism $f : \widetilde{X} \to X'$ of covering spaces such that $f(\widetilde{x}) = x'$.

Slogan. $(\widetilde{X}, \widetilde{x})$ represents the fiber functor ω_x.

Proof of Theorem 3.10. We will prove something stronger. We will in fact prove that the map

$$\pi_1(X; x, y) \longrightarrow \mathrm{Hom}(\omega_x, \omega_y)$$

is bijective (RHS above is the set of natural transformations from ω_x to ω_y). This proves the theorem and that any natural transformation between these fiber functors is an isomorphism.

To prove this, pick a universal cover $(\widetilde{X}, \widetilde{x})$ and consider the composition

$$\pi_1(X; x, y) \longrightarrow \mathrm{Hom}(\omega_x, \omega_y) \cong \widetilde{X}_y$$

(the isomorphism at the end is Yoneda). This composition is given by $\gamma \mapsto \gamma \cdot \widetilde{x}$. We only need to show that this is bijective. For any $\widetilde{y} \in \widetilde{X}_y$, there is (up to homotopy) a unique path $\widetilde{\gamma} : \widetilde{x} \to \widetilde{y}$ in $\widetilde{X}$ (since $\widetilde{X}$ simply connected); the image $\gamma \in \pi_1(X; x, y)$ of this path is the unique element with $\gamma \cdot \widetilde{x} = \widetilde{y}$. ■

3.3 The profinite étale fundamental groupoid

We have just seen that in the world of topology, $\pi_1(X; x, y) \simeq \mathrm{Isom}(\omega_x, \omega_y)$. Hence, one could use this to define the fundamental groupoid $\pi_1(X)$. Note that this definition no longer uses paths. One only needs a suitable notion of "covering spaces" and "fibers of covering spaces."

Goal. Our aim (to be completed next time) is to define "covering spaces of schemes" as well as suitable "fiber functors" associated to points. We'll use these to define π_1 of a scheme.

What sorts of covering spaces do we want to consider?

Let X be a scheme. A `finite étale covering` of X is a finite, étale morphism of schemes $p : X' \to X$.

Example 3.11. Let k be a field w/ $\mathrm{char}\, k \neq 2$. Then,

$$\begin{array}{ccc} \mathbb{G}_{m,k} & \longrightarrow & \mathbb{G}_{m,k} \\ z & \longmapsto & z^2 \end{array}$$

is finite étale. △

Theorem 3.12 (`Riemann Existence Theorem`)**.** *Let X be a f.type $\mathbb{C}$-scheme. If $p : X' \to X$ is finite étale, then $p : X'(\mathbb{C}) \longrightarrow X(\mathbb{C})$ is a covering space w/ finite fibers for the analytic topologies. This in fact gives an equivalence of categories $F\acute{E}t(X) \simeq \mathrm{Cov}(X(\mathbb{C}))_{fin}$.*

Remark 3.13. The covering space $\exp : \mathbb{C} \to \mathbb{C}^\times$ has infinite discrete fibers, so this is not algebraic. ○

We still need to say want we mean by fibers, which requires being careful about what we mean by 'point'.

Definition 3.14. A `geometric point` of X is a point $x \in X(\Omega)$ for some separably closed field Ω. ◇

If $p : X' \to X$ is a finite étale covering and x is a geometric point of X ($x \in X(\Omega)$), then we define

$$X'_x := \{x' \in X'(\Omega) : p(x') = x\}.$$

Note that X'_x is a finite set, of cardinality equal to the degree of the cover p. This construction defines a fibre functor

$$\begin{array}{rccc} \omega_x^{\text{ét}} : & \text{FÉt}(X) & \longrightarrow & \text{FinSet} \\ & (X' \xrightarrow{p} X) & \longmapsto & X'_x. \end{array}$$

Definition 3.15. Let X be a scheme and let x, y be geometric points. We define

$$\pi_1^{\text{ét}}(X; x, y) := \text{Isom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}}) = \text{Hom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}})$$

(it's a fact that any natural transformation between these is an isomorphism). These sets form a groupoid, called the profinite étale fundamental groupoid of X, with respect to composition of natural isomorphisms. This groupoid is denoted $\pi_1(X)$. ◇

4 Lecture 4 (2/2): The profinite étale fundamental groupoid, continued

Last time

- For X a scheme, can consider category FÉt(X) of finite, étale covers $X' \to X$
- If x is a geometric point, get a fiber functor

  $$\omega_x^{\text{ét}} : \text{FÉt}(X) \to \text{FinSet}.$$

  via $(X' \to X) \mapsto X'_x$ (really, the set of Ω-valued points of X'_x, where $x \in X(\Omega)$).
- $\pi_1^{\text{ét}}(X; x, y) := \text{Isom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}}) = \text{Hom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}})$

We've been calling this thing the *profinite* étale fundamental groupoid. This indicates that there should be a topology on this thing.

4.1 Topology on the étale fundamental groupoid

Fact. $\pi_1^{\text{ét}}(X; x, y)$ has a natural profinite topology.

If you want, profinite means compact, Hausdorff, and totally disconnected.
How does one construct this topology? Here are two definitions

(1) If $X' \to X$ is a finite, étale covering and $\gamma_0 : X'_x \xrightarrow{\sim} X'_y$ is a bijection, consider the set

$$U_{\gamma_0} := \left\{\gamma \in \text{Isom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}}) : \gamma_{X'} = \gamma_0\right\} \subset \pi_1^{\text{ét}}(X; x, y).$$

We give $\pi_1^{\text{ét}}(X; x, y)$ the topology generated by the U_{γ_0}'s (for all $X' \to X$, all γ_0).

(2) Consider the maps

$$F, G : \prod_{X' \in \text{FÉt}(X)} \text{Hom}(X'_x, X'_y) \rightrightarrows \prod_{f : X'' \to X'} \text{Hom}(X''_x, X'_y)$$

(right product over morphisms in $\mathrm{F\acute{E}t}(X)$ with target X') given by

$$F : \left(\gamma_{X'} : X'_x \to X'_y\right)_{X'} \longmapsto \left(X''_x \xrightarrow{\gamma_{X''}} X''_y \xrightarrow{f_y} X'_y\right)_f$$

and

$$G : \left(\gamma_{X'} : X'_x \to X'_y\right)_{X'} \longmapsto \left(X''_x \xrightarrow{f_x} X'_x \xrightarrow{\gamma_{X'}} X'_y\right)_f .$$

It may help to keep in mind the diagram

$$\begin{array}{ccc} X''_x & \xrightarrow{f_x} & X'_x \\ \downarrow{\scriptstyle \gamma_{X''}} & & \downarrow{\scriptstyle \gamma_{X'}} \\ X''_y & \xrightarrow{f_y} & X'_y \end{array}$$

which commutes when the $\gamma_{X'}$'s form a natural transformation. That is, note that

$$\mathrm{Hom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}}) \simeq \mathrm{Eq}(F, G)$$

The give $\mathrm{Hom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}})$ the subspace topology of the product topology on $\prod_{X'} \mathrm{Hom}(X'_x, X'_y)$ (where each factor is given the discrete topology). Note that $\mathrm{Hom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}})$ is a closed subspace (equalizer of continuous maps between two profinite spaces) of a profinite space, and so itself profinite.

The first definition is more concrete, but e.g. makes it harder to see why the topology is compact.

Proposition 4.1. *The topology on $\pi_1^{\acute{e}t}(X; x, y)$ is profinite, and the composition maps*

$$\pi_1^{\acute{e}t}(X; y, z) \times \pi_1^{\acute{e}t}(X; x, y) \longrightarrow \pi_1^{\acute{e}t}(X; x, z)$$

are continuous, as are the inversion maps $\pi_1^{\acute{e}t}(X; x, y) \to \pi_1^{\acute{e}t}(X; y, x)$.

(I guess this is saying we have a groupoid object in the category of profinite sets). In particular, $\pi_1^{\text{ét}}(X; x)$ is always a profinite group.

Example 4.2. Say $X = \operatorname{Spec} k$ for k a field. A geometric point of X is a field embedding $x : k \hookrightarrow \Omega$ with Ω separable closed. Furthermore, $\mathrm{F\acute{E}t}(X)$ is equivalent to $\{\text{finite étale } k\text{-algebras}\}^{\mathrm{op}}$ (these are finite products of finite, separable field extensions). The fiber functor is given by

$$\omega_x^{\text{ét}}(\operatorname{Spec} L) = \mathrm{Hom}_{k\text{-Alg}}(L, \Omega) = \mathrm{Hom}_{k\text{-Alg}}(L, k^s),$$

where k^s is the separable closure of k in Ω. In this case, one gets

$$\pi_1^{\text{ét}}(X; x) \simeq \mathrm{Gal}(k^s/k)$$

as profinite groups (give RHS the Krull topology). Given $\sigma \in \mathrm{Gal}(k^s/k)$, it acts in a natural way on $\omega_x^{\text{ét}}(\operatorname{Spec} L) = \mathrm{Hom}(L, k^s)$ and this gives a natural isomorphism $\sigma : \omega_x^{\text{ét}} \xrightarrow{\sim} \omega_x^{\text{ét}}$. The inverse map is "evaluation at k^s"[5]. △

[5] not literally because k^s isn't finite étale over k, but every element of k^s belongs to a finite étale cover of k, so this isn't actually an issue.

Definition 4.3. If Π is a group, its `profinite completion` is

$$\widehat{\Pi} := \varprojlim_N (\Pi/N)$$

with limit taken over finite index normal subgroups. ◇

Example 4.4. $\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$. △

One can also profinitely complete groupoids.

Definition 4.5. If Π is a groupoid, its `profinite completion` $\widehat{\Pi}$ is the groupoid on the same vertex set with path sets

$$\widehat{\Pi}(x,y) = \varprojlim_{N_x} (\Pi(x,y)/N_x) = \varprojlim_{N_y} (N_y \backslash \Pi(x,y)),$$

where N_x (resp. N_y) ranges over finite index normal subgroups of $\Pi(x)$ (resp. $\Pi(y)$). ◇

Exercise. Check above is well-defined and has a natural groupoid structure (e.g. define composition laws).

Theorem 4.6. *Suppose X is a f.type $\mathbb{C}$-scheme. Then, there is a canonical isomorphism*

$$\pi_1^{\acute{e}t}(X; x, y) \simeq \widehat{\pi}_1(X(\mathbb{C}); x, y)$$

for any $x, y \in X(\mathbb{C})$ (compatible with composition, identities, inverses, yadda yadda).

Remark 4.7.

(1) This is a consequence (slash rephrasing) of `Riemaann existence`.

(2) If K'/K is an extension of algebraically closed fields *of characteristic* 0, X/K is a finite type (separated?) K-scheme, and x, y are geometric points on $X_{K'}$, then the map

$$\pi_1^{\text{ét}}(X_{K'}; x, y) \longrightarrow \pi_1^{\text{ét}}(X; x, y)$$

is an isomorphism.

(3) If X is finite type (+ separated?) over $K = \overline{K}$ of characteristic 0, then $\pi_1^{\text{ét}}(X; x)$ is topologically finitely generated (i.e. there exists a finite subset generated a dense subgroup).

Proof Sketch. By **(2)**, it suffices to prove this for $K = \mathbb{C}$. Then, this follows from Theorem 4.6 since the analytic space of a f.type $\mathbb{C}$-scheme is homotopy equivalence to a finite CW complex. ■

○

Question 4.8 (Audience)**.** *What happens in char p?*

Answer. In char p, for smooth, projective varieties, everything is fine. Get f.generated fundamental groups which are invariant over passing to algebraically closed field. If you remove projective (maybe, really proper) things go bad. For example $\mathbb{A}^1_{\overline{\mathbb{F}}_p}$ does not have a f.generated fundamental group, and it changes if you change the algebraically closed field (both of theses come from looking at Artin-Schreier covers). ⋆

4.2 Universal coverings

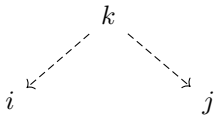
Let's start with a problem. The category $\mathrm{F\acute{E}t}(X)$ is "too small" to contain any kind of "universal" covering.

Example 4.9. The "universal cover" of $\operatorname{Spec} k$ should be $\operatorname{Spec} k^s$, but this is usually not finite over $\operatorname{Spec} k$. △

The solution is to enlarge $\mathrm{F\acute{E}t}(X)$ in some formal way. The proper way to do this is to introduce pro-categories[6]

Definition 4.10. A small category I is `cofiltered` if $I \neq \emptyset$ and

(1) For all $i, j \in I$, there exists some $k \in I$ along with morphisms $k \to i$ and $k \to j$.



(2) For all pairs of arrows $f, g : j \rightrightarrows i$ between the same objects in I, there exists an arrow $h : k \to j$ in I such that $f \circ h = g \circ h$.

$$k \dashrightarrow j \rightrightarrows i$$

◇

Definition 4.11. A `cofiltered diagram` in a category $\mathcal{C}$ is a diagram indexted by a cofiltered category, i.e. a functor $I \to \mathcal{C}$. ◇

Definition 4.12. A `cofiltered limit` in $\mathcal{C}$ is a (categorical) limit of a cofiltered diagram. ◇

Example 4.13. The category $I = \mathbb{N}$ with "arrows pointing downwards" is cofiltered. By this, we mean there's an arrow $j \to i$ when $j \geq i$. An I-shaped diagram in a category $\mathcal{C}$ simply looks like

$$\ldots \longrightarrow X_3 \longrightarrow X_2 \longrightarrow X_1.$$

Hence, any diagram of the above shape is cofiltered, and the limit of such a thing is a cofiltered limit. △

The `pro-category` pro–$\mathcal{C}$ of a locally small category $\mathcal{C}$ is what you get by formally adjoining all cofiltered limits in $\mathcal{C}$.

Definition 4.14. A `pro-object` in $\mathcal{C}$ is the same thing as a cofiltered diagram in $\mathcal{C}$. Depending on how we feel, we may denote such a thing as $(X_i)_{i \in I}$ or "$\varprojlim_{i \in I}$" X_i (keep the morphisms implicit in either case). ◇

Note 2. Personally, I kinda prefer $\varprojlim_{i \in I} X_i$ without the quotation marks, so I might use this at times.

Definition 4.15. `Morphisms in pro--`$\mathcal{C}$ are given by

$$\operatorname{Hom}\left(\text{“}\varprojlim_{i \in I}\text{”} X_i, \text{“}\varprojlim_{j \in J}\text{”} Y_j \right) := \varprojlim_{j \in J} \varinjlim_{i \in I} \operatorname{Hom}(X_i, Y_j).$$

The composition law is the "obvious one" once one unpacks what the above definition means. ◇

[6] $\mathrm{F\acute{E}t}(X)$ is an amateur.

Here are some properties of this construction

(1) $\mathcal{C}$ is a full subcategory of pro–$\mathcal{C}$

(View every object of $\mathcal{C}$ as a one-object diagram)

(2) pro–$\mathcal{C}$ has (all) cofiltered limits.

(If $\mathcal{C}$ had (all) finite limits, then pro–$\mathcal{C}$ has all (small) limits)

Warning 4.16. limits in $\mathcal{C}$ (when they exist) need not coincide with limits in pro–$\mathcal{C}$. •

Definition 4.17. Let $\mathcal{C}$ be a locally small category. A functor $F : \mathcal{C} \to \text{Set}$ is called `pro-representable` just when any of the following equivalent characterizations hold

(1) F is a filtered colimit[7] of representable functors.

(2) Note that F extends naturally to pro–$\mathcal{C}$ via

$$F\left(\text{“}\varprojlim_{i\in I}\text{”}\, X_i\right) = \varprojlim_{i\in I} F(X_i).$$

(1) is equivalent to asking that this extension be representable.

Remark 4.18. Note F preserves cofiltered limits in pro–$\mathcal{C}$ (by construction) even if it doesn't do so in $\mathcal{C}$. ◦

(3) There is a cofiltered diagram $(X_i)_{i\in I}$ in $\mathcal{C}$ and a compatible system of elements $x_i \in F(X_i)$ satisfying the following universal property: for any $Y \in \mathcal{C}$ and $y \in F(Y)$, there exists some $i \in I$ and some morphism $f_i : X_i \to Y$ in $\mathcal{C}$ such that $f_i(x_i) = y$. Moreover, this is unique "up to equivalence". ⋄

4.3 Back to scheme theory

Theorem 4.19. *Let X be a scheme, and let x be a geometric point. Then, $\omega_x^{\acute{e}t} : F\acute{E}t(X) \to \text{FinSet}$ is pro-representable.*

We call a pro-representing pro-object $(\widetilde{X}, \widetilde{x})$ – i.e. $\widetilde{X} \in \text{pro–F\'Et}(X)$ and $\widetilde{x} \in \widetilde{X}_x$ – a `universal covering` of X (at x).

Proof idea. For $\mathcal{C}$ an essentially small category w/ finite limits, a functor $F : \mathcal{C} \to \text{Set}$ is pro-representable iff F preserves finite limits. ■

Remember: There's a formal criterion for recognizing when a functor is pro-representable

Corollary 4.20. *Suppose that X is connected. Then, $\pi_1^{\acute{e}t}(X)$ is `connected`, i.e. $\pi_1^{\acute{e}t}(X; x, y) \neq \emptyset$ for any geometric points x, y.*

Proof. Let $(\widetilde{X}, \widetilde{x})$ be a universal covering at x. Write $\widetilde{X} = \text{“}\varprojlim_{i\in I}\text{”}\, \widetilde{X}_i$ for $\widetilde{X}_i \in \text{F\'Et}(X)$. Then,

$$\pi_1^{\text{ét}}(X; x, y) = \text{Hom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}}) \overset{\text{Yoneda}}{\cong} \widetilde{X}_y := \varprojlim_{i\in I} \widetilde{X}_{i,y}.$$

For all i, we know $\widetilde{X}_i \neq \emptyset$ simply because $\widetilde{X}_{i,x} \neq \emptyset$ (since $\widetilde{X}_x \neq \emptyset$). The map $\widetilde{X}_i \to X$ if finite, étale so open ($\Longleftarrow$ étale) and closed ($\Longleftarrow$ finite). As X is connected, this map must be surjective, so $\widetilde{X}_{i,y} \neq \emptyset$. Therefore, $\pi_1^{\text{ét}}(X; x, y)$ is an inverse limit of finite, nonempty sets. We know appeal to the following.

[7] Dual notation to cofiltered limit

Fact. Any cofiltered limit of non-empty finite sets is non-empty

(Can prove this e.g. using Mittag-Leffler). Hence, $\pi_1^{\text{ét}}(X; x, y) \neq \emptyset$. ■

Let's end by mentioning the Galois correspondence.

Theorem 4.21. *If X is connected and we fix a geometric point x, then $F\acute{E}t(X)$ is equivalent to the category*

$$\pi_1^{\acute{e}t}(X; x)\text{-}FinSet := \left\{\text{finite sets w/ cts } \pi_1^{\acute{e}t}(X; x) \text{ action}\right\}.$$

We won't really use this. We'll mainly stick w/ the direction of starting w/ a category of coverings and then obtaining a notion of fundamental groups.

5 Lecture 5,6 (2/{7, 9}) – Didn't go (See Lecture notes on (pro-)unipotent groups)

Note 3. These notes were added after the fact, based on Alex's lecture notes

The profinite étale fundamental group of a scheme X is great, but hard to study.

Example 5.1. Say $X = \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}$. Then, $\pi_1^{\text{ét}}(X; x) \simeq \widehat{F}_2$ is the profinite free group on 2 generators. It also has a natural action of $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. However, it is not known what this action is in any explicit sense (though sounds like some things are known about it). △

One way of phrasing the issue is to say that $\Pi = \pi_1^{\text{ét}}(X; x)$ to very non-abelian. Let $\Gamma^\bullet\Pi$ denote the descending central series of Π defined by $\Gamma^1\Pi = \Pi$, $\Gamma^2\Pi = \overline{[\Pi, \Pi]}$ (closure of commutator subgroup), and

$$\Gamma^{n+1}\Pi = \overline{[\Gamma^n\Pi, \Pi]} \text{ for } n \geq 1.$$

This gives a decreasing sequence of normal subgroups

$$\Pi = \Gamma^1\Pi \trianglerighteq \Gamma^2\Pi \trianglerighteq \dots$$

in which each quotient $\Gamma^n\Pi/\Gamma^{n+1}\Pi$ is *abelian*, and each extension

$$1 \longrightarrow \frac{\Gamma^n\Pi}{\Gamma^{n+1}\Pi} \longrightarrow \frac{\Pi}{\Gamma^{n+1}\Pi} \longrightarrow \frac{\Pi}{\Gamma^n\Pi} \longrightarrow 1$$

is central, i.e. $\Gamma^n\Pi/\Gamma^{n+1}\Pi \leq Z(\Pi/\Gamma^{n+1}\Pi)$. In particular, each quotient $\Pi/\Gamma^{n+1}\Pi$ is nilpotent, so not too far from being abelian.

Warning 5.2. When $\Pi = \widehat{F}_2$, one has

$$\bigcap_{n\geq 1} \Gamma^n\Pi \neq 1,$$

so there is more of Π than is captured by the descending central series. •

TODO: Prove this

Thus, we would like to replace $\pi_1^{\text{ét}}(X; x)$ by something easier to study. This will be the "$\mathbb{Q}_p$-pro-unipotent étale fundamental groupoid."

5.1 Unipotent groups

Let F be a field of characteristic 0.

Definition 5.3. A representation V of an affine algebraic group U/F is called `unipotent` just when there exists a finite U-stable filtration

$$0 = \mathrm{Fil}_{-1} V \leq \mathrm{Fil}_0 V \leq \cdots \leq \mathrm{Fil}_n V = V$$

such that the U-action on each graded piece $\mathrm{Fil}_i V / \mathrm{Fil}_{i-1} V$ is trivial. ◇

Definition 5.4. An affine algebraic group U/F is called `unipotent` just when any of the following equivalent conditions hold

(1) Every nonzero representation of U has a nonzero fixed vector, i.e. $V^U \neq 0$

(2) Every representation of U is unipotent

(3) U is a closed subgroup of the `standard unipotent group`

$$\mathrm{Un}_m = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \ddots & \vdots \\ & & 1 & * \\ & & & 1 \end{pmatrix} \right\} \leq \mathrm{GL}_m$$

for some m. ◇

Example 5.5. $\mathbb{G}_a = \mathrm{Un}_2 = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$ is unipotent. △

Example 5.6. Any finite dimensional F-vector space V can be viewed as an affine space over F via $\mathbb{A}(V) := \operatorname{Spec} \mathrm{Sym}^\bullet(V^*)$ (which represents the functor $\Lambda \mapsto \Lambda \otimes_F V$ for Λ an F-algebra). The additive group law on each $\Lambda \otimes_F V$ determines (via Yoneda) a group law on $\mathbb{A}(V)$, making it into a so called `vector group` $\mathbb{G}(V)$. △

Proposition 5.7. *The vector groups are exactly the abelian unipotent groups. Specifically, the functor*

$$\begin{array}{ccc} \mathrm{Vect}_F = \{\textit{f.d. vector spaces}\} & \longrightarrow & \{\textit{vector groups}\} \\ V & \longmapsto & \mathbb{G}(V) \end{array}$$

is an equivalence.

Note 4. Before coming back to write these notes, I often wrote Vect_F to mean (in my head) the category of all vector spaces w/o realizing it was meant to denote only the f.dim ones in this class. Because of this, in notes for the later lectures, you'll see an inconsistent mix-match of Vect_F's and $\mathrm{FinVect}_F$'s.

Example 5.8. Consider the `Heisenberg group` Un_3. There is a homomorphism

$$\begin{array}{ccc} \mathrm{Un}_3 & \longrightarrow & \mathbb{G}_a^2 \\ \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} & \longmapsto & (a, b) \end{array}$$

and a homomorphism

$$\begin{array}{ccc} \mathbb{G}_a & \longrightarrow & \mathrm{Un}_3 \\ c & \longmapsto & \begin{pmatrix} 1 & 0 & c \\ & 1 & 0 \\ & & 1 \end{pmatrix} \end{array}$$

making Un_3 into a central extension

$$1 \longrightarrow \mathbb{G}_a \longrightarrow \mathrm{Un}_3 \longrightarrow \mathbb{G}_a^2 \longrightarrow 1. \qquad \triangle$$

In general, let U be a unipotent group w/ descending central series

$$U = \Gamma^1 U \trianglerighteq \Gamma^2 U \trianglerighteq \Gamma^3 U \trianglerighteq \dots.$$

Then,

(1) The descending central series is finite, i.e. $\Gamma^n U = 1$ for $n \gg 0$.

(2) Each graded piece $V_n = \Gamma^n U / \Gamma^{n+1} U$ is abelian and unipotent, so a vector group.

(3) Each extension

$$1 \longrightarrow V_n \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1 \text{ with } U_n := U/\Gamma^{n+1}U$$

is central.

Slogan. Unipotent groups are iterated central extensions of vector groups

Fact. The category Unipt_F of unipotent groups is the smallest subcategory of affine algebraic groups containing the vector groups and closed under central extensions. In fact, Unipt_F is closed under all extensions, subobjects, quotients, and all finite limits.

5.2 Lie Algebras

Unipotent groups (in char 0) can be understood via their Lie algebras.

Non-example. Say $U = \mathbb{G}_a$ over a field k of characteristic $p > 0$. Let $F : \mathbb{G}_a \to \mathbb{G}_a, x \mapsto x^p$ be the Frobenius map. Then, $\alpha_p := \ker F$ is unipotent and $\alpha_p \ncong \mathbb{G}_a$. At the same time, $\mathrm{d}F : \mathrm{Lie}\,\mathbb{G}_a \to \mathrm{Lie}\,\mathbb{G}_a$ is the zero map, so $\mathrm{Lie}\,\alpha_p \xrightarrow{\sim} \mathrm{Lie}\,\mathbb{G}_a$. $\triangledown$

Definition 5.9. Let $\mathfrak{u}$ be a Lie algebra over F. Its `descending central series` is the sequence of Lie ideals defined by

$$\Gamma^1 \mathfrak{u} = \mathfrak{u} \text{ and } \Gamma^{n+1}\mathfrak{u} = [\Gamma^n \mathfrak{u}, \mathfrak{u}] \text{ for } n \geq 1.$$

We call $\mathfrak{u}$ `nilpotent` just when $\Gamma^n \mathfrak{u} = 0$ for $n \gg 0$. $\diamond$

If U is a unipotent group over F, then

$$\Gamma^n \mathrm{Lie}(U) \subset \mathrm{Lie}(\Gamma^n U)$$

(secretly, this is an equality), so $\mathrm{Lie}(U)$ is nilpotent.

Theorem 5.10. *The functor $U \mapsto \mathrm{Lie}(U)$ is an equivalence of categories*

$$\{\textit{unipotent groups}/F\} \longrightarrow \left\{ \begin{matrix} \textit{f.dim nilpotent} \\ \textit{Lie algebras}/F \end{matrix} \right\}.$$

We won't prove this. However, we can say what the inverse is. We first introduce the Baker-Campbell-Hausdorff series

$$\mathrm{BCH}(x,y) = x + y + \frac{1}{2}[x,y] + \frac{1}{12}[x,[x,y]] - \frac{1}{12}[y,[x,y]] + \dots,$$

which is the power series in non-commuting variables x, y defined by

$$\mathrm{BCH}(x,y) := \log(\exp(x)\exp(y))$$

(with $\log, \exp$ given by their usual power series). If $\mathfrak{u}$ is a f.dim nilpotent F-Lie algebra, we can define the binary operator

$$u \bullet v := \mathrm{BCH}(u,v)$$

on $\mathfrak{u}$, the BCH product. Note that $\mathrm{BCH}(u,v)$ will only have finitely many nonzero terms since $\mathfrak{u}$ is nilpotent, so this is well defined.

Lemma 5.11. *The BCH product make $\mathfrak{u}$ into a group with identity $0 \in \mathfrak{u}$ and inverses $u^{-1} = -u$.*

(see Alex's notes for proof)

Thus, from $\mathfrak{u}$ we get the affine algebraic group $\mathbb{G}(\mathfrak{u})$ representing the functor $\Lambda \mapsto \Lambda \otimes_F \mathfrak{u}$ equipped with the BCH product. $\mathfrak{u} \mapsto \mathbb{G}(\mathfrak{u})$ gives the desired quasi-inverse to $U \mapsto \mathrm{Lie}(U)$.

Consequences of the equivalence

(1) If U is unipotent, then $U(F)$ is a uniquely divisible group, i.e. for any $u \in U(F)$ and $n \in \mathbb{N}$, there's a unique $u^{1/n} \in U(F)$.

Proof. We may suppose $U = \mathbb{G}(\mathfrak{u})$. Then, $u^{1/n} = \frac{1}{n}u$. ■

(2) If $f : U' \to U$ is a homomorphism of unipotent groups, TFAE

- **(i)** f is surjective on underlying topological spaces
- **(ii)** f is dominant
- **(iii)** f is faithfully flat
- **(iv)** f is smooth
- **(v)** f is surjective on F-points
- **(vi)** f is surjective on Λ-points for any F-algebra Λ
- **(vii)** f is split as a morphism of F-schemes

Proof. May assume $f = \mathbb{G}(g)$ for a homomorphism $f : \mathfrak{u}' \to \mathfrak{u}$ of f.dim nilpotent Lie algebras. Then, it factors as

$$\mathbb{A}(\mathfrak{u}') \twoheadrightarrow \mathbb{A}(\mathrm{im}(g)) \hookrightarrow \mathbb{A}(\mathfrak{u})$$

w/ the first map an affine projection between affine spaces and the second an affine inclusion between affine spaces. The claim follows from this. ■

Remark 5.12. **(i)**–**(iv)** are equivalence for any homomorphism of connected affine algebraic groups in characteristic 0. ∘

5.3 Hopf Algebras

The other way to study unipotent groups is through their Hopf algebras. If U is an affine algebraic groups, there are two natural ways to associate a Hopf algebra to it, namely

(i) the affine ring, or algebra of functions, $\mathscr{O}(U)$

(ii) the group algebra $\mathbb{F}[\![U]\!] := \mathscr{O}(U)^*$.

(compare these to taking a finite group G and associating either the algebra of functions F^G or the group algebra $F[G]$)

Warning 5.13. $F[\![U]\!]$ is not quite a Hopf algebra in the usual sense since

$$(\mathscr{O}(U) \otimes_F \mathscr{O}(U))^* \neq \mathscr{O}(U)^* \otimes_F \mathscr{O}(U)^*$$

in general (so multiplication on $\mathscr{O}(U)$ won't dualize to a comultiplication on $F[\![U]\!]$). •

Instead, $F[\![U]\!]$ will be a Hopf algebra in the category of pro-finite dimensional vector spaces.

Definition 5.14. The category pro–Vect_F of pro-finite-dimensional vector spaces over F is the pro-category of the category of f.dim vector spaces. This category supports a completed tensor product

$$\text{“}\varprojlim_{i\in I}\text{”} V_i \widehat{\otimes}_F \text{“}\varprojlim_{j\in J}\text{”} W_j := \text{“}\varprojlim_{(i,j)\in I\times J}\text{”}(V_i \otimes_F W_j). \qquad \diamond$$

Proposition 5.15. *pro–Vect_F is dual to the category Mod_F of all vector spaces, taking $\widehat{\otimes}$ to $\otimes$.*

In the first 10 lectures, I often missed the distinction between Vect_F and Mod_F... Whoops

Proof. Given $V = \text{“}\varprojlim_{i\in I}\text{”} V_i \in$ pro–Vect_F, we define

$$V^* := \varinjlim_{i\in I} V_i^*$$

(colimit takin in Mod_F). Conversely, given $W \in \mathrm{Mod}_F$, we can write $W = \mathrm{colim}_{i\in I} W_i$ as a union/colimit of f.dim vector subspaces, and then set

$$W^* := \text{“}\varprojlim_{i\in I}\text{”} W_i^* \in \text{pro–}\mathrm{Vect}_F. \qquad \blacksquare$$

Corollary 5.16. *pro–$\mathrm{Vect}_F \simeq \mathrm{Mod}_F^{op}$ is an F-linear abelian tensor category, satisfying Grothendieck's axioms AB3+AB4 (existence + exactness of small coproducts) and AB3*+AB4*+AB5* (existence + exactness of small products and cofiltered limits).*

Warning 5.17. In pro–Vect_F, cofiltered limits are well-behaved, not filtered colimits. This is the opposite of what happens in Mod_F. •

We can now say what type of object $F[\![U]\!]$ is.

Definition 5.18. A complete Hopf algebra is a Hopf algebra object in the tensor category (pro–$\mathrm{Vect}_F, \widehat{\otimes}, F$), i.e. it is a pro-finite dimensional vector space H equipped w/

- multiplication $\mu : H\widehat{\otimes}H \to H$
- unit $\eta : F \to H$

- comultiplication $\Delta : H \to H \widehat{\otimes} H$
- counit $\varepsilon : H \to F$
- antipode $S : H \to H$

satisfying the usual list of axioms for Hopf algebras. ◇

Now, $F[\![U]\!] = \mathscr{O}(U)^*$ is a cocommutative complete Hopf algebra (w.r.t. to the dualized Hopf algebra operations). What do we get from U being unipotent?

Definition 5.19. Let H be a complete cocommutative Hopf algebra. Its `augmentation ideal` $I \trianglelefteq H$ is the kernel of the counit $\varepsilon : H \to F$. For $n \geq 1$, we define I^n to be the image of the multiplication map $I^{\widehat{\otimes} n} \to H$. We say that H is *I-`adically complete`* just when, equivalently,

(1) $\bigcap_{n \geq 1} I^n = 0$

(2) The map $H \to \varprojlim_n (H/I^{n+1})$ is an isomorphism in pro–Vect_F.

These are equivalent b/c one can take the limit of the exact sequences $0 \to I^{n+1} \to H \to H/I^{n+1} \to 0$ to get an exact sequence

$$0 \longrightarrow \bigcap_n I^n \longrightarrow H \longrightarrow \varprojlim_n (H/I^{n+1}) \longrightarrow 0.$$ ◇

Proposition 5.20. *U is unipotent if and only if $F[\![U]\!]$ is I-adically complete.*

(See Alex's notes for proof)
We end with a definition

Definition 5.21. A `groupoid in affine` *F-`schemes`* consists of

- a set V of "vertices"
- for $x, y \in V$, an affine F-scheme $U(x, y)$
- for $x, y, z \in V$, a "composition map"

$$U(y, z) \times U(x, y) \longrightarrow U(x, z)$$

  (morphism of affine F-schemes)
- for $x \in V$, an "identity" $1_x \in U(x, x)(F)$
- for $x, y \in V$, an "inverse map" $U(x, y) \to U(y, x)$

These are required to satisfy the usual axioms (associativity, identities, inverses). ◇

(I guess this is a groupoid enriched over affine F-schemes, *not* a groupoid object in AffSch_F)
We say a groupoid U in affine F-schemes is `pro-unipotent` just when $U(x) := U(x, x)$ is pro-unipotent for all $x \in V$.

6 Lecture 7 (2/14): Malčev completion

(Pset3 on the website)

Goal. Produce a $\mathbb{Q}_p$-linearised version of the profinite étale fundamental groupoid.

We've talked about how to define the profinite étale fundamental groupoid associated to any scheme. This is hard to understand completely/explicitly, so we seek an easier $\mathbb{Q}_p$-lineraized version of this. We'll obtain such a thing in two ways. The first way, today, is via Malv̌ec completion, which answers the following question.

Question 6.1. *How do I turn a profinite group into a pro-unipotent group?*

If Π is a finitely generated abelian profinite group, then the natural choice is $\mathbb{Q}_p \otimes_{\widehat{\mathbb{Z}}} \Pi$. We'd like somehow to define "$\mathbb{Q}_p \otimes_{\widehat{\mathbb{Z}}} \Pi$" when Π is non-abelian. This will be made precise by Malčev completion (sometimes called `pro-unipotent completion`).

Proposition 6.2. *Let Π be a f.g. profinite group w/ $\mathbb{Q}_p$-Malčev completion $\Pi_{\mathbb{Q}_p}$. Then, $\Pi_{\mathbb{Q}_p}$ is a f.g. pro-unipotent group over $\mathbb{Q}_p$, and the graded pieces of its descending central series (DCS) are*

$$\mathrm{gr}^n_\Gamma(\Pi_{\mathbb{Q}_p}) = \mathbb{G}\big(\mathbb{Q}_p \otimes_{\widehat{\mathbb{Z}}} \mathrm{gr}^n_\Gamma \Pi\big)$$

(Above $\mathbb{G}(-)$ is the functor turning a vector space into the corresponding vector group scheme).

(This gives one sense in which Malčev completion is analogous to tensor products)

Remark 6.3. `finitely generated profinite group` means there's a finite subset generating a dense subgroup, and `finitely generated ($\mathbb{Q}_p$)-prounipotent group` means there's a finite subset (of its $\mathbb{Q}_p$-points) s.t. the subgroup scheme it generates is Zariski dense. ◦

6.1 Malčev completion

Let F be a topological field of characteristic 0 (e.g. $F = \mathbb{Q}_p$).

Fact. If Z is an affine F-scheme, then there is a canonical topology on $Z(F)$ uniquely characterized by the following

- If $Z = \mathbb{A}^1_F$, then $Z(F) = F$ has the given topology.
- If $f : Z' \to Z$ is a morphism of affine F-schemes, then the induced $Z'(F) \to Z(F)$ is continuous.
- If $\iota : Z' \hookrightarrow Z$ is a closed immersion, then the induced $Z'(F) \hookrightarrow Z(F)$ is a closed embedding.
- If $Z = \varprojlim_i Z_i$, then $Z(F) = \varprojlim_i Z_i(F)$ as topological spaces.

  Example 6.4. $(Z_1 \times Z_2)(F) = Z_1(F) \times Z_2(F)$ has the product topology. △

(This is not hard to prove, but we'll save time by not giving the proof)

Why do these uniquely characterize the topologies. The first bullet point pins down the topology on $\mathbb{A}^1$, the fourth then pins it down on $\mathbb{A}^n$, the third then pins it down on any f.type affine F-scheme (closed subscheme of $\mathbb{A}^n$), and then any affine F-scheme is a limit of f.type ones, so everything else is determined by 4th bullet.

In particular, if U is an affine group scheme, then $U(F)$ is automatically a topological group.

Definition 6.5 (really, theorem)**.** Let Π be a topological group. The functor

$$\begin{array}{ccc} \text{pro–Unipt}_F & \longrightarrow & \text{Set} \\ U & \longmapsto & \text{Hom}_{\text{cts}}(\Pi, U(F)) \end{array}$$

is representable. The representing object is called the `Malčev completion` Π_F of Π. This means there is a continuous group homomorphism

$$\varphi : \Pi \longrightarrow \Pi_F(F)$$

such that for any continuous group homomorphism $f : \Pi \to U(F)$ (with U pro-unipotent), there exists a unique homomorphism of pro-unipotent groups $\widetilde{f} : \Pi_F \to U$ such that

$$\Pi \xrightarrow[\varphi]{} \Pi_F(F) \xrightarrow[\widetilde{f}]{} U(F), \qquad \Pi \xrightarrow{\ f\ } U(F)$$

commutes. ◇

(Compare this w/ the universal property satisfied by tensor products)

Proof of Existence. pro–Unipt$_F$ is the pro-category of Unipt$_F$. From this perspective, the Malčev completion is the pro-unipotent group pro-representing the restriction Unipt$_F \to$ Set (sending $U \mapsto \text{Hom}_{\text{cts}}(\Pi, U(F))$). Such a functor is pro-representable iff it preserves finite limits, which it does. ■

To be clear, to get representability above, we are using

- Unipt$_F$ is essentially small and has finite limits.
- The functor $U \mapsto \text{Hom}_{\text{cts}}(\Pi, U(F))$ preserves finite limits.

6.1.1 Explicit description

Let $F = \mathbb{Q}_p$, and let Π be a f.g. profinite group. Define

$$\mathbb{Z}_p[\![\Pi]\!] := \varprojlim_{\substack{\text{open} \\ N \trianglelefteq \Pi}} \mathbb{Z}_p[\Pi/N]\,.$$

Then, $\mathbb{Z}_p[\![\Pi]\!]$ is a complete topological $\mathbb{Z}_p$-algebra, and has a natural augmentation

$$\varepsilon : \mathbb{Z}_p[\![\Pi]\!] \longrightarrow \mathbb{Z}_p[\Pi/\Pi] = \mathbb{Z}_p.$$

Define the `augmentation ideal` $I \trianglelefteq \mathbb{Z}_p[\![\Pi]\!]$ to be the kernel of ε, and set $I^n \trianglelefteq \mathbb{Z}_p \text{ds}\Pi$ to be the closure of the nth power of I. Finally, we set

$$\mathbb{Q}_p[\![\Pi]\!] := \varprojlim_n \left(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \left(\mathbb{Z}_p[\![\Pi]\!] / I^{n+1}\right)\right)$$

Warning 6.6. The order of operations matters a lot in the above expression. •

Each quotient $\mathbb{Z}_p[\![\Pi]\!] / I^{n+1}$ is a f.g. $\mathbb{Z}_p$-module, so $\mathbb{Q}_p[\![\Pi]\!]$ is an inverse limit of f.dim $\mathbb{Q}_p$-algebras, i.e. $\mathbb{Q}_p[\![\Pi]\!]$ has the structure of a pro-finite dimensional $\mathbb{Q}_p$-vector space w/ an algebra structure.

Proposition 6.7. *There is a cocommutative comultiplication, counit and antipode on $\mathbb{Q}_p[\![\Pi]\!]$ which make it into an I-adically complete cocommutative Hopf algebra.*

We saw last week that the category of prounipotent groups is canonically equivalent to the category of I-adically complete cocommutative Hopf algebras. In fact, this $\mathbb{Q}_p[\![\Pi]\!]$ corresponds to the Malčev completion of Π, i.e.

$$\Pi_{\mathbb{Q}_p} = \operatorname{Spec} \mathbb{Q}_p[\![\Pi]\!]^* .$$

Equivalently, $\mathscr{O}(\Pi_{\mathbb{Q}_p}) = \mathbb{Q}_p[\![\Pi]\!]^*$. Equivalently, $\mathbb{Q}_p\left[\!\left[\Pi_{\mathbb{Q}_p}\right]\!\right] = \mathbb{Q}_p[\![\Pi]\!]$.

Remark 6.8. The * above is the duality between pro–$\mathrm{FinVect}_{\mathbb{Q}_p}$ and $\mathrm{Vect}_{\mathbb{Q}_p}$. ∘

6.2 Fundamental Groups

We are now ready to give one of the main definitions of the course.

Definition 6.9. Let K be a field of characteristic 0 w/ algebraic closure $\overline{K}$. Let X/K be a smooth variety, and let x be a geometric point of $X_{\overline{K}}$. We define the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $(X_{\overline{K}}, x)$ to be

$$\pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x) := \pi_1^{\text{ét}}(X_{\overline{K}}; x)_{\mathbb{Q}_p}$$

(the Malčev completion of the étale fundamental group). ◇

Example 6.10. Say Π is a finitely generated, abelian profinite group. Then,

$$\Pi_{\mathbb{Q}_p} = \mathbb{G}\big(\mathbb{Q}_p \otimes_{\widehat{\mathbb{Z}}} \Pi\big)$$

Pf: there is certainly a continuous homomorphism

$$\varphi : \Pi \longrightarrow \mathbb{G}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Pi)(\mathbb{Q}_p) = \mathbb{Q}_p \otimes_{\widehat{\mathbb{Z}}} \Pi.$$

Say $U/\mathbb{Q}_p$ is unipotent and we have a continuous homomorphism $f : \Pi \to U(\mathbb{Q}_p)$. We claim that f factors through an abelian subgroup of U.

Say $v_1, \dots, v_r \in \Pi$ are topological generators, so $f(v_1), \dots, f(v_r) \in U(\mathbb{Q}_p)$ commute. Hence, $\log f(v_1), \dots, \log f(v_r) \in \mathrm{Lie}(U)$ commute. Therefore, they span an abelian Lie subalgebra which corresponds to some abelian subgroup $U' \subset U$. By construction, U' contains $f(v_1), \dots, f(v_r)$ and so contains the entire image of Π.

The upshot is that $\Pi_{\mathbb{Q}_p}$ must be abelian since $\Pi \longrightarrow \Pi_{\mathbb{Q}_p}(\mathbb{Q}_p)$ factors through an abelian subgroup. Hence, it pro-represents the functor

$$\begin{array}{ccc} (\text{Vector groups}) & \longrightarrow & \text{Set} \\ U & \longmapsto & \mathrm{Hom}_{\mathrm{cts}}(\Pi, U(\mathbb{Q}_p)), \end{array}$$

but vector groups are just f.dim vector spaces (via $V \mapsto \mathbb{G}(V)$), so we're really just looking at the functor $V \mapsto \mathrm{Hom}_{\mathrm{cts}}(\Pi, V)$ which is representable by $\mathbb{Q}_p \otimes_{\widehat{\mathbb{Z}}} \Pi$. △

This is implicitly using (the hard direction of the fact) that $u, v \in \operatorname{Lie} U$ commute for the BCH product $\iff [u, v] = 0$.

