Galois Theory and Diophantine geometry 4

Minhyong Kim

August, 2009

Cambridge

Main objects:

- $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.
- (X, b): Smooth projective pointed curve of genus $g \geq 2$ over $\mathbb{Q}$ with good reduction outside S.
- $T = S \cup \{p\}$ for a prime $p \notin S$.
- U: $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $\bar{X} = X \otimes \bar{\mathbb{Q}}$ with base-point b.
- $U^1 = U$, $U^{n+1} = [U, U^n]$, $U_n = U^{n+1} \backslash U$.
- $H^1_f(G, U)$: moduli space of crystalline principal U-bundles on $\mathrm{Spec}(\mathbb{Z}[1/T])$.

Construction of U:

Start with $\pi = \pi_1^p(\bar{X}, b)$, the pro-$p$ étale fundamental group of $\bar{X}$ and consider

$$\mathbb{Z}_p[[\pi]] := \varprojlim_H \mathbb{Z}_p[H],$$

where H runs over the finite quotient groups. Let $I \subset \mathbb{Z}_p[[\pi_1]]$ be the augmentation ideal, and consider the pro-algebra

$$\mathbb{Q}_p[[\pi]] := ((\mathbb{Z}_p[[\pi]]/I^n) \otimes \mathbb{Q}_p)_{n \in \mathbb{N}}$$

and the map of pro-algebras

$$\Delta : \mathbb{Q}_p[[\pi]] \rightarrow \mathbb{Q}_p[[\pi]] \otimes \mathbb{Q}_p[[\pi]]$$

induced by the map $g \rightarrow g \otimes g$.

Then

$$U := \{x \in \mathbb{Q}_p[[\pi]]^\times : \Delta(x) = x \otimes x\}.$$

Action of G on π factors through $G_T = \mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$ where $\mathbb{Q}_T$ is the maximal extension of $\mathbb{Q}$ unramified outside T. Induces action of G_T on U and each of the U_n. Can consider

$$H^1(G_T, U_n),$$

the continuous cohomology of G_T with values in U_n, and

$$H^1(G_T, U) := \varprojlim H^1(G_T, U_n).$$

Choose an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, inducing $G_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \rightarrow G_T$ and the localization map

$$\mathrm{loc}_p : H^1(G_T, U) \rightarrow H^1(G_p, U).$$

There is the subset

$$H_f(G_p, U) \subset H^1(G_p, U)$$

consisting of classes that trivialize under the map

$$H^1(G_p, U) \rightarrow H^1(G_p, U(B_{cr})),$$

and

$$H_f(G, U) := \mathrm{loc}_p^{-1}(H^1_f(G_p, U)) \subset H^1(G_T, U).$$

Path torsors:

For any other $x \in X(\mathbb{Q})$, need also the space $P(x)$ of $\mathbb{Q}_p$-unipotent étale paths from b to x.

Constructed from the torsor

$$\pi_1^p(\bar{X}; b, x)$$

of pro-p étale paths by push-out:

$$P(x) := \pi_1^p(\bar{X}; b, x) \times_\pi U.$$

Equipped with a U-action

$$P \times U \rightarrow P$$

and a compatible action of G_T.

Sometimes useful to think in terms of the sheaf E on $\bar{X}$ associated with the representation $\mathbb{Q}_p[[\pi]]$ of π (multiplication on the left). There is a map

$$\Delta : E \rightarrow E \otimes E$$

induced by the map of representations, so that we can consider the sheaf P of group-like elements in E. Then $P(x) = P_x$.

That is, P is actually a principal U-bundle on X

$$\begin{array}{c} P \\ \downarrow \\ X \end{array}$$

and using a point

$$X \underset{x}{\overset{\longrightarrow}{\longleftarrow}} \mathrm{Spec}(\mathbb{Q})$$

we can pull-back to a sheaf $P(x) = x^*P$ on $\mathrm{Spec}(\mathbb{Q})$.

