Selmer Schemes II

Minhyong Kim

Tucson, March, 2019

Disclaimer

These lecture slides come with a bibliography at the end. However, there has been no attempt at accurate attribution of mathematical results. Rather, the list mostly contains works the lecturer has consulted during preparation, which he hopes will be helpful for users.

I. Preliminaries on covering spaces and fundamental groups

Universal Covering Spaces

M: a locally contractible connected topological space.

A covering space

$$M' \longrightarrow M$$

is a locally trivial fibre bundle with discrete fibres:

There is a discrete set F and an open covering $M = \cup U_i$ such that

$$M'_{U_i} \simeq F \times U_i$$

for each i.

Universal Covering Spaces

A universal covering space

$$\pi : \tilde{M} \longrightarrow M$$

is a covering space with $\tilde{M}$ connected and simply connected.

It is not universal in a categorical sense: For any other covering space $M' \longrightarrow M$, there is a commutative diagram

$$\begin{tikzcd}
\tilde{M} \arrow[r] \arrow[dr] & M' \arrow[d] \\
& M
\end{tikzcd}$$

However, the diagram is *not unique*: There is no initial object in the category of covering spaces.

Universal Covering Spaces

Consider instead *pointed* covering spaces.

Having chosen a point $b \in M$, a pointed covering space is a map

$$(M', b') \longrightarrow (M, b).$$

Now we choose a point $\tilde{b} \in \tilde{M}_b$. Then the pair $(\tilde{M}, \tilde{b})$ is indeed an initial object in the category of pointed universal covering spaces:

$$\begin{tikzcd}
(\tilde{M}, \tilde{b}) \arrow[r, "\exists!"] \arrow[dr] & (M', b') \arrow[d] \\
& (M, b)
\end{tikzcd}$$

Note that the choice of a different $\tilde{c} \in \tilde{M}_b$ will give another initial object $(\tilde{M}, \tilde{c})$ which is uniquely isomorphic to $(\tilde{M}, \tilde{b})$.

Fibre Functors

Now consider the functor

$$F_b : \mathrm{Cov}(M) \longrightarrow \mathrm{Sets}$$

$$M' \mapsto M'_b,$$

and its automorphism group

$$\mathrm{Aut}(F_b).$$

By the definition of a natural transformation, an element γ of this group is a compatible sequence of bijections

$$\gamma_{M'} : M'_b \cong M'_b.$$

Fibre Functors

Compatibility here is with respect to maps of covering spaces:

If $f : M_1' \longrightarrow M_2'$ is a map of covering spaces, then

$$\begin{tikzcd} M'_{1,b} \arrow[r, "\gamma_{M_1}"] \arrow[d, "f"'] & M'_{1,b} \arrow[d, "f"'] \\ M'_{2,b} \arrow[r, "\gamma_{M_2}"] & M'_{2,b} \end{tikzcd}$$

$$f \circ \gamma_{M_1'} = \gamma_{M_2'} \circ f.$$

Fibre Functors

Define a map

$$\mathrm{Aut}(F_b) \longrightarrow \tilde{M}_b$$

by

$$\gamma \mapsto \gamma_{\tilde{M}}(\tilde{b}) \in \tilde{M}_b.$$

Proposition

This map induces a bijection

$$Aut(F_b) \cong \tilde{M}_b.$$

Fibre Functors

Injectivity:

Given any $b' \in M'_b$, there is a unique map $f : (\tilde{M}, \tilde{b}) \longrightarrow (M', b')$. Thus

$$\gamma_{M'}(b') = \gamma_{M'}(f(\tilde{b})) = f(\gamma_{\tilde{M}}(\tilde{b})),$$

and the action of γ on M'_b is determined by $\gamma_{\tilde{M}}(\tilde{b})$.

On the other hand, given $y \in \tilde{M}_b$, we would like to define γ such that $\gamma_{\tilde{M}}(\tilde{b}) = y$.

The point is that there is only one way to do it in a way that's compatible with maps of covering spaces and this gives us $\gamma_{M'}$ for every $M' \longrightarrow M$.