Lemma 6.11. *Let Π be a f.g. discrete group, with profinite completion $\widehat{\Pi}$. Then, the natural map*

$$\Pi_{\mathbb{Q}_p} \longrightarrow \left(\widehat{\Pi}\right)_{\mathbb{Q}_p} = \widehat{\Pi}_{\mathbb{Q}_p}$$

is an isomorphism.

Proof. Want to prove that if $U/\mathbb{Q}_p$ is (pro)unipotent, then any continuous group homomorphism $f : \Pi \to U(\mathbb{Q}_p)$ factors uniquely through $\widehat{\Pi}$. If $U(\mathbb{Q}_p)$ were profinite, this would be immediate, but it's not profinite, so some work is needed. One can reduce to proving this in the case that $U = \mathrm{Un}_m$ is the

standard group of $m \times m$ unipotent matrices. Define subgroups $\mathrm{Un}_m(p^{-k}\mathbb{Z}_p) \leq \mathrm{Un}_m(\mathbb{Q}_p)$ consisting of matrices of the form

$$\begin{pmatrix} 1 & p^{-k}* & p^{-2k}* & \dots \\ & 1 & p^{-k}* & \dots \\ & & \ddots & \dots \\ & & & 1 \end{pmatrix}$$

for $*$'s in $\mathbb{Z}_p$. One notes that $\mathrm{Un}_m(\mathbb{Q}_p) = \bigcup_k \mathrm{Un}_m\big(p^{-k}\mathbb{Z}_p\big)$ and so

$$\mathrm{Hom}(\Pi, \mathrm{Un}_m(\mathbb{Q}_p)) = \bigcup_k \mathrm{Hom}(\Pi, \mathrm{Un}_m(p^{-k}\mathbb{Z}_p)) = \mathrm{Hom}_{\mathrm{cts}}\Big(\widehat{\Pi}, \mathrm{Un}_m(\mathbb{Q}_p)\Big)$$

(each $\mathrm{Un}_m(p^{-k}\mathbb{Z}_p)$ is profinite). ■

Application. Suppose $\overline{K} \subset \mathbb{C}$. Then,

$$\pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x) := \pi_1^{\text{ét}}(X_{\overline{K}}; x)_{\mathbb{Q}_p} = \pi_1^{\text{ét}}(X_{\mathbb{C}}; x)_{\mathbb{Q}_p} = \widehat{\pi}_1(X(\mathbb{C}); x)_{\mathbb{Q}_p} = \pi_1(X(\mathbb{C}); x)_{\mathbb{Q}_p}.$$

Corollary 6.12. *The groups $\pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x)$ is finitely generated. In the case that X is a smooth, geometrically connected curve – say $X = \overline{X} \setminus D$ with $D \in \mathrm{Div}^r(\overline{X})$ and $\overline{X}$ projective of genus g – one has that $\pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x)$ is the $\mathbb{Q}_p$-pro-unipotent group generated by elements $a_1, \dots, a_g, b_1, \dots, b_g, c_1, \dots, c_r$ subject to the single relation*

$$\prod_{i=1}^{g} [a_i, b_i] \cdot \prod_{j=1}^{r} c_j = 1.$$

Example 6.13. Say $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Let $\mathfrak{f}_2$ denote the free $\mathbb{Q}_p$-Lie algebra on two generators, and let $\Gamma^\bullet \mathfrak{f}_2$ denote its descending central series. Then,

$$\pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x) = \text{free pro-unipotent group on 2 generators} = \varprojlim_n \mathbb{G}\left(\frac{\mathfrak{f}_2}{\Gamma^{n+1}\mathfrak{f}_2}\right).$$

The structure of the free Lie algebras, especially after quotient by their DCSs, is well understood. For example, one knows explicit bases for $\mathfrak{f}_2$ and each $\Gamma^n\mathfrak{f}_2$ (Hall bases or Lyndom bases) which let one deduce e.g. that

$$\dim_{\mathbb{Q}_p} \mathrm{gr}^1_\Gamma \mathfrak{f}_2 = 2 \qquad \dim_{\mathbb{Q}_p} \mathrm{gr}^2_\Gamma \mathfrak{f}_2 = 1$$
$$\dim_{\mathbb{Q}_p} \mathrm{gr}^3_\Gamma \mathfrak{f}_2 = 2 \qquad \dim_{\mathbb{Q}_p} \mathrm{gr}^4_\Gamma \mathfrak{f}_2 = 3$$

(note $\mathrm{gr}^1_\Gamma \mathfrak{f}_2$ is the abelianization of $\mathfrak{f}_2$ is simply a 2-dim vector space w/ trivial Lie bracket). In general,

$$\dim_{\mathbb{Q}_p} \mathrm{gr}^n_\Gamma \mathfrak{f}_k = \frac{1}{n} \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, k^d,$$

where μ is the usual Mobius function (see Theorem 25.15). △

Remark 6.14 (Audience). $\dim_{\mathbb{Q}_p} \mathrm{gr}^n_\Gamma \mathfrak{f}_p$ has the same formula as the number of degree n irreducible polynomials over $\mathbb{F}_p$. ∘

7 Lecture 8 (2/16): The Tannakian Formalism

Last time, we constructed unipotent fundamental groups via Malčev completion. Today we give a different construction/perspective of/on this object.

Recall 7.1. The profinite étale fundamental group is "produced" out of the category $\mathrm{F\acute{E}t}(X)$ of finite étale coverings. In fact, the converse is true as well (if X is connected)

$$\mathrm{F\acute{E}t}(X) \cong \{\text{finite continuous } \pi_1(X;x)\text{-sets}\}\,. \qquad \odot$$

In getting our $\mathbb{Q}_p$-linear unipotent fundamental group, we are attempting to linearize the fundamental group. Well, there's a natural candidate for linearizing $\pi_1^{\text{ét}}(X;x)$-sets. Just consider representations instead.

Question 7.2. *Can we extract a pro-unipotent group out of this category of representations?*

Example 7.3. If X is a nice topological space, then we say that $\mathrm{Cov}(X) \cong \{\pi_1(X;x)\text{-sets}\}$. We can linearize the RHS by consider the category of $\mathbb{Q}$-linear representations of $\pi_1(X;x)$. On the topological side, this is equivalent to the category of $\mathbb{Q}$-local systems on X, i.e. sheaves E of $\mathbb{Q}$-vector spaces on X which are locally isomorphic to $\underline{\mathbb{Q}}_X^{\oplus n}$.

Instead of considering all local systems, one could consider $\mathbb{Q}$-linear unipotent representations. These would correspond to $\mathbb{Q}$-linear *unipotent* local systems on X, where a local system E is unipotent if it has a finite filtration

$$0 = \mathrm{Fil}_{-1} E \leq \mathrm{Fil}_0 E \leq \cdots \leq \mathrm{Fil}_n E = E$$

with graded pieces $\mathrm{Fil}_i E/\mathrm{Fil}_{i-1} E \simeq \underline{\mathbb{Q}}_X^{\oplus n_i}$. $\qquad \triangle$

Question 7.4 (Audience)**.** *Are local systems the same thing as $\mathbb{Q}$-vector bundles on X?*

Answer (paraphrased)**.** Not quite. Vector bundles are locally isomorphic to $\mathscr{O}_X^{\oplus r}$ instead of $\underline{\mathbb{C}}_X^{\oplus r}$. One way of thinking of the difference is to think of a $\mathbb{C}$-local system as a map $V \to X$ which locally looks like $X \times \mathbb{C} \to X$ where $\mathbb{C}$ is given its discrete topology. $\qquad \star$

In order to define $\pi_1^{\mathbb{Q}_p}(X_{\overline{K}};x)$ in the setting of schemes, we'll carry out the following two steps

(1) Define a category $\mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}(X_{\overline{K},\text{ét}})$ of unipotent $\mathbb{Q}_p$-local systems on $X_{\text{ét}}$.

(2) Extract a $\mathbb{Q}_p$-pro-unipotent group out of this category.

We'll focus on **(2)** today.

7.1 The Tannakian formalism

Slogan. Take a category which "looks like" the category of local systems on a space, and output from this an affine group scheme whose category of representations is the category we started with.

What does it mean for a category to look like local systems on a space?

Setup 7.5. Fix F a field of characteristic 0.

Definition 7.6. An F-linear abelian $\otimes$-category $\mathcal{T}$ is really a tuple $\mathcal{T} = (\mathcal{T}, \otimes, \mathbf{1})$ (along w/ many given morphisms) is an abelian category $\mathcal{T}$ in which every Hom-group $\mathrm{Hom}_{\mathcal{T}}(E_1, E_2)$ is an F-vector space such that the composition maps

$$\mathrm{Hom}_{\mathcal{T}}(E_2, E_3) \times \mathrm{Hom}_{\mathcal{T}}(E_1, E_2) \longrightarrow \mathrm{Hom}_{\mathcal{T}}(E_1, E_3)$$

are F-bilinear.[8] Furthermore, $\mathcal{T}$ is endowed w/ a unit object $\mathbf{1} \in \mathcal{T}$ and an F-bilinear tensor product, i.e. a functor

$$\otimes : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$$

[8] This is F-linear abelian

making $(\mathcal{T}, \otimes, \mathbf{1})$ into a symmetric monoidal category, so e.g.[9]

$$E_1 \otimes (E_2 \otimes E_3) \simeq (E_1 \otimes E_2) \otimes E_3, \quad E \otimes \mathbf{1} \simeq E \simeq \mathbf{1} \otimes E, \quad \text{and} \quad E_1 \otimes E_2 \simeq E_2 \otimes E_1.$$

Given an object $E \in \mathcal{T}$, a strong dual[10] of E is an object $E^* \in \mathcal{T}$ equipped w/ an evaluation map $\mathrm{ev} : E^* \otimes E \to \mathbf{1}$ along with a coevaluation map $\delta : \mathbf{1} \to E \otimes E^*$ such that

$$E \xrightarrow[\delta \otimes 1]{} E \otimes E^* \otimes E \xrightarrow[1 \otimes \mathrm{ev}]{} E \quad \text{and} \quad E^* \xrightarrow[1 \otimes \delta]{} E^* \otimes E \otimes E^* \xrightarrow[\mathrm{ev} \otimes 1]{} E^*$$

(each composite is the identity, id)

commute. ◇

Example 7.7. Say $\mathcal{T} = \mathrm{Mod}_F$ is the category of all F-vector spaces. Then, a vector space V has a strong dual $\iff$ V is finite-dimensional. In this case, $V^* = \mathrm{Hom}_F(V, F)$ as you'd expect. The maps are

$$\begin{array}{rccc} \mathrm{ev}: & V^* \otimes V & \longrightarrow & F \\ & \psi \otimes v & \longmapsto & \psi(v) \end{array} \quad \text{and} \quad \begin{array}{rccc} \delta: & F & \longrightarrow & V \otimes V^* \\ & 1 & \longmapsto & \sum_i v_i \otimes \psi_i, \end{array}$$

where $v_i \in V$ is a basis of V w/ dual basis $\psi_i \in V^*$. In other words, δ sends 1 to the identity map $\mathrm{id}_V \in \mathrm{End}(V) \simeq V \otimes V^\vee$. △

In general, strong duals satisfy all the expected properties

(1) E^* is unique up to unique isomorphism (if it exists)

(2) $f : E_1 \to E_2$ induces a dual map $f^* : E_2^* \to E_1^*$

(3) $(E_1 \otimes E_2)^* = E_2^* \otimes E_1^*$.

Remark 7.8. A weak dual E^* of E is an object which represents the functor $E' \mapsto \mathrm{Hom}_{\mathcal{T}}(E' \otimes E, \mathbf{1})$. Any strong dual will be a weak dual, but the converse does not hold.

This might be one's first guess as to the definition of a 'dual', but the notion of strong dual is generally nicer to work with. For example, given a functor between tensor categories (that preserves tensor products), it is not obvious that is must preserve weak duals, but it is obvious that it must preserve strong duals. ○

Definition 7.9. A pre-Tannakian category is an essentially small F-linear abelian $\otimes$-category $\mathcal{T}$ in which every object has a strong dual (say $\mathcal{T}$ is "rigid"). ◇

Recall 7.10. When talking about covering spaces, in order to recover the fundamental group, we didn't just need the category of coverings. We needed it along with the functors outputing fibers above each point. ⊙

Definition 7.11. A fibre functor on a pre-Tannakian category $\mathcal{T}$ is an F-linear exact $\otimes$-functor

$$\begin{array}{rccc} \omega_x: & \mathcal{T} & \longrightarrow & \mathrm{Vect}_F \\ & E & \longmapsto & E_x. \end{array}$$

◇

Warning 7.12. ω_x is not required to be faithful. •

[9] First two monoidal, last one symmetric

[10] We've really defined a *strong right dual* of an object in a monoidal category

Remark 7.13. One should think that 'pre-Tannakian categories' look like local systems on a potentially disconnected space. For those on a connected space, we'll later define 'neutral Tannakian categories'. ∘

7.2 Tannakian fundamental groupoids

Let $\mathcal{T}$ be a pre-Tannakian category, and let ω_x, ω_y be fibre functors.

Definition 7.14. A ⊗-natural transformation $\gamma : \omega_x \to \omega_y$ is a natural transformation such that the diagrams

$$\begin{array}{ccc} (E_1 \otimes E_2)_x & \xrightarrow{\gamma_{E_1\otimes E_2}} & (E_1 \otimes E_2)_y \\ \simeq\downarrow & & \downarrow\simeq \\ E_{1,x} \otimes E_{2,x} & \xrightarrow{\gamma_{E_1}\otimes\gamma_{E_2}} & E_{1,y} \otimes E_{2,y} \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbf{1}_x & \xrightarrow{\gamma_{\mathbf{1}}} & \mathbf{1}_y \\ & \searrow^{\simeq} \quad \swarrow_{\simeq} & \\ & F & \end{array}$$

commute. It is a ⊗-natural isomorphism if it is furthermore a natural isomorphism. ◇

(All the maps labelled $\simeq$ above are extra data required in the full definition of a fibre functor)

Notation 7.15. If Λ is an F-algebra, then, we'll write $\omega_{x,\Lambda}$ for the composition functor

$$\mathcal{T} \xrightarrow{\omega_x} \mathrm{Mod}_F \xrightarrow{\Lambda\otimes_F(-)} \mathrm{Mod}_\Lambda .$$

If ω_x is a tensor functor, then so is $\omega_{x,\Lambda}$. Hence, we can talk of ⊗-natural transformations/isomorphisms $\omega_{x,\Lambda} \to \omega_{y,\Lambda}$.

Proposition 7.16 (Deligne)**.** *Any ⊗-natural transformation $\omega_{x,\Lambda} \to \omega_{y,\Lambda}$ is in fact a ⊗-natural isomorphism.*

Theorem 7.17. *Let $\mathcal{T}$ be pre-Tannakian. Let ω_x, ω_y be fibre functors. Then, the functor*

$$\begin{array}{ccc} \mathrm{Alg}_F & \longrightarrow & \mathrm{Set} \\ \Lambda & \longmapsto & \mathrm{Isom}^{\otimes}(\omega_{x,\Lambda}, \omega_{y,\Lambda}) \end{array}$$

is representable by an affine F-scheme, which we'll denote $\pi_1(\mathcal{T}; x, y)$. Composition of ⊗-natural transformations induces a composition map

$$\pi_1(\mathcal{T}; y, z) \times \pi_1(\mathcal{T}; x, y) \longrightarrow \pi_1(\mathcal{T}; x, z)$$

along with identity elements $1_x \in \pi_1(\mathcal{T}; x, x)(F)$ and reversal/inverse maps $\pi_1(\mathcal{T}; x, y) \to \pi_1(\mathcal{T}; y, x)$. These map $\pi_1(\mathcal{T}; -, -)$ into a groupoid in affine F-schemes, called the Tannakian fundamental groupoid of $\mathcal{T}$.

(by 'groupoid in affine F-schemes' I guess we mean a groupoid enriched over affine F-schemes)

Remark 7.18. Thus far, we haven't actually used characteristic 0 yet. ∘

Example 7.19. Take $\mathcal{T} = \{\mathbb{Q}\text{-local systems on a nice topological space } X\}$. This is pre-Tannakian. If $x \in X$ and E is a local system, then the stalk $E_x \in \mathrm{Vect}_{\mathbb{Q}}$ and $\omega_x : E \mapsto E_x$ is a fiber functor.

Question 7.20 (Audience)**.** *Are all fibre functors of this form?*

Answer. In general no. Even for the circle, I think there are other fiber functors. While the fundamental groupoid is defined using all fibre functors, in practice, we usually restrict attention to those coming from something we understand (like points). ⋆

If we replace $\mathcal{T}$ w/ the category of *unipotent* $\mathbb{Q}$-local systems, then $\pi_1(\mathcal{T}; x)$ is the $\mathbb{Q}$-Malčev completion of $\pi_1(X; x)$. △

Example 7.21. Let U/F be an affine group scheme, and take $\mathcal{T} = \mathrm{Rep}_F(U)$. This is pre-Tannakian and one example of a fiber functor is the forgetful functor $\omega_x : \mathrm{Rep}_F(U) \to \mathrm{Vect}_F$. In this case, $\pi_1(\mathcal{T}; x) = U$. △

7.3 Matrix Coefficients

Goal. Describe $\pi_1(\mathcal{T}; x, y)$ explicitly

Definition 7.22. An `abstract matrix coefficient` for $(\mathcal{T}, \omega_x, \omega_y)$ is a triple (E, v, φ) where $E \in \mathcal{T}$, $v \in E_x$, and $\varphi \in E_y^* = (E_y)^* = (E^*)_y$. Two matrix coeffs (E_1, v_1, φ_2) and (E_2, v_2, φ_2) are said to be `basic equivalent` just when there exists a morphism

$$\alpha : E_1 \longrightarrow E_2$$

such that $\alpha_x(v_1) = v_2$ and $\alpha_y^*(\varphi_2) = \varphi_1$. We define $H_{x,y}$ to be the set[11] of abstract matrix coefficients modulo the equivalence relation generated by basic equivalence. ◇

In fact, $H_{x,y}$ is an F-algebra.

- $(E_1, v_1, \varphi_1) + (E_2, v_2, \varphi_2) = (E_1 \oplus E_2, v_1 \oplus v_2, \varphi_1 \oplus \varphi_2)$
- $(E_1, v_1, \varphi_1) \cdot (E_2, v_2, \varphi_2) = (E_1 \otimes E_2, v_1 \otimes v_2, \varphi_1 \otimes \varphi_2)$

These make $H_{x,y}$ into a ring. To make it an F-algebra, one uses the ring homomorphism

$$\begin{array}{rccc} \eta : & F & \longrightarrow & H_{x,y} \\ & \lambda & \longmapsto & (\mathbf{1}, \lambda, 1). \end{array}$$

Remark 7.23. For any $E \in \mathcal{T}$, the map

$$\begin{array}{ccc} E_x \times E_y^* & \longrightarrow & H_{x,y} \\ (v, \varphi) & \longmapsto & (E, v, \varphi) \end{array}$$

is F-bilinear. ○

Running out of time, but here's a sneak peek of what we're heading towards.

Theorem 7.24 (Next time)**.** $\pi_1(\mathcal{T}, x, y) \simeq \mathrm{Spec}\, H_{x,y}$

Question 7.25 (Audience)**.** *Why are they called matrix coefficients?*

Answer. Any matrix coefficient (E, v, φ) gives rise to an element $f_{(E,v,\varphi)} \in \mathscr{O}(\pi_1(\mathcal{T}; -, -))$, i.e. a morphism $\pi_1(\mathcal{T}; x, y) \to \mathbb{A}^1$. This map is the composition

$$\pi_1(\mathcal{T}, x, y) \longrightarrow \mathbb{A}(\mathrm{Hom}_F(E_x, E_y)) \xrightarrow{\mathrm{ev}_v} \mathbb{A}(E_y) \xrightarrow{\varphi} \mathbb{A}^1.$$

Example 7.26. Take $\mathcal{T} = \mathrm{Rep}(\mathrm{GL}_n)$ and let E be the standard n-dimensional representation. Let v_j be the jth basis vector, and let φ_i be the ith coordinate projective. Then,

$$f_{(E,v_j,\varphi_i)} : \mathrm{GL}_n \longrightarrow \mathbb{A}^1$$

[11] Because $\mathcal{T}$ is essentially small

is exactly the map picking out the ijth entry in a matrix. △

⋆

Question 7.27 (Audience)**.** *When is $H_{x,y}$ f.type?*

Answer. When $\mathcal{T}$ is finitely generated in the sense that there's some finite list of objects s.t. every object is a subquotient (really, quotient of direct summand) of tensors of the objects in the finite list. ⋆

8 Lecture 9 (2/21): Tannakian formalism, ct'd

8.1 Last Time

Let F be a field of characteristic 0.

Recall 8.1. A `pre-Tannakian category` is an essentially small rigid F-linear abelian $\otimes$-category. A `fibre functor` is an exact F-linear $\otimes$-functor $\omega_x : \mathcal{T} \to \mathrm{Vect}_F$. ⊙

Note 5. I think Vect_F is meant to be only f.dim vector spaces, not all of them.

Theorem 8.2. *For all ω_x, ω_y, the functor*

$$\begin{array}{ccc} \mathrm{Alg}_F & \longrightarrow & \mathrm{Set} \\ \Lambda & \longmapsto & \mathrm{Isom}^{\otimes}(\omega_{x,\Lambda}, \omega_{y,\Lambda}) = \mathrm{Hom}^{\otimes}(\omega_{x,\Lambda}, \omega_{y,\Lambda}) \end{array}$$

is representable by an affine F-scheme $\pi_1(\mathcal{T}; x, y)$.

Recall 8.3. A `matrix coefficient` is a triple $(\mathcal{E} \in \mathcal{T}, \nu \in \mathcal{E}_x, \varphi \in \mathcal{E}_y^*)$. The set $H_{x,y} = \{\text{matrix coeffs}\}/\sim$ is an F-algebra w.r.t $\oplus, \otimes$. ⊙

8.2 This time, matrix coeffs

Let's describe some more structures on these algebras of matrix coefficients.

- Say we have three fiber functors $\omega_x, \omega_y, \omega_z$. Then, there are three algebras of matrix coefficients lying around, and they are related via a `cocomposition map`

$$\begin{array}{rccc} \Delta : & H_{x,z} & \longrightarrow & H_{y,z} \otimes H_{x,y} \\ & (\mathcal{E}, \nu, \varphi) & \longmapsto & \displaystyle\sum_i (\mathcal{E}, \nu_i, \varphi) \otimes (\mathcal{E}, \nu, \varphi_i), \end{array}$$

  where $\{v_i\}$ forms a basis of $\mathcal{E}_y$, and $\{\varphi_i\}$ is the dual basis of $\mathcal{E}_y^*$. One can check that this map is well-defined (independent of choices of basis and of representative of basic equivalence class) and is an F-algebra homomorphism.

- For all ω_x, there is a `counit map`

$$\begin{array}{rccc} \varepsilon : & H_{x,x} & \longrightarrow & F \\ & (\mathcal{E}, \nu, \varphi) & \longmapsto & \varphi(v). \end{array}$$

  This is also an F-algebra homomorphism.

- For all ω_x, ω_y, there is an `antipode map`

$$\begin{array}{rccc} S: & H_{y,x} & \longrightarrow & H_{x,y} \\ & (\mathcal{E}, \nu, \varphi) & \longmapsto & (\mathcal{E}^*, \varphi, \nu) \end{array}$$

Theorem 8.4. *For all ω_x, ω_y, $\pi_1(\mathcal{T}; x, y) \simeq \operatorname{Spec} H_{x,y}$ (canonically isomorphic), and these isomorphisms are all compatible with composition, identities, and inverses. That is, we have an equivalence of groupoids.*

We'll actually directly prove that $\operatorname{Spec} H_{x,y}$ represents the functor of $\otimes$-natural isomorphisms $\omega_x \to \omega_y$, and so also prove Theorem 7.17, which we only stated as fact before.

Proposition 8.5. *There is an isomorphism*

$$H_{x,y}^* \xrightarrow{\sim} \operatorname{Hom}(\omega_x, \omega_y)$$

of pro-finite-dimensional vector spaces.

(Note that these are all natural transformations, not just the $\otimes$-natural ones)

Remark 8.6. How do we view $\operatorname{Hom}(\omega_x, \omega_y)$ as a pro-finite-dimensional vector space? In fancy language, write is as the 'End' (a certain fancy kind of limit)

$$\operatorname{Hom}(\omega_x, \omega_y) = \int_{\mathcal{E} \in \mathcal{T}} \operatorname{Hom}(\mathcal{E}_x, \mathcal{E}_y),$$

where each $\operatorname{Hom}(\mathcal{E}_x, \mathcal{E}_y)$ is a f.dim vector space. Take the limit in pro–$\operatorname{FinVect}_F$ to endow $\operatorname{Hom}(\omega_x, \omega_y)$ w/ a pro-finite dimensional structure. ∘

Warning 8.7. Often in these notes, I have written Vect_F where I really should have written $\operatorname{FinVect}_F$. I won't go back and change these, and I won't stop making this mistake in the future. •

Proof of Proposition 8.5. For any $\mathcal{E} \in \mathcal{T}$, the map

$$\begin{array}{rccc} & \mathcal{E}_x \times \mathcal{E}_y^* & \longrightarrow & H_{x,y} \\ & (\nu, \varphi) & \longmapsto & (\mathcal{E}, \nu, \varphi) \end{array}$$

is F-bilinear. So, given an F-linear $f : H_{x,y} \to F$, we get an F-linear map $\gamma_{\mathcal{E}} : \mathcal{E}_x \to \mathcal{E}_y$ characterized by

$$\varphi(\gamma_{\mathcal{E}}(v)) = f(\mathcal{E}, v, \varphi)$$

for all $v \in \mathcal{E}_x$ and all $\varphi \in \mathcal{E}_y^*$. The $\gamma_{\mathcal{E}}$ are the components of a natural transformation $\omega_x \to \omega_y$. Indeed, given $\alpha : \mathcal{E} \to \mathcal{E}'$ in $\mathcal{T}$, for all $v \in \mathcal{E}_x$ and all $\varphi \in (\mathcal{E}'_y)^*$, we have

$$\varphi(\gamma_{E'}(\alpha_x(v))) = f(\mathcal{E}', \alpha_x(v), \varphi) = f(\mathcal{E}, v, \alpha_y^* \varphi) = \varphi(\alpha_y(\gamma_{\mathcal{E}}(v)))\,,$$

with middle equality because the inputs are basic equivalent, i.e.

$$\begin{array}{ccc} \mathcal{E}_x & \xrightarrow{\alpha_x} & \mathcal{E}'_x \\ {\scriptstyle \gamma_{\mathcal{E}}}\downarrow & & \downarrow{\scriptstyle \gamma_{\mathcal{E}'}} \\ \mathcal{E}_y & \xrightarrow{\alpha_y} & \mathcal{E}'_y \end{array}$$

commutes. This defines the map $H_{x,y}^* \to \operatorname{Hom}(\omega_x, \omega_y)$.

I may have missed something, but I think what was said was essentially that one can check this is an isomorphism by directly defining an inverse map (e.g. by reversing this argument)? ■

Lemma 8.8. *Under these isomorphisms* $H^*_{x,y} \simeq \mathrm{Hom}(\omega_x, \omega_y)$,

(1) *Cocomposition on* $H_{x,y}$ *is dual to composition of natural transformations.*

(2) *Counit is dual to the map* $\eta : F \to \mathrm{Hom}(\omega_x, \omega_x)$ *sending* $1 \mapsto \mathrm{id}$.

(3) *Antipode is dual to the map* $\mathrm{Hom}(\omega_x, \omega_y) \to \mathrm{Hom}(\omega_y, \omega_x)$ *sending* $\gamma = (\gamma_{\mathcal{E}})_{\mathcal{E}} \mapsto (\gamma^*_{\mathcal{E}^*})_{\mathcal{E}}$.

(Proof left as an exercise)
Write $\omega_x \boxtimes \omega_x : \mathcal{T} \times \mathcal{T} \longrightarrow \mathrm{Vect}_F$ for the functor

$$(\mathcal{E}, \mathcal{E}') \mapsto \mathcal{E}_x \otimes \mathcal{E}'_x.$$

Claim 8.9. *There is an isomorphism*

$$\mathrm{Hom}(\omega_x, \omega_y) \widehat{\otimes} \mathrm{Hom}(\omega_x, \omega_y) \cong \mathrm{Hom}(\omega_x \boxtimes \omega_y, \omega_x \boxtimes \omega_y)$$

sending $\gamma_1 \otimes \gamma_2 \mapsto \gamma_1 \boxtimes \gamma_2$, *where*

$$(\gamma_1 \boxtimes \gamma_2)_{(\mathcal{E}_1, \mathcal{E}_2)} = \gamma_{1,\mathcal{E}_1} \otimes \gamma_{2,\mathcal{E}'_2} : \mathcal{E}_{1,x} \otimes \mathcal{E}_{2,x} \longrightarrow \mathcal{E}_{1,y} \otimes \mathcal{E}_{2,y}.$$

Lemma 8.10 (continued from previous one)**.**

(4) *Multiplication*

$$H_{x,y} \otimes H_{x,y} \longrightarrow H_{x,y}$$

is dual to the map

$$\Delta : \mathrm{Hom}(\omega_x, \omega_y) \longrightarrow \mathrm{Hom}(\omega_x, \omega_y) \widehat{\otimes} \mathrm{Hom}(\omega_x, \omega_y) \cong \mathrm{Hom}\left(\omega_x^{\boxtimes 2}, \omega_y^{\boxtimes 2}\right)$$

given by

$$\Delta(\gamma)_{(\mathcal{E}_1, \mathcal{E}_2)} = \gamma_{\mathcal{E}_1 \otimes \mathcal{E}_2}.$$

(5) *The unit map* $\eta : F \to H_{x,y}$ *is dual to*

$$\begin{array}{ccc} \mathrm{Hom}(\omega_x, \omega_y) & \longrightarrow & F \\ \gamma & \longmapsto & \gamma_{\mathbf{1}} \end{array}$$

(Proof is a lot of chasing symbols around)

Corollary 8.11. $\mathrm{Hom}(\omega_x, \omega_y)$ *is a cocommutative coalgebra in pro–*Vect_F *and*

$$\mathrm{Hom}(\omega_x, \omega_y)^{gplike} = \mathrm{Hom}^{\otimes}(\omega_x, \omega_y).$$

This is because $\otimes$`-natural` means that $\gamma_{\mathcal{E}_1 \otimes \mathcal{E}_2} = \gamma_{\mathcal{E}_1} \otimes \gamma_{\mathcal{E}_2}$ and $\gamma_{\mathbf{1}} = 1$. Compare this to the definition of `grouplike`, which says that $\Delta(\gamma) = \gamma \otimes \gamma$ and $\varepsilon(\gamma) = 1$. In fact, more generally, one has

$$\mathrm{Hom}(\omega_x, \omega_y)^{\mathrm{gplike}}_{\Lambda} = \mathrm{Hom}^{\otimes}(\omega_{x,\Lambda}, \omega_{y,\Lambda}).$$

With this, we have all the ingredients in place necessary to prove the theorem.

Proof of Theorem. For any F-algebra Λ, we have

$$\begin{aligned}\mathrm{Spec}(H_{x,y})(\Lambda) &= \mathrm{Hom}_{\mathrm{Alg}_F}(H_{x,y}, \Lambda) \\ &= H^{*,\mathrm{gplike}}_{x,y,\Lambda} \\ &= \mathrm{Hom}(\omega_x, \omega_y)^{\mathrm{gplike}}_{\Lambda} \\ &= \mathrm{Hom}^{\otimes}(\omega_{x,\Lambda}, \omega_{y,\Lambda}),\end{aligned}$$

i.e. $\Lambda \mapsto \mathrm{Hom}^{\otimes}(\omega_x, \omega_y)$ is representable by $H_{x,y}$. ■

8.3 Neutral Tannakian categories

(Think of these as 'connected' pre-Tannakian categories)

Fact. Let $\omega : \mathcal{A} \to \mathcal{B}$ be an exact functor between abelian categories. Then, TFAE

(1) ω is `faithful`, i.e. for all $A_1, A_2 \in \mathcal{A}$, the induced map

$$\mathrm{Hom}_{\mathcal{A}}(A_1, A_2) \longrightarrow \mathrm{Hom}_{\mathcal{B}}(\omega(A_1), \omega(A_2))$$

is injective.

(2) ω is `conservative`, i.e. $\omega(f)$ is an isomorphism $\iff$ f is an isomorphism.

(3) ω `reflects zero objects`, i.e. $\omega(A) = 0 \iff A = 0$

(4) ω is `faithfully exact`, i.e. $0 \to A \to B \to C \to 0$ is exact iff $0 \to \omega(A) \to \omega(B) \to \omega(C) \to 0$ is exact.

(Think about the various characterizations of a faithfully flat R-module)

Example 8.12. Say $\mathcal{A} = \mathrm{Rep}(U)$ for some affine group scheme U, $\mathcal{B} = \mathrm{Vect}_F$, and ω is the forgetful functor. Then, ω is an exact functor and satisfies **(1)**–**(4)** above. △

Definition 8.13. Let $\mathcal{T}$ be pre-Tannakian. We say is is `neutral Tannakian` just when as any of the below equivalent conditions hold

(1) $\mathcal{T}$ has at least one faithful fiber functor.

(2) $\mathcal{T}$ has at least one fiber functor and all fiber functors are faithful.

(3) $\mathrm{End}(\mathbf{1}) = F$ and $\mathcal{T}$ has at least one fiber functor. ◇

Question 8.14 (Audience)**.** *How hard is to write down a pre-Tannakian category w/ no fiber functors?*

Answer (paraphrased)**.** Alex first remarked that there's a notion of `Tannakian category` which is required to satisfy $\mathrm{End}(\mathbf{1}) = F$ and is required to have a fiber functor defined over some field extension E/F. So, you should believe such things exist.

He then mentioned he's never seen a fiber functor for the following category. Let $K/\mathbb{Q}_p$ be a finite extension of reside degree > 1. Consider the category $\mathrm{Mod}(\varphi)$ of `φ-modules`. This is a K_0-vector space D along with a φ-semilinear map $D \to D$ (Here, $\varphi = \mathrm{Frob}$ and K_0 is the maximal unramified field extension of K). This is pre-Tannakian over $\mathbb{Q}_p$ (need to preserve φ-semilinearity). Does it have a fiber functor to $\mathrm{Vect}_{\mathbb{Q}_p}$? You could try, for example, to take φ-invariants, but this won't be exact. ⋆

Theorem 8.15. *Let $\mathcal{T}$ be neutral Tannakian. Then,*

$$\pi_1(\mathcal{T}; x, y) \neq \emptyset$$

for all ω_x, ω_y.

Theorem 8.16 (Tannakian Reconstruction Theorem)**.** *Let $\mathcal{T}$ be neutral Tannakian, and let ω_x be a fiber functor. Then, $\mathcal{T} \simeq \mathrm{Rep}_F(\pi_1(\mathcal{T}; x))$ (as F-linear abelian $\otimes$-categories), and this equivalence carries ω_x to the forgetful functor.*

Let's end with saying a bit about Theorem 8.15.

Proof Sketch of Theorem 8.15. We'll start with a separate proposition.

Proposition 8.17. *Let $\mathcal{T}$ be a pre-Tannakian category, and let $\omega_x : \mathcal{T} \to \mathrm{Vect}_F$ be a fibre functor. Then, ω_x is pro-representable. The pro-representing object $({}_x\mathcal{E}^{\mathcal{T}}, e_x^{\mathcal{T}})$ is called the* universal object *in $\mathcal{T}$.*

(One appeals the the abstract pro-representability theorem we've used a few times before).

Let $\mathcal{T}$ be neutral Tannakian, so ω_x is faithfully exact. Write ${}_x\mathcal{E}^{\mathcal{T}} = \text{“}\varprojlim_i\text{”}\, {}_x\mathcal{E}_i^{\mathcal{T}}$ for some ${}_x\mathcal{E}_i^{\mathcal{T}} \in \mathcal{T}$. Hence, there exists a unique morphism

$$\varepsilon : {}_x\mathcal{E}^{\mathcal{T}} \longrightarrow \mathbf{1}$$

in pro–$\mathcal{T}$ such that $\varepsilon(e_x^{\mathcal{T}}) = 1$. Without loss of generality, this ε is represented by a family of maps ${}_x\mathcal{E}_i^{\mathcal{T}} \longrightarrow \mathbf{1}$ (a priori only have such things for sufficiently large i). Now, $\varepsilon_{i,x} : {}_x\mathcal{E}_{i,x}^{\mathcal{T}} \to F$ is surjective as 1 is contained in the image. Thus, faithful exactness tells us that the map $\varepsilon_i : {}_x\mathcal{E}_i^{\mathcal{T}} \to \mathbf{1}$ is "surjective" (read: epiomorphic), so a second application of faithful exactness tells us that $\varepsilon_{i,y} : {}_x\mathcal{E}_{i,y}^{\mathcal{T}} \to F$ is surjective. Since cofiltered limits in pro–Vect_F are exact, we get that

$$\varepsilon_y : {}_x\mathcal{E}_y^{\mathcal{T}} \longrightarrow F$$

is surjective. In particular, ${}_x\mathcal{E}_y^{\mathcal{T}} \neq 0$. By universality (i.e. Yoneda), ${}_x\mathcal{E}_y^{\mathcal{T}} = \mathrm{Hom}(\omega_x, \omega_y) = H_{x,y}^*$, so $H_{x,y} \neq \emptyset$ which means $\pi_1(\mathcal{T}; x, y) = \mathrm{Spec}\, H_{x,y} \neq \emptyset$. ∎

9 Lecture 10 (2/23): Étale $\mathbb{Q}_p$-local systems

9.1 Course Announcements

- Class on March 7,9 will be bonus lectures on Grothendieck's anabelian programme
- OHs today on Grothendieck's ℓ-adic monodromy theorem, purity, and weight-monodromy
- next week OHs: Bloch-Kato Selmer groups?

9.2 Today's material

Plan to define $\pi_1^{\mathbb{Q}_p}(X_{\overline{K}})$:

(i) Define a category of unipotent "local systems" on $X_{\overline{K}}$

(ii) Extract from this category a pro-unipotent groupoid (via Tannakian formalism)

What is a local system on a scheme X?

(Idea 0) local systems on the underlying topological space X_{zar}

This is a bad idea.

(Idea 1) local system (= `locally constant sheaf`) on $X_{\text{ét}}$, i.e. a sheaf $\mathscr{F} : X_{\text{ét}}^{\text{op}} \to \text{Set}$ such that there exists an étale cover $\{U_i \to X\}_{i \in I}$ for which $\mathscr{F}|_{U_i}$ is the constant sheaf associated to some set/abelian group/vector space/etc. for all i.

This is better, but still not ideal. Here's one example of something we want to be a local system. Take $K = \mathbb{Q}, \mathbb{Q}_p, \ldots$, $X = \operatorname{Spec} K$, and define $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$ (μ_{p^n} a sheaf on $X_{\text{ét}}$). We would like this to be a "local system of $\mathbb{Z}_p$-modules." However, this is not locally constant. μ_{p^n} is locally constant, trivialized over $\operatorname{Spec} K(\mu_{p^n}) \to \operatorname{Spec} K$, but there's no single finite, separable field extension L/K over which all of these trivialize.

Remark 9.1 (Pedantic). Actually, $\varprojlim_n \mu_{p^n} = 0$ in $X_{\text{ét}}$ because $(\varprojlim_n \mu_{p^n})(\operatorname{Spec} L) = \varprojlim_n \mu_{p^n}(L) = 0$ since $\mu_{p^\infty}(L)$ is finite. ∘

Global sections is a right adjoint (to the constant sheaf functor), and so preserves limits

We'll fix things by carefully defining our way out of the problem.

Definition 9.2.

(1) A $\mathbb{Z}/p^n\mathbb{Z}$`-local system` on $X_{\text{ét}}$ is a locally constant sheaf of finite $\mathbb{Z}/p^n\mathbb{Z}$-modules, i.e. a sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules, locally on $X_{\text{ét}}$ isomorphic to the constant sheaf attached to a finite $\mathbb{Z}/p^n\mathbb{Z}$-module.

(2) A $\mathbb{Z}_p$`-local system` on $X_{\text{ét}}$ is a diagram

$$\ldots \longrightarrow E_3 \longrightarrow E_2 \longrightarrow E_1$$

where each E_n is a $\mathbb{Z}/p^n\mathbb{Z}$-local system on $X_{\text{ét}}$, each map $E_n \to E_{n-1}$ is $\mathbb{Z}/p^n\mathbb{Z}$-linear and induces an isomorphism

$$\mathbb{Z}/p^{n-1}\mathbb{Z} \otimes_{\mathbb{Z}/p^n\mathbb{Z}} E_n \xrightarrow{\sim} E_{n-1}$$

(the LHS is "$E_n/(p^{n-1}E_n)$").

Example 9.3. $\mathbb{Z}_p(1)$ is the local system represented by

$$\ldots \longrightarrow \mu_{p^3} \longrightarrow \mu_{p^2} \longrightarrow \mu_p.$$ △

Notation 9.4. If E is a $\mathbb{Z}_p$-local system, we'll write $E = \text{"}\varprojlim_n\text{"} E_n$.

(3) A $\mathbb{Q}_p$`-local system` on $X_{\text{ét}}$ is a formal symbol $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} E$ for E a $\mathbb{Z}_p$-local system. The `morphisms of` $\mathbb{Q}_p$`-local systems` are given by

$$\operatorname{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes E_1, \mathbb{Q}_p \otimes E_2) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \operatorname{Hom}_{\mathbb{Z}_p}(E_1, E_2).$$

Morphisms of $\mathbb{Z}_p$-local systems are what you'd expect, i.e. commutative diagrams of $\mathbb{Z}/p^n\mathbb{Z}$-linear maps between corresponding objects in the respective diagrams.

(4) $\mathbb{Q}_p$-local systems form a pre-Tannakian category $/\mathbb{Q}_p$. We say a $\mathbb{Q}_p$-local system E is `unipotent` just when there exists a filtration

$$0 = \operatorname{Fil}_{-1} E \leq \operatorname{Fil}_0 E \leq \cdots \leq \operatorname{Fil}_m E = E$$

by $\mathbb{Q}_p$-local systems such that the associated graded pieces $\mathrm{Fil}_i E/\mathrm{Fil}_{i-1} E \cong \underline{\mathbb{Q}}_p^{\oplus r_i}$ for all i (Here, $\underline{\mathbb{Q}}_p = \mathbb{Q}_p \otimes_{\mathbb{Z}_p}$ "$\varprojlim_n$"$(\underline{\mathbb{Z}/p^n\mathbb{Z}}_X)$. The category of unipotent $\mathbb{Q}_p$-local systems is all pre-Tannakian over $\mathbb{Q}_p$, which we denote $\mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}(X_{\text{ét}})$. ◇

Remark 9.5.

(1) The above given definition of $\mathbb{Q}_p$-local system is not always the correct one. It is the correct definition when X is smooth over a field. The issue in general (e.g. on singular varieties) is that the definition given here does not always glue. Definition **(3)** above is sometimes referred to as an "isogeny $\mathbb{Z}_p$-local system."

(2) Nowadays, there is an alternative definition of $\mathbb{Q}_p$-local systems, as genuine sheaves of modules under a sheaf of rings, using the pro-étale site of Bhatt-Scholze.

Question 9.6 (Audience). *What is this sheaf of rings, is it not just the constant sheaf attached to $\mathbb{Q}_p$?*

Answer. They first define $\widehat{\mathbb{Z}}_p := \varprojlim_n \left(\underline{\mathbb{Z}/p^n\mathbb{Z}}_{X_{\text{pro-ét}}}\right)$, which is *not* $\underline{\mathbb{Z}_p}_{X_{\text{pro-ét}}}$. A $\mathbb{Z}_p$-local system will then be certain sheaves of $\widehat{\mathbb{Z}}_p$-modules. ⋆

○

To define $\pi_1^{\mathbb{Q}_p}(X_{\overline{K}})$, we still need some fiber functors.