The sheaf P extends to a $\mathbb{Z}[1/T]$-model for X, so that the sheaf $P(x)$ extends to $\mathrm{Spec}(\mathbb{Z}[1/T])$. They are also all crystalline at p, giving rise to a map

$$X(\mathbb{Q}) \longrightarrow H^1_f(G, U);$$

$$x \mapsto [P(x)];$$

the *unipotent Albanese map* with target the *Selmer variety* of X.

Fundamental diagram:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ H^1_f(G, U_n) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_n) \end{array}$$

Basic fact:

If $\mathrm{loc}_p(H^1_f(G, U_n)) \subset H^1_f(G_p, U_n)$ is non-dense, then $X(\mathbb{Q})$ is finite.

Key point: There is a non-zero algebraic function ψ

$$\begin{array}{ccc} X(\mathbb{Q}) & \rightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ H^1_f(G, U_n) & \rightarrow & H^1_f(G_p, U_n) \\ & & \downarrow \psi \\ & & \mathbb{Q}_p \end{array}$$

vanishing on the image of loc_p. So its pull-back to $X(\mathbb{Q}_p)$ vanishes on $X(\mathbb{Q})$, but can be shown to have finitely many zeros.

At present, can show non-denseness of loc_p for $n >> 0$ when the image of G in $\mathrm{Aut}(U_1) = \mathrm{Aut}(V_p(J_X))$ is essentially abelian, using the sparseness of zeros of an 'algebraic p-adic L-function.'

However, this approach only shows the *existence* of a ψ.

Basic question remains of producing *natural functions* on $H^1_f(G_p, U_n)$, perhaps in a manner reminiscent of functions on moduli spaces of principal bundles in complex geometry.

Note that one can describe many 'local' functions on $H^1_f(G_p, U_n)$ obtained via

$$H^1_f(G_p, U_n) \simeq U^{DR}/F^0$$

that restrict to iterated integrals on $X(\mathbb{Q}_p)$. But we need to produce functions *of a global nature* directly on $H^1_f(G_p, U_n)$, whose *explicit form* can then be computed using the comparison isomorphism.

Why functions of 'a global nature'?

Consider the case of an elliptic curve (E, e), for which $U = U_1 = V_p(E)$. One has local duality:

$$< \cdot, \cdot >: H^1(G_p, V) \times H^1(G_p, V^*(1)) \rightarrow H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$$

making $H^1(G_p, V^*(1))$ into a source of functions on $H^1(G_p, V)$. More precisely,

$$H^1(G_p, V^*(1))/H^1_f(G_p, V^*(1))$$

gives functions on $H^1_f(G_p, V)$. Functions of a global nature come from the map

$$pr \circ \mathrm{loc}_p : H^1(G_T, V^*(1)) \rightarrow H^1(G_p, V^*(1))/H^1_f(G_p, V^*(1)).$$

The significance of such functions is the following:

> Suppose there exists $\alpha \in H^1(G_T, V^*(1))$ such that $pr \circ \mathrm{loc}_p(\alpha) \neq 0$. Then $E(\mathbb{Q})$ is finite.

Proof: The function $< \mathrm{loc}_p(\alpha), \cdot >$ is not identically zero on $H^1_f(G_p, V)$. But for the class $k(x) \in H^1(G, V)$ of a point $x \in E(\mathbb{Q})$, we have

$$\sum_{v \neq p} < \mathrm{loc}_v(\alpha), \mathrm{loc}_v(k(x)) > + < \mathrm{loc}_p(\alpha), \mathrm{loc}_p(k(x)) >= 0.$$

All the other terms are zero, so that

$$< \mathrm{loc}_p(\alpha), \mathrm{loc}_p(k(x)) >= 0.$$

That is, $< \mathrm{loc}_p(\alpha), \cdot >$ pulled back to $E(\mathbb{Q}_p)$ is a non-zero analytic function that annihilates global points.

When α is constructed naturally (and there is *not* much choice) the function $< \mathrm{loc}_p(\alpha), \cdot >$ is related to L-values, e.g.,

$$< \mathrm{loc}_p(\alpha), c(z) >= L_p(E,1) \int_e^z dx/y.$$

Thus, key desiderata are:

(1) Non-abelian local duality, giving a cohomological description of functions on $H^1_f(G_p, U)$.

