Galois Theory and Diophantine geometry ± 12

Minhyong Kim

Heidelberg, February, 2010

Notation and Review

F: Number field.

S: finite set of primes of F.

$R := \mathcal{O}_F[1/S]$, the ring of S integers in F.

p: odd prime not divisible by primes in S and v a prime of F above p with $F_v = \mathbb{Q}_p$.

$T := S \cup \{w|p\}$.

$G := \mathrm{Gal}(\bar{F}/F)$. $G_T := \mathrm{Gal}(F_T/T)$.

$\mathcal{X}$: smooth curve over $\mathrm{Spec}(R)$ with good compactification. (Itself might be compact.)

X: generic fiber of $\mathcal{X}$, assumed to be hyperbolic.

$b \in \mathcal{X}(R)$, possibly tangential.

$U := \pi_1^{et,\mathbb{Q}_p}(\bar{X}, b)$, the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $\bar{X} = X \otimes \bar{\mathbb{Q}}$.

$U^i \subset U$, lower central series, normalized so that $U^1 = U$.

$U_i = U^{i+1} \backslash U$.

$U_j^i = U^{i+1} \backslash U^j$ for $j \leq i$.

$U^{DR} := \pi_1^{DR}(X \otimes \mathbb{Q}_p, b)$, with corresponding notation for the characteristic subquotients.

$P(x) := \pi_1^{et,\mathbb{Q}_p}(\bar{X}; b, x)$, $P_n(x) = P(x) \times_U U_n$.

$P^{DR}(x) := \pi_1^{DR}(X \otimes \mathbb{Q}_p; b, x)$, etc.

Unipotent descent tower:

$$\begin{tikzcd}
 & \vdots \\
\vdots & H^1_f(G, U_4) \arrow[d] \\
 & H^1_f(G, U_3) \arrow[d] \\
 & H^1_f(G, U_2) \arrow[d] \\
\mathcal{X}(R) \arrow[r] \arrow[ur] \arrow[uur] \arrow[uuur] & H^1_f(G, U_1)
\end{tikzcd}$$

$$x \in \mathcal{X}(R) \mapsto [P(x)] \in H^1_f(G, U).$$

$$
\begin{tikzcd}
\mathcal{X}(R) \arrow[r] \arrow[d] & \mathcal{X}(R_v) \arrow[d] \arrow[dr] & \\
H^1_f(G, U_n) \arrow[r, "\mathrm{loc}_v"] & H^1_f(G_v, U_n) \arrow[r, "\simeq"] & U_n^{DR}/F^0
\end{tikzcd}
$$

$H^1_f(G, U)$: moduli space of U-torsors on $\mathrm{Spec}(R[1/p])$ that are crystalline at all $w|p$.

$H^1_f(G_v, U_n)$: moduli space of crystalline U-torsors on $\mathrm{Spec}(F_v)$.

The subgroup $F^0 \subset U^{DR}$ is the zeroth level of the *Hodge filtration*, so that U/F^0 classifies U^{DR} torsors with compatible action of Frobenius and reduction of structure group to F^0.

The map

$$H^1_f(G_v, U_n) \longrightarrow U_n^{DR}/F^0$$

sends a U-torsor $Y = \mathrm{Spec}(A)$ to

$$D(Y) := \mathrm{Spec}([A \otimes B_{cr}]^{G_v}),$$

and diagram commutes by comparison isomorphism of non-abelian p-adic Hodge theory.

The focus of the study then is the localization map

$$H^1_f(G, U_n) \xrightarrow{\mathrm{loc}_v} H^1_f(G_v, U_n)$$

and its image.

Current status:

1. Whenever the image is not Zariski dense, $\mathcal{X}(R)$ is finite.

$$\mathcal{X}(R) = \mathcal{X}(R_v) \cap \mathrm{loc}_v(H^1_f(G, U_n)).$$

Difficult to prove non-denseness in any situation where the corresponding Galois theory is genuinely non-abelian.

2. Suppose $F = \mathbb{Q}$ and

$$Im(G) \subset Aut(H_1(\bar{X}, \mathbb{Q}_p)$$

is essentially abelian. Then loc_v is not dominant for $n >> 0$.