Fibre Functors

Given $b' \in M'_b$, there is a unique $f_{b'} : (\tilde{M}, \tilde{b}) \longrightarrow (M', b')$. Define

$$\gamma_{M'}(b') = \gamma_{M'}(f_{b'}(\tilde{b}))(= f_{b'}(\gamma_{\tilde{M}}(\tilde{b}))) := f_{b'}(y).$$

Compatibility comes from commutative triangles

$$\begin{tikzcd}
(\tilde{M}, \tilde{b}) \arrow[r, "f_{b'}"] \arrow[dr, "f_{h(b')}"'] & (M', b') \arrow[d, "h"] \\
& (M", h(b'))
\end{tikzcd}$$

that imply

$$h(\gamma_{M'}(b')) = h(f_{b'}(y)) = f_{h(b')}(y) = \gamma_{M"}(h(b')).$$

Fibre Functors

An identical proof gives us:

Proposition

For two points $b, x \in M$,

$$Isom(F_b, F_x) \simeq \tilde{M}_x.$$

That is, an element $p \in \mathrm{Isom}(F_b, F_x)$ is determined by $p_{\tilde{M}}(\tilde{b})$, and any $y \in \tilde{M}_x$ determines such a p.

Note that $\mathrm{Isom}(F_b, F_x)$ is a principal bundle for $\mathrm{Aut}(F_b)$. As an exercise, try to describe for yourself the action of $\tilde{M}_b$ on $\tilde{M}_x$.

Homotopy classes of paths

Consider the usual definition of $\pi_1(M; b, x)$ using homotopy classes of paths. There is a classical isomorphism

$$\pi_1(M; b, x) :\cong \mathrm{Isom}(F_b, F_x)$$

defined via path lifting.

That is, a path $p : I = [0, 1] \longrightarrow M$ such that $p(0) = b$ and $p(1) = x$ acts on the fibres of a covering $M' \longrightarrow M$ via the unique lifting diagram:

$$\begin{tikzcd}
 & (M', b') \arrow[d] \\
(I, 0) \arrow[r, "p"] \arrow[ur, "p'"] & (M, b)
\end{tikzcd}$$

That is $p \cdot b' = p'(1)$.

Homotopy classes of paths

The endpoint $p'(1)$ depends only on the homotopy class of p because of the discreteness of the fibres.

If $f : (M_1', b_1') \longrightarrow (M_2', b_2')$ is a map of pointed covering spaces, then $f \circ p_1' = p_2'$ by uniqueness.

Thus, path lifting defines a compatible collection of isomorphisms

$$p_{M'} : M_b' \cong M_x'.$$

In particular, loops based at b will act compatibly on all fibres M_b'.

Homotopy classes of paths

The easiest way to see that this gives an isomorphism

$$\pi_1(M; b, x) \cong \mathrm{Isom}(F_b, F_x)$$

uses $\tilde{M}_b$ again.

That is, denote by $\tilde{p}$ the lifting of p to $\tilde{M}$ such that $\tilde{p}(0) = \tilde{b}$. In that case, we get that

Proposition

The map $p \mapsto \tilde{p}(1)$ defines a bijection

$$\pi_1(M; b, x) \cong \tilde{M}_x.$$

Homotopy classes of paths

The inverse is given by mapping $y \in \tilde{M}_x$ to the homotopy class $[\pi \circ q]$, where q is any path in $\tilde{M}$ from $\tilde{b}$ to y. The homotopy class is independent of q since $\tilde{M}$ is simply connected.

However, this map clearly factors through

$$\pi_1(M; b, x) \longrightarrow \mathrm{Isom}(F_b, F_x) \cong \tilde{M}_b,$$

proving that the first map is also an isomorphism.

In other words, the choice of base-points gives us an expression

$$\tilde{M} = \cup_{x \in M} \pi_1(M; b, x).$$

The fibers of $\tilde{M}$ give us a concrete model of path spaces, which generalises to situations where physical paths are missing.

Homotopy classes of paths

To summarise, we have the bijections

$$\pi_1(M; b, x) \cong \mathrm{Isom}(F_b, F_x) \cong \tilde{M}_x.$$

The second two objects generalise to other settings.

II. Preliminaries on Tannakian formalism

Tannakian formalism

G: finite group;

Rep_k^G: category of finite-dimensional representations of G on k-vector space.

A pointed representation is a representation V together with a vector $v \in V$.

Proposition

The left-regular pointed representation

$$(k[G], 1)$$

is the universal pointed representation of G.

Given any pointed representation (V, v), we get a unique map $(k[G], 1) \longrightarrow (V, v)$ that sends g to gv.

Tannakian formalism

Let

$$F : \mathrm{Rep}_k^G \longrightarrow \mathrm{Vect}_k$$

be the forgetful functor to k-vector spaces.