(2) A non-abelian local-global duality, relating to global reciprocity.

(3) Construction of global elements in non-abelian cohomology.

(4) Local analytic computation of such functions.

(Non-abelian) Example:

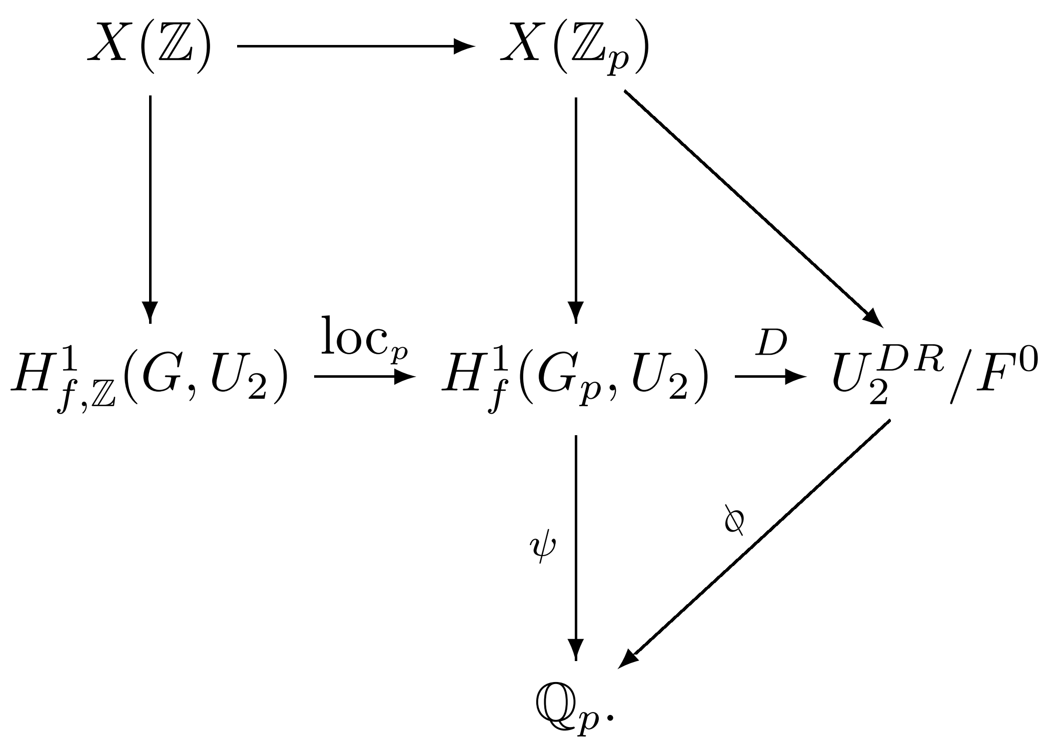
Let $X = E \setminus \{e\}$, where E is an elliptic curve of rank 1 with $Ш(E)[p^\infty] = 0$. Hence, we get

$$loc_p : E(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq H^1_f(G_p, V_p(E))$$

and

$$H^2(G_T, V_p(E)) = 0.$$

We will construct a diagram:



Here, $H^1_{f,\mathbb{Z}}(G, U_2)$ refers to the classes that are trivial at all places $l \neq p$.

The Galois action on the Lie algebra of U_2 can be expressed as

$$L_2 = V \oplus \mathbb{Q}_p(1)$$

if we take a tangential base-point at e. The cocycle condition for

$$\xi : G_p \longrightarrow U_2 = L_2$$

can be expressed terms of components $\xi = (\xi_1, \xi_2)$ as

$$d\xi_1 = 0, \qquad d\xi_2 = (-1/2)[\xi_1, \xi_1].$$

Define

$$\psi(\xi) := [\mathrm{loc}_p(x), \xi_1] + \log \chi_p \cup (-2\xi_2) \in H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

where

$$\log \chi_p : G_p \to \mathbb{Q}_p$$

is the logarithm of the $\mathbb{Q}_p$-cyclotomic character and x is a *global* solution, that is,

$$x : G_T \to V_p,$$

to the equation

$$dx = \log \chi_p \cup \xi_1.$$

Theorem 1 *ψ vanishes on the image of*

$$loc_p : H^1_{f,\mathbb{Z}}(G, U_2) \to H^1_f(G_p, U_2).$$

Proof is a simple consequence of

$$0 \to H^2(G_T, \mathbb{Q}_p(1)) \to \oplus_{v \in T} H^2(G_v, \mathbb{Q}_p(1)) \to \mathbb{Q}_p \to 0.$$