Construction 9.7. Let x be a geometric point of X. If $E = \mathbb{Q}_p \otimes$ "$\varprojlim_n E_n$" is a $\mathbb{Q}_p$-locally stem on X, we define

$$E_x := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n E_{n,x}$$

($E_{n,x}$ is the stalk of E_n at x). This defines a fibre functor

$$\omega_x^{\text{ét}} : \mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}(X_{\text{ét}}) \longrightarrow \mathrm{FinVect}_{\mathbb{Q}_p}. \qquad \bigcirc$$

Definition 9.8. Let Y be a smooth variety over a characteristic zero field K, and let x, y be two geometric points of $Y_{\overline{K}}$. Define the $\mathbb{Q}_p$-pro-unipotent étale path space

$$\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)$$

to be the Tannakian path-space $\pi_1(\mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}(Y_{\overline{K},\text{ét}}); \omega_x^{\text{ét}}, \omega_y^{\text{ét}})$. ◇

These together form a groupoid in affine $\mathbb{Q}_p$-schemes, whose vertices are the geometric points of $Y_{\overline{K}}$.

Remark 9.9. The groupoid $\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}})$ is pro-unipotent. Suppose for simplicity that $Y_{\overline{K}}$ is connected ($\implies \mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}(Y_{\overline{K},\text{ét}})$ is neutral Tannakian, so equivalent to $\mathrm{Rep}_{\mathbb{Q}_p}(\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x))$). By definition, all objects are unipotent (i.e. have filtration w/ trivial graded pieces), so all $\mathbb{Q}_p$-representations of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x)$ are unipotent, but this was our definition of being pro-unipotent. ○

To end, let's convince ourselves that this Tannakian definition of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}})$ agrees w/ the earlier definition using Malčev completion.

Lemma 9.10 (Descent for finite étale coverings)**.** *Let X be a scheme. Then, the functor*

$$\begin{array}{ccc} F\acute{E}t(X) & \longrightarrow & \{\textit{locally constant sheaves of finite sets on } X_{\acute{e}t}\} \\ (X' \to X) & \longmapsto & \mathrm{Hom}_X(-, X') \end{array}$$

is an equivalence.

Ideas in the proof

(1) Why is $\mathrm{Hom}_X(-, X')$ a locally constant sheaf of finite sets?

Assume for simplicity that $X' \to X$ has degree 2. Consider the diagonal

$$\begin{array}{ccc} X' & \xrightarrow{\Delta} & X' \times_X X' \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

By cancellation (+ properness/étaleness of $X' \to X$), $X' \to X' \times_X X'$ is finite étale, a closed immersion, and an open immersion. Let $X'' = X' \times_X X' \setminus \Delta(X')$, still finite étale over X. This is surjective (any point of X has two distinct geometric lifts). Now, $X' \times_X X'' \cong X'' \times \{1, 2\}$ over X''. To convince yourself of this, stare at the diagram

$$\begin{array}{ccc} X' \times_X X'' & \longrightarrow & X' \\ \circlearrowleft \downarrow & \nearrow & \downarrow \\ X'' & \longrightarrow & X \end{array}$$

(Keep in mind the two maps $X'' \rightrightarrows X'$ never agree). Hence, $\mathrm{Hom}_X(-, X')|_{X''}$ is constant.

(2) If $\mathscr{F}$ is a locally constant sheaf of finite sets, trivialized over $\{U_i \to X\}_i$, then $\mathscr{F}|_{U_i}$ is represented by a finite étale covering $V_i \to U_i$. The sheaf condition for $\mathscr{F}$ gives descent datum for the V_i's, i.e. isomorphisms

$$\varphi_{ij} : \pi_j^* V_j \xrightarrow{\sim} \pi_i^* V_i \text{ for } \pi_i : U_{ij} = U_i \times_X U_j \to U_i$$

which satisfy the cocycle condition. This descent datum is effective because the covers are finite (so affine, so can glue sheaves instead, see e.g. [SGA1, IX, 4.9]).

Corollary 9.11. *Let X be connected. We have equivalences of $\otimes$-categories*

$$\left\{ \begin{array}{c} \mathbb{Z}/p^n\mathbb{Z}\text{-local systems} \\ \text{on } X_{\acute{e}t} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{continuous representations} \\ \text{of } \pi_1^{\acute{e}t}(X; x) \text{ on finite } \mathbb{Z}/p^n\mathbb{Z}\text{-modules} \end{array} \right\}$$

and

$$\{\mathbb{Z}_p\text{-local systems}\} \longleftrightarrow \left\{ \begin{array}{c} \text{continuous representations of } \pi_1^{\acute{e}t}(X; x) \\ \text{on f.generated } \mathbb{Z}_p\text{-modules} \end{array} \right\}$$

and

$$\{\mathbb{Q}_p\text{-local systems}\} \longleftrightarrow \left\{ \begin{array}{c} \text{continuous representations of } \pi_1^{\acute{e}t}(X; x) \\ \text{on f.dim } \mathbb{Q}_p\text{-vector spaces} \end{array} \right\}$$

Proof for first part. We know

$$\left\{ \begin{array}{c} \text{locally constant sheaves} \\ \text{of finite sets} \end{array} \right\} \leftrightarrow \mathrm{F\acute{E}t}(X) \leftrightarrow \left\{ \begin{array}{c} \text{finite sets w/ a} \\ \text{continuous } \pi_1^{\acute{e}t}(X; x)\text{-action} \end{array} \right\}.$$

This induces equivalences between the $\mathbb{Z}/p^n\mathbb{Z}$-modules in each of the categories on the ends. ∎

So we know (assuming $Y_{\overline{K}}$ is connected)

$$\mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}(Y_{\overline{K}}) \simeq \mathrm{Rep}^{\mathrm{un}}_{\mathbb{Q}_p}(\pi_1^{\acute{\mathrm{e}}\mathrm{t}}(Y_{\overline{K}}; x))$$

(w/ fiber functor at x on LHS corresponding to the forgetful functor on the RHS). Hence, to show our definitions are equivalence, we want to show

Lemma 9.12. *Let Π be a profinite group, and let $\mathcal{T} = \mathrm{Rep}^{\mathrm{un}}_{\mathbb{Q}_p}(\Pi)$ (category of continuous unipotent $\mathbb{Q}_p$-linear representations). Write $\omega_x : \mathcal{T} \to \mathrm{Vect}_{\mathbb{Q}_p}$ for the forgetful functor. Then,*

$$\pi_1(\mathcal{T}; x) \simeq \Pi_{\mathbb{Q}_p},$$

i.e. the Tannakian fundamental group is (canonically) isomorphic to the Malčev completion.

Proof. For any m, we have a bijection between {continuous group homomorphism $\Pi \to \mathrm{Un}_m(\mathbb{Q}_p)$} and {algebraic group homomorphisms $\Pi_{\mathbb{Q}_p} \to \mathrm{Un}_m$}, so

$$\mathrm{Rep}^{\mathrm{un}}_{\mathbb{Q}_p}(\Pi) \simeq \mathrm{Rep}^{\mathrm{un}}_{\mathbb{Q}_p}(\Pi_{\mathbb{Q}_p}) = \mathrm{Rep}_{\mathbb{Q}_p}(\Pi_{\mathbb{Q}_p})$$

(compatible w/ forgetful functors). Taking Tannakian π_1 gives the statement we want. ∎

10 Office Hours

Note 6. Only started taking notes like 20 minutes in, so missing notes on a question in the beginning on why unipotent is enough for controlling arithmetic

Question 10.1 (Audience)**.** *What is weight, e.g. when we write $\mathbb{Q}_p(0)$ or $V_i^*(1)$?*

Let $K/\mathbb{Q}_p$ be a finite extension. Let V be a continuous G_K-rep on a f.dim $\mathbb{Q}_p$-vector space.

Assumption. Assume V is unramified, i.e. $I_K \trianglelefteq G_K$ acts trivially. Hence, the G_K actions factors through $G_K/I_K \simeq G_k \cong \widehat{\mathbb{Z}}$ (topologically generated by geometric Frobenius φ_k), with k the residue field.

Definition 10.2. Set $q = \#k$. A *q-Weil number of weight n* in some field of characteristic 0 is an element α such that $|\iota(\alpha)| = q^{n/2}$ for all $\iota : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$. An unramified representation V is called *pure of weight n* just when all the (generalized) eigenvalues of (geometric) Frobenius φ_k are q-Weil numbers of weight n. ◇

Example 10.3. Consider $\mathbb{Q}_p(1) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n \mu_{p^n}(\overline{K})$. Arithmetic Frobenius acts on $\mu_{p^n}(\overline{K})$ by $x \mapsto x^q$, so acts on $\mathbb{Q}_p(1)$ by $x \mapsto qx$. Hence, the *geometric* Frobenius acts via $\varphi_K(x) = q^{-1}x$. q^{-1} is a q-Weil number of weight -2, so $\mathbb{Q}_p(1)$ is pure of weight -2. △

Remember: $\mathbb{Q}_p(1)$ is pure of weight -2

Remark 10.4. $\mathbb{Q}_p(-1) = \mathrm{H}^2_{\text{ét}}(\mathbb{P}^1, \mathbb{Q}_p)$ is "cohomological" and so should be given a nonnegative weight. ○

Example 10.5. Suppose X/K is smooth, projective and has good reduction. Then, $\mathrm{H}^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is unramified and pure of weight i (Deligne). △

Non-example. Say E/K an elliptic curve, and consider its p-adic Tate module

$$T_pE := \varprojlim_n E[p^n](\overline{K}) \curvearrowleft G_K \text{ and } V_pE = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_pE.$$

Note $V_pE \cong \mathrm{H}^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p)^*$. Hence, this is unramified if E has good reduction, and then V_pE is pure of weight -1. What if E has bad reduction? Say E has split multiplicative reduction.

Theorem 10.6 (Tate)**.** *$E(\overline{K}) \cong \overline{K}^\times / r^{\mathbb{Z}}$ for some $r \in \mathfrak{m}_K \setminus \{0\}$.*

In particular, we can work out that we have

$$0 \longrightarrow \mu_{p^n}(\overline{K}) \longrightarrow E[p^n](\overline{K}) \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

(First map coming from $\overline{K}^\times \to E(\overline{K})$ the natural quotient, and generator of cokernel represented by r^{1/p^n}). Everything above is Galois equivariant. Taking limits, we get

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow T_pE \longrightarrow \mathbb{Z}_p(0) \longrightarrow 0$$

(and similarly after tensoring with $\mathbb{Q}_p$). We see from this that the eigenvalues of φ_k acting on V_pE are $1, q^{-1}$. These are both Weil numbers, but of different weights $(0, -2)$. Note that these number average to -1. ▽

The previous example shows that our definition of 'pure of weight n' is poorly suited to cohomology of varieties w/ bad reduction.

10.1 Grothendieck's ℓ-adic monodromy theorem

Say $K/\mathbb{Q}_\ell$ is a finite extension. Let V be a $\mathbb{Q}_p$-linear representation of G_K, where $p \neq \ell$.

Theorem 10.7 (Grothendieck's ℓ-adic Monodromy Theorem)**.** *There exists a finite index open subgroup $I_L \leq I_K$ inside the inertia group of K which acts unipotently on V.*

(Exercise b/c low on time)

Exercise Solution (added after the fact). (Disclaimer: this is not the most efficient route to proving this, but oh well)

We will prove the claim via a series of reductions. In a sense, we will work our way down the following tower of field extensions. Let k denote the size of the K's residue field.

$$\begin{array}{ccc}
\overline{K} & & \\
\Big| P_K & & \\
K^t & = & K^{\mathrm{un}}\big(\sqrt[m]{\pi} : m \nmid \ell\big) \\
\Big| \cong \prod_{r\neq \ell,p} \mathbb{Z}_r & & \\
L & = & K^{\mathrm{un}}\big(\sqrt[p^n]{\pi} : n \geq 1\big) \\
\Big| \cong \mathbb{Z}_p & & \\
K^{\mathrm{un}} & = & K(\zeta_{k^n-1} : n \geq 1) \\
\Big| \widehat{\mathbb{Z}} & & \\
K. & &
\end{array} \qquad I_K$$

Let $\rho : G_K \to \mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{Q}_p)$ be the representation under consideration. Note that the inertia group I_K sits in an exact sequence

$$0 \longrightarrow P_K \longrightarrow I_K \longrightarrow I_K^t \longrightarrow 0$$

with P_K wild inertia and I_K^t tame inertia. Furthermore, $I_K^t \cong \prod_{r\neq\ell} \mathbb{Z}_r$.

(1) Reduce to ρ being tame.

Note that the wild inertia group P_K is pro-ℓ. At the same time, G_K is compact, so by considering the open covering $\mathrm{GL}_n(\mathbb{Q}_p) = \bigcup_{m\geq 0} p^{-m}\,\mathrm{GL}_n(\mathbb{Z}_p)$, we see that $\rho(G_K) \subset p^{-m}\,\mathrm{GL}_n(\mathbb{Z}_p)$ for some

m.[12] Thus, up to composing with the (injective) multiplication by p^m map, we may assume that ρ lands in $\mathrm{GL}_n(\mathbb{Z}_p)$. We next note that $\mathrm{GL}_n(\mathbb{Z}_p)$ breaks apart as

$$1 \longrightarrow I + p\,\mathrm{End}(\mathbb{Z}_p^n) \longrightarrow \mathrm{GL}_n(\mathbb{Z}_p) \longrightarrow \mathrm{GL}_n(\mathbb{F}_p) \longrightarrow 1,$$

with pro-p kernel $I + p\,\mathrm{End}(\mathbb{Z}_p^n)$. Thus, $\rho(P_K) \cap I + p\,\mathrm{End}(\mathbb{Z}_p^n)$ is trivial (both pro-p and pro-ℓ), so $\rho(P_K) \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)$ is finite. Since we are only interested in finding a finite index subgroup which acts unipotently, we can pass to a finite field extension (corresponding to $\ker \rho|_{P_K}$) in order to assume that $P_K \subset \ker \rho$.

(2) Assume ρ is tame (i.e. ρ factors through G_{K^t}). We next reduce to the case that ρ factors through G_L.

Note that $\mathrm{Gal}(K^t/L) \cong \prod_{r \neq \ell, p} \mathbb{Z}_r$, and temporarily fix some prime $r \neq p, \ell$. By the same argument as in **(1)**, the map

$$\mathbb{Z}_r \hookrightarrow \mathrm{Gal}(K^t/L) \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{Q}_p)$$

has finite image, so factors through $\mathbb{Z}_r/r^m\mathbb{Z}_r$ for some $m = m_r \geq 0$. Hence, given $a \in \mathbb{Z}_r$, $\rho(a) \in \mathrm{GL}_n(\mathbb{Q}_p)$ acts by a matrix, all of whose eigenvalues are roots of unity. By considering the characteristic polynomial of $\rho(a)$, we must in fact have that all of its eigenvalues are roots of unity which are of degree $\leq n$ over $\mathbb{Q}_p$. This means that all eigenvalues of $\rho(a)$ must be Nth roots of unity for some number N which is independent of r. Thus, if $r \gg 0$ (e.g. $r > N$ so $r \nmid N$), then, since the eigenvalues of $\rho(a)$ must be Nth roots of unity and r^mth roots of unity, all the eigenvalues of $\rho(a)$ must be 1, i.e. a must act unipotently. That is, $\rho|_{\mathrm{Gal}(K^t/L)}$ factors through the finite quotient

$$\prod_{\substack{r \text{ prime} \\ r \neq \ell.p \\ r \leq N}} \mathbb{Z}_r/r^{m_r}\mathbb{Z}_r,$$

so can pass to a finite field extension in order to assume that $\mathrm{Gal}(K^t/L) \subset \ker \rho$.

(3) Assume ρ factors through G_L. We'll produce a finite index subgroup of inertia which acts unipotently.

Let $G = \mathrm{Gal}(L/K)$, so G is an extension

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow G \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0,$$

with the $\mathbb{Z}_p$ being its inertia subgroup. Let $a \in \mathbb{Z}_p$ be a generator, written multiplicatively. We only need to show there's some $N \geq 1$ so that a^N acts unipotently. Note that $a \in \mathrm{Gal}(L/K)$ acts via

$$a\left(\sqrt[p^n]{\pi}\right) = \zeta_{p^n}\sqrt[p^n]{\pi}$$

for some compatible system $(\zeta_{p^n})_n$ of primitive p^nth roots of unity. Let $F \in \widehat{\mathbb{Z}}$ be arithmetic Frobenius, i.e. $F(\zeta) = \zeta^k$ for any mth root of unity ζ for any m coprime to ℓ.

Lemma 10.8. *The conjugation action $\widehat{\mathbb{Z}} \curvearrowright \mathbb{Z}_p$ of this extension is given by*

$$FaF^{-1} = a^k$$

(where k is the cardinality of K's residue field).

This holds already for the conjugation action of $\widehat{\mathbb{Z}} \curvearrowright \prod_{r \neq \ell} \mathbb{Z}_r \cong I_K^t$ w/ the same proof, so step **(2)** was secretly unnecessary.

[12] In fact, $\rho(G_K)$ will be contained in some conjugate of $\mathrm{GL}_n(\mathbb{Z}_p)$ e.g. via [BC, Lemma 1.2.6]

Proof. Let $F \in G = \mathrm{Gal}(L/K)$ denote an arbitrary lift of $F \in \widehat{\mathbb{Z}}$. Then, for every n, there is some (not necessarily primitive) p^nth root of unity $\beta_n \in K^{\mathrm{un}}$ such that

$$F\left(\sqrt[p^n]{\pi}\right) = \beta_n \sqrt[p^n]{\pi},$$

and these furthermore must satisfy $\beta_n^p = \beta_{n-1}$. With this in mind, we compute

$$FaF^{-1}\left(\sqrt[p^n]{\pi}\right) = Fa\left(\beta_n^{-1/k} \sqrt[p^n]{\pi}\right) = F\left(\beta_n^{-1/k}\zeta_{p^n} \sqrt[p^n]{\pi}\right) = \zeta_{p^n}^k \sqrt[p^n]{\pi} = a^k\left(\sqrt[p^n]{\pi}\right). \qquad \blacksquare$$

Now, we're in luck. The Lemma tells us that $\rho(a)$ is conjugate to $\rho(a^k)$, so the two matrices have the same eigenvalues! In other words, in E is the set of eigenvalues of $\rho(a)$, then the map

$$\begin{array}{rccc} \sigma: & E & \longrightarrow & E \\ & \lambda & \longmapsto & \lambda^k \end{array}$$

is a bijection. By group theory, the composition $\sigma^{n!}$ must then be the identity, i.e. $\lambda^{k^{n!}} = \lambda$ for all $\lambda \in E$. Let $N := k^{n!} - 1$. We have just seen that every eigenvalue of $\rho(a)$ is a Nth root of unity, so $\langle a^N \rangle \subset \mathbb{Z}_p$ is a finite index subgroup of inertia acting unipotently on V. $\blacksquare$

Let's use this to give the general definition of purity. Pick some $\sigma \in I_K$ which acts unipotently on V, and assume $\sigma \notin W_K$ (wild inertia). Define $N = \log \sigma \in \mathrm{End}(V)$ (the monodromy operator). This satisfies

$$N\varphi_K = q^{\pm 1} \cdot \varphi_K N.$$

Let V_i denote the largest subspace of V on which φ_K acts w/ generalized eigenvalues of weight i. The above condition implies that $N : V_i \to V_{i-2}$ (this being a -2 will tell you the correct sign above).

Definition 10.9. We say that V is pure of weight n iff both

- $V = \bigoplus_i V_i$, i.e. every eigenvalue of φ_k is a q-Weil number; and
- For all $i \geq 0$, $N^i : V_{n+i} \longrightarrow V_{n-i}$ should be an isomorphism. $\diamond$

Remark 10.10.

(1) If E/K is an elliptic curve w/ split multiplicative reduction, then $N \neq 0$. It maps $\mathbb{Q}_p(0)$ to $\mathbb{Q}_p(1)$ in the extension

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow V_pE \longrightarrow \mathbb{Q}_p(0) \longrightarrow 0.$$

From this, one sees that V_pE is pure of weight -1.

(2) If X/K is smooth + projective, then $\mathrm{H}^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is pure of weight i for $i = 0, 1, 2, 2\dim X - 2, 2\dim X - 1, 2\dim X$. $\circ$

Conjecture 10.11 (Weight-Monodromy Conjecture)**.** ***(2)*** *above should hold for all i.*

11 Lecture 11 (2/28): Galois action on the fundamental groupoid

Note 7. Like 7 minutes late

Admistrative stuff

- OH on Thursday on Bloch-Kato Selmer groups

- Next week bonus lectures instead of normal ones

So far: We have defined the $\mathbb{Q}_p$-pro-unipotent étale fundamental groupoid of a scheme/smooth variety in 2 ways

- As $\mathbb{Q}_p$-Malčev completion of profinite étale fundamental groupoid
- as the Tannakian groupoid of $\mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}(X_{\text{ét}})$, category of unipotent $\mathbb{Q}_p$-local systems

We are interested in the following setup

Setup 11.1. K a field of characteristic 0 w/ algebraic closure $\overline{K}$. Y/K a smooth variety and $x, y \in Y(K)$. We'll be interested in $\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)$. Note that G_K acts on $(Y_{\overline{K}}; x, y)$.

Remark 11.2. Everything we've constructed has been functorial in morphisms of 2-pointed schemes, even if we haven't been explicitly mentioning this. This is where the action $G_K \curvearrowright \pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)$ comes from (since Y, x, y all defined over K). ∘

Today we want to discuss properties of this Galois action, e.g. related to continuity, unramifiedness, and purity.

11.1 Continuity

(Recall we typically work within the context of Setup 11.1)

Theorem 11.3.

$$\mathrm{Lie}\left(\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x)\right) \quad \textit{and} \quad \mathbb{Q}_p\left[\!\left[\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)\right]\!\right]$$

are both pro-continuous representations of G_K, i.e. cofiltered limits of f.dim continuous G_K-reps.

Corollary 11.4. *Suppose Λ is a $\mathbb{Q}_p$-algebra. Endow Λ w/ the colimit topology of the natural topology on its f.dim $\mathbb{Q}_p$-subspaces (i.e. view $\Lambda = \mathbb{Q}_p^{\oplus I}$). This topology makes Λ into a topological ring, and also puts a natural topology on $Z(\Lambda)$ for any affine $\mathbb{Q}_p$-scheme Z. With all this in place, the action of G_K on $\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)(\Lambda)$ is continuous for all Λ.*

Proof of Continuity (Theorem 11.3). We will show that the action of G_K on $\pi_1^{\text{ét}}(Y_{\overline{K}}; x, y)$ (the usual profinite étale fundamental group) is continuous. Let's first unpack the definition of the G_K-action. Note that G_K naturally acts on $\mathrm{FÉt}(Y_{\overline{K}})$ via pullback, i.e. $\sigma \in G_K$ sends a finite, étale covering $Y' \to Y_{\overline{K}}$ to $\sigma^*(Y') \to Y_{\overline{K}}$ defined as the fiber product

$$\begin{array}{ccc} \sigma^*(Y') & \longrightarrow & Y' \\ \downarrow & \ulcorner & \downarrow \\ Y_{\overline{K}} & \xrightarrow{\sigma} & Y_{\overline{K}}. \end{array}$$

Warning 11.5. $\sigma^*(Y')$ is isomorphic to Y' as schemes, but not as $Y_{\overline{K}}$-schemes. •

For any K-rational point $x \in Y(K)$, we have a canonical identification $\sigma^*(Y')_x = Y'_x$ since x is defined over K. Thus, given a natural transformation $\gamma : \omega_x^{\text{ét}} \to \omega_y^{\text{ét}}$, we can define $\sigma(\gamma) : \omega_x^{\text{ét}} \to \omega_y^{\text{ét}}$ to be the natural transformation with components

$$\sigma(\gamma)_{Y'} := \gamma_{\sigma^*(Y')}.$$

That is, we have a commutative diagram

$$\begin{array}{ccc} \sigma^*(Y')_x & \xrightarrow{\gamma_{\sigma^*(Y')}} & \sigma^*(Y')_y \\ \| & & \| \\ Y'_x & \xrightarrow{\sigma(\gamma)_{Y'}} & Y'_y. \end{array}$$

This describes the action of G_K on $\pi_1^{\text{ét}}(Y_{\overline{K}}; x, y) = \text{Hom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}})$. Why is it continuous?

Fix a covering $Y' \to Y_{\overline{K}}$. There will exist s a finite extension L/K instead $\overline{K}$ along with a finite étale covering $Y'_0 \to Y_L$ defined over L, so that $Y' \to Y_{\overline{K}}$ is the base change of $Y'_0 \to Y_L$. Enlarging L if necessary, we may assume wlog that the fibers of Y'_0 over x, y split completely over L. This implies that there exists an isomorphism $Y' \xrightarrow{\sim} \sigma^*(Y')$ in $\text{FÉt}(Y_{\overline{K}})$ whenever $\sigma \in G_L$ (because Y' defined over L); furthermore, this isomorphism will induce the identity on $Y'_x = \sigma^*(Y')_x$ (and similarly for y). If $\sigma \in G_L$ and $\gamma \in \pi_1^{\text{ét}}(Y_{\overline{K}}; x, y)$, then $\gamma_{Y'} = \gamma_{\sigma^*(Y')} = \sigma(\gamma)_{Y'}$, so the fibers of the map

$$\pi_1^{\text{ét}}(Y_{\overline{K}}; x, y) \longrightarrow \text{Hom}(Y'_x, Y'_y)$$

are stable under G_L. These fibers are basic open (see Section 4.1), so for every basic open subset of $\pi_1^{\text{ét}}(Y_{\overline{K}}; x, y)$, there is an open subgroup of G_K fixing it setwise. From this, basic topology will tell us that G_K acts continuous on $\pi_1^{\text{ét}}(Y_{\overline{K}}; x, y)$.

How do we get the corresponding statement for $\pi_1^{\mathbb{Q}_p}$? From the Malčev perspective, use

$$\mathbb{Q}_p\left[\!\left[\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)\right]\!\right] = \mathbb{Q}_p\left[\!\left[\pi_1^{\text{ét}}(Y_{\overline{K}}; x, y)\right]\!\right]$$

(See Section 6.1.1). ■

Recall 11.6.

- If U is an affine group scheme over $\mathbb{Q}_p$, we set

$$\mathbb{Q}_p[\![U]\!] := \mathscr{O}(U)^*,$$

  the dual of the ring of functions.

- If Π is finitely generated profinite, we set

$$\mathbb{Z}_p[\![\Pi]\!] := \varprojlim_{N \overset{\text{open}}{\trianglelefteq} \Pi} \mathbb{Z}_p[\Pi/N] \quad \text{and} \quad \mathbb{Q}_p[\![\Pi]\!] := \text{“}\varprojlim_n\text{”}\left(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![\Pi]\!]/I^n\right).$$

If $x \neq y$, the definitions are a bit more technical. The above definitions can be generalized to only using groupoid structure. ⊙

11.2 Unramifiedness

Assumption. Now assume $K/\mathbb{Q}_p$ a finite extension. Let $I_K \trianglelefteq G_K$ denote the inertia subgroup.

Theorem 11.7. *Fix a prime $\ell \neq p$. If Y is smooth, proper and has good reduction, then the action of G_K on the path scheme $\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)$ is unramified for all $x, y \in Y(K)$, i.e. I_K acts trivially.*

More generally, suppose Y is the generic fiber of some $\mathcal{Y}/\mathscr{O}_K$ where $\mathcal{Y} = \mathcal{X} \setminus \mathcal{D}$ for $\mathcal{X}$ smooth, proper over $\mathscr{O}_K$ and $\mathcal{D}$ a relative normal crossings divisor. In this case, the G_K-action on $\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)$ is unramified for all $x, y \in \mathcal{Y}(\mathscr{O}_K)$.

Example 11.8. Take $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_\ell}$ and $\mathcal{D} = \{-1, 0, 1, \infty\}$. This is relative normal crossings when $\ell \neq 2$ (when $\ell = 2$, $-1, 1$ reduce to the same point). Let $\mathcal{Y} = \mathcal{X} \setminus \mathcal{D}$ ad $Y = \mathcal{Y}_{\mathbb{Q}_\ell}$. Then, $\pi_1^{\text{ét}}(Y_{\overline{\mathbb{Q}}_\ell}; -2, 2)$ is unramified when $\ell \geq 5$ (when $\ell = 3$, $2 \equiv -1 \pmod 3$, so 2 won't be an integral point). △

Remember: For curves, relative normal crossings is being étale over the base

In the interest of time, we won't prove this theorem.

Remark 11.9.

(1) There is much more that can be said about the connection between reduction types and ramification of the Galois action: see e.g. Oda, Asada-Matsumoto-Oda, Betts-Dogra

(2) There is also an $\ell = p$ version of this theorem.

Theorem 11.10 (Sketch). *Suppose $\ell = p$. Then, $\mathbb{Q}_p\left[\!\left[\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x, y)\right]\!\right]$ is also pro-de Rham, and is moreover pro-crystalline when "$(Y; x, y)$ has good reduction".*

There is a converse theorem here due to Andreatta-Iovita-Kim. ○

11.3 Purity

Assumption. Now let K be a finite extension of $\mathbb{Q}_\ell$, $\ell \neq p$. Let k be the residue field, and set $q = \#k$.

Definition 11.11. A `q-Weil number of weight` n in some (characteristic 0) field is an element α, algebraic over $\mathbb{Q}$, such that $|i(\alpha)| = q^{n/2}$ for all complex embeddings $\iota : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$. ◇

Definition 11.12. An unramified G_K-rep is called `pure of weight` n just when all eigenvalues of *geometric* Frobenius are q-Weil numbers of weight n. ◇

(There is a more general definition of purity for ramified reps, see lecture notes and/or Definition 10.9)

Example 11.13.

(1) $\mathbb{Q}_p(1)$ is pure of weight -2 (arithmetic Frobenius has eigenvalue p, so geometric frobeinus has eigenvalue $p^{-1} = p^{(-2)/2}$).

(2) If Y/K is smooth, projective and of good reduction, then $\mathrm{H}^i_{\text{ét}}(Y_{\overline{K}}, \mathbb{Q}_p)$ is unramified and pure of weight i for all i (Deligne)

(3) Say Y/K smooth, proper. Then, $\mathrm{H}^i_{\text{ét}}(Y_{\overline{K}}, \mathbb{Q}_p)$ is potentially ramified, but will still be pure of weight i if $i = 0, 1, 2$ (Rapoport-Zink) or $i = 2\dim Y, 2\dim Y - 1, 2\dim Y - 2$ (use Poincaré duality)

Conjecture 11.14 (`Weight-Monodromy Conjecture`)**.** *Above pure of weight i for all i.*

(4) Say Y is a smooth curve, $Y = X \setminus D$ (X smooth, projective curve). Then, $\mathrm{H}^1_{\text{ét}}(Y_{\overline{K}}, \mathbb{Q}_p)$ is *not* usually pure. E.g. consider the Gysin sequence

$$0 \to \underbrace{\mathrm{H}^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)}_{\text{weight 1}} \to \mathrm{H}^1_{\text{ét}}(Y_{\overline{K}}, \mathbb{Q}_p) \to \underbrace{\mathrm{H}^0_{\text{ét}}(D_{\overline{K}}, \mathbb{Q}_p)(-1)}_{\text{weight 2}}$$

(note X, D both proper). In general, expect cohomology of smooth varieties to be mixed like this. △

Definition 11.15. Say Y/K is smooth. Write $Y = X \setminus D$ for X smooth + proper and $D \subset X$ a normal crossings divisor. Fix some $x \in Y(K)$. Write $\pi_1^{\mathbb{Q}_p} := \pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x)$. Definite a filtration

$$\pi_1^{\mathbb{Q}_p} = W_{-1}\pi_1^{\mathbb{Q}_p} \trianglerighteq W_{-1}\pi_1^{\mathbb{Q}_p} \trianglerighteq \dots$$

by $W_{-1}\pi_1^{\mathbb{Q}_p} = \pi_1^{\mathbb{Q}_p}$, $W_{-2}\pi_1^{\mathbb{Q}_p} = \ker\left(\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x) \to \pi_1^{\mathbb{Q}_p}(X_{\overline{K}}, x)^{\mathrm{ab}}\right)$, and

$$W_{-k}\pi_1^{\mathbb{Q}_p} := \left[\pi_1^{\mathbb{Q}_p}, W_{1-k}\pi_1^{\mathbb{Q}_p}\right] \cdot \left[W_{-2}\pi_1^{\mathbb{Q}_p}, W_{2-k}\pi_1^{\mathbb{Q}_p}\right] \text{ for } k \geq 3.$$

These are normal subgroup schemes, the graded pieces are all commutative, and the extensions

$$1 \longrightarrow \frac{W_{-k}}{W_{-k-1}} \longrightarrow \frac{\pi_1^{\mathbb{Q}_p}}{W_{-k-1}} \longrightarrow \frac{\pi_1^{\mathbb{Q}_p}}{W_{-k}} \longrightarrow 1$$

are all central. We call this the `weight filtration`. ◇

Think of this as a "weighted version of the descending central series."

Example 11.16. If Y is smooth and proper, then $W_{-k}\pi_1^{\mathbb{Q}_p} = \Gamma^k\pi_1^{\mathbb{Q}_p}$, so we simply recover the descending central series. In general, $\Gamma^k\pi_1^{\mathbb{Q}_p} \leq W_{-k}\pi_1^{\mathbb{Q}_p} \leq \Gamma^{\lfloor k/2 \rfloor}\pi_1^{\mathbb{Q}_p}$. △

Theorem 11.17 ("`Weight-Monodromy for` π_1"). *In the above setup (e.g. Y smooth, $K/\mathbb{Q}_\ell$ finite, $\ell \neq p$), the weight filtration is G_K-stable and*

$$\mathrm{gr}_{-k}^W \pi_1^{\mathbb{Q}_p}$$

($(-k)$th graded piece of the weight filtration) is pure of weight $-k$.

(The Galois stability is obvious. The content is in the purity)

Remark 11.18. There also is an $\ell = p$ version. ○

Sounds like the proof of this comes from knowing the result for H^1's and H^2's. Maybe a bit of this at the beginning of next time.

12 Lecture 12 (3/2): Galois action on the fundamental groupoid

Let K be a field of characteristic 0, Y/K smooth, $x \in Y(K)$, and $\pi_1 = \pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x)$.

Recall 12.1. Let $Y = X \setminus D$ with X smooth, proper and D a normal crossings divisor. The (increasing) *weight filtration* on π_1 is defined by $W_{-1}\pi_1 = \pi_1$, $W_{-2}\pi_1 = \ker\left(\pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x) \to \pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x)^{\mathrm{ab}}\right)$, and

$$W_{-k}\pi_1 = [W_{-1}\pi_1, W_{1-k}\pi_1] \cdot [W_{-2}\pi_1, W_{2-k}\pi_1]$$

for $k \geq 3$.

Theorem 12.2. *Suppose $K/\mathbb{Q}_\ell$ is finite. Then, $W_{-k}\pi_1$ is G_K-stable and $\mathrm{gr}_{-k}^W\pi_1$ is pure of weight $-k$ for all k.* ⊙

Let's start by giving an idea of the proof of Theorem 12.2 when $Y = X$ is a smooth projective curve. In this case, $W_{-k}\pi_1 = \Gamma^k\pi_1$ is simply a funny way of writing the descending central series. The proof here will be inductive.

- Start with the case $k = 1$, i.e. $\mathrm{gr}^1_\Gamma \pi_1 = \pi_1^{\mathrm{ab}}$.

  Theorem 12.3 (Hurewicz for the fundamental group)**.** *There exists a canonical, G_K-equivariant isomorphism*

  $$\pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x)^{ab} \cong \mathrm{H}^1_{\acute{e}t}(X_{\overline{K}}; \mathbb{Q}_p)^*.$$

  (there are at least two approaches to proving this, but we'll start with just one of them)

  Proof.

  (Step 1) Let $\mathcal{T}$ be a unipotent[13] neutral Tannakian category over some field F, and let ω_x be a fiber functor. Then, there exists a canonical isomorphism

  $$\pi_1(\mathcal{T}; x)^{\mathrm{ab}} \simeq \mathrm{Ext}^1_{\mathcal{T}}(\mathbf{1}, \mathbf{1})^*$$

  (in pro–Vect_F).
  By definition,

  $$\big(\pi_1(\mathcal{T}; x)^{\mathrm{ab}}\big)^* = \mathrm{Hom}\big(\pi_1(\mathcal{T}; x)^{ab}, \mathbb{G}_a\big) = \mathrm{Hom}(\pi_1(\mathcal{T}; x), \mathbb{G}_a)$$

  is simply the group of additive characters of π_1. We want this to be $\mathrm{Ext}^1_{\mathcal{T}}(\mathbf{1}, \mathbf{1})$. Given an extension

  $$0 \longrightarrow \mathbf{1} \longrightarrow E \longrightarrow \mathbf{1} \longrightarrow 0,$$

  get extension $0 \to F \to E_x \to F \to 0$ in the category $\mathrm{Rep}(\pi_1(\mathcal{T}; x))$. Thus, w.r.t. an appropriate basis, $\pi_1(\mathcal{T}, x)$ acts by matrices of the form

  $$\begin{pmatrix} 1 & \chi \\ 0 & 1 \end{pmatrix}$$

  for some $\chi : \pi_1(\mathcal{T}; x) \to \mathbb{G}_a$. This defines a map $\mathrm{Ext}^1_{\mathcal{T}}(\mathbf{1}, \mathbf{1}) \to \mathrm{Hom}(\pi_1(\mathcal{T}; x), \mathbb{G}_a)$. By reversing the argument, this map is bijective.

  (Step 2) $\mathrm{Ext}^1_{\mathrm{Loc}^{\mathrm{un}}_{\mathbb{Q}_p}}(\underline{\mathbb{Q}}_p, \underline{\mathbb{Q}}_p) \simeq \mathrm{H}^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$.
  Proof of this is omitted.

  The identifications in the above two steps are canonical/functorial/Galois-equivariant/nice adjectives/etc. ∎

  Corollary 12.4. *π_1^{ab} is pure of weight -1.*

- What about $k = 2$?

  Need to use that we know what π_1 looks like. It is the $\mathbb{Q}_p$-Malčev completion of the surface group

  $$\Sigma_g = \left\langle a_1, \ldots, a_g, b_1, \ldots, b_g \;\middle|\; \prod_{i=1}^{g} [a_i, b_i] = 1 \right\rangle.$$

  One can check by computation that there is an exact sequence

  $$0 \longrightarrow \mathbb{Z} \longrightarrow \bigwedge^2 \Sigma_g^{\mathrm{ab}} \longrightarrow \mathrm{gr}^2_\Gamma \Sigma_g \longrightarrow 0,$$

[13] every object is an iterated extension of $\mathbf{1}^{\oplus r_i}$'s

where the maps are

$$1 \mapsto \sum_{i=1}^{g} a_i \wedge b_i \text{ and } a \wedge b = [a, b].$$

Back in the setting of étale π_1, this is telling us that we have an exact sequence

$$0 \longrightarrow \mathbb{Q}_p(1) \xrightarrow{\cup^*} \bigwedge^2 \pi_1^{\mathrm{ab}} \longrightarrow \mathrm{gr}_\Gamma^2 \pi_1 \longrightarrow 0,$$

where $\cup^*$ is the dual of the cup product

$$\cup : \bigwedge^2 \mathrm{H}^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \longrightarrow \mathrm{H}^2_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) = \mathbb{Q}_p(-1).$$

We know $\mathbb{Q}_p(1)$ is pure of weight -2 and that $\bigwedge^2 \pi_1^{\mathrm{ab}}$ is pure of weight -2, so the quotient must be pure of weight -2 as well.

Question 12.5 (Audience)**.** *Does it follow easily from the definition of Malčev completion that it preserves exact sequences, or does that take some effort to check?*

Answer. Malčev completion doesn't preserve exact sequences in full generality, but it does preserve exact sequences of nilpotent groups. This is enough for us here. ⋆

- $k \geq 3$

  In general, we use the fact that the $\mathbb{Q}_p$-Malčev completion of Σ_g is the pro-unipotent group attached to the pro-nilpotent Lie algebra

$$\mathfrak{u}_g := \left\langle \alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g \;\middle|\; \sum_{i=1}^{g} [\alpha_i, \beta_i] = 0 \right\rangle.$$

  Warning 12.6. This is not as easy to prove as it seems. One gets for free that $\mathfrak{u}_g$ is generated by $\log a_1, \ldots, \log a_g, \log b_1, \ldots, \log b_g$ such that $\log(\prod_{i=1}^{g} [a_i, b_i]) = 0$, but the logarithm of this relation is not $\sum_{i=1}^{g} [\log a_i, \log b_i]$, so one needs to fiddle around w/ generators. •

  Observe that $\mathfrak{u}_g$ is naturally graded, e.g. put each α_i, β_j in degree -1 (and then the relation is in degree -2). This implies that $\mathrm{gr}_\Gamma^\bullet \mathrm{Lie}(\pi_1)$ is the quotient of the free graded pro-nilpotent Lie algebra generated by $\mathrm{H}^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)^*$ in degree -1 modulo the ideal generated by the image of $\cup^* : \mathbb{Q}_p(1) \to \bigwedge^2 \mathrm{H}_{\text{ét}}(-)^*$ in degree -2. The upshot is that we get an exact sequence

$$\mathfrak{f}(1)[2] \longrightarrow \mathfrak{f} \longrightarrow \mathrm{gr}_\Gamma^\bullet \mathrm{Lie}\, \pi_1 \longrightarrow 0$$

  ($\mathfrak{f}$ is the free graded pro-nilpotent Lie algebra generated by $\mathrm{H}^1_{\text{ét}}(X_{\overline{K}}; \mathbb{Q}_p)^*$) of graded pro-f.dim vector spaces. Purity of graded pieces of $\mathfrak{f}$ (and $\mathfrak{f}(1)[2]$) imply purity of $\mathrm{gr}_\Gamma^k \mathrm{Lie}\, \pi_1$.

This feels vaguely reminiscent of Milnor K-theory, at least in so far as you've replaced a complicated object by a simpler one using only the relations present in degree ± 2.

Remark 12.7 (Response to audience question, `free Lie algebra on vector space`). If V is a f.dim vector space, have the free Lie algebra $\mathfrak{f}$ on V. This is a graded Lie algebra[14]

$$\mathfrak{f} = V \oplus \bigwedge^2 V \oplus \ldots$$

satisfying some universal property. Note it must be graded as $K^\times$ acts on V via multiplication, so $K^\times$ acts on $\mathfrak{f}$, so $\mathfrak{f} = \bigoplus_{k \geq 1} V_k$ where $\lambda \in K^\times$ acts on V_k via λ^k.

[14] elements looks like $[[x, [x, z]], w]$ and so on...

The free pronilpotent Lie algebra generated by V is equivalently either of

- the completion of $\mathfrak{f}$ along its descending central series
- $\prod_{k\geq 1} V_k$ w/ the natural Lie bracket (note it is graded in a natural way) ∘

Remark 12.8. In the proof, we used the fact that the category of pure representations of weight k is closed under cokernels (and kernels) in the category of all G_K-reps. If X has good reduction and $\ell \neq p$, then π_1 is actually an unramified representations, and the category of $\mathbb{Q}_\ell$-unramified representations is furthermore closed under all quotients and subobjects. In this case, the argument simplifies. Once we know $\mathrm{gr}^1_\Gamma \pi_1 = \pi_1^{\mathrm{ab}}$ is pure of weight -1, for all $k \geq 2$, we have a surjective map

$$\left(\pi_1^{\mathrm{ab}}\right)^{\otimes k} \twoheadrightarrow \mathrm{gr}^k_\Gamma \pi_1$$

via $a_1 \otimes \cdots \otimes a_k \mapsto [a_1, [a_2, [a_3, [\ldots, [a_{k-1}, a_k]] \ldots]$. This implies that $\mathrm{gr}^k_\Gamma \pi_1$ is pure of weight $-k$. ∘

Non-example. Say E is an elliptic curve w/ multiplicative reduction. Then, one has a short exact sequence

$$0 \longrightarrow \mathbb{Q}_p(0) \longrightarrow \mathrm{H}^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p) \longrightarrow \mathbb{Q}_p(-1) \longrightarrow 0,$$

and $\mathrm{H}^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_p)$ is pure of weight 1. However, it has a subobject and a quotient which is not pure of weight 1. ▽

We'll end with a preview of what's gonna come up in a couple weeks, after Arizona Winter School. We have now finished the first part of the course.

12.1 L8: Non-abelian cohomology (preview of Part II: Selmer schemes)

Say $X/\mathbb{Q}$ is a smooth, projective curve of good reduction p. Let U be a $G_{\mathbb{Q}}$-equivariant quotient of $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; x)$ $(x \in X(\mathbb{Q}))$. We will usually take U be be f.dimensional. We want to build a $\mathbb{Q}_p$-pro-unipotent descent square

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle j_p} \\ \mathrm{Sel}_U(X) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, U). \end{array}$$

Think of this "U-Selmer scheme $\mathrm{Sel}_U(X)$" as some version of $\mathrm{H}^1_f(G_{\mathbb{Q}}, U)$. The bottom row above consists of "Selmer schemes," which are built out of U using "non-abelian Galois cohomology."