Consider the endomorphisms

$$\mathrm{End}(F)$$

of F.

Thus, an element $a \in \mathrm{End}(F)$ is a compatible sequence of linear transformations $a_V : V \longrightarrow V$ as V runs over representations of G:

$$\begin{tikzcd}
V \arrow[r, "a_v"] \arrow[d, "\phi"'] & V \arrow[d, "\phi"'] \\
W \arrow[r, "a_W"] & W
\end{tikzcd}$$

Tannakian formalism

Proposition

The map

$$a \mapsto a_{k[G]}(1)$$

defines an isomorphism $End(F) \cong k[G]$.

Tannakian formalism

There is an augmentation map $e^* : k[G] \longrightarrow k$ and the map $G \longrightarrow G \times G$, $g \mapsto (g, g)$ induces the comultiplication map

$$\Delta : k[G] \longrightarrow k[GxG] \simeq k[G] \otimes k[G].$$

Given representations V and W, $V \otimes_k W$ is initially a representation of $k[G] \otimes k[G]$ which is turned into a representation of $k[G]$ and G via Δ.

Proposition

G itself can be recovered as the group-like elements of $k[G]$, i.e., $a \in k[G]$ such that $e^*(a) = 1$ and

$$\Delta(a) = a \otimes a.$$

Tannakian formalism

Proposition

G is isomorphic to $Aut^{\otimes}F$, the tensor-compatible automorphisms of the forgetful functor F from Rep_G^k to $Vect_k$

Here, an element $f \in \mathrm{Aut}(F)$ is tensor-compatible if $f_{V\otimes W} = f_v \otimes f_W$.

If we let

$$A = \mathrm{Hom}_k(k[G], k),$$

$$\Delta^* : A \otimes A \cong \mathrm{Hom}(k[G] \otimes k[G], k) \longrightarrow A$$

gives it the structure of a commutative k-algebra. Of course,

$$G \hookrightarrow \mathrm{Hom}_k(A, k).$$

Corollary

$G = Spec(A)(k) = Hom_{k-alg}(A, k).$

III. Return to arithmetic fundamental groups

Arithmetic setting

K: a number field or a finite extension of $\mathbb{Q}_p$.

X: a smooth curve over K

$\bar{X}$: the basechange of X to $\bar{K}$.

$b, x \in X(K)$ viewed sometimes as geometric points:

$$\mathrm{Spec}(\bar{K}) \longrightarrow \bar{X} \longrightarrow X.$$

In the local case, let $\mathcal{X}$ be a smooth scheme over $\mathcal{O}_K$ with good compactification and generic fiber X. and let Y be the special fiber of $\mathcal{X}$ over $k = \mathcal{O}_K / m_K$.

Profinite étale fundamental group

[Szamuely] $\mathrm{Cov}(\bar{X})$: category of finite étale covering spaces of $\bar{X}$.

There is a fibre functor

$$F_b : \mathrm{Cov}(\bar{X}) \longrightarrow \mathrm{FinSet};$$

$$(Y \longrightarrow \bar{X}) \mapsto Y_b.$$

Define

$$\hat{\pi}_1(\bar{X}; b, x) := \mathrm{Isom}(F_b, F_x).$$

Profinite étale fundamental group

Proposition

There is a 'universal' pro-étale cover

$$\tilde{\bar{X}} = (\bar{X}_i) \longrightarrow \bar{X}$$

with the property that we get a diagram

$$\begin{tikzcd}
\tilde{\bar{X}} \arrow[r] \arrow[dr] & Y \arrow[d] \\
 & \bar{X}
\end{tikzcd}$$

for any finite étale cover $Y \longrightarrow \bar{X}$.

The arrow $\tilde{\bar{X}} \longrightarrow Y$ is an element of $\varinjlim \mathrm{Hom}(\bar{X}_i, Y)$.

Profinite étale fundamental group

Pick a 'point' $\tilde{b} \in \tilde{\bar{X}}$, by which we mean a compatible sequence of points $b_i \in \bar{X}_{i,b}$. Then $(\tilde{\bar{X}}, \tilde{b})$ is a universal pointed pro-étale cover:

Proposition

We get a diagram

$$\begin{tikzcd} (\tilde{\bar{X}}, \tilde{b}) \arrow[r, "\exists!"] \arrow[dr] & (Y, b_Y) \arrow[d] \\ & (\bar{X}, b) \end{tikzcd}$$

for any finite étale cover $(Y, b_Y) \longrightarrow (\bar{X}, b)$.