Easy to check that for the class

$$k(x) = H^1_f(G_p, \mathbb{Q}_p(1)) \subset H^1_f(G_p, U_2)$$

of a number $x \in \mathbb{Z}_p^\times$, we have $\psi(k(x)) = \pm \log \chi_p(rec(x))$, and hence, that ψ is not identically zero.

Explicit formula on De Rham side:

Choose a Weierstrass equation for E and let

$$\alpha = dx/y, \quad \beta = x dx/y.$$

Define

$$\log_\alpha(z) := \int_b^z \alpha, \quad \log_\beta(z) := \int_b^z \beta,$$

$$D_2(z) := \int_b^z \alpha\beta,$$

via (iterated) Coleman integration.

Corollary 2 *Suppose* $y \in X(\mathbb{Z})$ *has infinite order in* $E(\mathbb{Q})$. *Then for any point* $z \in X(\mathbb{Z}_p)$, *we have*

$$\psi(z) = Res_e(wdx/y)^{-1}[D_2(z) - \log_\alpha(z)\log_\beta(z)$$

$$-(\frac{D_2(y) - \log_\alpha(y)\log_\beta(y)}{\log_\alpha^2(y)})\log_\alpha^2(z)].$$

where $dw = xdx/y$ *locally.*

An interpretation:

There is a central extension

$$0 \rightarrow \mathbb{Q}_p(1) \rightarrow \mathcal{G} \rightarrow L_2^*(1) \rtimes U_2 \rightarrow 0.$$

that uses the grading on L_2. That is, the linear map

$$d : L_2 \rightarrow L_2$$

that multiplies by i on degree i is a derivation, or a cocycle in $H^1(L_2, L_2)$. This contributes to $H^2(L_2^*(1) \rtimes L_2, \mathbb{Q}_p(1))$, giving rise to the extension $\mathcal{G}$.

The previous function then arises from the diagram

$$
\begin{array}{ccc}
H^1_{f,\mathbb{Z}}(G, L_2^*(1) \rtimes U_1) & \xrightarrow{\mathrm{loc}_p} & H^1(G_p, L_2^*(1) \rtimes U_1) \\
\downarrow & & \\
H^1_{f,\mathbb{Z}}(G, \mathbb{Q}_p \times U_1) & & H^1_f(G_p, U_2) \\
\uparrow & & \downarrow \\
H^1_{f,\mathbb{Z}}(G, U_1) & \longrightarrow & H^1_f(G_p, U_1)
\end{array}
$$

where the upward arrow sends a class ξ_1 to $(\log \chi_p, \xi_1)$, and the diagram:

$$
\begin{array}{ccccc}
 & & H^1(G_p, U^3\backslash U^2) & = & H^1(G_p, U^3\backslash U^2) \\
 & & \downarrow & & \downarrow \\
H^1(G_p, L_2^*(1)) & \longrightarrow & H^1_f(G_p, L_2^*(1) \rtimes U_2) & \longrightarrow & H^1_f(G_p, U_2) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(G_p, L_2^*(1)) & \longrightarrow & H^1_f(G_p, L_2^*(1) \rtimes U_1) & \longrightarrow & H^1_f(G_p, U_1) \\
 & & \downarrow & & \downarrow \\
 & & H^2(G_p, U^3\backslash U^2) & = & H^2(G_p, U^3\backslash U^2)
\end{array}
$$

illustrating that the middle right square is Cartesian.