Let G and Π be topological groups, with $G \curvearrowright \Pi$ (from the left, continuous). If Π is abelian, we have continuous Galois cohomology groups $\mathrm{H}^i(G, \Pi)$ for all $i \geq 0$. How necessary is the abelian assumption here?

If Π is non-abelian, only get part of this story.

Definition 12.9.

(0) $\mathrm{H}^0(G, \Pi) := \Pi^G = \{u \in \Pi, \sigma(u) = u \text{ for all } \sigma \in G\}$.

(1) A `continuous 1-cocycle` is a continuous map

$$\xi : G \to \Pi \text{ such that } \xi(\sigma\tau) = \xi(\sigma) \cdot \sigma(\xi(\tau)) \text{ for all } \sigma, \tau \in G.$$

We write $Z^1(G,\Pi) = \{\text{continuous 1-cocycles } \xi : G \to \Pi\}$. Note that Π acts on $Z^1(G,\Pi)$ from the right via $\xi \mapsto \xi^u$ $(u \in \Pi)$ where

$$\xi^u(\sigma) = u^{-1}\xi(\sigma)\sigma(u).$$

One defines

$$\mathrm{H}^1(G,\Pi) := Z^1(G,\Pi)/\Pi.$$

Warning 12.10. $\mathrm{H}^1(G,\Pi)$ is not a group, but only a pointed set (w/ distinguished element $*$ the class the of trivial cocycle $\xi(\sigma) = 1$). •

(2) We won't try to define $\mathrm{H}^i(G,\Pi)$ for $i \geq 2$. ◇

Example 12.11. Say Π is abelian, w/ operation written additively. Then,

$$Z^1(G,\Pi) = \{\xi : G \to \Pi : \sigma(\xi(\tau)) - \xi(\sigma\tau) + \xi(\sigma) = 0\}$$

is the usual group of cocycles. Furthermore, Π acts on $Z^1(G,\Pi)$ via $u : \xi \mapsto \xi + \mathrm{d}(u)$, where $\mathrm{d}(u)(\sigma) = \sigma(u) - u$. Thus, $\mathrm{H}^1(G,\Pi)$ is the usual group cohomology group. △

13 Bonus Lectures (3/7,9) – Didn't Go

14 Lecture 13, I guess (3/21): Non-abelian Cohomology

OHs on Thursday: Bloch-Kato exponential++

Recall 14.1. Let G, Π be topological groups where $G \curvearrowright \Pi$ on the left. One defines the group

$$\mathrm{H}^0(G,\Pi) = \Pi^G,$$

as well as the pointed set

$$\mathrm{H}^1(G,\Pi) = Z^1(G,\Pi)/\Pi,$$

where $Z^1(G,\Pi) = \{\text{cts } \xi : G \to \Pi : \xi(\sigma\tau) = \xi(\sigma) \cdot \sigma\xi(\tau)\}$ and $u \in \Pi$ acts on $\xi \in Z^1(G,\Pi)$ via $\xi^u(\sigma) = u^{-1}\xi(\sigma) \cdot \sigma(u)$. ⊙

We talk about how one works with these nonabelian cohomology groups/sets. As in the abelian case, the main tool is certain "long" exact sequences.

Recall 14.2. If

$$0 \longrightarrow Z \longrightarrow \Pi \longrightarrow Q \longrightarrow 0$$

is a G-equivariant exact sequences with Z, Π, Q all abelian, then you get (modulo caveats) a long exact sequence

$$\ldots \longrightarrow \mathrm{H}^i(G,Z) \longrightarrow \mathrm{H}^i(G,\Pi) \longrightarrow \mathrm{H}^i(G,Q) \longrightarrow \mathrm{H}^{i+1}(G,Z) \longrightarrow \ldots$$

in cohomology. ⊙

What are the caveats alluded to above?

Definition 14.3. Let Π, Z, Q be topological groups. A sequence

$$1 \longrightarrow Z \longrightarrow \Pi \longrightarrow Q \longrightarrow 1$$

of continuous group homomorphisms is called a `topologically split exact sequence` just when

(0) it is an exact sequence of (abstract) groups

(1) $Z \subset \Pi$ has the subspace topology

(2) $\Pi \to Q$ admits a continuous splitting (not necessarily compatible with the group structure) ◇

Remark 14.4. If you're working with discrete groups, then **(1)** and **(2)** above are vacuous. ○

Theorem 14.5. *Let*

$$1 \longrightarrow Z \longrightarrow \Pi \longrightarrow Q \longrightarrow 1$$

be a G-equivariant topologically split central extension[15] *of topological groups. Then, there are coboundary maps*

$$\delta^0 : \mathrm{H}^0(G, Q) \to \mathrm{H}^1(G, Z) \text{ and } \delta^1 : \mathrm{H}^1(G, Q) \to \mathrm{H}^2(G, Z)$$

such that the sequence

$$1 \to \mathrm{H}^0(G, Z) \to \mathrm{H}^0(G, \Pi) \to \mathrm{H}^0(G, Q) \xrightarrow{\delta^0} \mathrm{H}^1(G, Z) \to \mathrm{H}^1(G, \Pi) \to \mathrm{H}^1(G, Q) \xrightarrow{\delta^1} \mathrm{H}^2(G, Z)$$

is exact.

Remark 14.6.

(1) A sequence $X_0 \to X_1 \xrightarrow{f} X_2$ of maps of pointed sets is called exact (at X_1) iff $\mathrm{im}(X_0 \to X_1) = \ker(X_1 \to X_2) := f^{-1}(*)$ (with $* \in X_2$ the distinguished point).

(2) When Π is abelian, the sequence in Theorem 14.5 is (part of) the usual long exact sequence.

(3) This LES is functorial w.r.t. morphisms of G-equivariant topologically split central extensions.

(4) δ^0 is a group homomorphism, and δ^1 is a map of pointed sets. ○

We won't carefully prove Theorem 14.5, but we'll at least define the coboundary maps.

Construction 14.7. Fix some $u \in Q^G$. Choose some $\widetilde{u} \in \Pi$ mapping to u. For any $\sigma \in G$, we get $\widetilde{u}^{-1}\sigma(\widetilde{u}) \in Z$. We define $\delta^0(u)$ to be the class represented by the cocycle

$$\xi_{\widetilde{u}} : \sigma \mapsto \widetilde{u}^{-1}\sigma(\widetilde{u}).$$

(This is continuous because Z has the subspace topology in Π). One can check that this gives a well-defined cohomology class.

Fix some $\xi \in Z^1(G, Q)$. This lifts to a continuous map $\widetilde{\xi} : G \to \Pi$ (using the existence of a continuous splitting). We define $\delta^1(\xi)$ to be the class represented by the (continuous) 2-cocycle

$$\eta(\sigma, \tau) = \sigma\widetilde{\xi}(\tau) \cdot \widetilde{\xi}(\sigma\tau)^{-1} \cdot \widetilde{\xi}(\sigma)$$

($\eta(\sigma, \tau) \in Z$ since ξ is a 1-cocycle). Checking that this is a 2-cocycle, i.e. checking that

$$\rho \cdot \eta(\sigma, \tau) \cdot \eta(\rho\sigma, \tau)^{-1} \cdot \eta(\rho, \sigma\tau) \cdot \eta(\rho, \sigma)^{-1} = 1 \text{ for all } \rho, \sigma, \tau \in G$$

is some tedious symbol pushing. Finally, one can check that the class of η in $\mathrm{H}^2(G, Z)$ is independent of the choice of continuous splitting and of the representative ξ of its cohomology class. ◯

[15] i.e. Z lands in the center of Π, so Z is in particular abelian

With these maps constructed, one can now check exactness of the claimed sequence.

Warning 14.8. If $X_1 \to X_2$ is a map of pointed sets, then $\ker(f) = \{*\} \not\Rightarrow f$ is injective. Being an exact sequence of pointed sets is rather a weak property. •

To circumvent issues like this, we will need to utilise an extra structure on the LES. Consider

$$\mathrm{H}^0(G, Q) \longrightarrow \mathrm{H}^1(G, Z) \longrightarrow \mathrm{H}^1(G, \Pi) \longrightarrow \mathrm{H}^1(G, Q).$$

It turns out that the group $\mathrm{H}^1(G, Z)$ acts on the set $\mathrm{H}^1(G, \Pi)$ (from the right).

Construction 14.9. If $\xi \in Z^1(G, \Pi)$ and $\alpha \in Z^1(G, Z)$, the pointwise product

$$\xi \cdot \alpha : G \to \Pi$$

is also a 1-cocycle (using that Z is central). ⬡

Moreover, the map $\mathrm{H}^1(G, Z) \to \mathrm{H}^1(G, \Pi)$ is simply given by acting on the distinguished point, i.e. it is

$$[\xi] \mapsto [\xi \cdot *]$$

(This is just unpacking definitions. Recall $*$ is the trivial cocycle $x \mapsto 1$).

Proposition 14.10. *In the above setup, the fibers of* $\mathrm{H}^1(G, \Pi) \to \mathrm{H}^1(G, Q)$ *are exactly the orbits of* $\mathrm{H}^1(G, Z)$ *acting on* $\mathrm{H}^1(G, \Pi)$.

Proof. Let $\xi_1, \xi_2 \in Z^1(G, \Pi)$. If $[\xi_1]$ and $[\xi_2]$ lie in the same orbit, then there must exist a 1-cocycle $\alpha : G \to Z$ and some $u \in \Pi$ such that

$$\xi_2 = \xi_1^u \cdot \alpha.$$

Hence, if $\overline{\xi}_2, \overline{\xi}_1 \in Z^1(G, Q)$ and $\overline{u} \in Q$ denote their images, then we see that $\overline{\xi}_2 = \overline{\xi}_1^{\overline{u}}$, so $[\overline{\xi}_1] = [\overline{\xi}_2] \in \mathrm{H}^1(G, Q)$. Hence, each orbit lies in a single fiber.

Conversely, say ξ_1, ξ_2 lie in the same fiber. Then, there exists some $\overline{u} \in Q$ such that $\overline{\xi}_2 = \overline{\xi}_1^{\overline{u}}$. Lift $\overline{u}$ to some $u \in \Pi$, and then define $\alpha : G \to Z$ via $\alpha = (\xi_1^u)^{-1} \xi_2$. Finally, check that α is a cocycle. ■

Remark 14.11. If Π, Z, Q are abelian, then the action of $\mathrm{H}^1(G, Z)$ on $\mathrm{H}^1(G, \Pi)$ is the addition action. ∘

14.1 Serre Twisting

Consider

$$\mathrm{H}^0(G, Q) \xrightarrow{\delta^0} \mathrm{H}^1(G, Z) \longrightarrow \mathrm{H}^1(G, \Pi).$$

From above discussion, we have that

$$\mathrm{im}(\delta^0) = \mathrm{Stab}(*) \subset \mathrm{H}^1(G, Z).$$

What about the other stabilizers?

Let Π be a topological group w/ a continuous G-action. Choose some 1-cycle $\xi \in Z^1(G, \Pi)$. Define the ξ-twisted G-action on Π via

$$\sigma * u := \xi(\sigma) \cdot \sigma(u) \cdot \xi(\sigma)^{-1}$$

for $\sigma \in G$ and $u \in \Pi$. That is, we conjugate the original action by ξ. As the name suggests, this defines a new continuous action of G on Π by group homomorphisms.

Definition 14.12. The Serre twist ${}_\xi\Pi$ of Π is the same underlying topological group Π, but now with the ξ-twisted G-action. ◇

Remark 14.13. In the abelian case, ${}_\xi\Pi = \Pi$ because conjugation does nothing. ○

Proposition 14.14. *There is a canonical bijection* $\mathrm{H}^1(G, {}_\xi\Pi) \xrightarrow{\sim} \mathrm{H}^1(G, \Pi)$ *given by*

$$[\xi'] \mapsto [\xi' \cdot \xi],$$

where $\xi' \in Z^1(G, {}_\xi\Pi)$.

Note in particular that this bijection sends the distinguished element of $\mathrm{H}^1(G, {}_\xi\Pi)$ to $[\xi] \in \mathrm{H}^1(G, \Pi)$.

Proposition 14.15. *If we have*

$$1 \longrightarrow Z \longrightarrow \Pi \longrightarrow Q \longrightarrow 1$$

as before, then for any $\xi \in Z^1(G, \Pi)$*, the* ξ*-twisted sequence*

$$1 \longrightarrow Z \longrightarrow {}_\xi\Pi \longrightarrow {}_\xi Q \longrightarrow 1$$

is again a G*-equivariant topologically split central extension. Furthermore, the bijection*

$$\mathrm{H}^1(G, {}_\xi\Pi) \xrightarrow{\sim} \mathrm{H}^1(G, \Pi)$$

is $\mathrm{H}^1(G, Z)$*-equivariant.*

Corollary 14.16. *For any* $\xi \in Z^1(G, \Pi)$*, the stabilizer of* $[\xi] \in \mathrm{H}^1(G, \Pi)$ *under the action of* $\mathrm{H}^1(G, Z)$ *is* $\mathrm{im}\left(\mathrm{H}^0(G, {}_\xi Q) \xrightarrow{\delta^0} \mathrm{H}^1(G, Z)\right)$.

Remark 14.17. This gives a way of detecting when the action $\mathrm{H}^1(G, Z) \curvearrowright \mathrm{H}^1(G, \Pi)$ is free. ○

14.2 Non-abelian cohomology and groupoids

Let Π be a connected groupoid in topological spaces (in particular, all $\Pi(x, y)$'s are nonempty topological spaces). Suppose there is a topological group G acting on all $\Pi(x, y)$'s compatibly w/ compositions, etc.

Example 14.18. Galois group acting on étale fundamental groupoid. △

Fix a base vertex $x_0 \in V(\Pi)$. Then, the action of G on $\Pi(x_0, y)$ is determined by the action of G on the group $\Pi(x_0)$ and the action on any chosen path $\gamma_0 \in \Pi(x_0, y)$. This is simply because a general path is $\gamma_0 \cdot u$ for some $u \in \Pi(x_0)$, and $\sigma(\gamma_0 u) = \sigma(\gamma_0)\sigma(u)$ by compatibility w/ composition.

Remark 14.19. If γ_0 is G-fixed, then the identification

$$\begin{array}{ccc} \Pi(x_0) & \longrightarrow & \Pi(x_0, y) \\ u & \longmapsto & \gamma_0 u \end{array}$$

will be G-equivariant. ○

In general, the failure of this map to be equivariant is controlled by the map

$$\begin{array}{rccc} \xi_{\gamma_0} : & G & \longrightarrow & \Pi(x_0) \\ & \sigma & \longmapsto & \gamma_0^{-1}\sigma(\gamma_0). \end{array}$$

Lemma 14.20. *ξ_{γ_0} is a continuous 1-cocycle, and its class in $\mathrm{H}^1(G, \Pi(x_0))$ is independent of the choice of $\gamma_0 \in \Pi(x_0, y)$.*

Hence, we get a function

$$j : V(\Pi) \longrightarrow \mathrm{H}^1(G, \Pi(x_0)),$$

called the abstract non-abelian Kummer map.

Remark 14.21. $j(y) = * \iff \Pi(x_0, y)^G \neq \emptyset$. ∘

We'll most often use this with $G = \mathrm{Gal}(K^s/K)$ and $\Pi = \pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; -, -)(\mathbb{Q}_p)$ for some geometrically connected K-variety Y. We then get a map

$$Y(K) \longrightarrow \mathrm{H}^1\Big(G_K, \pi_1^{\mathbb{Q}_p}(Y_{\overline{K}}; x_0)\,(\mathbb{Q}_p)\Big),$$

which will give part of the our desired non-abelian descent square (Recall Section 2.3).

15 Lecture 14 (3/23): Cohomology of pro-unipotent groups

Setup 15.1. For today, suppose that G is a profinite group acting continuously on a pro-unipotent group $U/\mathbb{Q}_p$.

By "acting continuously," we mean that $\mathrm{Lie}(U)$ is a cofiltered limit of f.dim continuous G-reps. In this case, G acts continuously on $U(\mathbb{Q}_p)$ (w/ standard p-adic topology), so we get a pointed set $\mathrm{H}^1(G, U(\mathbb{Q}_p)) \in \mathrm{Set}_*$.

Goal. Put an algebraic structure on this set. Specifically, we want to realize it as the $\mathbb{Q}_p$-points of an affine $\mathbb{Q}_p$-scheme.

Let's start by setting some conventions

- If Λ is a $\mathbb{Q}_p$-algebra, we topologise it by taking the colimit topology of the natural topology on its f.dim subspaces. That is, $\Lambda \simeq \mathbb{Q}_p^{\oplus I}$ as topological $\mathbb{Q}_p$-vector spaces.
- We then topologize $U(\Lambda)$ in the natural way.
  - If U is unipotent, then $U(\Lambda) \cong \Lambda \otimes_{\mathbb{Q}_p} \mathrm{Lie}(U)$ and the RHS carries a natural topology.
  - For U pro-unipotent, take an inverse limit of these topologies.

With these conventions, $G \curvearrowright U(\Lambda)$ (it acts on U and acts trivially on Λ) and does so continuously, so we also have

$$\mathrm{H}^1(G, U(\Lambda)) \in \mathrm{Set}_*.$$

This construction define a functor

$$\mathrm{H}^1(G, U) : \mathrm{Alg}_{\mathbb{Q}_p} \longrightarrow \mathrm{Set}_*.$$

Goal. Give a criterion for this functor to be representable by an affine $\mathbb{Q}_p$-scheme.

Remark 15.2 (Response to Audience Question). One way to think of this functor is as a cocycle functor (spitting out $Z^1(-,-)$'s) quotiented out by an action of U. If this action has stabilizers, should not expect this thing to be representable. ∘

Suppose that U comes w/ a separated[16] G-stable filtration

$$U = W_{-1}U \trianglerighteq W_{-2}U \trianglerighteq \dots$$

[16] i.e. $\bigcap_{n \geq 1} W_{-n}U = 1$

where

- $[W_{-i}U, W_{-j}U] \leq W_{-i-j}U$
- $W_{-n}U$ is finite codimension in U, i.e. $U/W_{-n}U$ is (f.dim) unipotent.

Notation 15.3. Set

$$U_n = U/W_{-n-1}U \text{ and } V_n = W_{-n}U/W_{-n-1}U.$$

Note that all V_n's are vector groups, and the extensions

$$1 \longrightarrow V_n \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1$$

are central. Furthermore, G acts continuously on everything in sight. Our main theorem for today will be.

Theorem 15.4. *Suppose that*

- $\mathrm{H}^0(G, V_n) = 0$*; and*
- $\mathrm{H}^1(G, V_n)$ *is f.dim*

for all n. Then, $\mathrm{H}^1(G, U)$ is representable by an affine $\mathbb{Q}_p$-scheme. Moreover, $\mathrm{H}^1(G, U)$ is a closed subscheme of $\prod_{n\geq 1} \mathrm{H}^1(G, V_n)$.

Above, $\mathrm{H}^1(G, V_n)$ is a f.dim $\mathbb{Q}_p$-vector space, and so an affine scheme in a natural way.

Remark 15.5.

(0) We write $\mathrm{H}^1(G, U)$ both for the functor and the representing scheme. We call this the `cohomology scheme`.

(1) We're mostly interested in the case that U is `finitely generated`, i.e. there is a finite subset of the $\mathbb{Q}_p$ points which generate a Zariski dense subgroup. In this case, $W_{-n}U$ is always of finite codimension.

(2) If U is unipotent, then $\mathrm{H}^1(G, U)$ is of finite type (e.g. b/c it's a closed subscheme of a finite product of f.dim vector spaces), and in fact $\dim \mathrm{H}^1(G, U) \leq \sum_n \dim \mathrm{H}^1(G, V_n)$.

(3) We say that G has `property (F)` just when for all $d \in \mathbb{N}$, G has only finitely many open subgroups of index d.

Property (F) $\implies$ $\mathrm{H}^i(G, V)$ are f.dim for all i and all continuous representations V. ∘

The proof of Theorem 15.4 will ultimately be by induction (on n). For the base case, we want to consider continuous actions on vector groups.

Proposition 15.6. *Let V be a continuous representation of G, and let Λ be a $\mathbb{Q}_p$-algebra. Then, the natural map*

$$\Lambda \otimes \mathrm{H}^i(G, V) \longrightarrow \mathrm{H}^i(G, \Lambda \otimes V)$$

is an isomorphism of Λ-modules for all i.

Proof. Omitted.[17] ■

Remember: By convention, when we talk about 'representations' we always mean f.dimensional ones.

[17] Compare this proposition with [Kim05, Lemma 6].

Corollary 15.7. *Let $\mathbb{G}(V)$ be the associated vector group. Let $\mathrm{H}^i(G, \mathbb{G}(V))$ be the associated cohomology functor. Then*

(1) *$\mathrm{H}^i(G, \mathbb{G}(V))$ is representable iff $\mathrm{H}^i(G, V)$ is f.dimensional. In which case,*

$$\mathrm{H}^i(G, \mathbb{G}(V)) = \mathbb{G}(\mathrm{H}^i(G, V)).$$

(2) *In general, $\mathrm{H}^i(G, \mathbb{G}(V))$ is `subrepresentable`, i.e. its a subfunctor of a representable functor.*

(For **(2)**, it's a subfunctor of $\operatorname{Spec} \operatorname{Sym}^*\big(\mathrm{H}^i(G, V)^*\big)$, i.e. of $\Lambda \mapsto \operatorname{Hom}_{\mathbb{Q}_p}\big(\mathrm{H}^i\, G, V^*, \Lambda\big)$)
Back in the setup of the theorem, we know that

- $\mathrm{H}^0(G, V_n) = 0$
- $\mathrm{H}^1(G, V_n)$ is representable by a vector group (by Corollary 15.7)

In particular, as $U_1 = V_1$, we know that $\mathrm{H}^1(G, U_1)$ is representable. Now we proceed by induction.

Proof of Theorem 15.4. Fix some $n \geq 2$. Suppose that $\mathrm{H}^1(G, U_{n-1})$ is representable. In the central extension

$$1 \longrightarrow V_n \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1,$$

the surjection $U_n \to U_{n-1}$ splits as a morphism of $\mathbb{Q}_p$-schemes (see the end of Section 5.2). Hence, the sequence

$$1 \longrightarrow V_n(\Lambda) \longrightarrow U_n(\Lambda) \longrightarrow U_{n-1}(\Lambda) \longrightarrow 1$$

is topologically split for all Λ, so we can take the long exact sequence in cohomology:

$$1 \to \mathrm{H}^0(G, V_n) \to \mathrm{H}^0(G, U_n) \to \mathrm{H}^0(G, U_{n-1}) \xrightarrow{\delta^0} \mathrm{H}^1(G, V_n) \to \mathrm{H}^1(G, U_n) \to \mathrm{H}^1(G, U_{n-1}) \xrightarrow{\delta^1} \mathrm{H}^2(G, V_n)$$

(exact sequence of functors). Recall this includes an action $\mathrm{H}^1(G, V_n) \curvearrowright \mathrm{H}^1(G, U_n)$.

We only check representability carefully, not the added fact that it lives in a product of affine spaces.

- Claim 1: $\mathrm{H}^1(G, V_n)$ acts strictly (= simply) transitively on the fibers of $\mathrm{H}^1(G, U_n) \to \mathrm{H}^1(G, U_{n-1})$.

  We know for free that the action is transitive. Why is it free? If $\Lambda \in \mathrm{Alg}_{\mathbb{Q}_p}$ and $\xi \in Z^1(G, U_n(\Lambda))$, then we know that the stabiliser of $[\xi] \in \mathrm{H}^1(G, U_n(\Lambda))$ is the image of $\delta^0 : \mathrm{H}^0(G, {}_\xi U_{n-1}(\Lambda)) \to \mathrm{H}^1(G, V_n(\Lambda))$, so it suffices to prove that $\mathrm{H}^0(G, {}_\xi U_{n-1}(\Lambda)) = 1$. Indeed, for all $m < n$, we have an exact sequence

  $$1 \to V_m(\Lambda) \to {}_\xi U_m(\Lambda) \to {}_\xi U_{m-1}(\Lambda) \to 1 \rightsquigarrow \mathrm{H}^0(G, V_m(\Lambda)) \to \mathrm{H}^0(G, {}_\xi U_m(\Lambda)) \to \mathrm{H}^0(G, {}_\xi U_{m-1}(\Lambda)).$$

  Thus, an easy induction argument using the exact sequence on the right above shows that $\mathrm{H}^0(G, {}_\xi U_m(\Lambda)) = 1$ for all $m < n$. As such, $\mathrm{Stab}([\xi]) = 1$ for all ξ, so $\mathrm{H}^1(G, V_n)$ acts freely on $\mathrm{H}^1(G, U_n)$.

- Claim 2: $\ker\big(\delta^1 : \mathrm{H}^1(G, U_{n-1}) \to \mathrm{H}^2(G, V_n)\big)$ is representable by a closed subscheme of $\mathrm{H}^1(G, U_{n-1})$.

  By Corollary 15.7, so know $\mathrm{H}^2(G, V_n)$ is subrepresentable, so choose some $\mathrm{H}^2(G, V_n) \hookrightarrow X$ for some scheme X. This is monomorphism, so

  $$\ker(\delta^1) = \ker\big(\mathrm{H}^1(G, U_{n-1}) \longrightarrow X\big)$$

  (the distinguished element of X is the image of the distinguished element of $\mathrm{H}^1(G, U_{n-1}(\mathbb{Q}_p))$). This kernel is now representable by a closed subscheme, the fiber of the (scheme!) map $\mathrm{H}^1(G, U_{n-1}) \to X$ over the distinguished point.

- Claim 3: the surjection
$$\mathrm{H}^1(G, U_n) \twoheadrightarrow \ker(\delta^1)$$
splits.

  By the previous claim, $\ker(\delta^1) = \operatorname{Spec} R$ for some R, i.e. it is the functor $\operatorname{Hom}(R, -)$, so we have a map $\mathrm{H}^1(G, U_n)(R) \twoheadrightarrow \operatorname{Hom}(R, R)$. There exists some $\xi \in \mathrm{H}^1(G, U_n)(R)$ mapping to $\mathrm{id} \in \operatorname{Hom}(R, R)$, so Yoneda tells us that ξ corresponds to a morphism $\operatorname{Hom}(R, -) = \operatorname{Spec} R \to \mathrm{H}^1(G, U_n)$. Can check this is a section of $\mathrm{H}^1(G, U_n) \twoheadrightarrow \ker \delta^1$.

  Remark 15.8. In general, if you have an epimorphism onto a representable functor, then it must split. ∘

At this point, we have
$$\mathrm{H}^1(G, V_n) \curvearrowright \mathrm{H}^1(G, U_n) \twoheadrightarrow \ker(\delta^1),$$
with the above surjection being split. Choosing a splitting $s : \ker(\delta^1) \to \mathrm{H}^1(G, U_n)$, the map
$$\begin{array}{ccc} \ker(\delta^1) \times \mathrm{H}^1(G, V_n) & \longrightarrow & \mathrm{H}^1(G, U_n) \\ (a, b) & \longmapsto & s(a) \cdot b \end{array}$$
is an isomorphism. Thus, $\mathrm{H}^1(G, U_n)$ is representable.

This shows that $\mathrm{H}^1(G, U_n)$ is representable for all n. To finish (in the case U is pro-unipotent), need to show that
$$\mathrm{H}^1(G, U) = \varprojlim_n \mathrm{H}^1(G, U_n)$$
in order to conclude that $\mathrm{H}^1(G, U)$ is representable. ■

Remark 15.9. It's not hard to see from the proof that $\mathrm{H}^1(G, U_n)$ is a closed subscheme of a product of affine spaces. To get the same for $\mathrm{H}^1(G, U)$ takes a bit more work (gotta worry about various noncanonical embeddings being chosen compatibly). ∘

16 Office Hours

Question 16.1. *Do you need G profinite in Theorem 15.4?*

If I heard correctly, profiniteness was only used in one place, to know that cohomology commutes w/ infinite direct sums (presumably in proof of Proposition 15.6). This is true also for $\mathbb{Z}$.

Corollary 16.2. *Suppose $U/\mathbb{Q}_p$ pro-finite with $W_{-\bullet}U$ as before. Assume U comes equipped w/ an automorphism φ preserving $W_{-\bullet}U$. If $V_n^{\varphi=1} = 0$, then the map*
$$\begin{array}{ccc} U & \longrightarrow & U \\ u & \longmapsto & u^{-1}\varphi(u) \end{array}$$
is an isomorphism of schemes.

Proof. This gives action $\mathbb{Z} \curvearrowright U$ which is automatically continuous ($\mathbb{Z}$ discrete). We know by assumption that $\mathrm{H}^0(\mathbb{Z}, UV_n) = 0$ and $\mathrm{H}^1(\mathbb{Z}, V_n)$ is f.dim. Then implies that $\mathrm{H}^0(\mathbb{Z}, U_n) = 1$ and that $\mathrm{H}^1(\mathbb{Z}, U_n) = 1$ as it's contained in
$$\prod_{n \geq 1} \mathrm{H}^1(\mathbb{Z}, V_n) \text{ where } \mathrm{H}^1(\mathbb{Z}, V_n) = V_n/(\varphi - 1) = 0.$$

$\mathrm{H}^1(\mathbb{Z}, U_n) = 1$ is equivalent to the statement. ■

Remark 16.3 (Response to Audience Question). If $\varphi \curvearrowright \operatorname{Lie} U$ has no $\mathbb{Z}_p$-sublattice (e.g. if φ is multiplication by p), then it doesn't give a continuous action of $\widehat{\mathbb{Z}}$. ∘

16.1 Bloch-Kato Stuff

Recall from last time

- $K/\mathbb{Q}_p$ finite
- V a de Rham representation of G_K
- $\mathrm{H}^1_e(G_K, V) := \ker\Big(\mathrm{H}^1(G_K, V) \to \mathrm{H}^1(G_K, B_{\mathrm{cris}}^{\varphi=1} \otimes_{\mathbb{Q}_p} V)\Big)$
- $\mathrm{H}^1_f(G_K, V) := \ker\big(\mathrm{H}^1(G_K, V) \to \mathrm{H}^1(G_K, B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)\big)$
- $\mathrm{H}^1_g(G_K, V) := \ker\big(\mathrm{H}^1(G_K, V) \to \mathrm{H}^1(G_K, B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)\big)$

Here are some facts to know/accept

- $B_{cris}^{\varphi=1} \leq B_{cris} \leq B_{dR}$
- Hence, these Bloch-Kato Selmer groups have containments

$$0 \leq \mathrm{H}^1_e(G_K, V) \leq \mathrm{H}^1_f(G_K, V) \leq \mathrm{H}^1_g(G_K, V) \leq \mathrm{H}^1(G_K, V).$$

  - The quotient f/e is like "unramified cohomology H^1_{nr} in the $\ell \neq p$ case"
  - The quotient g/e is like "H^1 in the $\ell \neq p$ case"
- There's a "Poincaré duality" pairing realizing $\mathrm{H}^1(G_K, V)$ as dual to $\mathrm{H}^1(G_K, V^*(1))$. Under this, H^1_e is dual to H^1_g and H^1_f is dual to itself.
- The cristalline period ring comes w/ a Frobenius endomorphism
- B_{dR} comes w/ a Hodge filtration, whose 0th step is $B_{dR}^+ \subset B_{dR}$.
- $B_{cris}^{\varphi=1} \cap B_{dR}^+ = \mathbb{Q}_p$ inside of B_{dR}. Moreover,

$$B_{cris}^{\varphi=1} + B_{dR}^+ = B_{dR}.$$

  One can package this as the following "fundamental exact sequence"

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_{\mathrm{cris}}^{\varphi=1} \oplus B_{\mathrm{dR}}^+ \longrightarrow B_{\mathrm{dR}} \longrightarrow 0. \tag{16.1}$$

Here's an idea: tensor the above exact sequence with V and then look at the resulting sequence in Galois cohomology:

$$0 \to V^{G_K} \to D_{\mathrm{cris}}^{\varphi=1}(V) \oplus D_{\mathrm{dR}}^+(V) \to D_{\mathrm{dR}}(V) \to \mathrm{H}^1(G_K, V) \xrightarrow{\beta} \mathrm{H}^1(G_K, B_{\mathrm{cris}}^{\varphi=1} \otimes V) \oplus \mathrm{H}^1(G_K, B_{\mathrm{dR}}^+ \otimes V) \to \mathrm{H}^1(G_K, B_{\mathrm{dR}} \otimes V)$$

(to continue this, would need to know the tensored sequence is topologically split). Note that there is an H^1_e hiding above.

Fact (Uses that V is de Rham)**.** The map

$$\mathrm{H}^1(G_K, B_{dR}^+ \otimes V) \to \mathrm{H}^1(G_K, B_{dR} \otimes V)$$

is injective.

As a consequence, $\ker(\beta) = \mathrm{H}^1_e(G_K, V)$. The $\subset$ inclusion is obvious. For the latter, given $\xi \in \mathrm{H}^1(G_K, V)$, write $\beta(\xi) = (\xi_{cris}, \xi_{dR})$. By examples, the images of ξ_{cris}, ξ_{dR} in $\mathrm{H}^1(G_K, B_{dR} \otimes V)$ agree. If $\xi \in \mathrm{H}^1_e$, then $\xi_{cris} = 0$, so $\xi_{dR} \in \ker\big(\mathrm{H}^1(B_{dR}^+ \otimes V) \to \mathrm{H}^1(B_{dR} \otimes V)\big) = 0$, so $\xi \in \ker(\beta)$.

This gives us the Bloch-Kato exponential exact sequence

$$0 \longrightarrow V^{G_K} \longrightarrow D_{\mathrm{cris}}^{\varphi=1}(V) \oplus D_{\mathrm{dR}}^+(V) \longrightarrow D_{\mathrm{dR}}(V) \longrightarrow \mathrm{H}^1_e(G_K, V) \longrightarrow 0.$$

(Equivalently,

$$0 \longrightarrow V^{G_K} \longrightarrow D_{\mathrm{cris}}^{\varphi=1}(V) \longrightarrow \frac{D_{\mathrm{dR}}(V)}{D_{\mathrm{dR}}^+(V)} \longrightarrow \mathrm{H}^1_e(G_K, V) \longrightarrow 0.$$

)

Example 16.4. Say A is an abelian variety over K, and let $V = V_p(A)$ be its $\mathbb{Q}_p$-linear p-adic Tate module. We know that $\dim \mathrm{H}^1(G_K, V_pA) = 2g[K : \mathbb{Q}_p]$. Why?

Fact (Euler-Poincaré Characteristic Formula)**.** Let $K/\mathbb{Q}_\ell$ finite and $V/\mathbb{Q}_p$ representation of G_K. Then,

$$\sum_{i=0}^{2} (-1)^i \dim_{\mathbb{Q}_p} \mathrm{H}^i(G_K, V) = \begin{cases} 0 & \text{if } \ell \neq p \\ -[K : \mathbb{Q}_p] \dim(V) & \text{if } \ell = p. \end{cases}$$

In the present case, $\mathrm{H}^0(G_K, V_pA) = \mathbb{Q}_p \otimes \varprojlim_n \mathrm{H}^0(G_K, A[p^n])$ and $\mathrm{H}^0(G_K, A_{\mathrm{tors}})$ is finite, so this inverse limit is finite, so $\mathrm{H}^0(G_K, V_pA) = 0$. By Poincaré duality, we also have

$$\dim \mathrm{H}^2(G_K, V_pA) = \dim \mathrm{H}^0(G_K, (V_pA)^*(1)) = \dim \mathrm{H}^0(G_K, V_p(A^\vee)) = 0.$$

Thus, the fact gives $\dim \mathrm{H}^1(G_K, V_pA) = 2g[K : \mathbb{Q}_p]$.

Now, let's compute $\dim \mathrm{H}^1_e(G_K, V_p)$. First observe that

$$D_{\mathrm{cris}}^{\varphi=1}(V_pA) = 0$$

as V_pA is pure of weight -1. Let's unpack this a bit, but to make life easy, assume $K = \mathbb{Q}_p$ and A is semistable. This implies that $V = V_pA$ is semistable, in an appropriate sense.

Definition 16.5. Let V be a semistable representation of $G_{\mathbb{Q}_p}$. Note that $D_{\mathrm{st}}(V)$ is a $\mathbb{Q}_p$-vector space of dimension $= \dim V$ equipped w/ two additional structures:

- $\varphi \in \mathrm{Aut}(D_{st}(V))$, the "crystalline Frobenius"
- $N \in \mathrm{End}(D_{st}(V))$, the "monodromy operator"

These satisfy the relation $N \circ \varphi = p \cdot \varphi \circ N$. We say V is pure of weight n just when

- all eigenvalues of φ are p-Weil numbers.

- If $D_{st}(V)_i$ denotes the weight i generalized eigenspace of φ,[18] then the map

$$N^i : D_{st}(V)_{n+i} \longrightarrow D_{st}(V)_{n-i}$$

is an isomorphism for all $i \geq 0$. ◇

Fact. If $X/\mathbb{Q}_p$ is smooth and proper, then $\mathrm{H}^n_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ is pure of weight n for all $n \leq 2$.

(Conjecturally, this holds for all n).

Lemma 16.6. *If V is pure of weight $-n < 0$, then $D^{\varphi=1}_{cris}(V) = 0$.*

Proof. $D^{\varphi=1}_{cris}(V) = D_{st}(V)^{\varphi=1, N=0}$.[19] If $v \in D^{\varphi=1}_{cris}(V)$, then $v \in D_{st}(V)_0$ and $N(v) = 0$. At the same time, we have an isomorphism

$$N^n : D_{st}(V)_0 \xrightarrow{\sim} D_{st}(V)_{-2n},$$

so $v = 0$ as $N^n(v) = 0$. ■

Let's get back to our sequence

$$0 \longrightarrow V^{G_K} \longrightarrow D^{\varphi=1}_{\text{cris}}(V) \longrightarrow \frac{D_{\text{dR}}(V)}{D^+_{\text{dR}}(V)} \longrightarrow \mathrm{H}^1_e(G_K, V) \longrightarrow 0.$$

We just showed $D^{\varphi=1}_{cris}(V) = 0$. The comparision theorem tells us that

$$D_{dR}(V_pA) = D_{dR}(\mathrm{H}^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_p)^*) = \mathrm{H}^1_{\text{dR}}(A/K)^*,$$

so $\dim_{\mathbb{Q}_p} D_{dR}(V_pA) = 2g[K : \mathbb{Q}_p]$. The $^+$ part is the 0th step in the Hodge filtration, so $D^+_{dR}(V_pA)$ has dimension $g[K : \mathbb{Q}]$. Thus,

$$\dim_{\mathbb{Q}_p} \mathrm{H}^1_e(G_K, V) = g[K : \mathbb{Q}].$$

What about the other subspaces? Well, $\mathrm{H}^1_g(G_K, V_p)$ is the annihilator of

$$\mathrm{H}^1_e(G_K, \underbrace{(V_pA)^*(1)}_{V_p(A^\vee)}) \subset \mathrm{H}^1(G_K, (V_pA)^*(1)),$$

so $\dim \mathrm{H}^1_g = g[K : \mathbb{Q}_p]$. Hence, $\mathrm{H}^1_e = \mathrm{H}^1_f = \mathrm{H}^1_g$ in this case. △

17 Lecture 15 (3/28): Bloch-Kato Selmer schemes

Recall 17.1 (Theorem 15.4)**.** Let $U/\mathbb{Q}_p$ be a pro-unipotent group endowed with a continuous action of a profinite group G. Suppose that U has a separated G-stable filtration

$$U = W_{-1}U \trianglerighteq W_{-2}U \trianglerighteq \dots$$

by subgroup schemes of finite codimension such that

(a) $\mathrm{H}^0(G, V_n) = 0$; and

(b) $\dim \mathrm{H}^1(G, V_n) < \infty$

[18] The commutation relation between N and φ implies that $N : D_{st}(V)_i \to D_{st}(V)_{i-2}$

[19] If I heard correctly, $D_{cris}(V) = D_{st}(V)^{N=0}$ is just the kernel of the monodromy map

for all n. Then, the cohomology functor

$$\mathrm{H}^1(G,U) : \mathrm{Alg}_{\mathbb{Q}_p} \longrightarrow \mathrm{Set}_*$$

is representable by an affine $\mathbb{Q}_p$-scheme, which is of finite type if U is unipotent. ⊙

Remark 17.2.

- If U is finitely generated, then $W_{-n}U$ is automatically of finite codimension.
- If G has property (F), then **(b)** is automatic. ∘

We will (almost) always apply this theorem to f.g. pro-unipotent groups, and (almost) always apply it to G satisfying property (F).

Goal. Today, we want to combine our discussions of cohomology functors and of Bloch-Kato Selmer groups (the latter happened in office hours)

17.1 Bloch-Kato Selmer groups

Note 8. Apparently the notes [Bel09] are a good reference.

Let $K/\mathbb{Q}_\ell$ be a finite extension. Let V be $\mathbb{Q}_p$-linear representation of G_K, assume de Rham if $\ell = p$. Then, we can isolate certain subspaces of $\mathrm{H}^1(G_K, V)$.

(Case $\ell \neq p$) The only subspace we care about here is the unramified one

$$\mathrm{H}^1_{\mathrm{nr}}(G_K,V) := \ker\big(\mathrm{H}^1(G_K,V) \to \mathrm{H}^1(I_K,V)\big)\,.$$

One usually studies this using `inflation-restriction`

$$0 \longrightarrow \mathrm{H}^1(\widehat{\mathbb{Z}}, V^{I_K}) \longrightarrow \mathrm{H}^1(G_K,V) \longrightarrow \mathrm{H}^1(I_K,V)^{\widehat{\mathbb{Z}}},$$

which tells us that

$$\mathrm{H}^1_{\mathrm{nr}}(G_K,V) = \mathrm{H}^1(\widehat{\mathbb{Z}}, V^{I_K}) = V^{I_K}/(\varphi - 1).$$

(Case $\ell = p$) In this case, there are three interesting subspaces.

$$\begin{aligned}
\mathrm{H}^1_e(G_K,V) &= \ker\big(\mathrm{H}^1(G_K,V) \longrightarrow \mathrm{H}^1(G_K, B^{\varphi=1}_{\mathrm{cris}} \otimes V)\big)\\
\mathrm{H}^1_f(G_K,V) &= B_{\mathrm{cris}}\\
\mathrm{H}^1_g(G_K,V) &= B_{\mathrm{dR}}.
\end{aligned}$$

One should know that there are inclusions $B^{\varphi=1}_{cris} \subset B_{cris} \subset B_{dR}$, and so inclusions

$$\mathrm{H}^1_e \leq \mathrm{H}^1_f \leq \mathrm{H}^1_g \leq \mathrm{H}^1\,.$$

One often studies H^1_e using the `Bloch-Kato exponential sequence`

$$0 \longrightarrow V^{G_K} \longrightarrow D^{\varphi=1}_{\mathrm{cris}}(V) \oplus D^{+}_{\mathrm{dR}}(V) \longrightarrow D_{\mathrm{dR}}(V) \longrightarrow \mathrm{H}^1_e(G_K,V) \longrightarrow 0 \tag{17.1}$$

where $D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes V)^{G_K}$ (and similarly for the other D_{blah}'s).

Fact. If V is pure of negative weight, then $D^{\varphi=1}_{cris}(V) = 0$ and $\mathrm{H}^1_f = \mathrm{H}^1_e$.

Question 17.3 (Audience)**.** *What's a de Rham representation?*

Answer. First, $B_{\mathrm{dR}}^{G_K} = K$, so this $D_{\mathrm{dR}}(V)$ will always be a K-vector space. In general,

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

We say that V is `de Rham` if equality holds above. This isolates a nice class of representations (closed under tensor products, duals, etc.). Moreover, anything coming from geometry will always be de Rham. ⋆

We'd like the replicate the definition of these $\mathrm{H}^1_{\mathrm{nr,e,f,g}}$'s in the case that V is replaced by a pro-unipotent group U.

17.2 Local Bloch-Kato Selmer schemes

Let $K/\mathbb{Q}_\ell$ finite, and let $U/\mathbb{Q}_p$ be a finitely generated pro-unipotent group endowed with a continuous action of G_K. If $\ell = p$, we assume that U is `de Rham`, i.e. that $\operatorname{Lie} U$ is pro-de Rham.

Assumption. Assume that U is `mixed with negative weights`, i.e. comes with a G_K-stable separated filtration $W_\bullet U$ whose graded pieces $V_n = W_{-n}U/W_{-n-1}U$ are all pure of weight $-n$.