Profinite étale fundamental group

Furthermore,

Proposition

The cover $(\tilde{\bar{X}}, \tilde{b})$ is defined over K. That is, there is a cover

$$(\tilde{X}, \tilde{b}) \longrightarrow (X, b)$$

with $\tilde{b}$ rational, whose base change to $\bar{K}$ is $(\tilde{\bar{X}}, \tilde{\bar{b}})$.

Be warned that in spite of the notation, $\tilde{X} \longrightarrow X$ is not the universal cover of X. The universal cover of X is

$$\tilde{\bar{X}} \longrightarrow \bar{X} \longrightarrow X.$$

The cover $\tilde{X} \longrightarrow X$ is a K-model of the universal cover of $\bar{X}$.

Profinite étale fundamental group

Examples:

$(\mathbb{G}_m, 1)$

Then

$$\widetilde{\mathbb{G}_m} = (\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m)_n$$

with basepoint 1.

E an elliptic curve over K with basepoint $O \in E(K)$.

Then

$$\tilde{E} = (E \xrightarrow{n} E)_n$$

with basepoint (O).

Profinite étale fundamental group

Theorem

The map

$$\gamma \mapsto (\gamma_{\bar{X}_i}(b_i)) \in \tilde{\bar{\tilde{X}}}_x = \tilde{X}_b(\bar{K})$$

induces a G_K-equivariant isomorphism

$$\hat{\pi}_1(\bar{X}; b, x) \simeq \tilde{\bar{\tilde{X}}}_x = \tilde{X}_x(\bar{K})$$

This isomorphism gives a concrete way of 'computing' the action of $\mathrm{Gal}(\bar{K}/K)$ on $\hat{\pi}_1(\bar{X}; b, x)$.

Profinite étale fundamental group

The formal definition of the action on the left is given as follows.

For $g \in G_K$ and $p \in \hat{\pi}_1(\bar{X}; b, x)$, $g(p)$ associates to $X' \longrightarrow X$ the lower arrow that makes the diagram commute:

$$\begin{tikzcd}
g^*(X')_b \arrow[r, "p_{g^*(X)}"] \arrow[d, "g"'] & g^*(X')_x \arrow[d, "g"'] \\
X_b \arrow[r, "g(p)"] & X_x
\end{tikzcd}$$

$$g(p)_X = g \circ p_{g^*(X')} g^{-1}.$$

Profinite étale fundamental group

$$\hat{\pi}_1(\bar{\mathbb{G}}_m, 1) = (\widetilde{\mathbb{G}_m})_1 = \hat{\mathbb{Z}}(1).$$

$$\hat{\pi}_1(\bar{E}, O) = \tilde{E}_1 = \hat{T}(E).$$

$$\hat{\pi}_1(\bar{\mathbb{G}}_m; 1, x) = (\widetilde{\mathbb{G}_m})_x = (x^{1/n}).$$

$$\hat{\pi}_1(\bar{E}; O, x) = \tilde{E}_x = (\frac{1}{n}x).$$

Profinite étale fundamental group

General construction:

If $P \longrightarrow M$ is a principal G-bundle and G (left-)acts continuously on a set A, then can form associated bundle

$$P \times_G A := [P \times A]/G,$$

where G acts on the product as $(p, a)g = (pg, g^{-1}a)$.

This is a fibre bundle over M with fibre A which varies according to the variation of P.

When $\rho : G \longrightarrow H$ is a group homomorphism, this construction $P \times_G H$ gives a principal H-bundle.

Profinite étale fundamental group

The cover

$$\tilde{\tilde{\bar{X}}} \longrightarrow \bar{X}$$

is a principal $\hat{\pi}_1(\bar{X}, b)$-bundle.

$$\tilde{\tilde{\bar{X}}}^{(p)} = \tilde{X} \times_{\hat{\pi}_1(\bar{X},b)} \hat{\pi}_1^{(p)}(\bar{X}, b),$$

which is a principal $\hat{\pi}_1^{(p)}(\bar{X}, b)$-bundle, is the universal pro-p étale cover.

In general, we might try to study the G_K-action on $\hat{\pi}_1(\bar{X}; b, x)$ via fibres of suitable quotient coverings like this.