Basic application of Euler characteristic formula

$$\dim H^0(G_T, U_n^n) - \dim H^1(G_T, U_n^n) + \dim H^2(G_T, U_n^n)$$

$$= \sum_{w|\infty} (H^0(G_w, U_n^n) - [F_w : \mathbb{R}] \dim U_n^n)$$

and control of H^2. In non-abelian situations, leads to difficult questions about Galois cohomology.

3. One expects greater precision coming from some version of duality for Galois cohomology.

Example:

$E/\mathbb{Q}$ elliptic curve with

$$\mathrm{rank} E(\mathbb{Q}) = 1,$$

integral j-invariant, and

$$|Ш(E)[p^\infty| < \infty$$

for a prime p of good reduction.

$X = E \setminus \{0\}$ given as a minimal Weierstrass model:

$$y^2 = x^3 + ax + b.$$

So

$$X(\mathbb{Z}) \subset E(\mathbb{Z}) = E(\mathbb{Q}).$$

Let $\alpha = dx/y$, $\beta = xdx/y$. Get analytic functions on $X(\mathbb{Q}_p)$,

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

$$\omega(z) = \int_b^z \alpha\beta.$$

Here, b is a tangential base-point at 0, and the integral is (iterated) *Coleman integration*.

Locally, the integrals are just anti-derivatives of the forms, while for the iteration,

$$d\omega = (\int_b^z \beta)\alpha.$$

Suppose there is a point $y \in X(\mathbb{Z})$ of infinite order in $E(\mathbb{Q})$. Then the subset

$$X(\mathbb{Z}) \subset X(\mathbb{Q}_p)$$

lies in the zero set of the analytic function

$$\psi(z) := \omega(z) - (1/2)\log_\alpha(z)\log_\beta(z)$$

$$-\frac{(\omega(y) - (1/2)\log_\alpha(y)\log_\beta(y))}{(\log_\alpha(y))^2}(\log_\alpha(z))^2.$$

A fragment of non-abelian duality and explicit reciprocity.

Linearization

Study the *tangential localization map*:

$$d\mathrm{loc}_v(c) : T_c H^1_f(G,U) \to T_{\mathrm{loc}_v(c)} H^1_f(G_v,U)$$

at a point $c \in H^1_f(G,U)$.

Formulae:

$$T_c H^1_f(G,U) \simeq H^1_f(G,L(c));$$

$$T_{\mathrm{loc}_v(c)} H^1_f(G_v,U) \simeq H^1_f(G_v,L(c));$$

where L is the Lie algebra of U with Galois action twisted by the cocycle c.

For non-denseness, suffices to show that $d\mathrm{loc}_v(c)$ is not surjective at generic points c.

Can formulate a criterion in terms of the cotangent space:

$$T^*_{\mathrm{loc}_v(c)} H^1_f(G_v, U) \simeq H^1(G_v, (L(c))^*(1))/H^1_f(G_v, (L(c))^*(1))$$

coming from local Tate duality.

Theorem 0.1 *Assume that for generic c there is a class*

$$z \in H^1(G_T, (L_n(c))^*(1))$$

such that $loc_w(z) = 0$ for $w \neq v$ and

$$loc_v(z) \notin H^1_f(G_v, (L_n(c))^*(1)).$$

Then

$$loc_v : H^1_f(G, U_n) \rightarrow H^1_f(G_v, U_n)$$

is not dominant.

Proof.

By Poitou-Tate duality, we know that the images of the localization maps

$$\mathrm{loc}_T : H^1(G_T, L_n(c)) \to \oplus_{w\in T} H^1(G_w, L_n(c))$$

and

$$\mathrm{loc}_T : H^1(G_T, (L_n(c))^*(1)) \to \oplus_{w\in T} H^1(G_w, (L_n(c))^*(1))$$

are exact annihilators under the natural pairing

$$< \cdot, \cdot >: \oplus_{w\in T} H^1(G_w, L_n(c)) \times \oplus_{w\in T} H^1(G_w, (L_n(c))^*(1)) \to \mathbb{Q}_p.$$

With respect to the pairing $< \cdot, \cdot >_v$ at v, $H^1_f(G_v, L_n(c))$ and $H^1_f(G_v, (L_n(c))^*(1))$ are mutual annihilators.