Example 17.4 (Theorem 12.2)**.** π_1 (in appropriate situations) satisfies the above assumption. △

With this assumption in place, $\mathrm{H}^1(G_K, U)$ is representable by an affine scheme. We want to fine interesting subschemes.

Definition 17.5. When $\ell \neq p$, the `unramified cohomology subfunctor` is the subfunctor $\mathrm{H}^1_{\mathrm{nr}}(G_K, U) \subset \mathrm{H}^1(G_K, U)$ defined as the kernel of

$$\mathrm{H}^1(G_K, U) \longrightarrow \mathrm{H}^1(I_K, U).$$ ◇

Is this subfunctor representable (by a closed subscheme)? The answer will be yes, and we'll get this by using inflation-restriction.

Proposition 17.6 (`non-abelian inflation-restriction`)**.** *We have an exact sequence of functors*

$$1 \longrightarrow \mathrm{H}^1(\widetilde{\mathbb{Z}}, U^{I_K}) \longrightarrow \mathrm{H}^1(G_K, U) \longrightarrow \mathrm{H}^1(I_K, U)^{\widehat{\mathbb{Z}}}$$

The upshot of this is that $\mathrm{H}^1_{\mathrm{nr}}(G_K, U) = \mathrm{H}^1(\widehat{\mathbb{Z}}, U^{I_K})$ as functors.

Proposition 17.7. *Under the assumptions we have made,* $\mathrm{H}^1_{nr}(G_K, U) = \{*\}$. *In particular, it is representable by a closed subscheme.*

Proof. Endow U^{I_K} with the restricted filtration, i.e. $W_{-n}\big(U^{I_K}\big) := (W_{-n}U) \cap U^{I_K}$. It's graded pices satisfy

$$V_n' := \frac{W_{-n}U^{I_K}}{W_{-n-1}U^{I_K}} \leq V_n^{I_K}.$$

In particular $(V_n')^{\widehat{\mathbb{Z}}} \leq V_n^{G_K} = 0$. The group $\widehat{\mathbb{Z}}$ has property (F), so Theorem 15.4 shows that $\mathrm{H}^1(\widehat{\mathbb{Z}}, U^{I_K})$ is representable by a closed subscheme of $\prod_n \mathrm{H}^1(\widehat{\mathbb{Z}}, V_n')$. At the same time, $\mathrm{H}^1(\widehat{\mathbb{Z}}, V_n') = V_n'/(\varphi - 1)$, so

$$\dim \mathrm{H}^1(\widehat{\mathbb{Z}}, V_n') = \dim \operatorname{coker}(\varphi - 1) = \dim \ker(\varphi - 1) = \dim \mathrm{H}^0(\widehat{\mathbb{Z}}, V_n') = 0.$$

Thus, $\mathrm{H}^1_{\mathrm{nr}}(G_K, U) = \mathrm{H}^1(\widehat{\mathbb{Z}}, U^{I_K})$ is the 1-point scheme. ■

(This was the first of two times we'll ever use this representability theorem for groups we don't know to be finitely generated)

Let's now talk about the $\ell = p$ case. Same setup, i.e. $G_K \curvearrowright U$ continuously.

Assumption. Assume U is de Rham and mixed w/ negative weights.

Definition 17.8. We define subfunctors

$$\mathrm{H}^1_e(G_K, U) \leq \mathrm{H}^1_f(G_K, U) \leq \mathrm{H}^1_g(G_K, U) \leq \mathrm{H}^1(G_K, U)$$

via

$$\begin{aligned}
\mathrm{H}^1_e(G_K, U)(\Lambda) &:= \mathrm{H}^1_e(G_K, U(\Lambda)) := \ker\left(\mathrm{H}^1(G_K, U(\Lambda)) \longrightarrow \mathrm{H}^1(G_K, U(B_{\mathrm{cris}}^{\varphi=1} \otimes_{\mathbb{Q}_p} \Lambda))\right) \\
\mathrm{H}^1_f(G_K, U)(\Lambda) &:= \mathrm{H}^1_f(G_K, U(\Lambda)) := B_{\mathrm{cris}} \\
\mathrm{H}^1_g(G_K, U)(\Lambda) &:= \mathrm{H}^1_g(G_K, U(\Lambda)) := B_{\mathrm{dR}}.
\end{aligned} \qquad \diamond$$

Remark 17.9.

- The G_K action on $U(B_{cris}^{\varphi=1} \otimes \Lambda)$ is the one induced from the actions on U and on $B_{\mathrm{cris}}^{\varphi=1}$.
- The topology on $B_{cris}^{\varphi=1} \otimes \Lambda$ is the one induce from an identification $B_{\mathrm{cris}}^{\varphi=1} \otimes \Lambda \cong \left(B_{\mathrm{cris}}^{\varphi=1}\right)^{\oplus I}$.
- If U is unipotent, the topology on $U(B_{\mathrm{cris}}^{\varphi=1} \otimes \Lambda) \cong \mathrm{Lie}(U) \otimes B_{\mathrm{cris}}^{\varphi=1} \otimes \Lambda$ is again the natural one.
- If U is pro-unipotent, take the inverse limit topology.
- But actually, the topology doesn't matter. More precisely, $\mathrm{H}^1_e(G_K, U(\Lambda))$ consists of cohomology classes represented by (continuous) cocycles $\xi : G_K \to U(\Lambda)$ which are the coboundary of some $u \in U(B_{\mathrm{cris}}^{\varphi=1} \otimes \Lambda)$, i.e. $\xi(\sigma) = u^{-1}\sigma(u)$. $\circ$

Theorem 17.10. $\mathrm{H}^1_e, \mathrm{H}^1_f, \mathrm{H}^1_g$ *are all representable by closed subschemes of* $\mathrm{H}^1(G_K, U)$.

(Apparently the first proof in the literature of such a representability statement is wrong, so be careful if you ever try to hunt down a reference for this statement)

Before getting to the proof, lets setup some notation.

Notation 17.11. For $B \in \left\{B_{\mathrm{cris}}^{\varphi=1}, B_{\mathrm{cris}}, B_{\mathrm{dR}}\right\}$, consider the functor

$$\begin{array}{rccc}
U_B : & \mathrm{Alg}_{\mathbb{Q}_p} & \longrightarrow & \mathrm{Grp}^{\mathrm{Top}} \\
& \Lambda & \longmapsto & U(B \otimes \Lambda)^{\cdot}
\end{array}$$

This allows us to write, e.g.

$$\mathrm{H}^1_e(G_K, U) = \ker\left(\mathrm{H}^1(G_K, U) \to \mathrm{H}^1(G_K, U_{B_{\mathrm{cris}}^{\varphi=1}})\right).$$

We also define functors

$$\begin{aligned}
D_{\mathrm{cris}}^{\varphi=1}(U) &: \mathrm{Alg}_{\mathbb{Q}_p} \longrightarrow \mathrm{Grp} \\
D_{\mathrm{cris}}(U) &: \mathrm{Alg}_{K_0} \longrightarrow \mathrm{Grp} \\
D_{\mathrm{dR}}(U) &: \mathrm{Alg}_{K} \longrightarrow \mathrm{Grp}
\end{aligned}$$

via

$$D^{\varphi=1}_{\mathrm{cris}}(U)(\Lambda) := U\Big(B^{\varphi=1}_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} \Lambda\Big)^{G_K} \quad \text{and} \quad D_{\mathrm{cris}}(U)(\Lambda) := U(B_{\mathrm{cris}} \otimes_{K_0} \Lambda)^{G_K}$$

($D_{\mathrm{dR}}(U)$ is defined as you'd expect). Above, $K_0 = (B_{\mathrm{cris}})^{G_K}$ is the maximal unramified (over $\mathbb{Q}_p$) subfield of K.

Proposition 17.12. *$D^{\varphi=1}_{cris}(U)$, $D_{cris}(U)$, $D_{dR}(U)$ are all three representable by pro-unipotent groups over $\mathbb{Q}_p, K_0, K$, respectively. Moreover, $D^{\varphi=1}_{cris}(U) = 1$.*

Proof for U unipotent. We use the logarithm isomorphism $U \cong \mathrm{Lie}(U)$. Hence, for example

$$D_{\mathrm{dR}}(U)(\Lambda) \cong \big(\mathrm{Lie}(U) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}} \otimes_K \Lambda\big)^{G_K} = \big(\mathrm{Lie}(U) \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}\big)^{G_K} \otimes_K \Lambda \cong D_{\mathrm{dR}}(\mathrm{Lie}(U)) \otimes_K \Lambda$$

under this identification. This directly says that $D_{\mathrm{dR}}(U)$ is isomorphic to the affine space attached to $D_{\mathrm{dR}}(\mathrm{Lie}(U))$. Moreover, the group law on $D_{\mathrm{dR}}(U)(\Lambda)$ corresponds to the BCH product on $D_{\mathrm{dR}}(\mathrm{Lie}\, U)$ (because D_{dR} is a $\otimes$-functor on de Rham reps, the Lie algebra structure on $\mathrm{Lie}\, U$ induces one on $D_{\mathrm{dR}}(\mathrm{Lie}\, U)$), so $D_{\mathrm{dR}}(U)$ is unipotent. The same sort of argument works for the other two functors.

We will need to prove that $D^{\varphi=1}_{\mathrm{cris}}(\mathrm{Lie}\, U) = 0$. We know that $D^{\varphi=1}_{\mathrm{cris}}(V_n) = 0$ for all n by our assumption on weights. Since $D^{\varphi=1}_{\mathrm{cris}}$ is left-exact, this suffices (argue by induction, using that $\mathrm{Lie}(U)$ is an iterated extension of the V_n's). ∎

We'll now prove representability of these Bloch-Kato Selmer functors. It sounds like the arguments for each are a little different. We'll first do $\mathrm{H}^1_e(G_K, U)$.

Proof that $\mathrm{H}^1_e(G_K, U)$ is representable, assuming U is unipotent. We'll show by induction that $\mathrm{H}^1_e(G_K, U_n)$ is representable for all n. Here, $U_n = U/W_{-n-1}U$ as usual (note $U = U_n$ for $n \gg 1$ when U is unipotent). The base case $n = 0$ is trivial. For the inductive step, use the central extension

$$1 \longrightarrow V_n \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1.$$

Assume that $\mathrm{H}^1_e(G_K, U_{n-1})$ is representable. Let $\mathrm{H}_{e,n}$ be the preimage of $\mathrm{H}^1_e(G_K, U_{n-1})$ under $\mathrm{H}^1(G_K, U_n) \to \mathrm{H}^1(G_K, U_{n-1})$. Equivalently,

$$\mathrm{H}_{e,n} = \ker\Big(\mathrm{H}^1(G_K, U_n) \to \mathrm{H}^1(G_K, U_{n-1, B^{\varphi=1}_{\mathrm{cris}}})\Big).$$

We know that $H_{e,n}$ is representable by a closed subscheme of $\mathrm{H}^1(G_K, U)$ (it's the preimage of a closed subscheme under a representable map) and that $\mathrm{H}^1_e(G_K, U_n) \subset \mathrm{H}_{e,n}$. For any $\Lambda \in \mathrm{Alg}_{\mathbb{Q}_p}$, the sequence

$$1 \longrightarrow V_n\Big(B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda\Big) \longrightarrow U_n(blah) \longrightarrow U_{n-1}(blah) \longrightarrow 1$$

is topologically split, so we get an exact sequence

$$\mathrm{H}^0(G_K, U_{n-1, B^{\varphi=1}_{cris}}) \to \mathrm{H}^1(G_K, V_{n, B^{\varphi=1}_{cris}}) \xrightarrow{\alpha} \mathrm{H}^1(G_K, U_{n, B^{\varphi=1}_{cris}}) \xrightarrow{\beta} \mathrm{H}^1(G_K, U_{n-1, B^{\varphi=1}_{cris}}).$$

Furthermore, $\ker\alpha = \{*\}$ as $\mathrm{H}^0(G_K, U_{n-1,blah}) = D^{\varphi=1}_{cris}(U_{n-1}) = 1$ by Proposition 17.12. Let

$$\psi : \mathrm{H}^1(G_K, U_n) \longrightarrow \mathrm{H}^1(G_K, U_{n, B^{\varphi=1}_{cris}}).$$

By construction, $\psi|_{\mathrm{H}_{e,n}}$ satisfies $\beta \circ \psi|_{\mathrm{H}_{e.n}} = 1$, and so lifts to a map

$$\widetilde{\psi} : \mathrm{H}_{e,n} \longrightarrow \mathrm{H}^1(G_K, V_{n,B_{cris}^{\varphi=1}}).$$

Now, it is not too hard to show that $\mathrm{H}^1(G_K, V_{n,blah})$ is subrepresentable. Hence, $\mathrm{H}^1_e = \ker \psi = \ker \widetilde{\psi}$ is a closed subscheme of $\mathrm{H}_{e,n}$, hence of $\mathrm{H}^1(G_K, U_n)$ as well. ■

18 Lecture 16 (3/30): Bloch-Kato Selmer Schemes

Note 9. About 6 minutes late

Recall 18.1. Let $K/\mathbb{Q}_p$ be a finite extension. Let U be a de Rham representation of G_K on a finitely generated pro-unipotent group over $\mathbb{Q}_p$. Assume U has a G_K-invariant separated filtration

$$U = W_{-1}U \trianglerighteq W_{-2}U \trianglerighteq \dots$$

such that V_n is pure of weight $-n$ for all n. In this situation, we have shown that $\mathrm{H}^1(G_K, U)$ is representable by an affine $\mathbb{Q}_p$-scheme.

Notation 18.2. Given such a filtration, we always set

$$U_n = U/W_{-n-1}U \text{ and } V_n = W_{-n}U/W_{-n-1}U,$$

so V_n is a vector group, and we have a central extension

$$1 \longrightarrow V_n \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1.$$

Define subfunctors of $\mathrm{H}^1(G_K, U)$ by

$$\begin{aligned}
\mathrm{H}^1_e(G_K, U)(\Lambda) &:= \mathrm{H}^1_e(G_K, U(\Lambda)) := \ker\left(\mathrm{H}^1(G_K, U(\Lambda)) \longrightarrow \mathrm{H}^1(G_K, U(B_{\mathrm{cris}}^{\varphi=1} \otimes_{\mathbb{Q}_p} \Lambda))\right) \\
\mathrm{H}^1_f(G_K, U)(\Lambda) &:= \mathrm{H}^1_f(G_K, U(\Lambda)) := B_{\mathrm{cris}} \\
\mathrm{H}^1_g(G_K, U)(\Lambda) &:= \mathrm{H}^1_g(G_K, U(\Lambda)) := B_{\mathrm{dR}}.
\end{aligned}$$

Last time, we ended by proving the following.

Theorem 18.3. *$\mathrm{H}^1_e(G_K, U) \subset \mathrm{H}^1(G_K, U)$ is representable by a closed subscheme.* ⊙

In fact, we stated the following stronger result.

Theorem 18.4 (Theorem 17.10)**.** *$\mathrm{H}^1_e(G_K, U) \subset \mathrm{H}^1_f(G_K, U) \subset \mathrm{H}^1_g(G_K, U)$ are all representable by closed subschemes of $\mathrm{H}^1(G_K, U)$.*

Question 18.5 (Audience)**.** *For abelian local B-K Selmer groups, there was a duality between $\mathrm{H}^1_e(V)$ and $\mathrm{H}^1_g(V^*(1))$. Is there something similar for unipotent groups? What's $U^*(1)$?*

Answer (paraphrased)**.** As far as I know, there's no nice lift of this duality for unipotent groups. In particular, there's no definition for $U^*(1)$. ⋆

Remark 18.6. Sounds like the proof of representability of H^1_g is similar to the proof for H^1_e, so we'll omit it in lecture. The details are in the lecture notes though. ∘

Question 18.7 (Audience)**.** *What are these subfunctors supposed to be capturing?*

Answer. In the abelian case, say $V = V_pA$ is the Tate module of an abelian variety, then $\mathrm{H}^1_e = \mathrm{H}^1_f = \mathrm{H}^1_g = \mathbb{Q}_p \cdot \mathrm{im}\big(A(K) \to \mathrm{H}^1(G_K, V_pA)\big)$. If A is only semi-abelian, then $\mathrm{H}^1_e = \mathrm{H}^1_f$ is the $\mathbb{Q}_p$-span of the image of the integral points $\mathcal{A}(\mathscr{O}_K)$ on some integral model (assuming I heard correctly), and H^1_g is something else. Alex said more after this, but I missed it. ⋆

(There was also another question that I missed, about some detail that comes up in the proof of representability of H^1_g)

Today, though, we'll prove representability of H^1_f via the following proposition.

Proposition 18.8. *Under the assumptions laid out in Recall 18.1,*

$$\mathrm{H}^1_f(G_K, U) = \mathrm{H}^1_e(G_K, U).$$

This will in particular use the weight filtration.

Lemma 18.9. *For any $\mathbb{Q}_p$-algebra Λ, the map*

$$\mathrm{Res}_{K_0/\mathbb{Q}_p} D_{cris}(U)(\Lambda) \longrightarrow \mathrm{Res}_{K_0/\mathbb{Q}_p} D_{cris}(U)(\Lambda)$$

(recall above that $\mathrm{Res}_{K_0/\mathbb{Q}_p} D_{cris}(U)(\Lambda) = U\big(B_{cris} \otimes_{\mathbb{Q}_p} \Lambda\big)^{G_K}$) given by

$$w \longmapsto w^{-1}\varphi(w)$$

(above, φ is crystalline Frobenius) is bijective.

Proof. The Frobenius φ defines an action of $\mathbb{Z}$ on $U_{\mathrm{cris}} := \mathrm{Res}^{K_0}_{\mathbb{Q}_p} D_{\mathrm{cris}}(U)$. Equip U_{cris} with the filtration induced by the weight filtration on U, and write $V_{n,cris}$ for its graded pieces. We know that

$$V_{n,cris} \leq \mathrm{Res}^{K_0}_{\mathbb{Q}_p} D_{\mathrm{cris}}(V_n),$$

so $V^{\varphi=1}_{n,cris} \leq D^{\varphi=1}_{\mathrm{cris}}(V_n) = 0$. This shows that $\mathrm{H}^0(\mathbb{Z}, V_{n,cris}) = 0$. We also know that

$$\mathrm{H}^1(\mathbb{Z}, V_{n,cris}) = V_{n,cris}/(\varphi - 1)$$

is f.dimensional. One can use the representability theorem[20] to get that $\mathrm{H}^1(\mathbb{Z}, U_{cris})$ is representable by a closed subscheme of $\prod_n \mathrm{H}^1(\mathbb{Z}, V_{n,cris})$. At the same time,

$$\dim \mathrm{H}^1(\mathbb{Z}, V_{n,cris}) = \dim \mathrm{coker}(\varphi - 1) = \dim \ker(\varphi - 1) = \dim \mathrm{H}^0(\mathbb{Z}, V_{n,cris}) = 0,$$

so we must in fact that $\mathrm{H}^1(\mathbb{Z}, U_{cris}) = 1$. As such, $\mathrm{H}^1(\mathbb{Z}, U_{cris}(\Lambda)) = 1$, so any cocycle ξ is a coboundary, i.e. there is some $w \in U_{cris}(\Lambda)$ such that $\xi(n) = w^{-1}\varphi^n(w)$ for all n. This show surjectivity of $w \mapsto w^{-1}\varphi(w)$. Injectivity comes from $\mathrm{H}^0(\mathbb{Z}, U_{cris}) = 1$. ■

(Compare above with Corollary 16.2 from OH)

Proof of Proposition 18.8. Suppose that $\xi \in Z^1(G_K, U)$ represents a class in $\mathrm{H}^1_f(G_K, U)$. We aim to show that it represents a class in H^1_e. By assumption, there exists some $u \in U(B_{\mathrm{cris}} \otimes \Lambda)$ whose coboundary is ξ, i.e. such that

$$\xi(\sigma) = u^{-1}\sigma(u) \text{ for all } \sigma \in G_K.$$

[20] We stated this for profinite groups, but it also works for $\mathbb{Z}$

As $\xi(\sigma) \in U(\Lambda) \subset U(B_{\mathrm{cris}} \otimes \Lambda)^{\varphi=1}$, we know that

$$\varphi(u^{-1}\sigma(u)) = u^{-1}\sigma(u).$$

Commuting the σ, φ actions, this says

$$\sigma\big(u\varphi(u)^{-1}\big) = u\varphi(u)^{-1} \text{ for all } \sigma \in G_K,$$

so $u\varphi(u)^{-1} \in U(B_{\mathrm{cris}} \otimes \Lambda)^{G_K} = \mathrm{Res}^{K_0}_{\mathbb{Q}_p} D_{\mathrm{cris}}(U)(\Lambda)$. By Lemma 18.9, there is a unique $w \in U(B_{\mathrm{cris}} \otimes \Lambda)^{G_K}$ such that $u\varphi(u)^{-1} = w^{-1}\varphi(w)$, i.e. $\varphi(wu) = wu$. Thus,

$$wu \in U(B_{\mathrm{cris}}^{\varphi=1} \otimes \Lambda) \text{ and } (wu)^{-1}\sigma(wu) = u^{-1}\sigma(u) = \xi(\sigma)$$

for all $\sigma \in G_K$, so ξ is the coboundary of an element of $U(B_{\mathrm{cris}}^{\varphi=1} \otimes \Lambda)$. This, by definition, means that $[\xi] \in \mathrm{H}^1_e$. ■

18.1 The non-abelian (read: unipotent) Bloch-Kato exponential

Recall 18.10. Let V be a de Rham representation of G_K. Then, there is an exact sequence

$$0 \longrightarrow V^{G_K} \longrightarrow D_{\mathrm{cris}}^{\varphi=1}(V) \oplus D_{\mathrm{dR}}^{+}(V) \longrightarrow D_{\mathrm{dR}}(V) \longrightarrow \mathrm{H}^1_e(G_K, V) \longrightarrow 0$$

(coming from the fundamental exact sequence $0 \to \mathbb{Q}_p \to B_{\mathrm{cris}}^{\varphi=1} \oplus B_{\mathrm{dR}}^{+} \to B_{\mathrm{dR}} \to 0$). If you like, you can write this as

$$\mathrm{H}^1_e(G_K, V) = \frac{D_{\mathrm{dR}}(V)}{D_{\mathrm{dR}}^{+}(V) + D_{\mathrm{cris}}^{\varphi=1}(V)}. \qquad \odot$$

Theorem 18.11 (non-abelian Bloch-Kato exponential)**.** *Let U be a de Rham representation of G_K on a f.g. pro-unipotent group. Then, there exists a canonical isomorphism of functors*

$$\mathrm{H}^1_e(G_K, U) \cong \mathrm{Res}^K_{\mathbb{Q}_p} D^{+}_{dR}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{dR}(U) \Big/ D^{\varphi=1}_{cris}(U)$$

(the quotients are taken pointwise).

The $\longleftarrow$ map is called the Bloch-Kato exponential $\exp_{\mathrm{BK}}$. The $\longrightarrow$ map is called the Bloch-Kato logarithm $\log_{\mathrm{BK}}$.

Note there's no weight assumption above.

Remark 18.12. Suppose U is mixed with negative weights. This in particular implies that $D_{\mathrm{cris}}^{\varphi=1}(U) = 1$, so

$$\mathrm{H}^1_f(G_K, U) = \mathrm{H}^1_e(G_K, U) \cong \mathrm{Res}^K_{\mathbb{Q}_p} D_{\mathrm{dR}}^{+}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{\mathrm{dR}}(U).$$

This gives a new proof of representability (though not necessarily by a closed subspace of H^1). This also implies (via a problem[21] on pset5) that $\mathrm{H}^1_f = \mathrm{H}^1_e$ is isomorphic to an affine space/$\mathbb{Q}_p$ if U is unipotent. Furthermore, if U is unipotent, we see that

$$\dim_{\mathbb{Q}_p} \mathrm{H}^1_e = [K : \mathbb{Q}_p]\big(\dim_K D_{\mathrm{dR}}(U) - \dim_K D_{\mathrm{dR}}^{+}(U)\big) = [K : \mathbb{Q}_p] \sum_n \big(\dim_K D_{\mathrm{dR}}(V_n) - \dim_K D_{\mathrm{dR}}^{+}(V_n)\big).$$

In practice, the RHS above is relatively easy to compute. One can also use this (along with the fact that $D_{\mathrm{dR}}(U_n) \twoheadrightarrow D_{\mathrm{dR}}(U_{n-1})$) to show that $\mathrm{H}^1_f(G_K, U_n)$ is an $\mathrm{H}^1_f(G_K, V_n)$-torsor over $\mathrm{H}^1_f(G_K, U_{n-1})$. ∘

[21] See Problem A.3 (and Proposition 17.12)

Question 18.13 (Audience)**.** *What's exponential about this?*

Answer. We'll answer this in office hours [the tagline for today's OH that was written on the board at the beginning of lecture was "why is the Bloch-Kato exponential an exponential?"] ⋆

Office hours ended up being taken up by various audience questions, so (I think) we didn't quite get to this.

Let's construct these exponential and logarithm maps (hopefully it'll be clear that they're inverse). We start with the exponential

$$\exp_{\mathrm{BK}} : \mathrm{Res}^K_{\mathbb{Q}_p} D^+_{\mathrm{dR}}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{\mathrm{dR}}(U) \Big/ D^{\varphi=1}_{\mathrm{cris}}(U) \longrightarrow \mathrm{H}^1_e(G_K, U).$$

Lemma 18.14. *Let $U/\mathbb{Q}_p$ be a pro-unipotent group. Then,*

(a) *The multiplication map*

$$U\big(B^+_{dR} \otimes \Lambda\big) \times U\Big(B^{\varphi=1}_{cris} \otimes \Lambda\Big) \longrightarrow U(B_{dR} \otimes \Lambda)$$

is surjective.

(b) *Inside $U(B_{dR} \otimes \Lambda)$,*

$$U(B^+_{dR} \otimes \Lambda) \cap U(B^{\varphi=1}_{cris} \otimes \Lambda) = U(\Lambda)$$

with its usual topology.

Proof. **(b)** The validity of this statement is preserved under limits, so it suffices to prove it assuming U is unipotent. Identifying U with its Lie algebra, the claim becomes

$$\big(\mathrm{Lie}(U) \otimes B^+_{\mathrm{dR}} \otimes \Lambda\big) \cap \Big(\mathrm{Lie}(U) \otimes B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda\Big) = \mathrm{Lie}(U) \otimes \Lambda \subset \mathrm{Lie}(U) \otimes B_{\mathrm{dR}} \otimes \Lambda.$$

The LHS above is $\mathrm{Lie}(U) \otimes \Big(B^+_{\mathrm{dR}} \cap B^{\varphi=1}_{\mathrm{cris}}\Big) \otimes \Lambda$, so we win as $B^+_{\mathrm{dR}} \cap B^{\varphi=1}_{\mathrm{cris}} = \mathbb{Q}_p$.

(a) We'll actually prove a stronger statement. Choose $\overline{B} \subset B^{\varphi=1}_{\mathrm{cris}}$ a complement of $\mathbb{Q}_p$, i.e. $B^{\varphi=1}_{\mathrm{cris}} = \mathbb{Q}_p \oplus \overline{B}$. This $\overline{B}$ is not a ring, but we won't let that stop us. For U unipotent, define

$$U(\overline{B} \otimes \Lambda) := \mathrm{Lie}(U) \otimes \overline{B} \otimes \Lambda \subset U(B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda).$$

Extend this to pro-unipotent U by taking limits. We'll prove that the multiplication map

$$U\big(B^+_{\mathrm{dR}} \otimes \Lambda\big) \times U\big(\overline{B} \otimes \Lambda\big) \xrightarrow{\mu} U(B_{\mathrm{dR}} \otimes \Lambda)$$

is bijective (which is stronger than **(a)**). This statement is stable under small limits, so we may and do assume that U is unipotent.

We do this by induction. U is abelian, μ is the addition map

$$\big(\mathrm{Lie}(U) \otimes B^+_{\mathrm{dR}} \otimes \Lambda\big) \oplus \big(\mathrm{Lie}(U) \otimes \overline{B} \otimes \Lambda\big) \longrightarrow \mathrm{Lie}(U) \otimes B_{\mathrm{dR}} \otimes \Lambda.$$

This is bijective simply because $B_{\mathrm{dR}} = B^+_{\mathrm{dR}} \oplus \overline{B}$. In general, proceed by induction, noting that for $B \in \big\{B^+_{\mathrm{dR}}, B_{\mathrm{dR}}, \overline{B}\big\}$, $U_n(B \otimes \Lambda)$ is a $V_n(B \otimes \Lambda)$-torsor over $U_{n-1}(B \otimes \Lambda)$, so if μ is bijective for $U = U_{n-1}, V_n$, then its a torsor morphism (so bijective) for $U = U_n$. ∎

We have to stop here. We'll start next time w/ the definition of the BK exponential.

19 Office Hours

An analogy to keep in mind between the $\ell = p$ and $\ell \neq p$ cases of this $\mathrm{H}^1_{e,f,g}$ stuff.

- $\mathrm{H}^1_f \,/\, \mathrm{H}^1_e$ is like unramified cohomology H^1_{nr} in the $\ell \neq p$ case.
- $\mathrm{H}^1_g \,/\, \mathrm{H}^1_e$ is like the whole cohomology H^1 in the $\ell \neq p$ case.

As an example of this, compare Proposition 17.7 and Proposition 18.8.

Note 10. There was some more discussion in this direction that I didn't follow.

Question 19.1 (Audience)**.** *Why expect representability of these* H^1*'s?*

Answer. Great question. If you replace a unipotent group by a reductive group, you shouldn't expect these things to be representable. (Got distracted by sweets, so the answer ended here) ⋆

Question 19.2 (Audience)**.** *Can you remind us how these cohomology functors relate the non-abelian Chabauty?*

Answer. Vague idea it to understand how $X(\mathbb{Q})$ sits inside of $X(\mathbb{Q}_p)$ via cohomological information. One does this by forming a square

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle j_p} \\ \mathrm{H}^1(G_{\mathbb{Q}}, ?) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1(G_p, ?), \end{array}$$

which gives an obstruction to a p-adic point being rational. Namely, if $x \in X(\mathbb{Q}_p)$ is actually rational, then $j_p(x) \in \mathrm{im}(\mathrm{loc}_p)$.

For us, let U be (a quotient of) the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $X_{\overline{\mathbb{Q}}}$ based at some rational point $b \in X(\mathbb{Q})$. This will replace the ? in the above square. Also, $X/\mathbb{Q}$ will be a smooth connected variety with $X(\mathbb{Q}) \neq \emptyset$. The map $j : X(\mathbb{Q}) \to \mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p))$ is defined as follows. For $x \in X(\mathbb{Q})$, we have a path torsor

$$\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b, x) \curvearrowleft G_{\mathbb{Q}}.$$

Fix a choice of path $\gamma \in \pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b, x)(\mathbb{Q}_p)$, and define $\xi(\sigma) = \gamma^{-1}\sigma(\gamma)$. Then, $\xi \in Z^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p))$ and we set $j(x) = [\xi]$.

One wants a handle on this localization map. We know (Theorem 15.4) that $\mathrm{H}^1(G_p, U(\mathbb{Q}_p))$ is the $\mathbb{Q}_p$-points of an affine scheme. Suppose the same is true for $\mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p))$.[22] Then, loc_p is algebraic, and we may define

$$X(\mathbb{Q}_p)_U := \left\{x \in X(\mathbb{Q}_p) : j_p(x) \in \text{scheme-theoretic image of } \mathrm{loc}_p\right\}$$

(the "Chabauty locus associated to U").

What about all this Selmer stuff? Assume we've chosen a prime p of good reduction for X. Also assume that X is projective. In this case, the local Kummer map will land in $\mathrm{H}^1_f(G_p, U(\mathbb{Q}_p))$. Similarly, the global Kummer map will land in the (to-be-defined) Selmer scheme $\mathrm{Sel}_U(X)$.[23]

Theorem 19.3. *If* $\dim_{\mathbb{Q}_p} \mathrm{Sel}_U(X) < \dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_p, U)$*, then* $X(\mathbb{Q})$ *is not Zariski dense.* ⋆

[22] This is not literally true

[23] This will actually be representable. Part of the issue with $\mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p))$ is that $G_{\mathbb{Q}}$ doesn't satisfy property (F) (e.g. there are infinitely many index 2 subgroups/quadratic extensions of $\mathbb{Q}$)

Question 19.4 (Audience)**.** *Can you say a bit of history? How do you get from Chabauty's original $r < g$ argument to considering something like these descent squares?*

Answer. Here's an ahistorical answer. First note $\pi_1^{\mathrm{ab}} = V_pJ$ ($\pi_1 = \pi_1^{\mathbb{Q}_p}$). Then, $j_p : X(\mathbb{Q}_p) \to \mathrm{H}^1_f(G_p, V_pJ)$ is the composition of Abel-Jacobi and the usual Kummer map.[24] The Bloch-Kato exponential gives an isomorphism

$$\mathrm{H}^1_f(G_p, V_pJ) \cong \frac{D_{\mathrm{dR}}(V_pJ)}{D^+_{\mathrm{dR}}(V_pJ)} = \left(F^0 D_{\mathrm{dR}}(V_pJ^*)\right)^* = \mathrm{H}^0(X, \Omega^1)^*$$

and the composition $X(\mathbb{Q}_p) \to \mathrm{H}^0(X, \Omega^1)^*$ is integration. On the global side, $J(\mathbb{Q}) \otimes \mathbb{Q}_p \subset \mathrm{Sel}_{V_pJ}(X)$ (w/ equality if Sha is finite). So when $U = \pi_1^{\mathrm{ab}} = V_pJ$, the descent square looks like

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ J(\mathbb{Q}) \otimes \mathbb{Q}_p & \longrightarrow & \mathrm{H}^0(X, \Omega^1)^*, \end{array}$$

and essentially recovers classic Chabauty. ⋆

Question 19.5 (Audience, paraphrase)**.** *What was the start of looking at the pro-unipotent fundamental group? Was a theory set up already before Kim's work on Chabauty?*

Answer. The first paper looking at this sort of stuff is "Le group fondamental de la droite projective moins trois points" by Deligne. Deligne approached this using the perspective of motives.

Note 11. Alex said a few motivational/introductory remarks on motives that I missed.

If you have a variety X, you get a whole zoo of cohomology theories: étale, de Rham, cristaline (of special fiber), Betti, etc. These aren't all that different from each, e.g. they all have the same dimension. In fact, there are various comparison theorems like

$$\mathrm{H}^*_B(X, \mathbb{Q}) \otimes \mathbb{C} \cong \mathrm{H}^*_{\mathrm{dR}}(X/\mathbb{Q}) \otimes \mathbb{C}.$$

They aren't all quite the same though, since they have different extra structures on them. For example $\mathrm{H}^*_{\text{ét}}$ is a $G_{\mathbb{Q}}$-rep, $\mathrm{H}^*_{\mathrm{dR}}$ is a filtered vector space, $\mathrm{H}^*_B + \mathrm{H}^*_{\mathrm{dR}}$ is a pure Hodge structure, $\mathrm{H}^*_{\mathrm{cris}} + \mathrm{H}^*_{\mathrm{dR}}$ is a filtered φ-module. The idea of motives then, is that there should exist an abelian category $\underline{\mathrm{Mot}}_{\mathbb{Q}}$ of motives supporting

- A cohomology theory $\mathrm{H}^* : \mathrm{Var}_{\mathbb{Q}} \longrightarrow \underline{\mathrm{Mot}}_{\mathbb{Q}}$; and
- realization functors $\rho^{\text{ét}} : \underline{\mathrm{Mot}}_{\mathbb{Q}} \to \mathrm{Rep}(G_{\mathbb{Q}})$, etc.

such that, e.g. $\mathrm{H}^*_{\text{ét}} = \rho^{\text{ét}}\,\mathrm{H}^*$. The category of motives should also have other, extra nice properties in addition to the one written above.

Back to Deligne's paper, he asked, "what about π_1?" Is there a motivic π_1? If so, should get various realizations. Delgine constructs pro-unipotent étale, de Rham, Betti, (nowadays also crystalline) fundamental groups along with all relevant comparision isomorphisms. ⋆

Question 19.6 (Audience, paraphrase)**.** *What does chabauty look like when used for integral points instead of rational points?*

[24] Alex initially called this the "non-abelian Kummer map," and then (after some laughter) followed this up with "I told you I [have a habit of] inserting the word 'non-abelian', even in conversation with normal people." (paraphrase)

Answer. Say $\mathcal{Y}/\mathbb{Z}_S$ is a curve over the S-integers. Assume $\mathcal{Y} = \mathcal{X} \setminus \mathcal{D}$ where $\mathcal{X}/\mathbb{Z}_S$ is a proper integral curve, and $\mathcal{D}$ is a horizontal divisor. Use roman letters for generic fibers. Choose $p \notin S$. Assume "p is of good reduction," i.e. $\mathcal{X}$ is smooth over $\mathbb{Z}_p$, $\mathcal{D}$ is étale over $\mathbb{Z}_p$, and the implicit basepoint $b \in \mathcal{Y}(\mathbb{Z}_p)$. You then get a square like

$$\begin{array}{ccc} \mathcal{Y}(\mathbb{Z}_S) & \longrightarrow & \mathcal{Y}(\mathbb{Z}_p) \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle j_p} \\ \mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S) & \xrightarrow{\mathrm{loc_p}} & \mathrm{H}^1_f(G_p, U(\mathbb{Q}_p)). \end{array}$$

⋆

Question 19.7 (Audience)**.** *When do we use smoothness in all of this?*

Answer. Smooth implies the fundamental group only has negative weights.

Example 19.8. For a nodal cubic, apparently one has $\pi_1^{\mathbb{Q}_p} = \mathbb{Q}_p(0)$. △

⋆

20 Lecture 17 (4/4): Local Bloch-Kato Selmer schemes

Recall 20.1. Let $K/\mathbb{Q}_p$ be a finite extension.

Theorem 20.2 (Non-abelian Bloch-Kato exponential, Theorem 18.11)**.** *Let U be a de Rham representation of G_K on a finitely generated pro-unipotent group over $\mathbb{Q}_p$. Then, there exists a canonical isomorphism of functors*

$$\exp_{BK} : \mathrm{Res}^K_{\mathbb{Q}_p} D^+_{dR}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{dR}(U) \Big/ D^{\varphi=1}_{cris}(U) \longrightarrow \mathrm{H}^1_e(G_K, U).$$

Lemma 20.3 (Lemma 18.14)**.** *Let $U/\mathbb{Q}_p$ be a pro-unipotent group. Then,*

(a) *The multiplication map*

$$U\big(B^+_{dR} \otimes \Lambda\big) \times U\Big(B^{\varphi=1}_{cris} \otimes \Lambda\Big) \longrightarrow U(B_{dR} \otimes \Lambda)$$

is surjective.

(b) *Inside $U(B_{dR} \otimes \Lambda)$,*

$$U(B^+_{dR} \otimes \Lambda) \cap U(B^{\varphi=1}_{cris} \otimes \Lambda) = U(\Lambda)$$

with its usual topology.

Also, some period ring stuff

- $B^{\varphi=1}_{\mathrm{cris}} \subset B_{\mathrm{cris}} \subset B_{\mathrm{dR}} \supset B^+_{\mathrm{dR}}$
- $B^+_{\mathrm{dR}} \cap B^{\varphi=1}_{\mathrm{cris}} = \mathbb{Q}_p$ (compare this to **(b)** above)
- $B^+_{\mathrm{dR}} + B^{\varphi=1}_{\mathrm{cris}} = B_{\mathrm{dR}}$ (compare this to **(a)** above) ⊙

With these recollections out of the way, we can define the Bloch-Kato exponential

$$\exp_{\mathrm{BK}} : \mathrm{Res}^K_{\mathbb{Q}_p} D^+_{\mathrm{dR}}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{\mathrm{dR}}(U) \Big/ D^{\varphi=1}_{\mathrm{cris}}(U) \longrightarrow \mathrm{H}^1_e(G_K, U).$$

Construction 20.4. Let Λ be a $\mathbb{Q}_p$-algebra, and choose some $u \in \mathrm{Res}^K_{\mathbb{Q}_p} D_{\mathrm{dR}}(U)(\Lambda) = U(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} \Lambda)^{G_K}$. By Lemma 20.3, we can write $u = u_{\mathrm{dR}} u_{\mathrm{cris}}^{-1}$ for some $u_{\mathrm{dR}} \in U(B^+_{\mathrm{dR}} \otimes \Lambda)$ and $u_{\mathrm{cris}} \in U(B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda)$. Because $u = u_{\mathrm{dR}} u_{\mathrm{cris}}^{-1}$ is G_K-fixed, we can arrange that

$$\xi(\sigma) := u_{\mathrm{dR}}^{-1} \sigma(u_{\mathrm{dR}}) = u_{\mathrm{cris}}^{-1} \sigma(u_{\mathrm{cris}}) \text{ for all } \sigma \in G_K.$$

Now,

$$\xi(\sigma) \in U(B^+_{\mathrm{dR}} \otimes \Lambda) \cap U(B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda) \overset{\text{Lemma 20.3}}{=} U(\Lambda),$$

so $\xi \in Z^1(G_K, U(\Lambda))$. Furthermore, $[\xi] \in \mathrm{H}^1_e(G_K, U(\Lambda))$ because ξ is the coboundary of $u_{\mathrm{cris}} \in U(B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda)$. ⎔

Claim 20.5. $[\xi]$ *is independent of*

- *choice of factorization of* $u = u_{dR} u_{cris}^{-1}$
- *the actions of* $\mathrm{Res}^K_{\mathbb{Q}_p} D^+_{dR}(U) \times D^{\varphi=1}_{cris}(U)$

Thus, Construction 20.4 does indeed define a natural transformation

$$\exp_{\mathrm{BK}} : \mathrm{Res}^K_{\mathbb{Q}_p} D^+_{\mathrm{dR}}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{\mathrm{dR}}(U) \Big/ D^{\varphi=1}_{\mathrm{cris}}(U) \longrightarrow \mathrm{H}^1_e(G_K, U).$$

To see that it is a natural *isomorphism*, we will define an inverse, the Bloch-Kato logarithm.

Lemma 20.6. *Let* U *be a de Rham representation of* G_K *on a f.g. pro-unipotent group* $U/\mathbb{Q}_p$*. Then, the natural map*

$$\mathrm{H}^1(G_K, U(B^+_{dR} \otimes \Lambda)) \longrightarrow \mathrm{H}^1(G_K, U(B_{dR} \otimes \Lambda))$$

has trivial kernel.

Proof Sketch. We appeal to the following

Lemma 20.7 (Lemma 3.8.1, [BK90])**.** *If* V *is a de Rham representation of* G_K*, then*

$$\mathrm{H}^1(G_K, B^+_{dR} \otimes V) \longrightarrow \mathrm{H}^1(G_K, B_{dR} \otimes V)$$

is injective.

I guess this lemma is the reason there's no Bloch-Kato Selmer group associated to B^+_{dR}

This implies the lemma when U is abelian. When U is unipotent, induct along the descending central series. In general (U pro-unipotent), take a limit. ■

Note 12. Alex did the diagram chase in the induction step on the board, but I didn't copy this down. TL;DR use the (injectivity half of the) 5-Lemma and that $U_n(B_{\mathrm{dR}})^{G_K} \twoheadrightarrow U_{n-1}(B_{\mathrm{dR}})^{G_K}$ (proving this requires using that D_{dR} is exact).

Remark 20.8. The "trivial kernel" in the statement of Lemma 20.6 is weaker than "injective" (because these are pointed sets, not groups). However, the proof sketch suggests the statement is probably still true if one says "injective" instead of "trivial kernel." ∘

Exercise. Convince yourself that Lemma 20.6 still (or no longer) holds when "trivial kernel" is replaced by "injective".