For example, if X is a modular curve, then the tower

$$X_{\mathrm{Mod}} \longrightarrow X$$

of modular curves, corresponds to the 'modular quotient group' of $\hat{\pi}_1(\bar{X}, b)$.

Profinite étale fundamental group

Given a continuous $\mathbb{Q}_p$-representation V of $\hat{\pi}_1(\bar{X}, b)$, we get a locally constant sheaf of $\mathbb{Q}_p$-vector spaces

$$\tilde{\bar{X}} \times_{\hat{\pi}_1(\bar{X},b)} V,$$

giving a functor

$$Rep^{\mathbb{Q}_p}_{\hat{\pi}_1(\bar{X},b)} \longrightarrow Loc^{\mathbb{Q}_p}(\bar{X})$$

which is inverse to the fibre functor

$$F_b : \mathcal{L} \mapsto \mathcal{L}_b.$$

This is a version of the 'vector bundle associated to a principal G-bundle and a linear representation of G,' familiar from usual geometry. However, to do this carefully in this case, you need to construct the correspondence with finite coefficients first and then consider projective systems. (This is where you need the continuity.)

III. Unipotent fundamental groups

Unipotent fundamental groups

[Deligne]
We linearise categories.

$\mathrm{Un}(\bar{X}, \mathbb{Q}_p)$: The category of unipotent $\mathbb{Q}_p$-locally constant sheaves on the étale site of $\bar{X}$.

A local system $\mathcal{F}$ is unipotent if it admits a filtration

$$\mathcal{F} = \mathcal{F}^0 \supset \mathcal{F}^1 \supset \cdots \supset \mathcal{F}^n = 0$$

such that

$$\mathcal{F}^i / \mathcal{F}^{i+1} \simeq (\mathbb{Q}_p)^{r_i}_{\bar{X}}$$

for each i. With this notation, we say $\mathcal{F}$ has index of unipotency $\leq n$.

Unipotent fundamental groups

Theorem

There is a universal pointed pro-object in $Un(\bar{X}, \mathbb{Q}_p)$. This is a projective system

$$(\mathcal{E}, v) = ((\mathcal{E}_n, v_n))_n$$

with $v_n \in (\mathcal{E}_n)_b$ such that for any $\mathcal{F} \in Un(\bar{X}, \mathbb{Q}_p)$ and $w \in \mathcal{F}_b$, there is a unique map

$$f : (\mathcal{E}, v) \longrightarrow (\mathcal{F}, w).$$

Again,

$$\mathrm{Hom}(\mathcal{E}, \mathcal{F}) = \varinjlim \mathrm{Hom}(\mathcal{E}_n, \mathcal{F}).$$

Unipotent fundamental groups

The $\mathcal{E}_n$ as above corresponds to the representation

$$\mathcal{E}_{n,b} = E_n := (\mathbb{Z}_p[[\hat{\pi}_1(\bar{X}, b)]]/I^{n+1}) \otimes \mathbb{Q}_p,$$

where $I \subset \mathbb{Z}_p[[\hat{\pi}_1(\bar{X}, b)]]$ is the augmentation ideal, and $v_n = 1$.

We put

$$E = \varprojlim E_n = \varprojlim (\mathbb{Z}_p[[\hat{\pi}_1(\bar{X}, b)]]/I^{n+1}) \otimes \mathbb{Q}_p.$$

We think of this as non-commutative power series in $\gamma - 1$, where γ are topological generators of $\hat{\pi}_1(\bar{X}, b)$. Contains elements like

$$\gamma^a = \exp(a \log(\gamma))$$

for $a \in \mathbb{Q}_p$.

Unipotent fundamental groups

The pointed local system $(\mathcal{E}_n, v_n)$ is universal among unipotent local systems of index of unipotency $\leq n$. Thus we get unique maps

$$\mathcal{E}_{m+n} \mapsto \mathcal{E}_m \otimes \mathcal{E}_n$$

that send v_{m+n} to $v_m \otimes v_n$. These come together to a map

$$\Delta : \mathcal{E} \longrightarrow \mathcal{E} \hat{\otimes} \mathcal{E}.$$

Using the fibre functor

$$F_b : \mathrm{Un}(\bar{X}, \mathbb{Q}_p) \longrightarrow \mathrm{Vect}_{\mathbb{Q}_p}.$$

we now define

$$U(\bar{X}, b) := \mathrm{Aut}^{\otimes}(F_b);$$

$$P(\bar{X}; b, x) := \mathrm{Isom}^{\otimes}(F_b, F_x).$$

Unipotent fundamental groups

Lemma

$$End(F_b) \cong \mathcal{E}_b.$$

Theorem

The pro-algebraic group $U(\bar{X}, b)$ is isomorphic to the group-like elements in $\mathcal{E}_b$, while $P(\bar{X}; b, x)$ is given by the group-like elements in $\mathcal{E}_x$.