Given any element $(a_w) \in \oplus_{w \in T} H^1(G_w, L_n(c))$, we have

$$< \mathrm{loc}_T(z), (a_w) >=< \mathrm{loc}_v(z), a_v >_v .$$

Hence, for any $a \in H^1_f(G, L_n(c))$, we get

$$< \mathrm{loc}_v(a), \mathrm{loc}_v(z) >_v =< \mathrm{loc}_T(a), \mathrm{loc}_T(z) >= 0.$$

Since $< \cdot, \mathrm{loc}_v(z) >$ defines a non-trivial linear functional on $H^1_f(G_v, L_n(c))$, this implies the desired results. $\square$

Duality in families

In the following, Γ is G_T or G_v.

Given a point c of $H^1(\Gamma, U)$ in a $\mathbb{Q}_p$-algebra R, compose it with a section s of the projection

$$Z^1(\Gamma, U) \rightarrow H^1(\Gamma, U)$$

to get an element of $Z^1(\Gamma, U)(R) = Z^1(\Gamma, U(R))$.

Given representation

$$\rho : U \rightarrow \mathrm{Aut}(E)$$

of U, twist it with the cocycle c to get ρ_c acting on $E(R) = E \otimes_{\mathbb{Q}_p} R$ defined by

$$\rho_c(g)x = Ad(c(g))\rho(g)x.$$

The cocycles $Z^i(\Gamma, E(c)(R))$ and the cohomology $H^i(\Gamma, E(c)(R))$, acquire structures of R modules, defining a sheaf $H^i(\Gamma, \mathcal{L})$ of modules on $H^i(\Gamma, U)$.

Carry this out for the Lie algebra L to get the sheaf $H^i(\Gamma, \mathcal{L})$, as well as for the dual $L^*(1)$ to get the Tate dual sheaf $H^i(\Gamma, \mathcal{L}^*(1))$.

Similarly, for each term L^i_j occurring in the descending central series:

$$H^i(\Gamma, \mathcal{L}^i_j), \quad H^i(\Gamma, (\mathcal{L}^i_j)^*(1)).$$

We have exact sequences,

$$0\to H^1(\Gamma, \mathcal{L}_n^n)(R)\to H^1(\Gamma, \mathcal{L}_n^i)(R)\to H^1(\Gamma, \mathcal{L}_{n-1}^i)(R)$$

$$\xrightarrow{\delta} H^2(\Gamma, \mathcal{L}_n^n)(R)$$

and

$$H^0(\Gamma, (\mathcal{L}_n^n)^*(1))$$

$$\to H^1(\Gamma, (\mathcal{L}_{n-1}^i)^*(1))(R)\to H^1(\Gamma, (\mathcal{L}_n^i)^*(1))(R)\to H^1(\Gamma, (\mathcal{L}_n^n)^*(1))(R)$$

$$\xrightarrow{\delta} H^2(\Gamma, (\mathcal{L}_{n-1}^i)^*(1))(R)$$

Furthermore,

$$H^i(\Gamma, (\mathcal{L}_n^n)^*(1))(R) \simeq H^i(\Gamma, (L_n^n)^*(1))) \otimes R;$$

$$H^i(\Gamma, \mathcal{L}_n^n)(R) \simeq H^i(\Gamma, L_n^n) \otimes R.$$

By induction on n, we see that both $H^1(\Gamma, \mathcal{L}_n^i)$ and $H^1(\Gamma, (\mathcal{L}_n^i)^*(1))$ are coherent sheaves.

Now consider the case where $\Gamma = G_v$.

The sheaves

$$H^1(G_v, (\mathcal{L}_n^i)^*(1))$$

and

$$H^1(G_v, \mathcal{L}_n^i)$$

are locally free for $i \geq 2$, and we have arbitrary base-change

$$H^1(G_v, (\mathcal{L}_n^i)^*(1))(R) \otimes A = H^1(G_v, (\mathcal{L}_n^i)^*(1))(A);$$

$$H^1(G_v, \mathcal{L}_n^i)(R) \otimes A = H^1(G_v, \mathcal{L}_n^i)(A);$$

Global sheaves are more complicated in general.