Construction 20.9 (`Bloch-Kato logarithm`). Choose some $[\xi] \in \mathrm{H}^1_e(G_K, U(\Lambda))$. We know $[\xi]$ maps to $* \in \mathrm{H}^1(G_K, U(B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda))$, so it also maps to the distinguished point in $\mathrm{H}^1(G_K, U(B_{\mathrm{dR}} \otimes \Lambda))$. By

Lemma 20.6, this means is also maps to $* \in \mathrm{H}^1(G_K, U(B^+_{\mathrm{dR}} \otimes \Lambda))$. This means that ξ is the coboundary of some $u_{\mathrm{cris}} \in U(B^{\varphi=1}_{\mathrm{cris}} \otimes \Lambda)$ and of some $u_{\mathrm{dR}} \in U(B^+_{\mathrm{dR}} \otimes \Lambda)$, i.e.

$$\xi(\sigma) = u_{\mathrm{cris}}^{-1}\sigma(u_{\mathrm{cris}}) = u_{\mathrm{dR}}^{-1}\sigma(u_{\mathrm{dR}}).$$

Rearranging, $u := u_{\mathrm{dR}}U_{\mathrm{cris}}^{-1} \in U(B_{\mathrm{dR}} \otimes \Lambda)$ is G_K-fixed, so

$$u \in U(B_{\mathrm{dR}} \otimes \Lambda)^{G_K} = \mathrm{Res}^K_{\mathbb{Q}_p}\,({}_{\mathrm{dR}}U)(\Lambda). \qquad \bigcirc$$

Claim 20.10. *The image of u in*

$$\mathrm{Res}^K_{\mathbb{Q}_p} D^+_{dR}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{dR}(U) \Big/ D^{\varphi=1}_{cris}(U)$$

is independent of the choice of ξ, so Construction 20.4 really defines a natural transformation

$$\log_{BK} : \mathrm{H}^1_e(G_K, U) \longrightarrow \mathrm{Res}^K_{\mathbb{Q}_p} D^+_{dR}(U) \Big\backslash \mathrm{Res}^K_{\mathbb{Q}_p} D_{dR}(U) \Big/ D^{\varphi=1}_{cris}(U).$$

This map is inverse to the $\exp_{\mathrm{BK}}$ defined earlier. Once you're convinced this is true, Theorem 18.11 is proved.

20.1 L10.5: Global Bloch-Kato Selmer schemes

Before talking about global Bloch-Kato Selmer schemes, let's talk about global Bloch-Kato Selmer groups.

Setup 20.11. Let K be a *number field*, and let V be a ($\mathbb{Q}_p$-linear) representation of G_K such that

- V is unramified outside a finite set of places of K.
- V is de Rham at all p-adic places

Question 20.12 (Audience, unimportant)**.** *Does being unramified at a real place mean being trivial there, or is there no condition there?*

Answer. Since we only care about being unramified outside a finite set, the answer doesn't matter for us. We won't worry about ramification at infinite or p-adic places. What the answer morally *should* be in general (for real places) probably depends on the context. $\star$

We have $\mathrm{H}^1(G_K, V)$, and we want to specify interesting subspaces by imposing local conditions. We'll be flexible in which conditions we allow.

Definition 20.13. A `Selmer structure` for V is a choice of subspaces $\mathfrak{S}_v \leq \mathrm{H}^1(G_v, V)$ for all finite places v of K such that

$$\mathfrak{S}_v = \mathrm{H}^1_{\mathrm{nr}}(G_v, V) \text{ for all but finitely many } v.$$

The corresponding `Selmer group` is

$$\mathrm{Sel}_{\mathfrak{S},V} := \left\{\alpha \in \mathrm{H}^1(G_K, V) : \alpha_v \in \mathfrak{S}_v \text{ for all } v\right\}. \qquad \diamond$$

Example 20.14. Take the `''f'' Selmer structure`

$$\mathfrak{S}_v = \begin{cases} \mathrm{H}^1_{\mathrm{nr}}(G_v, V) & \text{if } v \nmid p \\ \mathrm{H}^1_f(G_v, V) & \text{if } v \mid p \end{cases}$$

Remember: You should think $\mathrm{H}^1_e \subset \mathrm{H}^1_f \subset \mathrm{H}^1_g$ is analogous to $0 \subset \mathrm{H}^1_{\mathrm{nr}} \subset \mathrm{H}^1$

"Global cohomology classes which are everywhere unramified away from p and crystalline at p." The corresponding Selmer group is denoted $\mathrm{H}^1_f(G_K, V)$. △

Example 20.15 (''f outside S'' Selmer structure)**.** Let S be a finite set of finite places of K. Take

$$\mathfrak{S}_v = \begin{cases} \mathrm{H}^1_{\mathrm{nr}}(G_v, V) & \text{if } v \nmid p, v \notin S \\ \mathrm{H}^1(G_v, V) & \text{if } v \nmid p, v \in S \\ \mathrm{H}^1_f(G_v, V) & \text{if } v \mid p, v \notin S \\ \mathrm{H}^1_g(G_v, V) & \text{if } v \mid p, v \in S \end{cases}.$$

The corresponding Selmer group is denoted $\mathrm{H}^1_{f,S}(G_K, V)$. △

Lemma 20.16. $\mathrm{Sel}_{\mathfrak{S},V}$ *is always finite-dimensional, even though* $\mathrm{H}^1(G_K, V)$ *need not be.*

Warning 20.17. G_K does *not* have property (F). •

Remark 20.18 (Response to audience question, paraphrased). One can interpret $\mathrm{H}^1_{\mathrm{nr}}(G_v, V)$ as the set of extensions

$$0 \longrightarrow V \longrightarrow E \longrightarrow \mathbf{1} \longrightarrow 0$$

such that

$$0 \longrightarrow V^{I_v} \longrightarrow E^{I_v} \longrightarrow \mathbf{1} \longrightarrow 0$$

is exact. When V is unramified, this is asking that E be unramified as well. Furthermore, if $V = V_pA$ for A/K an abelian variety, then H^1_f sits in a short exact sequence

$$0 \longrightarrow \mathbb{Q}_p \otimes A(K) \longrightarrow \mathrm{H}^1_f(G_K, V_pA) \longrightarrow V_p Ш(A/K) \longrightarrow 0.$$ ∘

Proof of Lemma 20.16. Choose a finite set T of places such that

- $\{v \mid p\} \subset T$
- $\{v : V \text{ ramified at } v\} \subset T$
- $\{v : \mathfrak{S}_v \neq \mathrm{H}^1_{nr}(G_v, V)\} \subset T$

Let $G_{K,T}$ be the maximal quotient of G_K unramified outside T (so V is a representation of $G_{K,T}$). Then,

$$\mathrm{Sel}_{\mathfrak{S},V} \subset \mathrm{H}^1(G_{K,T}, V) \subset \mathrm{H}^1(G_K, V). \tag{20.1}$$

Why? Let $N := \ker(G_K \twoheadrightarrow G_{K,T})$, so N is the closed normal subgroup generated by the conjugates of I_v for $v \notin T$. Then, inflation-restriction gives

$$0 \longrightarrow \mathrm{H}^1(G_{K,T}, V) \longrightarrow \mathrm{H}^1(G_K, V) \longrightarrow \mathrm{Hom}(N, V)^{G_{K,T}}.$$

Thus, (20.1) follows from the claim that $\mathrm{Sel}_{\mathfrak{S},V} \to \mathrm{Hom}(N, V)$ is the zero map. To see this, consider some $\xi \in Z^1(G_K, V)$ s.t. $[\xi] \in \mathrm{Sel}_{\mathfrak{S},V}$. By assumption, ξ maps to 0 in $\mathrm{Hom}(I_v, V)$ for all $v \notin T$. One can check that

$$\ker(\xi) = \{\sigma \in G_K : \xi(\sigma) = 0\}$$

is a closed, *normal subgroup* of G_K. Thus, $N \leq \ker(\xi)$, proving (20.1). Once this is proven, we finish by remarking that $\mathrm{H}^1(G_{K,T}, V)$ is finite-dimensional by Hermite-Minkowski. In fact, Hermite-Minkowski implies that it has property (F). ■

21 Lecture 18 (4/6): Global Bloch-Kato Selmer Schemes

Note 13. There was some discussion before class about technicalities related to functoriality of $\pi_1^{\text{ét}}$. I didn't take notes on this.

OHs today will be focussed on people's questions, but in particular, could be a good place to ask about the formalism of admissible representations, e.g. D_{dR} and whatnot.

21.1 Picking up from last time

Setup 21.1.

- Let K be a number field (e.g. $K = \mathbb{Q}$)
- Let U be a continuous representation of G_K on a finitely generated $\mathbb{Q}_p$-pro-unipotent group such that
  - the action of G_K on U is unramified outside a finite set of places
  - the action of G_K on U is de Rham at all $v \mid p$
  - U is `mixed with negative weights`, i.e. has a filtration

$$U = W_{-1}U \trianglerighteq W_{-2}U \trianglerighteq \dots$$

such that $V_n = W_{-n}U/W_{-n-1}U$ is `pure of weight` $-n$ for all n (this means pure at *all* v).[25]

Goal. Define a "*global Selmer scheme*" inside $\mathrm{H}^1(G_K, U)$.

Definition 21.2. A `Selmer structure` for U is a choice of *closed subscheme* $\mathfrak{S}_v \subset \mathrm{H}^1(G_v, U)$ for all finite v such that

$$\mathfrak{S}_v = \mathrm{H}^1_{\text{nr}}(G_v, U)$$

for almost all v. ◇

Recall 21.3 (Proposition 17.7)**.** For U as we have here, $\mathrm{H}^1_{\text{nr}}(G_v, U) = \{*\}$ for any $v \nmid p$. ⊙

Definition 21.4. Given a Selmer structure $\mathfrak{S}$, we define the `global Selmer scheme`

$$\mathrm{Sel}_{\mathfrak{S},U} \subset \mathrm{H}^1(G_K, U)$$

to be the preimage of

$$\prod_v \mathfrak{S}_v \subset \prod_v \mathrm{H}^1(G_v, U)$$

under the localization map

$$\mathrm{H}^1(G_K, U) \longrightarrow \prod_v \mathrm{H}^1(G_v, U).$$

Put another way,

$$\mathrm{Sel}_{\mathfrak{S},U}(\Lambda) = \left\{\xi \in \mathrm{H}^1(G_K, U(\Lambda)) : \xi_v \in \mathfrak{S}_v(\Lambda) \text{ for all } v\right\}. \qquad \diamond$$

[25] Sometimes people use 'purity of global representations' to mean 'pure outside a finite set.'

Example 21.5. Suppose S is a finite set of finite places. Define the Selmer structure

$$\mathfrak{S}_v = \begin{cases} \mathrm{H}^1_{\mathrm{nr}}(G_v, U) = \{*\} & \text{if } v \nmid p, v \notin S \\ \mathrm{H}^1(G_v, U) & \text{if } v \nmid p, v \in S \\ \mathrm{H}^1_f(G_v, U) = \mathrm{H}^1_e(G_v, U) & \text{if } v \mid p, v \notin S \\ \mathrm{H}^1_g(G_v, U) & \text{if } v \mid p, v \in S \end{cases}.$$

The associated Selmer scheme is denoted $\mathrm{H}^1_{f,S}(G_K, U)$ (or $\mathrm{H}^1_f(G_K, U)$ if $S = \emptyset$). △

Proposition 21.6. *$\mathrm{Sel}_{\mathfrak{S},U}$ is representable by an affine $\mathbb{Q}_p$-scheme, which is of finite type if U is unipotent.*

Warning 21.7. $\mathrm{H}^1(G_K, U)$ is *not* representable. •

Lemma 21.8. *Let T be a finite set of finite places of K, containing*

- *all $v \mid p$*
- *all v where the action on U ramifies*
- *all places $v \nmid p$ where $\mathfrak{S}_v = \mathrm{H}^1_{nr}$.*

Then,

$$\mathrm{Sel}_{\mathfrak{S},U} \subset \mathrm{H}^1(G_{K,T}, U)$$

as subfunctors of $\mathrm{H}^1(G_K, U)$.

Above, $G_{K,T}$ is the maximal quotient of G_K unramified outside T. Note it has property (F) by Hasse-Minkowski.

Proof. There is a non-abelian inflation-restriction sequences

$$1 \longrightarrow \mathrm{H}^1(G_{K,T}, U) \hookrightarrow \mathrm{H}^1(G_K, U) \longrightarrow \mathrm{H}^1(N, U),$$

where $N := \ker(G_K \twoheadrightarrow G_{K,T})$. This N is the closed, normal subgroup generated by inertia I_v for all $v \notin T$. Given this, it suffices to show that the composition

$$\mathrm{Sel}_{\mathfrak{S},U} \longrightarrow \mathrm{H}^1(G_K, U) \longrightarrow \mathrm{H}^1(N, U) = \mathrm{Hom}^{\mathrm{out,cts}}(N, U)$$

is trivial. Above,

$$\mathrm{H}^1(N, U(\Lambda)) = \{\text{cts homomorphisms } \xi : N \to U(\Lambda)\} / \text{conjugation by elements of } U(\Lambda)$$

(because N acts trivially on U). Choose $[\xi] \in \mathrm{Sel}_{\mathfrak{S},U}(\Lambda)$ represented by some cocycle $\xi \in Z^1(G_K, U(\Lambda))$. By definition, $[\xi]|_{I_v} \in \mathfrak{S}_v(\Lambda) = \{*\}$ for all $v \notin T$. Hence, $\xi|_{I_v} = 1$. The cocycle condition implies that $\ker(\xi : G_K \to U(\Lambda))$ is a closed, normal subgroup, so $N \subset \ker(\xi)$, i.e. $[\xi] \in \mathrm{H}^1(G_{K,T}, U)$. ■

Proof of Proposition 21.6. We have a pullback square (of functors)

$$\begin{array}{ccc} \mathrm{Sel}_{\mathfrak{S},U} & \hookrightarrow & \mathrm{H}^1(G_{K,T}, U) \\ \downarrow & & \downarrow \\ \prod_{v \in T} \mathfrak{S}_v & \hookrightarrow & \prod_{v \in T} \mathrm{H}^1(G_v, U). \end{array}$$

We know everything other than $\mathrm{Sel}_{\mathfrak{S},U}$ is representable (by affines), so $\mathrm{Sel}_{\mathfrak{S},U}$ must be an affine, closed subscheme of $\mathrm{H}^1(G_{K,T}, U)$. ∎

Corollary 21.9 (weak)**.** $\mathrm{Sel}_{\mathfrak{S},U}$ *is a closed subscheme of*

$$\prod_n \mathrm{H}^1(G_{K,T}, V_n),$$

so $\dim \mathrm{Sel}_{\mathfrak{S},U} \leq \sum_n \dim \mathrm{H}^1(G_{K,T}, V_n)$.

We'll need a better dimension bound than this.

Proposition 21.10. *Assume* $\mathfrak{S}$ *is chosen so that* $\mathfrak{S}_v = \mathrm{H}^1_f(G_v, U)$ *for all* $v \mid p$*. Then,* $\mathrm{Sel}_{\mathfrak{S},U}$ *is a closed subscheme of*

$$\prod_{v \nmid p} \mathfrak{S}_v \times \prod_n \mathrm{H}^1_f(G_K, V_n).$$

In particular, $\dim \mathrm{Sel}_{\mathfrak{S},U} \leq \sum_{v \nmid p} \dim \mathfrak{S}_v + \sum_n \dim \mathrm{H}^1_f(G_K, V_n)$.

Usually, $\dim \mathrm{H}^1_f(G_K, V_n) < \dim \mathrm{H}^1(G_{K,T}, V_n)$. Let's prove this, and then next Tuesday, we'll take all this Selmer scheme stuff and use it to formulate Chabauty-Kim.

Notation 21.11. Let T be as before, and define Sel_n via the pullback (the bottom arrow is not a closed immersion)

$$\begin{array}{ccc} \mathrm{Sel}_n & \longrightarrow & \mathrm{H}^1(G_{K,T}, U_n) \\ \downarrow & & \downarrow \\ \prod_{v \in T_0} \mathfrak{S}_v \times \prod_{v \mid p} \mathrm{H}^1_f(G_v, U_n) & \longrightarrow & \prod_{v \in T} \mathrm{H}^1(G_v, U_n), \end{array}$$

where $T_0 = T \setminus \{v \mid p\}$ and $U_n = U/W_{-n-1}U$. In other words,

$$\mathrm{Sel}_n(\Lambda) = \left\{ (\xi, (\xi_v)_v) \in \mathrm{H}^1(G_{K,T}, U_n(\Lambda)) \times \prod_{v \in T_0} \mathfrak{S}_v(\Lambda) \;\middle|\; \begin{array}{c} \xi|_{G_v} \text{ is crystalline for } v \mid p \\ \text{and } \xi|_{G_v} = \text{image of } \xi_v \text{ for all } v \in T_0 \end{array} \right\}$$

($\xi|_{G_v}$ being `crystalline` means $\xi_v \in \mathrm{H}^1_f$).

In words, Sel_n parameterizes classes where are crystalline above p and in the Selmer structure away from p.

Note that Sel_n is representable by a finite type affine $\mathbb{Q}_p$-scheme. What else do we know about it?

- $\mathrm{Sel}_0 = \prod_{v \in T_0} \mathfrak{S}_v = \prod_{v \nmid p} \mathfrak{S}_v$ (use that $U_0 = U/W_{-1}U = 1$)
- The map $U_n \to U_{n-1}$ induces a map
$$\mathrm{Sel}_n \longrightarrow \mathrm{Sel}_{n-1},$$
and $\mathrm{Sel}_{\mathfrak{S},U} = \varprojlim_n \mathrm{Sel}_n$ (recall our assumption on $\mathfrak{S}_v$).

Claim 21.12. *For all* $n \geq 1$*, the pointwise image of*

$$\mathrm{Sel}_n \longrightarrow \mathrm{Sel}_{n-1}$$

is a closed subscheme of Sel_{n-1}*, and* Sel_n *is an* $\mathrm{H}^1_f(G_K, V_n)$*-torsor over this image.*

Remember: For Chabauty-Kim, you want global Selmer to have lower dimension than local Selmer

This is kinda saying you've started with the H^1_f Selmer structure and modified it away from p (to get $\mathfrak{S}$), and then the difference in the dimensions of the original thing and the modification is bounded above dimensions of the modifications you've made.

Proof of Proposition 21.10, assuming Claim 21.12. Let $Z \subset \mathrm{Sel}_{n-1}$ denote the pointwise image. Then, $\mathrm{Sel}_n \twoheadrightarrow Z$ is a surjection of representable functors, so it splits. Hence (noncanonically),

$$\mathrm{Sel}_n \cong \mathrm{H}^1_f(G_k, V_n) \times Z \hookrightarrow \mathrm{H}^1_f(G_K, V_n) \times \mathrm{Sel}_{n-1}\,.$$

Use induction. ∎

Proof of Claim 21.12. Recall from the proof of representability of cohomology schemes (Theorem 15.4) that $\mathrm{H}^1(G_{K,T}, V_n)$ acts simply transitively on the fibers of $\mathrm{H}^1(G_{K,T}, U_n) \to \mathrm{H}^1(G_{K,T}, U_{n-1})$. This restricts to an action of $\mathrm{H}^1_f(G_K, V_n) \le \mathrm{H}^1(G_{K,T}, V_n)$ on Sel_n. That is, if $\alpha \in \mathrm{H}^1_f(G_K, V_n)$ and $(\xi, (\xi_v)_{v\in T_0}) \in \mathrm{Sel}_n$, then $(\alpha\cdot\xi, (\xi_v)_{v\in T_0}) \in \mathrm{Sel}_n$ as well. Why? For $v \in T_0$, $\alpha|_{G_v} = 0 \in \mathrm{H}^1(G_v, V_n)$, so $(\alpha\cdot\xi)|_{G_v} = \xi|_{G_v}$ is the image of ξ_v still. For $v \mid p$, we have $\alpha|_{G_v}, \xi|_{G_v} \in \mathrm{H}^1_f(G_v, V_n)$, so their product lies in here as well.

- Claim 1: $\mathrm{H}^1_f(G_K, V_n)$ acts simply transitively on the fibers.

  The action is free since it's the restriction of a free action. The content is in showing transitivity. Suppose $(\xi, (\xi_v)_{v\in T_0})$ and $(\xi', (\xi'_v)_{v\in T_0})$ lie in the same fiber of

  $$\begin{array}{ccc} \mathrm{Sel}_n & \longrightarrow & \mathrm{Sel}_{n-1} \\ & \searrow \quad \swarrow & \\ & \displaystyle\prod_{v\in T_0} \mathfrak{S}_v. & \end{array}$$

  Then, $\xi_v = \xi'_v$ for all $v \in T_0$. Moreover, $\xi, \xi' \in \mathrm{H}^1(G_{K,T}, U_n)$ must have the same image in $\mathrm{H}^1(G_{K,T}, U_{n-1})$, so $\exists!\alpha \in \mathrm{H}^1(G_{K,T}, V_n)$ such that $\alpha\cdot\xi = \xi'$. We need to show $\alpha \in \mathrm{H}^1_f(G_K, V_n)$.

  - $v \in T_0$: image of $\xi_v = \xi'|_{G_v} = \alpha|_{G_v}\cdot\xi|_{G_v} = \alpha|_{G_v}\cdot$(image of ξ_v), so $\alpha|_{G_v} = 0 \in \mathrm{H}^1(G_v, V_n)$ (because this group is acting freely).
  - $v \mid p$: we know $\xi|_{G_v}, \xi'|_{G_v} \in \mathrm{H}^1_f(G_v, U_n)$. This is enough to conclude that $\alpha|_{G_v} \in \mathrm{H}^1_f(G_v, V_n)$, because $\mathrm{H}^1_f(G_v, V_n)$ acts simply transitively on the fibers of $\mathrm{H}^1_f(G_v, U_n) \to \mathrm{H}^1_f(G_v, U_{n-1})$.

  Thus, $\alpha \in \mathrm{H}^1_f(G_K, V_n)$ as desired.

- Claim 2: The pointwise image of $\mathrm{Sel}_n \to \mathrm{Sel}_{n-1}$ is a closed subscheme.

  Let $\mathrm{Sel}'_{n-1} \subset \mathrm{Sel}_{n-1}$ be the image. Define $\mathrm{Sel}''_{n-1} \subset \mathrm{Sel}_{n-1}$ via

  $$\mathrm{Sel}''_{n-1} = \left\{ (\xi, (\xi_v)_{v\in T_0}) \in \mathrm{Sel}_{n-1} \,\middle|\, \begin{array}{c} \xi \text{ lies in the image of} \\ \mathrm{H}^1(G_{K,T}, U_n) \to \mathrm{H}^1(G_{K,T}, U_{n-1}) \end{array} \right\}.$$

  We'll show both inclusions $\mathrm{Sel}'_{n-1} \subset \mathrm{Sel}''_{n-1} \subset \mathrm{Sel}_{n-1}$ are closed immersions. The latter is since $\mathrm{im}(\mathrm{H}^1(G_{K,T}, U_n) \to \mathrm{H}^1(G_{K,T}, U_{n-1}))$ is closed. For the former, let A_n be the funny vector space

  $$A_n := \prod_{v\mid p} \frac{\mathrm{H}^1(G_v, V_n)}{\mathrm{H}^1_f} \times \prod_{v\in T_0} \mathrm{H}^1(G_v, V_n).$$

  Set $C_n := \mathrm{coker}\big(\mathrm{H}^1(G_{K,T}, V_n) \to A_n\big)$. We want to show there is a natural transformation of functors

  $$\mathrm{Sel}''_{n-1} \longrightarrow C_n$$

  whose kernel is Sel'_{n-1}. How do you define this?

Question: (When) did we show this?

Answer: I don't think we gave a detailed proof, but it was mentioned in Remark 18.12.

Construction 21.13. For $(\xi, (\xi_v)_v) \in \mathrm{Sel}''_{n-1}$, we know ξ lifts to some $\widetilde{\xi} \in \mathrm{H}^1(G_{K,T}, U_n)$.

- For $v \in T_0$, we know $\widetilde{\xi}|_{G_v}$ and the image of ξ_v differ by some element $\alpha_v \in \mathrm{H}^1(G_v, V_n)$.
- For $v \mid p$, the image of $\widetilde{\xi}|_{G_v} \in \mathrm{H}^1(G_v, U_n)$ in $\mathrm{H}^1(G_v, U_{n-1})$ lies in H^1_f, so $\widetilde{\xi}_{G_v}$ differs from an element of $\mathrm{H}^1_f(G_v, U_n)$ by some $\alpha_v \in \mathrm{H}^1(G_v, V_n)$.

The desired map is given by

$$(\xi, (\xi_v)_{v \in T_0}) \longmapsto (\alpha_v)_{v \in T}\,. \qquad \bigcirc$$

We're out of time, so let's stop here.[26] ■

22 Office Hours

Question 22.1 (Audience)**.** *Are these global cohomology functors Ind-representable?*

Answer. When U is abelian, this is the case. Unclear off the top of the head, if this extends to U (pro-)unipotent. We used at least two facts about representable functors

- kernel of morphism of pointed representable functors is representable.
- A surjection of representable functors splits

Proof. Say $F, G : \mathcal{C} \to \mathrm{Set}$ are functors on some category, and say $f : F \twoheadrightarrow G$ is a surjection of functors. Assume G is representable. We'll show f splits. Well, $G = \mathrm{Hom}(X, -)$ for some $X \in \mathcal{C}$, so $\mathrm{id} \in \mathrm{Hom}(X, X) \twoheadleftarrow F(X) : f_X$ lifts to some $x \in F(X)$. By Yoneda, this x corresponds to some splitting $G \to F$. ■

⋆

Question 22.2 (Audience, paraphrased)**.** *We had this theorem that said something like, start w/ the unramified Selmer structure, modify it at finitely many places (away from p), and then the resulting Selmer scheme has dimension bounded in terms of the modifications and the naive bound for the dimension of the unramified Selmer scheme. Can the naive bound be replaced w/ the true dimension, e.g. can one prove*

$$\dim \mathrm{Sel}_{\mathfrak{S},U} \leq \sum_{v \nmid p} \dim \mathfrak{S}_v + \dim \mathrm{H}^1_f(G_K, U)?$$

Answer. Not sure if this statement is true in this context. The most straightforward way to access dimension is via this sort of iterated torsor argument, and that won't give what you want.

In sufficient generality, it's probably false. Consider something like

$$\mathrm{H}^1_f(G_K, U) \longrightarrow \mathrm{Sel}_{\mathfrak{S},U} \longrightarrow \prod_{v \nmid p} \mathfrak{S}_v.$$

You can ask what the fibers of this looks like. Not sure what the answer should be. ⋆

Question 22.3 (Audience)**.** *What's a representation that's ramified at infinitely many places?*

[26] Unclear to me if we got to the end of the proof, but I think we did not...

Answer. You can find infinite dimensional examples. If you want finite-dimensional ones, look at

$$\rho : G_K \longrightarrow \mathrm{GL}_n(\mathbb{Z}_p)$$

Because $\mathrm{GL}_n(\mathbb{Z}_p)$ is an extension of $\mathrm{GL}_n(\mathbb{F}_p)$ by a pro-p group, any such thing will be tamely ramified almost everywhere. This doesn't obstruct have ramification at infinitely many places though...

How about this? Consider an additive character $G_K \to \mathbb{Z}_p$ (can embed $\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p^\times$ to get a 1-dim rep) and use class field theory. This tells you the additive character will be something like

$$\prod_v \mathscr{O}_v^\times \longrightarrow \mathbb{Z}_p.$$

Unclear what to do here... Probably infinitely ramified representations exist, but can't construct one immediately. ⋆

Question 22.4 (Audience)**.** *What's an example of a non-de Rham representation?*

Answer. Say $K = \mathbb{Q}_p$. One can show $\mathrm{H}^1_g(G_p, \mathbb{Q}_p(0)) \neq 0$, so there should exist non-de Rham extensions of $\mathbb{Q}_p$ by $\mathbb{Q}_p$. How to write one down?

$$\mathrm{H}^1(G_p, \mathbb{Q}_p(0)) = \mathrm{Hom}(G_p^{\mathrm{ab}}, \mathbb{Z}_p(0)) = \mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{Z}_p).$$

If I remember correctly, H^1_g corresponds to the characters $\chi : \mathbb{Q}_p^\times \to \mathbb{Z}_p$ such that $\chi|_{\mathbb{Z}_p^\times}$ is trivial (i.e. χ unramified).

To answer the question, take a ramified character $\chi : G_p \to \mathbb{Q}_p(0)$, and use it to form the representation (e.g. $\chi = \log_p$)

$$\rho = \begin{pmatrix} 1 & \chi \\ & 1 \end{pmatrix}.$$

This should not be de Rham.

Fact. For general $K/\mathbb{Q}_p$ finite, a character $\chi : G_K \to \mathbb{Z}_p^\times$ is de Rham iff $\chi =$ (finite order character) $\cdot$ χ_{cyc}^n. ⋆

Question 22.5 (Audience, paraphrased)**.** *Examples showing that* $\mathrm{H}^1_e \subset \mathrm{H}^1_f \subset \mathrm{H}^1_g$ *is like* $0 \subset \mathrm{H}^1_{nr} \subset \mathrm{H}^1_g$*?*

Answer. Let's look at $\mathbb{Q}_p(1)$ ($K/\mathbb{Q}_p$ finite). In this case, $\mathrm{H}^1(G_K, \mathbb{Q}_p(1))$ has dimension $[K : \mathbb{Q}_p] + 1$. Furthermore, $\mathrm{H}^1_g = \mathrm{H}^1$ while $\mathrm{H}^1_e = \mathrm{H}^1_f$ has dimension $[K : \mathbb{Q}_p]$.

Note that $\mathbb{Q}_p(1) = T_p\mathbb{G}_m$ is the Tate module of $\mathbb{G}_m$. Have Kummer map

$$\kappa : K^\times \longrightarrow \mathrm{H}^1(G_K, \mathbb{Q}_p(1)) = \mathrm{Ext}^1(\mathbb{Q}_p(0), \mathbb{Q}_p(1))$$

sending

$$x \longmapsto \mathrm{H}_1^{\text{ét}}(\mathbb{G}_{m,\overline{K}}; \{1, x\}).$$

this relative étale homology sits in a sequence

$$0 \longrightarrow \mathrm{H}_1^{\text{ét}}(\mathbb{G}_{m,\overline{K}}) \longrightarrow \mathrm{H}_1^{\text{ét}}(\mathbb{G}_{m,\overline{K}}; \{1, x\}) \longrightarrow \mathrm{H}_0^{\text{ét}}(\{1, x\}) \longrightarrow \mathrm{H}_0^{\text{ét}}(\mathbb{G}_{m,\overline{K}})$$

which looks like

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow \mathrm{H}_1^{\text{ét}}(\mathbb{G}_{m,\overline{K}}; \{1, x\}) \longrightarrow \mathbb{Q}_p(0)^2 \xrightarrow{+} \mathbb{Q}_p(0).$$

In this case, $\kappa(\mathscr{O}_K^\times) \subset \mathrm{H}^1_f$ and $\kappa(K^\times) \subset \mathrm{H}^1_g$. ⋆

23 Lecture 19 (4/11): The non-abelian Chabauty method, I

23.1 Course Announcements

- OHs on Thursday: models and reductions of curves
- April 26 (Wed) is last official day of classes
  - Lecture on April 27
  - No lecture May 2
  - Lecture on May 4
  - Maybe lecture May 9,11?
- Course will continue as informal lecture course next semester

  Will talk about, for example, "how do you make Chabauty effective in practice?"

23.2 Material

Let's turn all this Bloch-Kato Selmer group/scheme stuff into a method for controlling rational points on varieties.

Setup 23.1. From now on

- X is a smooth, projective curve of genus ≥ 2 over $K = \mathbb{Q}$.

  We'll occasionally want to consider affine curves. More generally, we'll write Y for a smooth hyperbolic curve over $\mathbb{Q}$. We'll write $Y = X \setminus D$ for X smooth, projective and $D \subset X$ a reduced divisor. We allow $D = \emptyset$ (i.e. $Y = X$).
- We set $g = g(X)$
- We set $r = \deg D$

  Above, `hyperbolic` means that $\chi(Y) := 2 - 2g - r$ is (strictly) negative. That is Y is
  - genus 0 minus ≥ 3 points
  - genus 1 minus ≥ 1 point
  - genus ≥ 2 minus ≥ 0 points.

Goal. Study rational points on X, or more generally, S-integral points on Y using a "pro-unipotent descent obstruction."

Recall 23.2. For any $x, y \in Y(\mathbb{Q})$, we have $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x, y)$, the $\mathbb{Q}_p$-pro-unipotent étale torsor of paths from x to y. This is an affine $\mathbb{Q}_p$-scheme.

(1) The schemes $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; -, -)$ form a groupoid, i.e. we have composition maps

$$\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; y, z) \times \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x, y) \longrightarrow \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x, z).$$

(2) The action of $G_{\mathbb{Q}}$ on $Y_{\overline{\mathbb{Q}}}$ induces a $G_{\mathbb{Q}}$-action on each $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; -, -)$.

See Theorem 11.3.

Similarly for $x, y \in Y(\mathbb{Q}_\ell)$, we have $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; x, y)$ w/ composition, etc. and a G_ℓ-action. ⊙

Let's continue to remind ourselves of various facts we've collected over the lectures.

Proposition 23.3.

(1) *When $x = y$, $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x)$ is a $\mathbb{Q}_p$-pro-unipotent group, isomorphic to the $\mathbb{Q}_p$-Malčev completion of*

$$\Sigma_{g,r} := \left\langle a_1, \dots, a_g, b_1, \dots, b_g, c_1, \dots, c_r \;\middle|\; \prod_{i=1}^{g} [a_i, b_i] \cdot \prod_{j=1}^{r} c_j = 1 \right\rangle.$$

This ultimately came from comparison with analytic topology over $\mathbb{C}$.

Furthermore, $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x, y)(\mathbb{Q}_p) \neq \emptyset$ for all x, y. This is ultimately because $Y_{\overline{\mathbb{Q}}}$ is connected.

Warning 23.4 (response to audience question)**.** The $\mathbb{Q}$-Malčev completion of $\Sigma_{g,r}$ is the $\mathbb{Q}$-pro-unipotent group $\Sigma_{g,r,\mathbb{Q}} = \mathbb{G}(\mathfrak{u}_{g,r})$ associated to the Lie algebra

$$\mathfrak{u}_{g,r} = \left\langle \alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g, \gamma_1, \dots, \gamma_r \;\middle|\; \sum_i [\alpha_i, \beta_i] + \sum_j \gamma_j = 0 \right\rangle.$$

However, it is *not* the case that $\alpha_i = \log(a_i)$, etc. •

(2) *The action of $G_{\mathbb{Q}}$ (or G_ℓ) on $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x, y)$ is continuous (e.g. on $\mathbb{Q}_p$-points).*

(3) *For the third property, we'll need to introduce some terminology.*

Definition 23.5. We say that Y has `good reduction` at a prime ℓ just when there exists a smooth, proper $\mathbb{Z}_\ell$-scheme $\mathcal{X} = \mathcal{X}_{\mathbb{Z}_\ell}$ whose generic fiber is $X_{\mathbb{Q}_\ell}$ along w/ a divisor $\mathcal{D} = \mathcal{D}_{\mathbb{Z}_\ell} \subset \mathcal{X}$ which is étale over $\mathbb{Z}_\ell$ whose generic fiber is $D_{\mathbb{Q}_\ell}$. If such a $(\mathcal{X}_{\mathbb{Z}_\ell}, \mathcal{D}_{\mathbb{Z}_\ell})$ exists, it is unique up to isomorphism, and we write $\mathcal{Y} = \mathcal{Y}_{\mathbb{Z}_\ell} := \mathcal{X}_{\mathbb{Z}_\ell} \setminus \mathcal{D}_{\mathbb{Z}_\ell}$ (so $\mathcal{Y}_{\mathbb{Z}_\ell}$ has generic fiber $Y_{\mathbb{Q}_\ell}$). ◇

Definition 23.6. If $x, y \in Y(\mathbb{Q})$, we say the triple (Y, x, y) has `good reduction` at ℓ if Y does and $x, y \in \mathcal{Y}(\mathbb{Z}_\ell)$. ◇

Remark 23.7. If $Y = X$ is proper, then $(Y; x, y)$ has good reduction $\iff$ Y has good reduction. ○

With that out of the way, if $\ell \neq p$ and $(Y; x, y)$ has good reduction at ℓ, then $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; x, y)$ is `unramified`, i.e. inertia I_ℓ acts trivially.

(4) *If $\ell = p$, then $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_p}; x, y)$ is de Rham, and if furthermore $(Y; x, y)$ has good reduction at p, then it is in fact crystalline.*

Question 23.8 (Audience, paraphrased)**.** *Is there a geometric condition causing $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_p}; x, y)$ to be $B_{cris}^{\varphi=1}$-admissible.*

Answer (paraphrased, not sure I heard it all (correctly))**.** A $B_{\text{cris}}^{\varphi=1}$-admissible representation is a B_{cris}-admissible representation V such that $D_{\text{cris}}(V)$ has trivial Frobenius action. Hence, you shouldn't expect this to happen usually. ⋆

(5) *$\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x)$ is mixed with negative weights, i.e. there's a weight filtration $W_\bullet \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; x)$ whose graded pieces W_{-n}/W_{-n-1} are pure of weight $-n$ at all prime ℓ.*

Setup 23.9. Let's fix a basepoint $b \in Y(\mathbb{Q})$.

For any $x \in Y(\mathbb{Q})$, choose some path $\gamma = \gamma_x \in \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b, x)(\mathbb{Q}_p)$ from b to x. For $\sigma \in G_{\mathbb{Q}}$, $\sigma(\gamma)$ is also a path from b to x, so

$$\xi(\sigma) := \gamma^{-1}\sigma(\gamma) \in \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)(\mathbb{Q}_p).$$

This defines a continuous 1-cocycle $\xi : G_{\mathbb{Q}} \to \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}, b)(\mathbb{Q}_p)$, whose class $j(x) := [\xi] \in \mathrm{H}^1(G_{\mathbb{Q}}, \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)(\mathbb{Q}_p))$ is independent of the choice of γ.

Definition 23.10. We have just constructed a well-defined map

$$j : Y(\mathbb{Q}) \longrightarrow \mathrm{H}^1\left(G_{\mathbb{Q}}, \pi_1^{\mathbb{Q}_p}\left(Y_{\overline{\mathbb{Q}}}; b\right)(\mathbb{Q}_p)\right),$$

called the `global unipotent Kummer map`. The same construction defines `local unipotent Kummer maps`

$$j_\ell : Y(\mathbb{Q}_\ell) \longrightarrow \mathrm{H}^1\left(G_\ell, \pi_1^{\mathbb{Q}_p}\left(Y_{\overline{\mathbb{Q}}_\ell}; b\right)(\mathbb{Q}_p)\right). \qquad \diamond$$

Remark 23.11. The (global) unipotent Kummer map is sometimes called the *non-abelian Kummer map* or *higher Albanese map*. $\circ$

Let's introduce a slight variant on this idea. Suppose that U is a $G_{\mathbb{Q}}$-equivariant quotient of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)$, e.g. $U = \pi_1^{\mathbb{Q}_p}/W_{-n-1}$. Then, we define j_U to be the composition

$$j_U : Y(\mathbb{Q}) \xrightarrow{j} \mathrm{H}^1(G_{\mathbb{Q}}, \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)(\mathbb{Q}_p)) \longrightarrow \mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p)),$$

and we define $j_{\ell,U}$ similarly.

Lemma 23.12. *Suppose that $\ell \neq p$ and that (Y, b) has good reduction at ℓ. Then, $j_\ell(x) = * \in \mathrm{H}^1(G_\ell, \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)(\mathbb{Q}_p))$ for all $x \in \mathcal{Y}(\mathbb{Z}_\ell)$.*

Proof. We know that the G_ℓ-actions on $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; b, x)$ and $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; b)$ are unramified (Proposition 23.3**(3)**), so $\xi|_{I_\ell} = 1$. Thus, $j_\ell(x) = [\xi] \in \mathrm{H}^1_{\mathrm{nr}}(G_\ell, \pi_1^{\mathbb{Q}_p})(\mathbb{Q}_p) = \{*\}$ by Proposition 17.7. $\blacksquare$

23.3 Global Selmer Scheme

Setup 23.13. Fix some extra data:

- a finite set S of primes
- a model $(\mathcal{X}, \mathcal{D})$ of (X, D) over $\mathbb{Z}_S$, i.e. $\mathcal{X}$ is a proper, flat, integral $\mathbb{Z}_S$-scheme w/ generic fiber X, and $\mathcal{D} \subset \mathcal{X}$ is a horizontal divisor.
- We set $\mathcal{Y} := \mathcal{X} \setminus \mathcal{D}$.

  We want to control its S-integral points.
- Fix a $G_{\mathbb{Q}}$-equivariant quotient U of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)$.

Remark 23.14. If $Y = X$ is projective, can always choose $S = \emptyset$ and $\mathcal{X}$ to be e.g. the minimal regular model of X. $\circ$

Definition 23.15. The `Selmer scheme` $\mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S) \subset \mathrm{H}^1(G_\mathbb{Q}, U)$ is the global Selmer scheme associated to the Selmer structure $\mathfrak{S}$ with

$$\mathfrak{S}_\ell = \begin{cases} j_{\ell,U}(\mathcal{Y}(\mathbb{Z}_\ell))^{\mathrm{Zar}} & \text{if } \ell \notin S \\ j_{\ell,U}(Y(\mathbb{Q}_\ell))^{\mathrm{Zar}} & \text{if } \ell \in S. \end{cases}$$

Above, $^{\mathrm{Zar}}$ denotes Zariski closure. ◇

That the above is a Selmer structure follows from Lemma 23.12.

Proposition 23.16. *The image of the global Kummer map*

$$j_U : \mathcal{Y}(\mathbb{Z}_S) \longrightarrow \mathrm{H}^1(G_\mathbb{Q}, U(\mathbb{Q}_p))$$

lands in the ($\mathbb{Q}_p$-points of the) Selmer scheme $\mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S)$.

Proof. For any ℓ, the square

$$\begin{array}{ccc} Y(\mathbb{Q}) & \longrightarrow & Y(\mathbb{Q}_\ell) \\ \downarrow{\scriptstyle j_U} & & \downarrow{\scriptstyle j_{\ell,U}} \\ \mathrm{H}^1(G_\mathbb{Q}, U(\mathbb{Q}_p)) & \xrightarrow{\mathrm{loc}_\ell} & \mathrm{H}^1(G_\ell, U(\mathbb{Q}_p)) \end{array}$$

commutes. Say $x \in \mathcal{Y}(\mathbb{Z}_S)$. Then, $\mathrm{loc}_\ell(j_U(x)) = j_{\ell,U}(x)$ lies in $j_{\ell,U}(\mathcal{Y}(\mathbb{Z}_\ell))$ if $\ell \notin S$ and in $j_{\ell,U}(Y(\mathbb{Q}_\ell))$ always. ■

Setup 23.17. Fix a prime $p \notin S$.

We have a commutative square

$$\begin{array}{ccc} \mathcal{Y}(\mathbb{Z}_S) & \longrightarrow & \mathcal{Y}(\mathbb{Z}_p) \\ \downarrow{\scriptstyle j_U} & & \downarrow{\scriptstyle j_{p,U}} \\ \mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S)(\mathbb{Q}_p) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1(G_p, U(\mathbb{Q}_p)). \end{array}$$

Definition 23.18. The `Chabauty-Kim locus` $\mathcal{Y}(\mathbb{Z}_p)_U \subset \mathcal{Y}(\mathbb{Z}_p)$ associated to U is the set of points $x \in \mathcal{Y}(\mathbb{Z}_p)$ such that $j_{p,U}(x)$ lies in the scheme-theoretic image of $\mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S) \xrightarrow{\mathrm{loc}_p} \mathrm{H}^1(G_p, U)$. ◇

Note that

$$\mathcal{Y}(\mathbb{Z}_S) \subset \mathcal{Y}(\mathbb{Z}_p)_U \subset \mathcal{Y}(\mathbb{Z}_p).$$

Let's end by saying what happens when $X = Y$, so you care instead about rational points.