Denoting by

$$\beta(\xi) \in H^1_f(G_p, L_2^*(1) \rtimes U_1)$$

the class obtained from the first diagram, we get the class

$$(\beta(\xi), \xi) \in H^1_f(G_p, L_2^*(1) \rtimes U_2).$$

Then

$$\psi(\xi) = \delta(\beta(\xi), \xi) \in H^2(G_p, \mathbb{Q}_p(1)).$$

Back to a general pointed curve (X, b).

The derivation $d : L_n \rightarrow L_n$ that was used to construct the central extension will usually not exist. However, Deligne pointed out that one might try to construct an extension

$$0 \rightarrow U \rightarrow E \rightarrow \mathbb{G}_m \rightarrow 0,$$

wherefrom one would obtain an extension

$$0 \rightarrow \mathbb{Q}_p(1) \rightarrow Lie E^*(1) \rightarrow L^*(1) \rightarrow 0.$$

Then

$$Lie E^*(1) \rtimes U$$

would be a central extension of $L^*(1) \rtimes U$.

Unfortunately, this seems also difficult. However, one can embed U into $\mathrm{Aut}^0(U)$, the group of automorphisms of U that act trivially on U_1.

This group fits naturally into the exact sequence

$$0 \to \mathrm{Aut}^0(U) \to \mathrm{Aut}^c(U) \to \mathbb{G}_m \to 0$$

where $\mathrm{Aut}^c(U) \subset \mathrm{Aut}(U)$ consists of the automorphisms that act as a scalar on U_1. Denote by D and D^c the Lie algebras of Aut^0 and Aut^c. Then we have the central extension

$$0 \to \mathbb{Q}_p(1) \to (D^c)^*(1) \to D^*(1) \to 0,$$

out of which we can construct the central extension

$$0 \to \mathbb{Q}_p(1) \to (D^c)^*(1) \rtimes U \to D^*(1) \rtimes U \to 0.$$

D consists of the derivations $\mathrm{Der}^0(L)$ on L that act as zero on L_1, and we have exact sequences

$$0 \to D^n \to D \to D_n \to 0,$$

where D^n consists of the derivation that act trivially on L_n. Define also $D_n^i \subset D_n$ with the exact sequence

$$0 \to D_n^i \to D_n \to D_i \to 0.$$

Thus, for each n, we have

$$D_n^*(1) \to [D_n^{n-1}]^*(1) \to 0.$$

$$
\begin{array}{ccc}
H^1_{f,\mathbb{Z}}(G, D_n^*(1) \rtimes U_{n-1}) & \xrightarrow{\mathrm{loc}_p} & H^1(G_p, D_n^*(1) \rtimes U_{n-1}) \\
\downarrow & & \\
H^1_{f,\mathbb{Z}}(G, [D_n^{n-1}]^*(1) \times U_{n-1}) & & H^1_f(G_p, U_n) \\
\uparrow & & \downarrow \\
H^1_{f,\mathbb{Z}}(G, U_{n-1}) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_{n-1})
\end{array}
$$

$$
\begin{CD}
@. H^1(G_p, U^{n+1}\backslash U^n) @= H^1(G_p, U^{n+1}\backslash U^n) \\
@. @VVV @VVV \\
H^1(G_p, D_n^*(1)) @>>> H^1_f(G_p, D_n^*(1) \rtimes U_n) @>>> H^1_f(G_p, U_n) \\
@VVV @VVV @VVV \\
H^1(G_p, D_n^*(1)) @>>> H^1_f(G_p, D_n^*(1) \rtimes U_{n-1}) @>>> H^1_f(G_p, U_{n-1}) \\
@. @VVV @VVV \\
@. H^2(G_p, U^{n+1}\backslash U^n) @= H^2(G_p, U^{n+1}\backslash U^n)
\end{CD}
$$

Assume that the map

$$H^1_{f,\mathbb{Z}}(G, D_n^*(1) \rtimes U_{n-1}) \rightarrow H^1_{f,\mathbb{Z}}(G, [D_n^{n-1}]^*(1) \times U_{n-1})$$

is surjective, and

$$\mathrm{loc}_p : H^1_{f,\mathbb{Z}}(G, U_{n-1}) \rightarrow H^1_f(G_p, U_{n-1})$$

is an isomorphism. Then for every choice of $c \in H^1(G_T, [D_n^{n-1}]^*(1))$, we get a well-defined class

$$\psi_c(\xi) = \delta(\alpha(\xi), \xi) \in H^2(G_p, \mathbb{Q}_p(1))$$

where $\alpha(\xi) \in H^1_f(G_p, [D_n]^*(1) \times U_{n-1})$ is obtained from the following procedure.