In fact, the lower central series

$$U = U^1 \supset U^2 \supset U^3 \cdots$$

is compatible with the filtration by I^n, so that $U_n = U/U^{n+1}$ are the group-like elements in E_n.

Unipotent fundamental groups

Put

$$\mathcal{A} = \mathrm{Hom}(\mathcal{E}, \mathbb{Q}_p) = \varinjlim \mathrm{Hom}(\mathcal{E}_n, \mathbb{Q}_p).$$

Then $\mathcal{A}$ is a sheaf of $\mathbb{Q}_p$-algebras via Δ^*.

Corollary

$$U(\bar{X}, b) = Spec(\mathcal{A}_b).$$

$$P(\bar{X}; b, x) = Spec(\mathcal{A}_x).$$

Unipotent fundamental groups

Some remarks on Galois actions.

(1) The action on $P(\bar{X}; b, x)$ is induced by the action on $\mathcal{E}_x$.

(2) The action on $\mathcal{E}_x$ uses $\tilde{\bar{X}}_x \times_{\hat{\pi}_1(\bar{X},b)} E$.

(3) The action on $\tilde{\bar{X}}_x$ is given by a cocycle

$$c_x : G_K \longrightarrow \hat{\pi}_1(\bar{X}, b).$$

That is, choose $\tilde{x} \in \tilde{\bar{X}}$. Then c_x is defined by

$$g(\tilde{x}) = \tilde{x} c_x(g)$$

and satisfies $c_x(g_1 g_2) = c(g_1) g_1 c(g_2)$.

Then $\mathcal{E}_x$ can be identified with E where the action is twisted:

$$g_x v = c_x(g) g v.$$

Unipotent fundamental groups

Some basic structural facts.

The map

$$g \mapsto [g-1]$$

induces an isomorphism

$$H_1(\bar{X}, \mathbb{Q}_p) = \hat{\pi}_1(\bar{X}, b)^{ab} \otimes \mathbb{Q}_p \cong I/I^2.$$

The multiplication map

$$(I/I^2)^{\otimes n} \longrightarrow I^n/I^{n+1}$$

includes an isomorphism

$$H_1^{\otimes n}/K_n \simeq I^n/I^{n+1}$$

where $T_n := H_1^{\otimes n}/K_n \simeq (R^n)^*$ and $R^n \subset (H^1)^{\otimes n}$ is defined inductively as follows.

Unipotent fundamental groups

$R^0 = \mathbb{Q}_p$, $R^1 = H^1$,

$$R^2 = \mathrm{Ker}(H^1 \otimes H^1 \xrightarrow{\gamma_1 := \cup} H^2).$$

We will have $R^{n+1} \subset R^n \otimes H^1$. Define the map γ_n inductively as

$$\gamma_n : R^n \otimes H^1 \longrightarrow R^{n-1} \otimes H^1 \otimes H^1 \longrightarrow R^{n-1} \otimes H^2,$$

and define

$$R^{n+1} = \mathrm{Ker}(\gamma_n).$$

Unipotent fundamental groups

This comes from a different tautological construction [AIK, Faltings1, Faltings2].

$$\mathrm{Ext}^1_{\bar{X}}((\mathbb{Q}_p)_{\bar{X}}, (H_1(\bar{X}))_{\bar{X}}) \simeq H^1(\bar{X}) \otimes H_1(\bar{X})) = \mathrm{Hom}(H_1, H_1).$$

So there is an extension

$$0 \longrightarrow H_1(\bar{X}) \longrightarrow \mathcal{E}_1 \longrightarrow \mathbb{Q}_p \longrightarrow 0$$

corresponding to the identity map on the right.