Remark 23.19. When $Y = X$ is projective, no need to choose S or $\mathcal{X}$ (because $\mathcal{X}(\mathbb{Z}) = X(\mathbb{Q})$ by valuative criterion. Similarly, $\mathcal{X}(\mathbb{Z}_\ell) = X(\mathbb{Q}_\ell)$). Here, the Selmer scheme

$$\mathrm{Sel}_U(X/\mathbb{Q}) \subset \mathrm{H}^1(G_\mathbb{Q}, U)$$

corresponds to the Selmer structure

$$\mathfrak{S}_\ell = j_{\ell,U}(X(\mathbb{Q}_\ell))^{\mathrm{Zar}}.$$

Then, one has a square

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ {\scriptstyle j_U}\downarrow & & \downarrow{\scriptstyle j_{p,U}} \\ \mathrm{Sel}_U(X/\mathbb{Q}) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1(G_p, U(\mathbb{Q}_p), \end{array}$$

and a corresponding Chabauty-Kim locus $X(\mathbb{Q}_p)_U \supset X(\mathbb{Q})$. ∘

Warning 23.20. The definition of the Selmer scheme (and so of the Chabauty-Kim locus) is inconsistent across the literature. For example, sounds like in Kim's first paper, he imposed no conditions at all at places of bad reduction. •

24 Lecture 20 (4/18): The non-abelian Chabauty method, I

Announcements

- OHs this week: models of curves
- OHs next Thursday: Pset6
- Lectures until May 11 (except May 2)

Recall 24.1 (setup)**.**

- $Y/\mathbb{Q}$ smooth hyperbolic curve, $b \in Y(\mathbb{Q})$ basepoint
  Write $Y = X \setminus D$ for X projective and D a divisor.
- U a $G_{\mathbb{Q}}$-equivariant quotient of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)$
- Unipotent Kummer maps

$$\begin{aligned} j_U &: Y(\mathbb{Q}) \longrightarrow \mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p)) \\ j_{\ell,U} &: Y(\mathbb{Q}_\ell) \longrightarrow \mathrm{H}^1(G_\ell, U(\mathbb{Q}_p)) \end{aligned}$$

- S a finite set of primes, $\mathcal{Y}/\mathbb{Z}_S$ a model of $Y/\mathbb{Q}$
  (unnecessary if $Y = X$ is projective)
- Global Selmer scheme

$$\mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S) \subset \mathrm{H}^1(G_{\mathbb{Q}}, U)$$

  associated to the Selmer structure

$$\mathfrak{S}_\ell = \begin{cases} j_{\ell,U}(\mathcal{Y}(\mathbb{Z}_\ell))^{\mathrm{Zar}} & \text{if } \ell \notin S \\ j_{\ell,U}(Y(\mathbb{Q}_\ell))^{\mathrm{Zar}} & \text{if } \ell \in S. \end{cases}$$

- For (fixed) $p \notin S$, Chabauty-Kim locus

$$\mathcal{Y}(\mathbb{Z}_p)_U = \{x \in \mathcal{Y}(\mathbb{Z}_p) : j_{p,u}(x) \in \mathrm{im}(\mathrm{loc}_p)\} \subset \mathcal{Y}(\mathbb{Z}_p)$$

(scheme-theoretic image above)

$$\begin{array}{ccc} \mathcal{Y}(\mathbb{Z}_S) & \longrightarrow & \mathcal{Y}(\mathbb{Z}_p) \\ {\scriptstyle j_U}\downarrow & & \downarrow{\scriptstyle j_{p,U}} \\ \mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S)(\mathbb{Q}_p) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1(G_p, U(\mathbb{Q}_p)) \end{array}$$

Note that $\mathcal{Y}(\mathbb{Z}_S) \subset \mathcal{Y}(\mathbb{Z}_p)_U$. ⊙

In order to progress a bit, we'll make a few simplifying assumptions from now on.

Assumption.

- $p \notin S$
- $\mathcal{Y}$ is good at p, i.e. the complement of an étale divisor in a smooth, proper $\mathbb{Z}_p$-scheme
- $b \in \mathcal{Y}(\mathbb{Z}_p)$ is integral

Theorem 24.2 (to be proven later)**.** *Under the above assumptions,*

(1) *U is crystalline at p.*[27]

(2) $j_{p,U}(\mathcal{Y}(\mathbb{Z}_p))^{Zar} = \mathrm{H}^1_f(G_p, U)$.

In fact, if $x_0 \in \mathcal{Y}(\mathbb{F}_p)$ has residue disc $\mathbb{D}_{x_0} =]x_0[\subset Y^{an}_{\mathbb{Q}_p}$, then the restriction of $j_{p,U}$ to $\mathbb{D}_{x_0}$ is rigid analytic, and

$$j_{p,U}(\mathbb{D}_{x_0}(\mathbb{Q}_p))^{Zar} = \mathrm{H}^1_f(G_p, U).$$

Question 24.3 (Audience)**.** *In **(2)** above, what's the residue disk?*

Answer. Say $\mathcal{X}/\mathbb{Z}_S$ model of X where $\mathcal{Y}$ lives. Then, we have a reduction map $\mathrm{red} : X(\mathbb{Q}_p) = \mathcal{X}(\mathbb{Z}_p) \to \mathcal{X}(\mathbb{F}_p)$. In this case,

$$\mathbb{D}_{x_0}(\mathbb{Q}_p) = \{x \in X(\mathbb{Q}_p) : \mathrm{red}(x) = x_0\}.$$

If $x_0 \in \mathcal{Y}(\mathbb{F}_p)$, then actually $\mathbb{D}_{x_0}(\mathbb{Q}_p) \subset \mathcal{Y}(\mathbb{Z}_p)$. ⋆

Theorem 24.4 (`Chabauty-Kim criterion`)**.** *Use assumptions as above. Suppose, moreover, that*

$$\dim_{\mathbb{Q}_p} \mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S) < \dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_p, U).$$

Then, $\mathcal{Y}(\mathbb{Z}_p)_U$ is finite, and so $\mathcal{Y}(\mathbb{Z}_S)$ is finite as well.

Proof, assuming Theorem 24.2. Consider the diagram

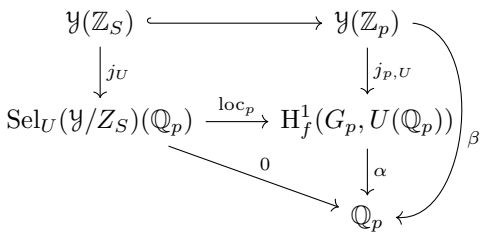
$$\begin{array}{ccc} \mathcal{Y}(\mathbb{Z}_S) & \longrightarrow & \mathcal{Y}(\mathbb{Z}_p) \\ {\scriptstyle j_U}\downarrow & & \downarrow{\scriptstyle j_{p,U}} \\ \mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S)(\mathbb{Q}_p) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, U(\mathbb{Q}_p)) \end{array}$$

(with bottom right object justified by Theorem 24.2). The dimension inequality implies that loc_p is not scheme-theoretically dense, i.e. that its scheme theoretic image is a proper subscheme of H^1_f. Because H^1_f (and so also $\mathrm{im}(\mathrm{loc}_p)$) is affine, there some exist some nonzero

$$\alpha : \mathrm{H}^1_f(G_p, U) \longrightarrow \mathbb{A}^1_{\mathbb{Q}_p}$$

[27] A priori, it's just de Rham

which vanishes on $\mathrm{im}(\mathrm{loc}_p)$. Consider the composition $\beta := \alpha \circ j_{p,U} : \mathcal{Y}(\mathbb{Z}_p) \to \mathbb{A}^1$.



This has the following properties

- β vanishes on $\mathcal{Y}(\mathbb{Z}_p)_U$
- β is (rigid) analytic on each residue disc
- β does not vanish uniformly on any residue disc

  Otherwise, $j_{p,U}(\mathbb{D}_{x_0}(\mathbb{Q}_p)) \subset \ker(\alpha) \subsetneq \mathrm{H}^1_f$, contradicting Theorem 24.2.

(2) + **(3)** together imply that β has only finitely many $\mathbb{Q}_p$-rational zeros (on each residue disk), as there are only finitely many residue disks. Combining this with **(1)** shows that $\mathcal{Y}(\mathbb{Z}_p)_U$ is finite. ■

Use, e.g., Weierstrass preparation

This prompts the question: how does verify the inequality in Theorem 24.4? We need to find a user-friendly way of understanding $\dim_{\mathbb{Q}_p} \mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S)$ and $\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_p, U)$.

Recall 24.5.

(1)

$$\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_p, U) = \sum_n \dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_p, V_n)$$

(Remark 18.12 + Recall 18.10 + Proposition 18.8).

(2)

$$\dim_{\mathbb{Q}_p} \mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S) \leq \sum_{\ell \neq p} \dim_{\mathbb{Q}_p} \mathfrak{S}_\ell + \sum_n \dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_{\mathbb{Q}}, V_n)$$

(Proposition 21.10). ⊙

Question 24.6 (Audience)**.** *When is* ***(2)*** *an equality?*

Answer. Gut feeling is that it should usually be an equality. It is possible to concoct examples where it is strict, though. ⋆

Proposition 24.7. *Let $\ell \neq p$. Then,*

(i) *$j_{\ell,U}(\mathcal{Y}(\mathbb{Z}_\ell))$ is finite.*

(ii) *$j_{\ell,U}(Y(\mathbb{Q}_\ell))^{Zar}$ has dimension ≤ 1.*

Corollary 24.8 (`Chabauty-Kim criterion, II`)**.** *Under the assumptions as above, suppose that*

$$\#S + \sum_n \dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_{\mathbb{Q}}, V_n) < \sum_n \dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_p, V_n).$$

Then, $\mathcal{Y}(\mathbb{Z}_p)_U$ is finite.

Proof of ***(i)*** *of Proposition 24.7.* We'll need a bit of rigid ℓ-adic geometry. Let $\mathbb{C}_\ell$ be a completed algebraic closure of $\mathbb{Q}_\ell$, and let $Z_{\mathbb{C}_\ell}$ be a rigid/Berkovich analytic space over $\mathbb{C}_\ell$. De Jong/Berkovich define a category $\mathrm{FÉt}(Z_{\mathbb{C}_\ell})$ of finite étale coverings of $Z_{\mathbb{C}_\ell}$. Moreover, for any $x \in Z_{\mathbb{C}_\ell}(\mathbb{C}_\ell)$, we get a fiber functor $\omega_x^{\text{ét}} : \mathrm{FÉt}(Z_{\mathbb{C}_\ell}) \longrightarrow \mathrm{FinSet}$, and so also a profinite étale fundamental groupoid $\pi_1^{\text{alg}}(Z_{\mathbb{C}_\ell}; x, y) = \mathrm{Isom}(\omega_x^{\text{ét}}, \omega_y^{\text{ét}})$.

Note 14. Much of what we'll quote is from "Étale fundamental groups of non-archimedean analytic spaces" by de Jong.

- If $Z_{\mathbb{C}_\ell}$ is connected, then $\pi_1^{\text{alg}}(Z_{\mathbb{C}_\ell}, x, y) \neq \emptyset$ always.
- There is a Galois correspondence $\mathrm{FÉt}(Z_{\mathbb{C}_\ell}) \cong \{\text{finite, continuous } \pi_1^{\text{alg}}(Z_{\mathbb{C}_\ell}; x)\text{-sets}\}$.

The crucial input we'll need is that "a disc is contractible."

Lemma 24.9 (Berkovich)**.** *Let $Z_{\mathbb{C}_\ell} = \mathbb{D}_{\mathbb{C}_\ell}$ be a disc (open or closed). Then,*

$$\pi_1^{alg}(\mathbb{D}_{\mathbb{C}_\ell}; x)^{(\ell')} = 1,$$

i.e. the maximal pro-(prime to ℓ) quotient is trivial.

For any $y \in \mathbb{D}_{\mathbb{C}_\ell}(\mathbb{C}_\ell)$, $\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; x, y)^{(\ell')}$ is defined to be the pushout (= contracted product) of $\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; x, y)$ along $\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; x) \to \pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; x)^{(\ell')}$. Equivalently, $\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; -, -)^{(\ell')}$ is the maximal quotient of $\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; -, -)$ such that each $\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; y)$ is pro-prime to ℓ. Thus,

$$\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; x, y)^{(\ell')} = 1 \text{ for all } x, y.$$

Now, let $\mathbb{D}$ be the disc over $\mathbb{Q}_\ell$. Then, G_ℓ acts on $\mathbb{C}_\ell$, so acts on $\mathbb{D}_{\mathbb{C}_\ell}$, and so acts on $\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; x, y)^{(\ell')} = 1$.

Now, let $\mathbb{D} \subset Y_{\mathbb{Q}_\ell}^{\text{an}}$ be an analytic disc. There is a functor

$$\mathrm{FÉt}(Y_{\mathbb{C}_\ell}) \longrightarrow \mathrm{FÉt}(\mathbb{D}_{\mathbb{C}_\ell})$$

(analytify and then restrict) which induces a morphism on fundamental groupoids, i.e. if $x, y \in \mathbb{D}(\mathbb{C}_\ell) \subset Y(\mathbb{C}_\ell)$, then there is a map

$$\pi_1^{\text{alg}}(\mathbb{D}_{\mathbb{C}_\ell}; x, y) \longrightarrow \pi_1^{\text{ét}}(Y_{\mathbb{C}_\ell}; x, y).$$

If $x, y \in \mathbb{D}(\mathbb{Q}_\ell)$, then this map is G_ℓ-equivariant. By the previous discussion, this produces for us a G_ℓ-invariant path, i.e. this shows that

$$\left(\pi_1^{\text{ét}}(Y_{\mathbb{C}_\ell}; x, y)^{(\ell')}\right)^{G_\ell} \neq \emptyset.$$

This implies that also $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; x, y)^{G_\ell} \neq \emptyset$. To compute the image of the local Kummer map, choose some path $\gamma_{b,x} \in \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; b, x)$ and then set

$$\gamma_{b,y} := \gamma_{x,y} \cdot \gamma_{b,x} \text{ for some } \gamma_{x,y} \in \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}_\ell}; x, y)^{G_\ell}.$$

Hence, $j_\ell(y)$ is the class of the cocycle

$$\xi(\sigma) := \gamma_{b,y}^{-1}\sigma(\gamma_{b,y}) = \gamma_{b,x}^{-1}\gamma_{x,y}^{-1}\sigma(\gamma_{x,y})\sigma(\gamma_{b,x}) = \gamma_{b,x}^{-1}\sigma(\gamma_{b,x}).$$

Thus, $j_\ell(y) = \jmath_\ell(x)$, so the local Kummer map j_ℓ collapses all residue disks. Finally, $\mathcal{Y}(\mathbb{Z}_\ell)$ can be covered by finitely many such discs by compactness, so $j_\ell(\mathcal{Y}(\mathbb{Z}_\ell))$ must be finite. ∎

Remark 24.10. For **(ii)** of Proposition 24.7, one needs to analyze the fundamental groupoid of punctured disks. Away from ℓ, these will be pro-cyclic (assuming I heard correctly). ∘

Remark 24.11. Apparently if you points reduce to the same component of the special fiber (not just the same point), then there will be a Galois-invariant path between them. ∘

25 Lecture 21 (4/20): The non-abelian Chabauty method, I

There's one problem on pset 6, giving an example of using Chabauty-Kim to prove finiteness.

Recall 25.1.

Theorem 25.2 (Chabauty-Kim criterion, Corollary 24.8)**.** *$Y/\mathbb{Q}$ a hyperbolic curve w/ basepoint $b \in Y(\mathbb{Q})$, U a quotient of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)$. $\mathcal{Y}/\mathbb{Z}_S$ an S-integral model. If*

$$\#S + \sum_{n\geq 1} \dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_n) < \sum_{n\geq 1} \dim \mathrm{H}^1_f(G_p, V_n),$$

then $\mathcal{Y}(\mathbb{Z}_p)_U$ is finite, so also $\mathcal{Y}(\mathbb{Z}_S)$ is finite.

Above, `hyperbolic` means smooth with negative Euler characteristic. ⊙

25.1 Example: Siegel's Theorem

This application was the one given in Kim's original paper [Kim05] on the subject.

Theorem 25.3 (`Siegel's Theorem`)**.** *Let S be a finite set of prime numbers. Then, there are only finitely many triples (a, b, c) of coprime integers – each only divisible by primes in S – such that*

$$a + b = c.$$

Example 25.4. If $S = \{2, 3\}$, up to signed permutations, the only solutions are

$$1 + 1 = 2 \quad 1 + 2 = 3 \quad 1 + 3 = 4 \quad 1 + 8 = 9$$ △

Let's reformulate Seigel a bit. Put another way, it says there are only finitely many solutions to the S-`unit equation`:

$$x + y = 1 \text{ for } x, y \in \mathbb{Z}_S^\times.$$

Equivalently, let $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}} \setminus \{0, 1, \infty\} = \operatorname{Spec} \mathbb{Z}\left[t^{\pm 1}, \frac{1}{1-t}\right]$. Then,

$$\mathcal{Y}(R) = \left\{x \in R^\times : 1 - x \in R^\times\right\} = \left\{(x, y) \in (\mathbb{R}^\times)^2 : x + y = 1\right\}.$$

Thus, Siegel's theorem is equivalent to $\mathcal{Y}(\mathbb{Z}_S)$ being finite for all S. This sounds something Chabauty-Kim could be used for.

Let $Y = \mathcal{Y}_{\mathbb{Q}}$ be the generic fiber. Fix any choice of basepoint $Y(\mathbb{Q})$. For the moment, let $U = \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)$. What is this group? By comparison with $\mathbb{C}$, we know that U is the $\mathbb{Q}_p$-Malčev completion of $\pi_1(Y(\mathbb{C}); b) = F_2$. Thus, U is the free $\mathbb{Q}_p$-pro-unipotent group on 2 generators. In order to apply our finiteness criterion, we also need to understand the Galois action on this.

Remark 25.5. As $\pi_1^{\mathbb{Q}_p}(\mathbb{P}^1_{\overline{\mathbb{Q}}}; b) = 1$ is trivial, the weight filtration (Definition 11.15) on U is nothing more than the descending central series:

$$W_{1-2n}U = W_{-2n}U = \Gamma^n U.$$

To see this, start with

$$W_{-1}U = U \text{ and } W_{-2}U = \ker\left(\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b) \to \pi_1^{\mathbb{Q}_p}(\mathbb{P}^1_{\overline{\mathbb{Q}}}; b)^{\mathrm{ab}}\right) = U,$$

and then use the inductive formula for the higher W_{-k}'s. In any case, note that $V_n = 0$ if n is odd. ∘

Claim 25.6. *$V_2 = U^{\mathrm{ab}} = \mathbb{Q}_p(1)^{\oplus 2}$ as a $G_{\mathbb{Q}}$-rep.*

Proof. Consider the map

$$\begin{array}{rccc} \iota: & Y & \longrightarrow & \mathbb{G}_m^2 \\ & t & \longmapsto & (t, 1-t) \end{array}$$

We claim that the induced map

$$i_* : \pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b) \longrightarrow \pi_1^{\mathbb{Q}_p}(\mathbb{G}^2_{m,\overline{\mathbb{Q}}}; b)$$

is the abelianization. Because this is a group theoretic statement, it suffices to prove the corresponding claim for Betti π_1's of $Y(\mathbb{C}) \to (\mathbb{C}^\times)^2$. Over $\mathbb{C}$, one can check that

$$F_2 = \pi_1(Y(\mathbb{C}); b) \longrightarrow \pi_1((\mathbb{C}^\times)^2; b) = \mathbb{Z}^2$$

is the map sending $\gamma_0 \mapsto (1, 0)$ and $\gamma_1 \mapsto (0, 1)$ (γ_x is a simple loop around the puncture at x). This proves the subclaim.

Now we win as $U^{\mathrm{ab}} \cong \pi_1^{\mathbb{Q}_p}(\mathbb{G}^2_{m,\overline{\mathbb{Q}}}; b) \simeq \mathbb{Q}_p(1)^{\oplus 2}$. ■

Remark 25.7 (Response to audience question). One can alternatively prove this by realizing U^{ab} is dual to $\mathrm{H}^1(Y_{\overline{\mathbb{Q}}}; \mathbb{Q}_p)$ (Hurewicz, Theorem 12.3).[28] ∘

Question 25.8 (Audience, paraphrased)**.** *Where's the* (1) *coming from above? Why is* $\pi_1^{\mathbb{Q}_p}(\mathbb{G}_{m,\overline{\mathbb{Q}}}; b) \cong \mathbb{Q}_p(1)$*?*

Answer. The covers of $\mathbb{G}_m$ are essentially all given by nth power maps $\mathbb{G}_m \to \mathbb{G}_m, z \mapsto z^n$. Thus, the Galois action will be via the cyclotomic character. ⋆

Question 25.9 (Audience)**.** *Why do Malčev completion and abelianization commute?*

Answer. The slickest way of saying this is that both are right adjoints, and these commute. You can check that the abelianization of the completion and the completion of the abelianization satisfy the same universal property. ⋆

Claim 25.10. *$V_{2n} = \mathbb{Q}_p(n)^{\oplus r_n}$ for some $r_n \geq 0$.*

Proof. The iterated commutator map

$$\begin{array}{ccc} (U^{\mathrm{ab}})^{\otimes n} & \longrightarrow & V_{2n} \\ x_1 \otimes \cdots \otimes x_n & \longmapsto & [x_1, [x_2, \ldots [x_{n-1}, x_n]] \ldots] \end{array}$$

[28] You can compute the latter e.g. by computing compactly supported cohomology and then using Poincaré duality.

is $G_{\mathbb{Q}}$-equivariant and surjective (by definition of descending central series), so V_{2n} is a quotient of $\mathbb{Q}_p(n)^{\oplus 2^n}$. ■

Claim 25.11. *$r_n \geq 1$ for $n \geq 1$. Consequently, U is legitimately pro-unipotent and not simply unipotent.*

Proof 1. Let $\mathfrak{u}^{\mathrm{PL}}$ be the (pronilpotent) `polylogarithmic Lie algebra`, i.e. $\mathfrak{u}^{\mathrm{PL}}$ has basis $f, (e_i)_{i\geq 1}$ and the Lie bracket is $[e_i, e_j] = 0$ and $[f, e_i] = e_{i+1}$. Let $\mathfrak{f}_2$ be the free pro-nilpotent Lie algebra on 2 generators x, y. Have

$$\psi : \mathfrak{f}_2 \longrightarrow \mathfrak{u}^{PL}$$

w/ $\psi(x) = f$ and $\psi(y) = e_1$. Then ψ is surjective, so also induces a surjection

$$\mathrm{gr}^n_\Gamma \mathfrak{f}_2 \twoheadrightarrow \mathrm{gr}^n_\Gamma \mathfrak{u}^{PL},$$

with target having dimension ≥ 1 (a basis is f, e_1 if $n = 1$ or e_n if $n \geq 2$). ■

Proof 2. In fact, we'll show that

$$r_n = \frac{1}{n} \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, 2^d > 0.$$

This can be done using the *Lyndon basis* of $\mathfrak{f}_2$.

Definition 25.12. An associative word w in two letters x, y is called `acyclic` if it is different from all of its cyclic permutations. An acyclic word is called `primitive` if it is smallest amongst its cyclic permutations in the lexicographical ordering ($x < y$). ◇

Example 25.13. $xxxy$ and $yxyy$ are acyclic. Of them, only $xxxy$ is primitive. △

Non-example. $xyxy$ is not acyclic. ▽

Remark 25.14. A primitive word has a longest acyclic proper subword/initial segment. For example, for $\underline{xxxy}$ this subword is just x. ○

Theorem 25.15 (`Lyndon`)**.** *$\mathfrak{f}_2$ has a basis in bijection with primitive acylic words in x, y. Say α_w is the basis element corresponding to a word $w = w_1 w_2$ w/ w_1, w_2 primitive acyclic (and w_1 longest such that this is the case), then $\alpha_w = [\alpha_{w_1}, \alpha_{w_2}]$. Furthermore, as you'd expect, $\alpha_x = x$ and $\alpha_y = y$. Finally, the words of length $\geq n$ give a basis of $\Gamma^n \mathfrak{f}_2$.*

See an illustration of this in Table 1. The upshot of this is that $r_n = \dim \mathrm{gr}^n_\Gamma \mathfrak{f}_2$ is equal to the number of Lyndom words of length n. The total number of words of length n is 2^n. Not all of these are aperiodic/acyclic, but each word has a period $d \mid n$ and is of the form (aperiodic word of length n/d)^d. Now, the number of aperiodic words of length n/d is $\frac{n}{d} r_{n/d}$. Thus,

$$2^n = \sum_{d|n} \frac{n}{d} r_{n/d} = \sum_{d|n} d r_d.$$

Lyndom words	Basis elements
x, y	x, y
xy	[x,y]
xxy, xyy	[x,[x,y]], [[x,y],y]
xxxy, xyyy, xxyy	[x,[x,[x,y]]], [[[x,y],y],y], [[x,[x,y]],y]

Table 1: All `Lyndom words` (primitive acyclic words) up to length 4. Equivalently, Lyndon basis elements of $\mathfrak{f}_2$ (free Lie algebra on 2 generators), up to depth 4.

Apply Möbious inversion to conclude that $nr_n = \sum_{d|n} \mu(n/d)2^d$, as desired. ∎

We now know that

$$V_{2n} = \mathbb{Q}_p(n)^{\oplus r_n} \text{ with } r_n = \frac{1}{n}\sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, 2^d \geq 1.$$

Claim 25.16. $\dim \mathrm{H}^1_f(G_p, \mathbb{Q}_p(n)) = 1$ *for* $n \geq 1$.

Proof. $D_{\mathrm{dR}}(\mathbb{Q}_p(n)) = \mathbb{Q}_p$ with filtration

$$F^i D_{\mathrm{dR}}(\mathbb{Q}_p(n)) = \begin{cases} \mathbb{Q}_p & \text{if } i \leq -n \\ 0 & \text{if } i > -n, \end{cases}$$

so $D^+_{\mathrm{dR}}(\mathbb{Q}_p(n)) = 0$. We win by $\mathrm{H}^1_f = D_{\mathrm{dR}}/D^+_{\mathrm{dR}}$. ∎

Claim 25.17 (Soulé)**.** $\dim \mathrm{H}^1_f(G_{\mathbb{Q}}, \mathbb{Q}_p(1)) = 0$ *and*

$$\dim \mathrm{H}^1(G_{\mathbb{Q}}, \mathbb{Q}_p(n)) = \begin{cases} 0 & \textit{if } n \geq 2 \textit{ even} \\ 1 & \textit{if } n \geq 2 \textit{ odd.} \end{cases}$$

($n = 1$ is Kummer theory, so not so bad. $n \geq 2$ is harder[29])

In our Chabauty application, let's take $U_{2N} = U/W_{-2N-1}U$ for $N \gg 0$. Then,

$$\#S + \sum_{n=1}^{N} \dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_{2n}) \leq \#S + \sum_{\substack{2 \leq n \leq N \\ n \text{ odd}}} r_n, \tag{25.1}$$

while

$$\sum_{n=1}^{N} \dim \mathrm{H}^1_f(G_p, V_{2n}) = \sum_{n=1}^{N} r_n. \tag{25.2}$$

For any fixed S, we will have (25.1) $<$ (25.2) for $N \gg 0$.[30] Thus, the Chabauty-Kim criterion (Corollary 24.8) implies that $\mathcal{Y}(\mathbb{Z}_S)$ is finite.

Remark 25.18 (Response to audience question). The Galois action on the fundamental group depends on the choice of basepoint. However, as we saw, the graded pieces had the same Galois action independent of this choice. The implicit choice of prime p also didn't matter here. ∘

Remark 25.19. In the end, there was a question about a third way of proving $r_n \geq 1$. I didn't take notes on this, but Alex sketched an approach via comparing natural Hilbert series for $\mathscr{O}(U) = \mathrm{Sym}^\bullet(\mathrm{Lie}(U)^*)$. ∘

26 Office Hours

Question 26.1 (Audience)**.** *How lucky did we get w/ today's example? It seemed surprisingly easy to compute the Galois actions on these quotients?*

Answer. Depends on what you mean by lucky. In general, the Galois actions on these V_n's will be built out of Tate modules of semiabelian varieties, so things like $\mathbb{Q}_p(m)$ and Tate modules of abelian varieties (mixed with sums, tensors, wedge powers, etc.). The hard part is computing global Bloch-Kato Selmer group dimensions. ⋆

[29] The $n = 1$ case is done in [Bel09, Proposition 2.12]

[30] $N \geq 2\#S + 2$ should work

Question 26.2 (Audience)**.** *Can you say a bit of how Soulé's proof goes?*

Note 15. I was distracted and missed too much of the answer to write down anything helpful. Apparently, Kim's first part cites the wrong Soulé paper for this result.

Question 26.3 (Audience)**.** *Can you get bounds on the number of solutions to the S-unit equation from what we're doing?*

Answer. From what we've done so far, no. The finiteness ultimately comes from choosing some nonzero map

$$\alpha : \mathrm{H}^1_f(G_p, U) \longrightarrow \mathbb{A}^1_{\mathbb{Q}_p}$$

which vanishes on the image of the localization map $\mathrm{Sel} \to \mathrm{H}^1_f(G_p, U)$. Once we have one, we can produce many more (e.g. $\alpha^2 - a\alpha$ or $\alpha^3 - a\alpha^2 - b\alpha$). The (number of) points where $\alpha \circ j_{p,U}$ vanishes depends on the specific α chosen, so to get a bound, you need to get control over this α. This can be done. Alex has a paper doing this for S-unit equation, for example, which shows something like $\#\mathcal{Y}(\mathbb{Z}_S) \leq 8 \cdot 6^{\#S} \cdot 2^{4^{\#S}}$. Analytic methods can do better though, e.g. $\#\mathcal{Y}(\mathbb{Z}_S) \leq 21 \cdot 7^{2\#S}$. ⋆

Remark 26.4 (Based on more questions). These Selmer schemes have more structure than we've been using. We've seen a shadow of this in thinking of them as iterated torsors over vector groups.

Theorem 26.5 (B.). $\mathrm{H}^1_f(G_p, U)$ *and* $\mathrm{Sel}_U(\mathcal{Y}/\mathbb{Z}_S)$ *come with weight filtrations on their affine rings such that*

$$\mathrm{loc}_p^* : \mathscr{O}(\mathrm{H}^1_f) \longrightarrow \mathscr{O}(\mathrm{Sel})$$

is filtered.

As a consequence, if $\dim W_m\mathscr{O}(\mathrm{Sel}) < \dim W_m\mathscr{O}(\mathrm{H}^1_f)$, then there exists some non-zero $\alpha \in W_m\mathscr{O}(\mathrm{H}^1_f)$ such that $\mathrm{loc}_p^*\,\alpha = 0$. This is extra useful because $W_m\mathscr{O}(\mathrm{H}^1_f)$ is a f.dim vector space, so it is possible to bound the number of zeros of $\alpha \circ j_{p,U}$. So, one ends up wanting to do a Hilbert series computation in order to compare the dimensions of these filtered pieces, e.g. look for an m such that the t^m coefficient in

$$\frac{1}{1-t}\prod_{n\geq 1}(1-t^n)^{-\dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_n)}$$

is less than that in

$$\frac{1}{1-t}\prod_{n\geq 1}(1-t^n)^{--\dim \mathrm{H}^1_f(G_p, V_n)}.$$

In the case of $\mathbb{P}^1 \setminus \{3 \text{ points}\}$, this latter thing turns out to be $(1-t)^{-1}(1-2t)^{-1}$. ∘

Question 26.6 (Audience)**.** *Has this been used to bound points on other hyperbolic curves?*

Answer. There's a precursor to this from a paper of Jen et al. Sounds like there's a preprint using their work to work out another bound. These are all meant to be versions/generalizations of Coleman's bound. However, whereas Coleman's bound is sometimes tight, these other tend to be very non-tight. ⋆

26.1 Models of Curves

Say we have an elliptic curve $E : y^2 = x^3 + 1 + p^5$. Can look at its reduction mod p: $y^2 = x^3 + 1$. Then you can, for example, try to bound the number of torsion points on E by counting (torsion) points over $\mathbb{F}_p$. However, it's good to know what these things are doing geometrically.

Warning 26.7. Someone might give you $y^2 = x^3 + p^6$ or $y^2 = x^3 + p^{-6}$. The first of these looks like it reduces to something singular $y^2 = x^3$, while for the second, it's maybe not clear what its reduction mod p should be. However, all three of these curves are isomorphic over $\mathbb{Q}$. •

When you write down an equation with integral coefficients, you should think of it as defining a curve over $\mathbb{Z}$ ($\mathbb{Z}[1/p]$ in the last case above) or $\mathbb{Z}_p$, and then reducing mod p corresponds to taking the fiber over $\mathbb{F}_p$. The reason we get seemingly different behaviors for the reduction at p for all of these $\mathbb{Q}$-isomorphic curves is that we've looked at 3 different models for this curve over $\mathbb{Z}$ (or $\mathbb{Z}[1/p]$).

Definition 26.8. A `model` of $X/\mathbb{Q}_p$ is a normal, proper, flat, integral $\mathbb{Z}_p$-scheme $\mathcal{X}$, along with an isomorphism $\mathcal{X}_{\mathbb{Q}_p} \simeq X$. ◇

Question 26.9. *Is there a best possible reduction/model?*

Sometimes models are regular, and that's useful.

Example 26.10. $y^2 = x^3 + p^6$ is not regular at $(x, y, p) = (0, 0, 0)$. Consider the surface

$$\left\{y^2 = x^3 + t^6\right\} \longrightarrow \mathbb{A}^1_t.$$

This is singular at the point $(0, 0, 0)$ e.g. because the equation defining the tangent space is

$$2y\mathrm{d}y = 3x^2\mathrm{d}x + 6t^5\mathrm{d}t.$$

This is meant to make you suspect that $y^2 = x^3 + p^6$ will be non-regular, even before you actually go through the trouble of checking this. △

Fact. Regular models of curves (e.g. over $\mathbb{Z}_p, \mathbb{Z}, \dots$) always exist.

Example 26.11. Consider $y^2 = x^3 + p$ is regular (say $p \neq 2, 3$). The analogous fibered surface over $\mathbb{A}^1_t$ has tangent space defined by $2y\mathrm{d}y = 3x^2\mathrm{d}x + \mathrm{d}t$ (which is 1-dimensional even at the singular point). △

In general, there are many different regular models.

Example 26.12. Consider e.g. $\mathbb{P}^1_{\mathbb{Q}_p} = \operatorname{Proj} \mathbb{Q}_p[x, y]$. One model is $\mathbb{P}^1_{\mathbb{Z}_p} = \operatorname{Proj} \mathbb{Z}_p[x, y]$. A different model is $\operatorname{Proj} \mathbb{Z}_p[px, y]$ (i.e. $\operatorname{Proj} \mathbb{Z}_p[s, y]$ where $s = px$ in the identification w/ the generic fiber). A third model is given by the blowup of $\mathbb{P}^1_{\mathbb{Z}_p}$ at the origin in the special fiber.

Write $\mathbb{A}^1_{\mathbb{Z}_p} = \operatorname{Spec} \mathbb{Z}_p[x]$, so the ideal defining the origin in the special fiber is generated by (x, p). The blowup effectively has coordinates x, p, X, P (capital letters are projective coordinates), and looks like

$$\operatorname{Proj}(\mathbb{Z}_p[x][X, P]/(xP - Xp)).$$

What do the fibers over $\mathbb{A}^1_{\mathbb{Z}_p}$ look like? These are points away from 0 (origin in special fiber) since either p or x will be invertible (e.g. where p is invertible, get $\operatorname{Proj} \mathbb{Z}_p[x][P]$). At 0, though, we get $\operatorname{Proj} \mathbb{F}_p[X, P] \simeq \mathbb{P}^1_{\mathbb{F}_p}$. This blowup $\operatorname{Bl}_0 \mathbb{P}^1_{\mathbb{Z}_p}$ will be a new regular model. △

In general, given a regular model, you can produce new ones by blowing up smooth points.

Theorem 26.13. *If $g \geq 1$, then there is a unique minimal regular model, i.e. every other regular model is a(n iterated) blowup.*

When people talk about "reductions of curves," they usually really mean "reductions of the *minimal regular model* of your curves."

Definition 26.14. A `semistable model` is a model for which the special fiber is a reduced normal crossings divisor. A `stable model` is a semistable model whose special fiber has no "unstable components." ◇

Theorem 26.15. *Assume $g \geq 2$. There always exists a finite extension $K/\mathbb{Q}_p$ such that X_K admits a regular semistable model (minimal regular model will work) as well as a stable model (not necessarily regular).*

(In genus 1, also always get a semistable model after base change)

For elliptic curves, semistable models have either good reduction or Kodaira type I_n reduction (special fiber is an n-gon of $\mathbb{P}^1$'s).

Example 26.16. In genus 2, can have a regular semistable model w/ special fiber looking like a genus 0 curve and a genus 1 curve meeting in two points. The corresponding stable model then looks like a genus 1 curve meeting itself in one point (blowdown the genus 0 curve). △

Question 26.17 (Audience)**.** *Is there a relationship between semistable models and semistable Galois reps?*

Answer. Can also talk about models of abelian varieties. By Néron-Ogg-Shaferavich, an abelian variety has a semistable model iff its ℓ-adic Tate module has inertia acting unipotently. It also turns out to be the case that a curve has semistable model iff its Jacobian does. ⋆

27 Lectures 22,23 (4/25,27): Quadratic Chabauty (Last lectures) – Didn't Go

Note 16. These notes are taken from a combination of a lecture recording (of the 27th) by a friend, notes from another friend, and Alex's online notes.

Slogan. Quadratic Chabauty is non-abelian Chabauty for the weight ≥ -2 parts of the fundamental group.

Recall 27.1. The `Néron-Severi` group $\mathrm{NS}(X)$ of a variety X is the gorup of divisors on X up to algebraic equivalence, i.e. $\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$. ⊙

Theorem 27.2 (`Theorem of the Base`)**.** $\mathrm{NS}(X)$ *is a finitely generated abelian group.*

Example 27.3. Say X is a smooth projective curve. Then, the degree map gives an isomorphism $\deg : \mathrm{NS}(X) \to \mathbb{Z}$. △

Example 27.4. Say $X = A$ is a principally polarized abelian variety, w/ polarization $\lambda : A \xrightarrow{\sim} \widehat{A}$. Then, $\mathrm{End}(A)$ has the `Rosati involution` given by

$$\mathrm{End}(A) \ni \chi \longmapsto \lambda^{-1} \circ \widehat{\chi} \circ \lambda \in \mathrm{End}(A).$$

Set $\mathrm{End}(A)^+ := \{\chi \in \mathrm{End}(A) : \chi \text{ fixed by Rosati}\}$. Then,

$$\mathrm{NS}(A)_{\mathbb{Q}} \cong \mathrm{End}(A)^+_{\mathbb{Q}}.$$

If $D \subset A$ is a divisor, can define the morphism $\lambda_D : A \to \widehat{A}, x \mapsto \tau_x^* D - D$ (where τ_x is translation by x), and so get a map $\mathrm{Div}(A) \to \mathrm{End}(A), D \mapsto \lambda_D$. This induces the claimed isomorphism. △

Warning 27.5. There is also a Néron-Severi group scheme $\underline{\mathrm{NS}}(X) = \underline{\mathrm{Pic}}(X)/\underline{\mathrm{Pic}}^0(X)$. This is a discrete algebraic group, corresponding to the finitely generated group $\mathrm{NS}(X_{\overline{K}})$ w/ Galois action. In particular,

$$\underline{\mathrm{NS}}(X)(K) = \mathrm{NS}(X_{\overline{K}})^{\mathrm{Gal}_K} \neq \mathrm{NS}(X). \qquad \bullet$$

Definition 27.6. The K-rational Picard number of X is $\rho_K(X) := \operatorname{rank} \mathrm{NS}(X)$. $\diamond$

Theorem 27.7 (Quadratic Chabauty)**.** *Let $X/\mathbb{Q}$ be a smooth, projective curve of genus g. Let $J = \mathrm{Jac}(X)$, $r = \operatorname{rank} J(\mathbb{Q})$, and $\rho := \rho_{\mathbb{Q}}(J)$. Then,*

$$r < g + \rho - 1 \implies X(\mathbb{Q}) \text{ is finite.}$$

Remark 27.8. $\rho \geq 1$ always, so $r < g + \rho - 1$ is, in general, weaker than the classical Chabauty condition $r < g$. $\circ$

To prove this, we'll find a suitable quotient of $\pi_1^{\mathbb{Q}_p}$. Fix an arbitrary basepoint $b \in X(\mathbb{Q})$.

Lemma 27.9. *Let $\mathrm{AJ} : X \hookrightarrow J$ be the Abel-Jacobi map. Then, the induced map*

$$\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b) \longrightarrow \pi_1^{\mathbb{Q}_p}(J_{\overline{\mathbb{Q}}}; b) = V_p J$$

is the abelianization of $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b)$

Proof. By Hurewicz (Theorem 12.3), we know that $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b)^{\mathrm{ab}} = \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^*$, so it suffices to prove that $\mathrm{AJ}^* : \mathrm{H}^1_{\text{ét}}(J_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) \to \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ is an isomorphism. This is a standard fact.[31] ■

27.1 $\mathbb{G}_m$-torsors on abelian varieties

Setup 27.10. Let $K/\mathbb{Q}$ be a field of characteristic 0. Let A/K be an abelian variety. Let L be a line bundle on A, and let $L^\times$ be the complement of the zero section in the total space of L, so $L^\times$ is a $\mathbb{G}_m$-torsor over A. Choose a point $\widetilde{0} \in L^\times(K)$ in the fiber over $0 \in A(K)$.

Note that we can map $\mathbb{G}_m \hookrightarrow L^\times$ via $g \mapsto g \cdot \widetilde{0}$.

Proposition 27.11. *The maps $\mathbb{G}_m \hookrightarrow L^\times \twoheadrightarrow A$ induce a central extension*

$$1 \longrightarrow \mathbb{Q}_p(1) \longrightarrow \pi_1^{\mathbb{Q}_p}(L_{\overline{K}}; \widetilde{0}) \longrightarrow V_p A \longrightarrow 1$$

whose commutator pairing $\bigwedge^2 V_p A \to \mathbb{Q}_p(1)$ is the Chern class

$$c_1^{\acute{e}t}(L) \in \mathrm{H}^2_{\acute{e}t}(A_{\overline{K}}, \mathbb{Q}_p(1)) = \mathrm{Hom}\left(\bigwedge^2 V_p A, \mathbb{Q}_p(1)\right).$$

Proof. WLOG $K = \mathbb{C}$. We will show there is a short exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(\mathbb{C}^\times; 1) & \longrightarrow & \pi_1(L^\times(\mathbb{C}); \widetilde{0}) & \longrightarrow & \pi_1(A(\mathbb{C}), 0) & \longrightarrow & 1 \\ & & \downarrow \wr & & & & & & \\ & & (2\pi i)\mathbb{Z} & & & & & & \end{array}$$

[31] Use the Kummer sequence $0 \to \mu_{p^n} \to \mathbb{G}_m \xrightarrow{(-)^{p^n}} \mathbb{G}_m \to 0$ (I guess, plus the fact that Jacobians are canonically principally polarized)

whose commutator pairing is the first Chern class $c_1(L) \in \mathrm{H}^2(A(\mathbb{C}), \mathbb{Z})(1) = \mathrm{Hom}(\bigwedge^2 \mathrm{H}^1(A(\mathbb{C}), \mathbb{Z}), 2\pi i)$ of L. Because $\mathbb{C}^\times \hookrightarrow L^\times(\mathbb{C}) \to A(\mathbb{C})$ is a locally trivial fibration, there is an induced homotopy exact sequence:

$$0 = \pi_2(A(\mathbb{C})) \longrightarrow \pi_1(\mathbb{C}^\times) \longrightarrow \pi_1(L^\times(\mathbb{C})) \longrightarrow \pi_1(A(\mathbb{C})) \longrightarrow \pi_0(\mathbb{C}^\times) = 1. \tag{27.1}$$

- (27.1) is a central extension.

  Consider the conjugation action of $\pi_1(A(\mathbb{C}))$ on $\mathbb{Z}(1) = \pi_1(\mathbb{C}^\times)$. This is the same as the monodromy action on $\mathrm{H}_1(\mathbb{C}^\times; \mathbb{Z}) = \pi_1(\mathbb{C}^\times)$. This action is trivial because $L^\times(\mathbb{C}) \to A(\mathbb{C})$ is an oriented[32] $\mathbb{C}^\times$-torsor.[33]

- The commutator pairing on (27.1) is the Chern class of L.

  Note 17. This is some explicit computation, omitted here.

■

27.2 Back to quadratic Chabauty

Recall 27.12. We fixed a smooth, projective curve $X/\mathbb{Q}$ of genus g. We also chose a basepoint $b \in X(\mathbb{Q})$, and so have an associated Abel-Jacobi map $\mathrm{AJ} : X \hookrightarrow J := \mathrm{Jac}(X)$. We also set $r = \mathrm{rank}\, J(\mathbb{Q})$ and $\rho = \mathrm{rank}\, \mathrm{NS}(J)$. ⊙

Remark 27.13. There's an induced map $\mathrm{AJ}^* : \mathrm{Pic}(J) \to \mathrm{Pic}(X)$, which furthermore restricts to an isomorphism $\mathrm{Pic}^0(J) \xrightarrow{\sim} \mathrm{Pic}^0(X)$. Thus, there is an induced map

$$\mathrm{AJ}^* : \mathrm{NS}(J) \longrightarrow \mathrm{NS}(X) = \mathbb{Z}.$$

This also means that the natural map

$$\mathcal{K} := \ker(\mathrm{AJ}^* : \mathrm{Pic}(J) \to \mathrm{Pic}(X)) \xrightarrow{\sim} \ker(\mathrm{AJ}^* : \mathrm{NS}(J) \to \mathrm{NS}(X))$$

is an isomorphism, so $\mathcal{K} \leq \mathrm{NS}(J)$ is a finitely generated (torsion free?) abelian group of rank $\rho - 1$. ∘

Example 27.14. Suppose that $\rho \geq 2$, so there must be some non-trivial line bundle L on J such that $\mathrm{AJ}^*(L) \simeq \mathscr{O}_X$. Thus, the Abel-Jacobi embedding lifts to an embedding

$$\begin{array}{ccc} \mathbb{G}_m \times X & \longrightarrow & L^\times \\ \downarrow & \nearrow_{\widetilde{\mathrm{AJ}}} & \downarrow \\ X & \xrightarrow{\mathrm{AJ}} & J \end{array}$$

of $X \hookrightarrow L^\times$.