(1) projecting $\xi \in H^1_f(G_p, U_n)$ to $\xi_{n-1} \in H^1_f(G_p, U_{n-1})$;

(2) pulling-back to $\mathrm{loc}_p^{-1}(\xi_{n-1}) \in H^1_{f,\mathbb{Z}}(G, U_{n-1})$;

(3) mapping to

$$(c, \mathrm{loc}_p^{-1}(\xi_{n-1})) \in H^1_{f,\mathbb{Z}}(G, [D_n^{n-1}]^*(1) \times U_{n-1});$$

(4) lifting to

$$(c, \widetilde{\mathrm{loc}_p^{-1}(\xi}_{n-1})) \in H^1_{f,\mathbb{Z}}(G, [D_n]^*(1) \times U_{n-1});$$

(5) localizing to

$$\alpha(\xi) = \mathrm{loc}_p((c, \widetilde{\mathrm{loc}_p^{-1}(\xi}_{n-1}))) \in H^1_{f,\mathbb{Z}}(G, [D_n]^*(1) \times U_{n-1}).$$

Note that the fiber of the map

$$H^1_{f,\mathbb{Z}}(G, D_n^*(1) \rtimes U_{n-1}) \longrightarrow H^1_{f,\mathbb{Z}}(G, [D_n^{n-1}]^*(1) \times U_{n-1})$$

over a point (c, u) is a torsor for $H^1(G_T, D_{n-1}^*(1)_u)$, where the subscript u refers to a twist of the Galois action by the cocycle u. This is also the fiber over u of the map

$$H^1_{f,\mathbb{Z}}(G, D_{n-1}^*(1) \rtimes U_{n-1}) \longrightarrow H^1_{f,\mathbb{Z}}(G, U_{n-1}).$$

Thus, the ambiguity in the lift from $H^1_{f,\mathbb{Z}}(G, [D_n^{n-1}]^*(1) \times U_{n-1})$ to $H^1_{f,\mathbb{Z}}(G, D_n^*(1) \rtimes U_{n-1})$ will be an element of

$$H^1_{f,\mathbb{Z}}(G, D_{n-1}^*(1) \rtimes U_{n-1}).$$

Proposition 3 *Suppose* $\xi = loc_p(\xi^{glob})$ *for* $\xi^{glob} \in H^1_{f,\mathbb{Z}}(G, U_n)$. *Then* $\psi_c(\xi) = 0$.

There is a natural *split* inclusion

$$L_n^{n-1} \hookrightarrow D_n^{n-1}$$

inducing also an inclusion

$$[L_n^{n-1}]^*(1) \hookrightarrow [D_n^{n-1}]^*(1).$$

So we also get an inclusion

$$H^1(G_T, [L_n^{n-1}]^*(1)) \hookrightarrow H^1(G_T, [D_n^{n-1}]^*(1)).$$

Proposition 4 *Suppose*

$$pr \circ loc_p(c) \in H^1(G_p, [L_n^{n-1}]^*(1))/H^1_f(G_p, [L_n^{n-1}]^*(1))$$

is non-zero. Then ψ_c *is not identically zero, and* $X(\mathbb{Q})$ *is finite.*

Thus, functions of a global nature should iteratively come from uniformly liftable elements

$$c \in H^1(G_T, [L_n^{n-1}]^*(1)),$$

that is, elements that lie in the image of

$$H^1(G_T, D_n^*(1)_u) \longrightarrow H^1(G_T, [D_n^{n-1}]^*(1))$$

for every $u \in H^1_{f,\mathbb{Z}}(G, U_{n-1})$, which furthermore have non-trivial local images.