Now we get an exact sequence

$$\mathrm{Hom}_{\bar{X}}(H_1, \mathbb{Q}_p)$$

$$\xrightarrow{\delta} \mathrm{Ext}^1_{\bar{X}}(\mathbb{Q}_p, \mathbb{Q}_p) \longrightarrow \mathrm{Ext}^1_{\bar{X}}(\mathcal{E}_1, \mathbb{Q}_p) \longrightarrow \mathrm{Ext}^1_{\bar{X}}(H_1, \mathbb{Q}_p)$$

$$\xrightarrow{\delta} \mathrm{Ext}^2_{\bar{X}}(\mathbb{Q}_p, \mathbb{Q}_p)$$

Unipotent fundamental groups

This can be written as

$$H^1 \xrightarrow{\delta} H^1 \longrightarrow \mathrm{Ext}^1_{\bar{X}}(\mathcal{E}_1, \mathbb{Q}_p) \longrightarrow H^1 \otimes H^1 \xrightarrow{\delta} H^2.$$

which induces the isomorphism

$$\mathrm{Ext}^1_{\bar{X}}(\mathcal{E}_1, \mathbb{Q}_p) \cong R^2 \cong T_2^*.$$

Hence,

$$Ext^1_{\bar{X}}(\mathcal{E}_1, T_2) \cong \mathrm{Hom}(T_2, T_2),$$

so that there is an extension

$$0 \longrightarrow T_2 \longrightarrow \mathcal{E}_2 \longrightarrow \mathcal{E}_1 \longrightarrow 0$$

corresponding to the identity on the right.

One continues in this way and the universal property can also be proved in a tautological manner.

Unipotent fundamental groups

Idea: When the index of unipotency is 1 we have a constant sheaf $V_{\bar{X}} \longrightarrow \bar{X}$. Of course there is a unique map

$$f_1 : [\mathbb{Q}_p]_{\bar{X}} \longrightarrow V_{\bar{X}}$$

that takes $1 \in \mathbb{Q}_p = [\mathbb{Q}_p]_{\bar{X},b}$ to any fixed $v \in V = V_{\bar{X}.b}$..

Now suppose you have

$$0 \longrightarrow W \longrightarrow \mathcal{F} \longrightarrow V \longrightarrow 0$$

with V and $\mathcal{F}^1$ constant. We would like to construct a lift f_2 as below

$$\begin{tikzcd}
0 \arrow[r] & T_1 \arrow[r] \arrow[d] & \mathcal{E}_1 \arrow[r] \arrow[d, "f_2"'] & \mathbb{Q}_p \arrow[r] \arrow[d, "f_1"'] & 0 \\
0 \arrow[r] & W \arrow[r] & \mathcal{F} \arrow[r] & V \arrow[r] & 0
\end{tikzcd}$$

Unipotent fundamental groups

The idea is to pull back by f_1 to get

$$0 \longrightarrow W \longrightarrow f_1^*\mathcal{F} \longrightarrow \mathbb{Q}_p \longrightarrow 0.$$

We would like to show this comes from $\mathcal{E}_1$ via a push-out along a map $\phi : T_1 \longrightarrow W$. But this extension is a class

$$c \in \mathrm{Ext}^1_X(\mathbb{Q}_p, W) = H^1 \otimes W.$$

Meanwhile, $\mathcal{E}_1$ corresponds to the class

$$I = \sum_i b^i \otimes b_i \in \mathrm{Ext}^1(\mathbb{Q}_p, H_1) = H^1 \otimes H_1,$$

where $\{b_i\}$ is a basis for H_1 and $\{b^i\}$ the dual basis.

Write $c = \sum_i b^i \otimes w_i$, and define ϕ to be the linear map that takes b_i to w_i.

Bibliography

- Andreatta, Fabrizio; Iovita, Adrian; Kim, Minhyong A p-adic nonabelian criterion for good reduction of curves. Duke Math. J. 164 (2015), no. 13, 2597-2642.
- Deligne, Pierre Le groupe fondamental de la droite projective moins trois points. Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 79–297, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.
- Faltings, Gerd Mathematics around Kim's new proof of Siegel's theorem. Diophantine geometry, 173?188, CRM Series, 4, Ed. Norm., Pisa, 2007.
- Faltings, Gerd The motivic logarithm for curves. The arithmetic of fundamental groups, PIA 2010, 107-125, Contrib. Math. Comput. Sci., 2, Springer, Heidelberg, 2012.
- Szamuely, Tamás Galois groups and fundamental groups. Cambridge Studies in Advanced Mathematics, 117. Cambridge University Press, Cambridge, 2009. x+270 pp.