Claim 27.15. $\widetilde{\mathrm{AJ}}_* : \pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b) \to \pi_1^{\mathbb{Q}_p}(L^\times_{\overline{\mathbb{Q}}}, \widetilde{0})$ *is surjective.*

Proof. Recall the extension from Proposition 27.11, we have the diagram

$$\begin{array}{ccccccccc} & & & & \pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}; b) & & & & \\ & & & & \downarrow{\scriptstyle \widetilde{\mathrm{AJ}}_*} & \searrow^{\mathrm{AJ}_*} & & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & \pi_1^{\mathbb{Q}_p}(L^\times_{\overline{\mathbb{Q}}}; \widetilde{0}) & \longrightarrow & V_pJ & \longrightarrow & 0 \end{array}$$

[32] all fibers are consistently oriented.

[33] The orientation gives a preferred generator of $\mathrm{H}_1(\mathbb{C}^\times; \mathbb{Z}) = \pi_(\mathbb{C}^\times) \simeq \mathbb{Z}$. Any loop on $A(\mathbb{C})$ will respect this preferred generator, and so the monodromy action is trivial.

V	$\dim V$	Computation of $\dim V$
$\mathrm{H}^1_f(G_{\mathbb{Q}}, V_1)$	p^∞-Selmer rank of J	Claim 27.18
$\mathrm{H}^1_f(G_{\mathbb{Q}}, V_2)$	0	Claim 25.17
$\mathrm{H}^1_f(G_p, V_1)$	g	Claim 27.17
$\mathrm{H}^1_f(G_p, V_2)$	$\rho - 1$	Claim 25.16

Table 2: The dimensions of the local/global Selmer groups attached to the quotient of $\pi_1^{\mathbb{Q}_p}(X)$ used in quadratic Chabauty. Here, $V_1 = V_pJ$ and $V_2 = \mathbb{Q}_p(1)^{\oplus(\rho-1)}$.

with bottom row exact. Above, AJ_* is surjective by Lemma 27.9. We also know that the commutator pairing

$$\bigwedge^2 V_pJ \longrightarrow \mathbb{Q}_p(1)$$

is surjective, simply because it is the first Chern class $c_1^{\text{ét}}(L)$ of L, which is nonzero (because $L \notin \mathrm{Pic}^0(J)$). This is enough to force $\widetilde{\mathrm{AJ}}_*$ to be surjective, as its image will contain a generator of $\mathbb{Q}_p(1)$ and surject onto V_pJ. ■

In other words, given such an L, we can produce a quotient of the fundamental group which is an extension of $V_pJ \simeq \pi_1^{\mathbb{Q}_p}(X)^{\mathrm{ab}}$ by $\mathbb{Q}_p(1)$. △

In general, we can choose independent line bundles $L_1, \dots, L_{\rho-1}$ on J such that $\mathrm{AJ}^* L_i \simeq \mathscr{O}_X$ for all i. We can then consider the fiber product

$$M := L_1^\times \times_J \dots \times_J L_{\rho-1}^\times,$$

and realize $\pi_1^{\mathbb{Q}_p}(M)$ as a quotient of $\pi_1^{\mathbb{Q}_p}(X)$ (via a lifted Abel-Jacobi map) fitting into a central extension

$$0 \longrightarrow \mathbb{Q}_p(1)^{\oplus\rho-1} \longrightarrow \pi_1^{\mathbb{Q}_p}(M) \longrightarrow V_pJ \longrightarrow 0.$$

Lemma 27.16. *$\pi_1^{\mathbb{Q}_p}(X)$ has a quotient U which is a central extension of V_pJ by $\mathbb{Q}_p(1)^{\oplus(\rho-1)}$.*

Let's feed this into Chabauty-Kim. Set

$$V_1 := V_pJ \text{ and } V_2 := \mathbb{Q}_p(1)^{\oplus(\rho-1)}.$$

This are the only interesting graded pieces of the U of Lemma 27.16. Hence, we would like to compute the dimensions of the following spaces:

$$\begin{matrix} \mathrm{H}^1_f(G_{\mathbb{Q}}, V_1) & \mathrm{H}^1_f(G_{\mathbb{Q}}, V_2) \\ \mathrm{H}^1_f(G_p, V_1) & \mathrm{H}^1_f(G_{\mathbb{Q}}, V_2) \end{matrix}$$

These dimensions are recorded in Table 2. We computed the dimensions of the cohomology of $\mathbb{Q}_p(1)$ during our discussion of Siegel's theorem. This handles V_2.

Claim 27.17. $\dim \mathrm{H}^1_f(G_p, V_pJ) = g$

(See Example 16.4 for a more detailed proof)

Remember: In general, these local Bloch-Kato Selmer groups are easier to compute than the global ones.

Proof. By the Bloch-Kato exponential sequence (17.1) along with the fact that $\mathrm{H}^1_e = \mathrm{H}^1_f$ (Proposition 18.8), this amounts to the claim that

$$g = \dim D_{\mathrm{dR}}(V_pJ) - \dim F^0 D_{\mathrm{dR}}(V_pJ).$$

Note that $V_pJ = \mathrm{H}^1_{\text{ét}}(J_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^*$, so

$$D_{\mathrm{dR}}(V_pJ) = \mathrm{H}^1_{\mathrm{dR}}(J/\mathbb{Q}_p)^*.$$

This space is understood quite well. In particular, this de Rham cohomology group is $2g$-dimensional and its de Rham filtration is

$$F^i \mathrm{H}^1_{\mathrm{dR}}(J/\mathbb{Q}_p) = \begin{cases} \mathrm{H}^1_{\mathrm{dR}}(J/\mathbb{Q}_p) & \text{if } i \leq 0 \\ \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1_J) & \text{if } i = 1 \\ 0 & \text{if } i \geq 2. \end{cases}$$

The claim follows, as $\dim \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1_J) = g$. ■

Claim 27.18. $\dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_p) = r_p := p^\infty$*-Selmer rank of* J.

Remark 27.19. $r_p = r$ if $Ш(J/\mathbb{Q})[p^\infty]$ is finite. ○

Proof of Claim 27.18. This $\mathrm{H}^1_f(G_{\mathbb{Q}}, V_pJ)$ is the $\mathbb{Q}_p$-linear Selmer group $\mathrm{Sel}_1(J/\mathbb{Q})$, which is known to sit in the exact sequence

$$0 \longrightarrow \mathbb{Q}_p \otimes J(\mathbb{Q}) \longrightarrow \mathrm{Sel}_1(J/\mathbb{Q}) \longrightarrow V_p Ш(J/\mathbb{Q}) \longrightarrow 0$$

(Theorem 2.7). ■

Remark 27.20 (Response to audience question). The hard part of the computation of $\mathrm{H}^1_f(G_{\mathbb{Q}}, V_p)$ is knowing that $r_p = r$. ○

Thus, the Chabauty-Kim criterion (Corollary 24.8) tells us that

$$r_p < g + \rho - 1 \implies X(\mathbb{Q}) \text{ is finite.}$$

This is almost the statement of Theorem 27.7, but not quite. How can we get from this to Theorem 27.7 without proving finiteness of Ш?

We define away the dependence on $Ш(J/\mathbb{Q})$.

Definition 27.21. Let $X/\mathbb{Q}$ be a smooth, projective curve w/ basepoint $b \in X(\mathbb{Q})$. Suppose that U is a quotient of $\pi_1^{\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}, b)$ which dominates the abelianization. Let $\mathcal{V}$ denote the image of the Kummer map

$$\mathbb{Q}_p \otimes J(\mathbb{Q}) \hookrightarrow \mathrm{H}^1_f(G_{\mathbb{Q}}, V_pJ).$$

The Balakrishnan-Dogra Selmer scheme $\mathrm{Sel}_U(X/\mathbb{Q})^{\mathrm{BD}}$ is defined to be the preimage of $\mathcal{V}$ under the natural map

$$\mathrm{Sel}_U(X/\mathbb{Q}) \subset \mathrm{H}^1(G_{\mathbb{Q}}, U) \longrightarrow \mathrm{H}^1_f(G_{\mathbb{Q}}, V_pJ).$$

We also define a corresponding obstruction set:

$$X(\mathbb{Q}_p)^{\mathrm{BD}}_U := \left\{ x \in X(\mathbb{Q}_p) : j_{p,U}(x) \in \text{scheme-theoretic image of } \mathrm{loc}_p : \mathrm{Sel}_U(X/\mathbb{Q})^{\mathrm{BD}} \to \mathrm{H}^1_f(G_p, U) \right\}. \quad \diamond$$

It's unclear to me if this is technically a 'Selmer scheme' in the sense of Definition 21.4 since we've made a global sort of modification

Observe that

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)^{\mathrm{BD}}_U \subset X(\mathbb{Q}_p)_U \subset X(\mathbb{Q}_p).$$

Remark 27.22. If you believe in finiteness of Ш, we have done nothing above (i.e. $\mathcal{V} = \mathrm{H}^1_f(G_{\mathbb{Q}}, V_pJ)$ and $\mathrm{Sel}_U(X/\mathbb{Q})^{\mathrm{BD}} = \mathrm{Sel}_U(X/\mathbb{Q})$). The point of this definition is just to be able to make unconditional assertions. ○

The machinery we have previously developed (I guess, in particular, Proposition 21.10) applies to show that, under the usual assumptions,

$$\dim \mathrm{Sel}(X/\mathbb{Q})_U^{\mathrm{BD}} \leq r + \sum_{n\geq 2} \dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_n).$$

Theorem 27.23. *If*

$$r + \sum_{n\geq 2} \dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_n) < g + \sum_{n\geq 2} \dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_n),$$

then $X(\mathbb{Q})_U^{BD}$ is finite (so also $X(\mathbb{Q})$ is finite).

(Compare: Recall 24.5 and Corollary 24.8)

Corollary 27.24. *Quadratic Chabauty, Theorem 27.7.*

27.3 Beyond quadratic Chabauty

Let's state a slightly more general version of this quadratic Chabauty method, and then mention some other applications of Chabauty-Kim.

Theorem 27.25. *Suppose there is a quotient A of $J = \mathrm{Jac}(X)$ such that*

$$\mathrm{rank}\, A(\mathbb{Q}) < \dim A + \mathrm{rank}\, \mathrm{NS}(A) + \mathrm{rank}\, \mathrm{NS}(A_{\overline{\mathbb{Q}}})^{cmplx\ conj=-1} - 1.$$

Then, $X(\mathbb{Q})$ is finite.

Remark 27.26. If I heard correctly, the new summand $\mathrm{rank}\, \mathrm{NS}(A_{\overline{\mathbb{Q}}})^{c=-1}$ comes from considering not only $\mathbb{G}_m$-torsors which trivialize over X, but also considering torsors under other tori as well. ∘

Example 27.27. Fix a prime $q \geq 5$, and consider the modular curve $X_1(q^s)$ (parameterizing elliptic curves equipped w/ a point of exact order q^s). You can use Hecke operators to understand the decomposition of Jacobians of modular curves like this one.

Fact (Manin)**.** There exists a simple abelian variety A such that A^s is a quotient of $J_1(q^s) := \mathrm{Jac}\, X_1(q^s)$ for all $s \geq 1$.

(In fact, this should hold for any simple factor of $J_1(q)$).

Let's use these quotients in Theorem 27.25. On the LHS, we get $\mathrm{rank}\, A^s(\mathbb{Q}) = s \cdot \mathrm{rank}\, A(\mathbb{Q})$. On the RHS, we get

$$\underbrace{\dim A^s}_{s \dim A} + \underbrace{\mathrm{rank}\, \mathrm{NS}(A^s)}_{\mathrm{rank}\, \mathrm{End}(A^s)^+} + \underbrace{\mathrm{rank}\, \mathrm{NS}(A^s_{\overline{\mathbb{Q}}})^{c=-1}}_{\geq 0} - 1$$

(see Example 27.4 for the second summand). Note that $\mathrm{rank}\, \mathrm{End}(A^s) \gg s^2 \cdot \mathrm{rank}\, \mathrm{End}(A)$. It turns out that

$$\mathrm{rank}\, \mathrm{End}(A^s)^+ \approx \binom{s}{2} \mathrm{rank}\, \mathrm{End}(A).$$

When $s \gg 1$ is very large, the RHS will be bigger than the LHS. Thus, Theorem 27.25 recovers

Theorem 27.28 (Manin-Demjaneko)**.** *$X_1(q^s)(\mathbb{Q})$ is finite for $s \gg 0$.*

I think this is explained e.g. in Serre's "Lectures on the Mordell-Weil Theorem"

This theorem predates both Mordell and Mazur (the results, not the people). △

The Chabauty-Kim criterion has been used to prove finiteness of rational/S-integral points in the following cases

- thrice-punctured line $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ (Kim)
- quadratic Chabauty (Besser-Müller-Balakrishnan)

  Sounds like Besser-Müller-Balakrishnan handled the case of affine curves, and Balakrishnan-Dogra handled the case of projective curves.
- punctured elliptic curves w/ CM (Kim)

  CM helps because the Tate module of an elliptic curve w/ CM is the induction of a character, so relatively easy to understand.
- projective curves w/ CM Jacobians (Kim-Coates)
- projective curves which are a ramified solvable coverings of $\mathbb{P}^1$, e.g. superelliptic curves (including hyperelliptic curves), of genus $g \geq 2$ (Ellenberg-Hast).

  Bogomolov-Tschinkel and Poonen have a construction relating any such curve to the particular curve $y^2 = x^6 - 1$ which has CM Jacobian. This is the secret to this result.

This is more-or-less a complete list of what is known unconditionally so far.[34]

However, it's expected that Chabauty-Kim applies in general (at least, over $\mathbb{Q}$).

27.3.1 Conditional Proof of Siegel-Faltings over $\mathbb{Q}$

Theorem 27.29 (Siegel-Faltings)**.** *Let Y/K be a hyperbolic curve over a number field, and let S be a finite set of places. Then, $Y(\mathscr{O}_{K,S})$ is finite.*

To end the course, we'll give a proof of this theorem over $\mathbb{Q}$, assuming the Fontaine-Mazur conjecture.

Conjecture 27.30 (Fontaine-Mazur)**.** *Let K be a number field, V a $\mathbb{Q}_p$-linear G_K-rep. Assume that V is unramified almost everywhere and that V is de Rham at all places over p.*

- *Then, V is a subquotient of $\mathrm{H}^i_{\acute{e}t}(X_{\overline{K}}, Y_{\overline{K}}, \mathbb{Q}_p)(j)$ for some K-varieties $Y \subset X$ and some integers i, j.*
- *If V is irreducible, then is is actually a subquotient of $\mathrm{H}^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)(j)$ for some smooth, projective K-variety X and some integers i, j.*

  In this case, V is pure of some weight k outside of a finite number of places.

Definition 27.31. Given a number field K, call a $\mathbb{Q}_p$-linear G_K-rep V geometric if it it unramified almost everywhere and is de Rham at all places over p. ◇

Definition 27.32 (Definition 2.6, [Bel09])**.** Let K be a number field, and let V be a $\mathbb{Q}_p$-linear G_K-rep. Then, we define

$$\mathrm{H}^1_g(G_K, V) := \bigcup_{S \text{ finite set of places}} \mathrm{H}^1_{f,S}(G_K, V) \subset \mathrm{H}^1(G_K, V)$$

(see also Example 20.15), so $\mathrm{H}^1_g(G_K, V)$ consists of global cohomology classes x such that $x_v \in \mathrm{H}^1_g(G_v, V)$ ($= \mathrm{H}^1(G_v, V)$ if $v \nmid p$) for all v, and furthermore $x_v \in \mathrm{H}^1_f(G_v, V)$ ($= \mathrm{H}^1_{\mathrm{nr}}(G_v, V)$ if $v \nmid p$) for all but finitely many v. ◇

Lemma 27.33. *Assume Fontaine-Mazur. Let K be a number field. Let V be a geometric $\mathbb{Q}_p$-linear G_K-rep which is pure of weight $k > 0$ at all but finitely many places. Then, $\mathrm{H}^1_g(G_K, V) = 0$.*

[34] You can handle some variants of these as well, e.g. $\mathbb{P}^1$ minus some divisor (see Problem A.5)

Proof. Every element of $\mathrm{H}^1_g(G_K, V)$ can be represented by a G_K-equivariant extension

$$1 \longrightarrow V \longrightarrow E \longrightarrow \mathbb{Q}_p(0) \longrightarrow 1,$$

for E is de Rham at all places above p. Fontaine-Mazur implies that such an E must be `mixed` in the sense that it has a G_K-invariant weight filtration $W_\bullet E$ with graded pieces $\mathrm{gr}^W_k E$ pure of weight k for all but finitely many places. This weight filtration is unique, so functorial w.r.t. morphisms of representations. Since V is pure of weight > 0, we see that $W_0 E \xrightarrow{\sim} W_0 \mathbb{Q}_p(0) = \mathbb{Q}_p(0)$, and so defines a splitting of the extension. Thus, $[E] = 0$. ∎

Proposition 27.34. *Let V be a geometric representation of G_K. Then,*

$$\dim \mathrm{H}^1_f(G_K, V) = \dim V^{G_K} + \dim \mathrm{H}^1_f(G_K, V^*(1)) - \dim V^*(1)^{G_K} + \sum_{v|p} \dim \mathrm{H}^1_f(G_v, V) - \sum_{v|\infty} \dim V^{G_v}.$$

(Sounds like this is due to Fontaine and Perrin-Rion)

Corollary 27.35. *Assuming Fontaine-Mazur, when V is pure of weight $k \leq -3$, then*

$$\dim \mathrm{H}^1_f(G_K, V) = \sum_{v|p} \dim \mathrm{H}^1_f(G_v, V) - \sum_{v|\infty} \dim V^{G_v}.$$

Proof. In this case, $V^*(1)$ is pure of weight $-k - 2 \geq 1$. This, plus the fact that $\mathrm{H}^1_f \subset \mathrm{H}^1_g$, gives the result. ∎

Now, let's show that Fontaine-Mazur implies that Chabauty-Kim implies Siegel-Faltings over $\mathbb{Q}$.

Theorem 27.36. *Assume the Fontaine-Mazur conjecture. Then, $\mathcal{Y}/\mathbb{Z}_S$ be an S-integral model of a hyperbolic curve $Y/\mathbb{Q}$, and choose a basepoint $b \in Y(\mathbb{Q})$. Then, the inequality*

$$\#S + \sum_{n=1}^{N} \dim \mathrm{H}^1_f(G_\mathbb{Q}, V_n) < \sum_{n=1}^{N} \dim \mathrm{H}^1_f(G_p, V_n)$$

holds for $N \gg 0$, where V_n is the nth weight-graded piece of $\pi_1^{\mathbb{Q}_p}(Y_{\overline{\mathbb{Q}}}; b)$. In particular, by Corollary 24.8, $\mathcal{Y}(\mathbb{Z}_S)$ is finite.

Proof. By Corollary 27.35, the inequality we hope to prove is

$$C + \sum_{n=3}^{N} \dim \mathrm{H}^1_f(G_p, V) - \sum_{n=3}^{N} \dim V_n^{\text{cmplx conj}} < c + \sum_{n=3}^{N} \dim \mathrm{H}^1_f(G_p, V_n),$$

where c, C are the following constants:

$$C = \#S + \sum_{n=1}^{2} \dim \mathrm{H}^1_f(G_\mathbb{Q}, V_n) \text{ and } c = \sum_{n=1}^{2} \dim \mathrm{H}^1_f(G_p, V_n).$$

Letting σ denote complex conjugation, it thus suffices to show that $\dim V_n^\sigma > 0$ for infinitely many n. Suppose not. Then, there would be some $n_0 \geq 0$ such that σ acts via -1 on all V_n with $n \geq n_0$. However, if $n_1, n_2 \geq n_0$, then σ would act by $1 = (-1)^2$ on $[V_{n_1}, V_{n_2}] \subset V_{n_1+n_2}$, so we'd have $[V_{n_1}, V_{n_2}] = 0$ for all $n_1, n_2 \geq n_0$, a contradiction. ∎

Appendices

A Some Exercise Solutions

Note 18. These are really more exercise *attempts* than they are *solutions*. No guarantees that anything below is correct.

Alex has been writing psets for this class. Maybe I should try doing some of the exercises. These are (roughly) in the order I did/attempted them, not in the order in which they appeared/were assigned.

Problem A.1 (pset5)**.** *Let $U/\mathbb{Q}_p$ be unipotent, and let G be a finite group acting continuously on U. Then, $\mathrm{H}^1(G, U(\Lambda)) = \{*\}$ for any $\mathbb{Q}_p$-algebra Λ.*

Proof. Every unipotent group U is formed from iterated central extensions of vector groups, so we may assume $U = \mathbb{G}(V)$ is a vector group. In this case, we conclude by functoriality. $\mathrm{H}^1(G, \mathbb{G}(V)(\Lambda)) = \mathrm{H}^1(G, V \otimes_{\mathbb{Q}_p} \Lambda)$ is a Λ-vector space which is killed by $\#G$, so must be trivial. ∎

Problem A.2 (pset5)**.** *Let K be a finite extension of $\mathbb{Q}_p$.*

(a) $\dim_{\mathbb{Q}_p} \mathrm{H}^1(G_K, \mathbb{Q}_p(1)) = [K : \mathbb{Q}_p] + 1$

Proof. $\mathbb{Q}_p(1) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n \mu_{p^n}$, so let's compute μ_{p^n}-cohomology to start.[35] The Kummer sequence $1 \to \mu_{p^n} \to \mathbb{G}_m \xrightarrow{p^n} \mathbb{G}_m \to 1$ gives[36]

$$\mathrm{H}^0(G_K, \mathbb{G}_m) \xrightarrow{p^n} \mathrm{H}^0(G_K, \mathbb{G}_m) \to \mathrm{H}^1(G_K, \mu_{p^n}) \longrightarrow \mathrm{H}^1(G_K, \mathbb{G}_m)[p^n] = 1,$$

so $\mathrm{H}^1(G_K, \mu_{p^n}) \cong K^\times/(K^\times)^{p^n}$. Before taking an inverse limit, we recall that the p-adic exponential $\exp_p$ (after scaling the input) realizes $\mathscr{O}_K$ as a finite-index subgroup of $\mathscr{O}_K^\times$. Since $K^\times \cong \mathscr{O}_K^\times \times \mathbb{Z}$, we conclude that

$$\mathscr{O}_K \times \mathbb{Z}_p \simeq \varprojlim_n \left(\frac{\mathscr{O}_K \times \mathbb{Z}}{p^n} \right) \hookrightarrow \varprojlim_n \left(\frac{\mathscr{O}_K^\times \times \mathbb{Z}}{p^n} \right) \simeq \varprojlim_n \mathrm{H}^1(G_K, \mu_{p^n}) = \mathrm{H}^1(G_K, \mathbb{Z}_p(1))$$

is a finite-index subgroup. Thus, $\mathrm{H}^1(G_K, \mathbb{Q}_p(1)) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{H}^1(G_K, \mathbb{Z}_p(1)) \simeq K \times \mathbb{Q}_p$ has rank $[K : \mathbb{Q}_p] + 1$ as claimed. ∎

(b) $\dim_{\mathbb{Q}_p} \mathrm{H}^1_e(G_K, \mathbb{Q}_p(1)) = [K : \mathbb{Q}_p]$

Proof. Consider the Bloch-Kato exponential sequence

$$0 \longrightarrow \mathbb{Q}_p(1)^{G_K} \longrightarrow D_{\mathrm{cris}}^{\varphi=1}(\mathbb{Q}_p(1)) \longrightarrow \frac{D_{\mathrm{dR}}(\mathbb{Q}_p(1))}{D_{\mathrm{dR}}^+(\mathbb{Q}_p(1))} \longrightarrow \mathrm{H}^1_e(G_K, \mathbb{Q}_p(1)) \longrightarrow 0.$$

[35] To justify that $\mathrm{H}^i(G_K, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n \mathrm{H}^i(G_K, \mu_{p^n})$, you may want to check out [Bel09, Proposition 2.1 + Exercise 2.1c]

[36] This same sequence also shows that $\mathrm{H}^2(G_K, \mu_{p^n}) \simeq \mathrm{Br}(K)[p^n] \simeq (\mathbb{Q}/\mathbb{Z})[p^n] \simeq \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/p^n\mathbb{Z}$ from which one concludes $\mathrm{H}^2(G_K, \mathbb{Z}_p(1)) \simeq \mathbb{Z}_p$ and $\mathrm{H}^2(G_K, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$.

Since $\mathbb{Q}_p(1)$ is pure of weight $-2 < 0$, we must have $D_{\text{cris}}^{\varphi=1}(\mathbb{Q}_p(1)) = 0$, so

$$\mathrm{H}^1_e(G_K, \mathbb{Q}_p(1)) \simeq \frac{D_{\text{dR}}(\mathbb{Q}_p(1))}{D^+_{\text{dR}}(\mathbb{Q}_p(1))}.$$

Note that $\dim_K D_{\text{dR}}(\mathbb{Q}_p(1)) = \dim_{\mathbb{Q}_p} \mathbb{Q}_p(1) = 1$. Furthermore, $D^+_{\text{dR}}(\mathbb{Q}_p(1))$ is the 0th step in the (decreasing) Hodge filtration, so $D^+_{\text{dR}}(\mathbb{Q}_p(1)) = 0$ as $\mathbb{Q}_p(1)$'s only Hodge-Tate weight is -1.[37] Hence, $\mathrm{H}^1_e(G_K, \mathbb{Q}_p(1)) \simeq D_{\text{dR}}(\mathbb{Q}_p(1))$ has dimension $[K : \mathbb{Q}_p]$. ■

(c) $\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_K, \mathbb{Q}_p(1)) = [K : \mathbb{Q}_p]$ and $\dim_{\mathbb{Q}_p} \mathrm{H}^1_g(G_K, \mathbb{Q}_p(1)) = [K : \mathbb{Q}_p] + 1$.

Proof. Under the natural perfect pairing

$$\mathrm{H}^1(G_K, \mathbb{Q}_p(1)) \times \mathrm{H}^1(G_K, \underbrace{\mathbb{Q}_p(1)^*(1)}_{\mathbb{Q}_p}) \longrightarrow \mathrm{H}^2(G_K, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

$\mathrm{H}^1_g(G_K, \mathbb{Q}_p(1))$ is the exact annihilator of $\mathrm{H}^1_e(G_K, \mathbb{Q}_p)$ (See [BK90, Proposition 3.8]). Hence, these two groups must have complimentary dimensions

$$\dim_{\mathbb{Q}_p} \mathrm{H}^1_g(G_K, \mathbb{Q}_p(1)) + \dim_{\mathbb{Q}_p} \mathrm{H}^1_e(G_K, \mathbb{Q}_p) = \dim_{\mathbb{Q}_p} \mathrm{H}^1(G_K, \mathbb{Q}_p(1)) = [K : \mathbb{Q}_p] + 1.$$

At the same time, $D^+_{\text{dR}}(\mathbb{Q}_p) = D_{\text{dR}}(\mathbb{Q}_p)$ (e.g. because $\mathbb{Q}_p$'s only Hodge-Tate weight is 0), so $\mathrm{H}^1_e(G_K, \mathbb{Q}_p) = 0$ by the Bloch-Kato exponential sequence. Thus, $\mathrm{H}^1_g(G_K, \mathbb{Q}_p(1)) = \mathrm{H}^1(G_K, \mathbb{Q}_p(1))$. To compute $\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_K, \mathbb{Q}_p(1))$, we follow Bloch-Kato[38] (see [BK90, Proposition 1.17+Corollary 3.8.4]) by considering the exact sequence

$$0 \longrightarrow \mathbb{Q}_p \xrightarrow{x \mapsto (x,x)} B_{\text{cris}} \oplus B^+_{\text{dR}} \xrightarrow{(x,y) \mapsto (x - \varphi(x), x - y)} B_{\text{dR}} \longrightarrow 0$$

(To get from (16.1) to this, one only needs to know that $1 - \varphi : B_{\text{cris}} \to B_{\text{cris}}$ is surjective). I'll skip the details, but one can analyze cohomology to arrive at an exact sequence

$$0 \longrightarrow V^{G_K} \longrightarrow D_{\text{cris}}(V) \oplus D^+_{\text{dR}}(V) \longrightarrow D_{\text{cris}}(V) \oplus D_{\text{dR}}(V) \longrightarrow \mathrm{H}^1_f(G_K, V) \longrightarrow 0 \tag{A.1}$$

for any de Rham representation V. Applying this to $V = \mathbb{Q}_p(1)$ yields

$$0 \longrightarrow D_{\text{cris}}(\mathbb{Q}_p(1)) \longrightarrow D_{\text{cris}}(\mathbb{Q}_p(1)) \oplus D_{\text{dR}}(\mathbb{Q}_p(1)) \longrightarrow \mathrm{H}^1_f(G_K, \mathbb{Q}_p(1)) \longrightarrow 0,$$

from which we see that $\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(G_K, \mathbb{Q}_p(1)) = \dim_{\mathbb{Q}_p} D_{\text{dR}}(\mathbb{Q}_p(1)) = [K : \mathbb{Q}_p]$ (so $\mathrm{H}^1_f(G_K, \mathbb{Q}_p(1)) = \mathrm{H}^1_e(G_K, \mathbb{Q}_p(1))$). ■

Problem A.3 (pset5)**.** *Let U be a unipotent group over a characteristic 0 field F, and let $U^+ \leq U$ be a subgroup-scheme (so U^+ is also unipotent). Let $V \leq \mathrm{Lie}(U)$ be a complement of $\mathrm{Lie}(U^+)$, i.e. $\mathrm{Lie}(U) = \mathrm{Lie}(U^+) \oplus V$.*

[37] An integer $n \in \mathbb{Z}$ is a `Hodge-Tate weight` of V of multiplicity m if $\dim_K (V \otimes_{\mathbb{Q}_p} \mathbb{C}_K(n))^{G_K} = m > 0$.

[38] Alternatively, $\mathbb{Q}_p(1)$ is pure of weight -2, so can apply Proposition 18.8.

(a) The map

$$\begin{array}{ccc} U^+ \times \mathbb{A}(V) & \longrightarrow & U \\ (u^+, v) & \longmapsto & u^+ \exp(v) \end{array}$$

is an isomorphism of varieties over F. Consequently, the functor

$$\begin{array}{rccc} U^+\backslash U: & \mathrm{Alg}_F & \longrightarrow & \mathrm{Set} \\ & \Lambda & \longmapsto & U^+(\Lambda)\backslash U(\Lambda) \end{array}$$

is representable by the affine space $\mathbb{A}(V)$.

Problem A.4 (pset4)**.** *Let X be a hyperelliptic curve over a field K of characteristic 0. Let $x_0 \in X(K)$ be a K-rational Weierstrass point. Let $U = \pi_1^{\mathbb{Q}_p}(X_{\overline{K}}; x_0)$ be the $\mathbb{Q}_p$-pro-unipotent étale fundamental group, let $U_n = U/\Gamma^{n+1}U$ denote the nth quotient by the descending central series, and let $V_n = \Gamma^n U/\Gamma^{n+1}U$ denote the nth graded piece of the descending central series, so the sequence*

$$1 \longrightarrow V_n \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1$$

is a G_K-equivariant central extension. For $n = 2$, the corresponding sequence

$$0 \longrightarrow V_2 \longrightarrow \mathrm{Lie}(U_2) \longrightarrow \mathrm{Lie}(U_1) \longrightarrow 0$$

of Lie algebras splits as a sequence of G_K-representations.

Problem A.5 (pset6)**.** *Let $Y = \mathbb{P}^1_{\mathbb{Q}} \setminus \{\pm i, \infty\} = \operatorname{Spec} \mathbb{Q}[t, 1/(t^2+1)]$. Let $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}} \setminus \{\pm i, \infty\} = \operatorname{Spec} \mathbb{Z}[t, 1/(t^2+1)]$. Let S be a finite set of prime numbers. Let U denote the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $Y_{\overline{\mathbb{Q}}}$, and let V_n denote its graded pieces w.r.t. to the weight filtration.*

(a) U is free on two generators and $V_n = 0$ for n odd.

Proof. U is the $\mathbb{Q}_p$-Malčev completion of $\pi_1(Y(\mathbb{C})) \simeq \mathbb{CP}^1 \setminus \{\pm i, \infty\}$, and so free on two generators. The fact that $V_n = 0$ for n odd follows by induction, once one observes that

$$W_{-2}U := \ker\Big(U \longrightarrow \pi_1^{\mathbb{Q}_p}(\mathbb{P}^1_{\overline{\mathbb{Q}}})^{\mathrm{ab}}\Big) = U. \qquad \blacksquare$$

(b) $V_2 = \mathbb{Q}_p(1) \oplus \mathbb{Q}_p(\chi)(1)$, where $\chi : G_{\mathbb{Q}} \to \{\pm 1\}$ is the quadratic character associated to the extension $\mathbb{Q}(i)/\mathbb{Q}$.

Proof. $V_2 = W_{-2}U/W_{-3}U = \frac{U}{[U, W_{-2}U]\cdot[W_{-2}U, W_{-1}U]} = \frac{U}{[U,U]} = U^{\mathrm{ab}}$. Thus, Hurewicz (Theorem 12.3) + Poincaré duality tell us that $V_2 \simeq \mathrm{H}^1_{\text{ét}}(Y_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^* \simeq \mathrm{H}^1_{c,\text{ét}}(Y_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)(1)$. To compute compactly supported cohomology, we use the exact sequences[39]

$$\begin{array}{ccccccc} \mathrm{H}^0_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, \mathbb{Z}/p^n\mathbb{Z}) & \longrightarrow & \mathrm{H}^0_{\text{ét}}(Z_{\overline{\mathbb{Q}}}, \mathbb{Z}/p^n\mathbb{Z}) & \longrightarrow & \mathrm{H}^1_{c,\text{ét}}(Y_{\overline{\mathbb{Q}}}, \mathbb{Z}/p^n\mathbb{Z}) & \longrightarrow & \mathrm{H}^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, \mathbb{Z}/p^n\mathbb{Z}) \\ \| & & \| & & & & \| \\ \mathbb{Z}/p^n\mathbb{Z} & & (\mathbb{Z}/p^n\mathbb{Z})^{\oplus 3} & & & & 0 \end{array}$$

[39] coming from $0 \to j_!\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to i_*\mathbb{Z}/p^n\mathbb{Z} \to 0$ on $\mathbb{P}^1$

for $n \geq 1$, where $Z := \{\pm i, \infty\} = \mathbb{P}^1_{\mathbb{Q}} \setminus Y$ (say, w/ the reduced scheme structure). Above, $G_{\mathbb{Q}}$ acts on $\mathrm{H}^0_{c,\text{ét}}(Z_{\overline{\mathbb{Q}}}, \mathbb{Z}/p^n\mathbb{Z})$ through $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ where complex conjugation exchanges the first/second factors of $(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 3}$. Thus, $\mathrm{H}^1_{c,\text{ét}}(Y_{\overline{\mathbb{Q}}}, \mathbb{Z}/p^n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2}$ w/ the Galois action (read: complex conjugation) exchanging the two coordinates.[40] Thus, $\mathrm{H}^1_{c,\text{ét}}(Y_{\overline{\mathbb{Q}}}, \mathbb{Z}/p^n\mathbb{Z}) \simeq \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^n\mathbb{Z}(\chi)$ (trivial Galois action on the first factor) via $(a, b) \mapsto (a + b, a - b)$. Finally,

$$V_2 \simeq \mathrm{H}^1_{c,\text{ét}}(Y_{\overline{\mathbb{Q}}}; \mathbb{Q}_p)(1) \simeq \mathbb{Q}_p(1) \otimes_{\mathbb{Z}_p} \varprojlim_n \mathrm{H}^1_{c,\text{ét}}(Y_{\overline{\mathbb{Q}}}; \mathbb{Z}/p^n\mathbb{Z}) \simeq \mathbb{Q}_p(1) \oplus \mathbb{Q}_p(\chi)(1),$$

as desired. ∎

(c) For $n \geq 1$, there are integers r_n^+ and r_n^- such that

$$V_{2n} = \mathbb{Q}_p(n)^{\oplus r_n^+} \oplus \mathbb{Q}_p(\chi)(n)^{\oplus r_n^-}.$$

Proof. This simply follows from the fact that V_{2n} is a quotient of

$$V_2^{\otimes n} \simeq \bigoplus_{k=0}^{n} \mathbb{Q}_p(\chi^k)(n)^{\oplus \binom{n}{k}} \simeq \mathbb{Q}_p(n)^{\oplus 2^{n-1}} \oplus \mathbb{Q}_p(\chi)(n)^{\oplus 2^{n-1}},$$

with last iso. because $\chi^2 = 1$ is trivial ∎

(d) $r_n^- \geq 1$ for all $n \geq 1$

Proof. One sees from **(b)** and Theorem 25.15 that r_n^- is equal to the number of length n Lyndon words (in the alphabet $\{x, y\}$) such that y appears an odd number of times. Thus, r_n^- is always nonzero as there's always the word $\underbrace{x \dots x}_{(n-1) \text{ times}} y$. Put another way, by Theorem 25.15, if $V_2^{\otimes n} \twoheadrightarrow V_{2n}$ is the natural quotient map (see Claim 25.10), $x \in \mathbb{Q}_p(1)$ is nonzero and $y \in \mathbb{Q}_p(\chi)(1)$ is nonzero, then $x \otimes \cdots \otimes x \otimes y$ has nonzero image in V_{2n}. ∎

(e) $\dim \mathrm{H}^1_f(G_p, \mathbb{Q}_p(\chi)(n)) = 1$ for all $n \geq 1$.

Remark A.1. If p splits in $\mathbb{Q}(i)$, then $\sqrt{-1} \in \mathbb{Q}_p$, so $\mathbb{Q}_p(\chi) \simeq \mathbb{Q}_p$ as G_p-reps, and hence the claim follows from Claim 25.16. ∘

Proof. $\mathbb{Q}_p(\chi)(n)^{G_p} = 0$, so (A.1) shows that

$$\dim \mathrm{H}^1_f(G_p, \mathbb{Q}_p(\chi)(n)) = \dim D_{\mathrm{dR}}(\mathbb{Q}_p(\chi)(n)) - \dim D^+_{\mathrm{dR}}(\mathbb{Q}_p(\chi)(n)).$$

Note that $B := B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\chi)(n)$ has decreasing $\mathbb{Z}$-filtration $F^i B$ with graded pieces

$$\mathrm{gr}^i_F B = F^i B / F^{i+1} B \simeq \mathbb{Q}_p(\chi)(i + n).$$

Taking Galois invariants, we see that

$$D^+_{\mathrm{dR}}(\mathbb{Q}_p(\chi)(n)) = (F^0 B)^{G_p} = 0 \text{ and } D_{\mathrm{dR}}(\mathbb{Q}_p(\chi)(n)) = B^{G_p} = (F^{-n} B)^{G_p} = \mathbb{Q}_p(\chi)^{G_p} = \cdots.$$

I'm confused. It really feels like $D_{\mathrm{dR}}(\mathbb{Q}_p(\chi)(n)) = 0$ unless p slits in $\mathbb{Q}(i)$ (i.e. unless $\sqrt{-1} \in \mathbb{Q}_p$), and is $\mathbb{Q}_p$ otherwise, but the problem statement suggests otherwise... ∎

[40] The map $\mathrm{H}^0_{c,\text{ét}}(Z_{\overline{\mathbb{Q}}}) \to \mathrm{H}^1_{c,\text{ét}}(Y_{\overline{\mathbb{Q}}})$ is $(a, b, c) \mapsto (a - c, b - c)$.

(f) Here's a more general statement of a theorem from lecture.

Theorem A.2 (Soulé)**.** *For any number field K and odd p, we have*

$$\dim \mathrm{H}^1(G_K, \mathbb{Q}_p(n)) = \begin{cases} r_K + s_K & \text{if } n \geq 3 \text{ odd} \\ s_K & \text{if } n \geq 2 \text{ even,} \end{cases}$$

where r_K is the number of real embeddings and s_K is the number of conjugate pairs of complex embeddings.

One can use this to show that

$$\dim \mathrm{H}^1(G_{\mathbb{Q}}, \mathbb{Q}_p(\chi)(n)) = \begin{cases} 0 & \text{if } n \geq 3 \text{ odd} \\ 1 & \text{if } n \geq 2 \text{ even.} \end{cases}$$

Proof. Let $K = \mathbb{Q}(i)$, and fix $n \geq 2$. Soulé tells us that $\dim \mathrm{H}^1(G_K, \mathbb{Q}_p(n)) = 1$, and inflation-restriction tells us that

$$\mathrm{H}^1(G_{\mathbb{Q}}, \mathbb{Q}_p(\chi)(n)) \xrightarrow{\sim} \mathrm{H}^1(G_K, \mathbb{Q}_p(\chi)(n))^{\mathrm{Gal}(K/\mathbb{Q})} = \mathrm{H}^1(G_K, \mathbb{Q}_p(n))^{\mathrm{Gal}(K/\mathbb{Q})}$$

since $\mathrm{Gal}(K/\mathbb{Q})$ is finite (so $\mathrm{H}^i(\mathrm{Gal}(K/\mathbb{Q}), \mathbb{Q}_p(\chi)(n)) = 0$ for $i \geq 1$). Given a cocycle $\varphi : G_K \to \mathbb{Q}_p(\chi)(n)$, the generator of $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ acts on it by sending it to $\overline{\varphi} : G_K \to \mathbb{Q}_p(\chi)(n)$ defined by

$$\overline{\varphi}(\sigma) := c^{-1} \cdot \varphi(c\sigma c^{-1}) = (-1)^{n+1}\varphi(c\sigma c),$$

where c is complex conjugation. We want to understand when $[\overline{\varphi}] = [\varphi] \in \mathrm{H}^1(G_K, \mathbb{Q}_p(n))$. Note that $H^1(G_K, \mathbb{Q}_p(n))$ is 1-dimensional by Soulé and $\overline{\overline{\varphi}} = \varphi$ by construction, so we necessarily have $[\overline{\varphi}] = \pm[\varphi]$ and the problem is to compute the sign.

I feel like I'm missing something obvious, but I don't see how to compute this... ∎

Remember: The action of G/H on $\mathrm{H}^i(H, M)$ comes from $(H, M) \to (H, M)$, $(h, m) \mapsto (ghg^{-1}, g^{-1}m)$. Note cohomology reverses directions, so you want the normal action on the target.

(g) $\mathcal{Y}(\mathbb{Z}_S)$ is finite. Consequently, there are only finitely many integers a such that all prime factors of $a^2 + 1$ lie in S.

Proof. By the Chabauty-Kim criterion (Corollary 24.8), to show $\mathcal{Y}(\mathbb{Z}_S)$ is finite, it suffices to show that

$$\#S + \sum_{n \leq N} \dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_{2n}) < \sum_{n \leq N} \dim \mathrm{H}^1_f(G_p, V_{2n}) \tag{A.2}$$

for $N \gg 1$. By previous parts of this problem, we bound the above sides:

$$\#S + \sum_{n \leq N} \dim \mathrm{H}^1_f(G_{\mathbb{Q}}, V_{2n}) \leq \#S + \sum_{\text{odd } n \leq N} r_n^+ + \sum_{\text{even } n \leq N} r_n^- \text{ and } \sum_{n \leq N} (r_n^+ + r_n^-) = \sum_{n \leq N} \dim \mathrm{H}^1_f(G_p, V_{2n}).$$

If you stare at the above long enough, you will see that (A.2) does hold once N is large enough (depending on $\#S$). This proves finiteness of $\#\mathcal{Y}(\mathbb{Z}_S)$.

Now, recall $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}} \setminus \{\pm i, \infty\} = \mathrm{Spec}\, \mathbb{Z}[t, 1/(t^2+1)]$. Thus, there are only finitely many (S-)integers a such that $a^2 + 1 \in \mathbb{Z}_S^\times$, i.e. such that the only primes appearing in $a^2 + 1$ are ones that appear in S. This is the second part of the claim. ∎

References

[BC] Olivier Brinon and Brian Conrad. Cmi summer school notes on p-adic hodge theory (preliminary version). https://math.stanford.edu/~conrad/papers/notes.pdf. 43

[Bel09] Joel Bellaîche. An introduction to the conjecture of bloch and kato. https://people.brandeis.edu/~jbellaic/BKHawaii5.pdf, 2009. 63, 94, 103, 105

[BK90] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990. 74, 106

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005. 57, 91

B List of Marginal Comments

Index