The cup product pairings

$$H^2(G_v, \mathcal{L}_n^i)(R) \times H^0(G_v, (\mathcal{L}_n^i)^*(1))(R) \rightarrow H^2(G_v, \mathbb{Q}_p(1)) \otimes R \simeq R;$$

$$H^1(G_v, \mathcal{L}_n^i)(R) \times H^1(G_v, (\mathcal{L}_n^i)^*(1))(R) \rightarrow H^2(G_v, \mathbb{Q}_p(1)) \otimes R \simeq R.$$

define maps

$$H^0(G_v, (\mathcal{L}_n^i)^*(1))(R) \rightarrow H^2(G_v, \mathcal{L}_n^i)(R)^*;$$

$$H^1(G_v, (\mathcal{L}_n^i)^*(1))(R) \rightarrow H^1(G_v, \mathcal{L}_n^i)(R)^*,$$

which are isomorphisms for $i \geq 2$.

Back to $\mathbb{P}^1 \setminus \{0, 1, \infty\}$

$X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

U is freely generated by two elements e and f lifting generators of $U_1 = \mathbb{Q}_p(1) \oplus \mathbb{Q}_p(1)$.

However, using tangential basepoint, can make f stable under the Galois action:

$$gf = \chi(g)f.$$

$I \subset Lie(U)$: ideal generated by Lie monomials in e and f degree at least two in f.

$N = \mathrm{Lie}(U)/I$ and M corresponding quotient group of U.

$N_1 = Lie(U)_1 = H_1(\bar{X}, \mathbb{Q}_p)$.

$N_k^k = N^{k+1} \backslash N^k$ is one-dimensional, generated by $ad(e)^{k-1}(f)$.

We have a decomposition of Galois representations

$$N^2 = \oplus_{i=2}^{\infty} N^{i+1} \backslash N^i$$

with $N^{i+1} \backslash N^i \simeq \mathbb{Q}_p(i)$.

Structure of $N(c)$ for c non-trivial can be more complicated.

However,

$$H^2(\Gamma, N_n^n) = H^2(\Gamma, \mathbb{Q}_p(n)) = 0$$

for $n \geq 2$. Furthermore, there exists a $K \geq 2$ such that

$$H^2(\Gamma, (N_n^n)^*(1)) = 0$$

for $n \geq K$.

As a consequence, global cohomology variety is smooth, and

$$\dim H^2(\Gamma, N_n(c)), \quad \dim H^2(\Gamma, (N_n(c))^*(1))$$

are bounded independently of n and c.

Short exact sequences:

$$0 \to H^1(\Gamma, \mathcal{N}_n^n) \to H^1(\Gamma, \mathcal{N}_n^i) \to H^1(\Gamma, \mathcal{N}_{n-1}^i) \to 0$$

$$0 \to H^1(\Gamma, (\mathcal{N}_n^n)^*(1)) \to H^1(\Gamma, (\mathcal{N}_n^i)^*(1)) \to H^1(\Gamma, (\mathcal{N}_{n-1}^i)^*(1)) \to 0$$

of locally-free sheaves and arbitrary base-change

$$H^1(\Gamma, \mathcal{N}_n^i)(R) \otimes A \simeq H^1(\Gamma, \mathcal{N}_n^i)(A),$$

$$H^1(\Gamma, (\mathcal{N}_n^i)^*(1))(R) \otimes A \simeq H^1(\Gamma, (\mathcal{N}_n^i)^*(1))(A)$$

locally and globally, for $i \geq K$.

Some consequences:

-We have an embedding

$$H^1(G_T, (\mathcal{N}_n^i)^*(1)) \hookrightarrow \prod_{w|p} \mathrm{loc}_w^* H^1(G_v, (\mathcal{N}_n^i)^*(1))$$

as a local direct factor for $i \geq K$.

-After base change to any smooth curve mapping to $H^1(G_T, M_n)$, the image of the map

$$H^1(G_T, (\mathcal{N}_n^i)^*(1)) \rightarrow \prod_{w|p, w \neq v} \mathrm{loc}_w^* H^1(G_v, (\mathcal{N}_n^i)^*(1))$$

is a local direct factor for $i \geq K$.

-The kernel Ker_n^i of the the above map is a local direct factor that commutes with base-change for $i \geq K$.

Now we analyze all these objects at the tangential base-point.

Define

$$N_n^+ := \oplus_{K \leq i \leq n, \text{even}} N^i / N^{i+1}.$$

Proposition 0.2 *Let F be totally real. There is a subspace $Z_n^K \subset H^1(G_T, [N_n^K]^*(1))$ such that $loc_w(Z_n^K) = 0$ for $w \neq v$ and*

$$loc_v : Z_n \simeq H^1(G_v, [N_n^+]^*(1)).$$

Key point is that

$$N_n^K = \oplus_{i=K}^n N_i^i.$$

and

$$H^1(G_T, \mathbb{Q}_p(1-i)) \simeq \oplus_{w|p} H^1(G_w, \mathbb{Q}_p(1-i))$$

for $i \geq K$ even, while

$$H^1(G_T, \mathbb{Q}_p(1-i)) = 0$$

for $i \geq K$ odd.

By deforming this subspace to the nearby fibers, we get

Proposition 0.3 *Let F be totally real. At a generic point c, there is a subspace $Z_n^K(c) \subset H^1(G_T, (N_n^K(c))^*(1))$ of dimension $\geq \lfloor (n-K)/2 \rfloor$ such that*

$$loc_w(Z_n^K(c)) = 0$$

for $w \neq v$ and

$$loc_v : Z_n^K(c) \hookrightarrow H^1(G_v, (N_n^K(c))^*(1)).$$

Proposition 0.4 *Let F be totally real. Then for n sufficiently large, and generic c there is an element $z \in H^1(G_T, N_n^*(1)(c))$ such that $loc_w(z) = 0$ for $w \neq v$ and*

$$loc_v(z) \notin H_f^1(G_v, N_n^*(1)(c)).$$

Proof.

Note that $\dim Z_n^K(c) \geq \lfloor (n-K)/2 \rfloor$. From the exact sequence

$$0 \rightarrow [N_{K-1}(c)]^*(1) \rightarrow [N_n(c)]^*(1) \rightarrow [N_n^K(c)]^*(1) \rightarrow 0,$$

we get

$$0 \rightarrow H^1(G_T, [N_{K-1}(c)]^*(1)) \rightarrow H^1(G_T, [N_n(c)]^*(1)) \rightarrow$$

$$\rightarrow H^1(G_T, [N_n^K(c)]^*(1)) \rightarrow H^2(G_T, [N_{K-1}(c)]^*(1)),$$

and an exact sequence

$$0 \rightarrow H^1(G_T, [N_{K-1}(c)]^*(1)) \rightarrow H^1(G_T, [N_n(c)]^*(1)) \rightarrow Im_n \rightarrow 0,$$

for a subspace

$$Im_n \subset H^1(G_T, [N_n^K(c)]^*(1))$$

of codimension at most $\dim H^2(G_T, [N_{K-1}(c)]^*(1))$.

Now we consider

$$
\begin{array}{ccccc}
0\to & H^1(G_T,[N_{K-1}(c)]^*(1)) & \to & H^1(G_T,[N_n(c)]^*(1)) \\
 & \downarrow & & \downarrow \\
0\to & \oplus_{w\in T, w\neq v} H^1(G_w,[N_{K-1}(c)]^*(1)) & \to & \oplus_{w|p, w\neq v} H^1(G_w,[N_n(c)]^*(1)) \\
 & & & \\
 & \to & Im_n & \to 0 \\
 & & \downarrow & \\
 & \to & \oplus_{w|p, w\neq v} H^1(G_w,[N_n^K(c)]^*(1)) & \to 0
\end{array}
$$

Clearly,

$$\dim Z_n^K(c) \cap Im_n \to \infty$$

as $n \to \infty$. But the cokernel of

$$H^1(G_T, [N_{K-1}(c)]^*(1)) \to \oplus_{w|p, w \neq v} H^1(G_w, [N_{K-1}(c)]^*(1))$$

has of course dimension bounded independently of n.

So we see from the snake lemma that there is an element

$$z \in H^1(G_T, [N_n(c)]^*(1))$$

lifting an element of $Z_n(c) \cap Im_n$, such that

$$\mathrm{loc}_w(z) = 0$$

for $w \in T, w \neq v$ and

$$\mathrm{loc}_v(z) \neq 0.$$

In fact, since z is being chosen to map to a non-zero element of $\dim Z_n(c) \cap Im_n$ and $H^1_f(G_v, [N_n^K(c)]^*(1)) = 0$, we see that

$$\mathrm{loc}_v(z) \notin H^1_f(G_v, [N_n(c)]^*(1)).$$

$\square$

Corollary 0.5 *For n sufficiently large,*

$$T_c H^1_f(G_T, M_n) \rightarrow T_{loc_v(c)} H^1_f(G_v, M_n)$$

is not surjective.