Galois Theory and Diophantine geometry

Minhyong Kim

July, 2009

Cambridge
Diophantine geometry

- theory of motives
- anabelian geometry
I. Preliminary Remarks

Points of a motive $M$: 

$$\text{Ext}^1(\mathbb{Q}(0), M).$$

Problematic for direct Diophantine applications, except in the case of $M = H_1(A)$, $A$ an abelian variety. Consequence of abelian nature of the theory of motives.
When

$$(X, b)$$

is a compact smooth pointed curve of genus $\geq 2$ defined over $\mathbb{Q}$, anabelian geometry proposes to study instead non-abelian (continuous) cohomology

$$H^1(G, \pi^e_t(\bar{X}, b)),$$

the classifying space for $\pi^e_t(\bar{X}, b)$ torsors over $\text{Spec}(\mathbb{Q})$.

($G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$)
Equipped with natural non-abelian Albanese map:

\[ \kappa^{na} : X(\mathbb{Q}) \longrightarrow H^1(G, \pi^e_1(\bar{X}, b)); \]

\[ x \mapsto [\pi^e_1(\bar{X}; b, x)]. \]

The map does not extend to cycles.

From this point of view, \( H^1(G, \pi^e_1(\bar{X}, b)) \) should be viewed as an étale, non-abelian Jacobian.
It has distinct advantages over other non-abelian Jacobians, e.g., moduli spaces of vector bundles considered by Weil. (‘Généralisation des fonctions abéliennes.’)

These moduli spaces were also supposed to provide a ‘theory of non-abelian $\pi_1$’ defined over $\mathbb{Q}$, but could not be applied to Diophantine geometry.
Grothendieck’s section conjecture: $\kappa^{na}$ induces a bijection

$$X(\mathbb{Q}) \simeq H^1(G, \pi^e_1(\overline{X}, b)).$$

Remarks:
- Injectivity is a consequence of Mordell-Weil theorem.
- Difficulty is surjectivity:
  
  Every $\pi^e_1(\overline{X}, b)$-torsor is supposed to be a path torsor.
- Instructive to compare with the conjecture

\[ \hat{E}(\mathbb{Q}) \cong H_f^1(G, \pi_1(\bar{E}, e)) \]

for an elliptic curve \((E, e)\).

- Grothendieck’s conjecture implies that the set of rational points on a curve of higher genus has a natural categorical interpretation, \textit{purely in terms of the fundamental group}.
Interlude/Remark

Note that one can study the variation of

$$\pi_1(X; b, x)$$

as a function of $x$ in any theory of $\pi_1$ with flexible base-points, each time obtaining a classifying map

$$X \to H^1(\pi_1(X, b))$$

of sorts.
II. Unipotent Albanese maps

The *motivic fundamental group*

\[ \pi^M_1(\bar{X}, b) \]

lies between the pro-finite fundamental group and homology:

\[ \hat{\pi}_1(\bar{X}, b) \]

\[ \pi^M_1(\bar{X}, b) \]

\[ H_1(\bar{X}) \]
Correspondingly, we have the classifying space of motivic torsors

\[ H^1(G, \pi_1^M(\overline{X}, b)), \]

substantially more informative than \( \text{Ext}^1(\mathbb{Q}, h_1(X)) \), but much more tractable than \( H^1(G, \hat{\pi}_1(\overline{X}, b)) \).

Note: We will be discussing motives only at the level of certain realizations, so the classifying space is also a compatible system of classifying spaces.
The most important is the $\mathbb{Q}_p$-étale realization

$$U = U^{et} = \pi_{1,\mathbb{Q}_p}(\bar{X}, b),$$

for a prime $p$ of good reduction, where we have a tower of diagrams:

\[
\begin{array}{c}
\vdots \\
\vdots \\
H_f^1(G, U_4) \downarrow \\
H_f^1(G, U_3) \downarrow \\
H_f^1(G, U_2) \downarrow \\
H_f^1(G, U_1) = H_f^1(G, T_p \otimes \mathbb{Q}_p)
\end{array}
\]
Brief description of the constructions.

1. The étale site of $\bar{X}$ defines a category

$$\text{Un}(\bar{X}, \mathbb{Q}_p)$$

of locally constant unipotent $\mathbb{Q}_p$-sheaves on $\bar{X}$. A sheaf $\mathcal{V}$ is unipotent if it can be constructed using successive extensions by the constant sheaf $[\mathbb{Q}_p]_{\bar{X}}$.

2. We have a fiber functor

$$F_b : \text{Un}(\bar{X}, \mathbb{Q}_p) \rightarrow \text{Vect}_{\mathbb{Q}_p}$$

that associates to a sheaf $\mathcal{V}$ its stalk $\mathcal{V}_b$. Then

$$U := \text{Aut}^\otimes(F_b),$$

the tensor-compatible automorphisms of the functor. $U$ is a pro-algebraic pro-unipotent group over $\mathbb{Q}_p$. 
3. 

\[ U = U^1 \supset U^2 \supset U^3 \supset \cdots \]

is the descending central series of \( U \), and 

\[ U_n = U^{n+1} \backslash U \]

are the associated quotients. There is an identification

\[ U_1 = H_1^{et}(\bar{X}, \mathbb{Q}_p) = V_p(J) := T_pJ \otimes \mathbb{Q}_p \]

at the bottom level and exact sequences

\[ 0 \to U^{n+1} \backslash U^n \to U_n \to U_{n-1} \to 0 \]

for each \( n \).
4. $U$ has a natural action of $G$ lifting the action on $V_p$, and $H^1(G, U_n)$ denotes continuous Galois cohomology with values in the points of $U_n$. For $n \geq 2$, this is *non-abelian cohomology*, and hence, does not have the structure of a group.

5. $H^1_f(G, U_n) \subset H^1(G, U_n)$ denotes a subset defined by local ‘Selmer’ conditions that require the classes to be

(a) unramified outside the set $T = S \cup \{p\}$, where $S$ is the set of primes of bad reduction;

(b) and *crystalline* at $p$, a condition coming from $p$-adic Hodge theory.
6. The system

\[ \cdots \rightarrow H^1_f(G, U_{n+1}) \rightarrow H^1_f(G, U_n) \rightarrow H^1_f(G, U_{n-1}) \rightarrow \cdots \]

is a pro-algebraic variety, the *Selmer variety* of $X$. That is, each $H^1_f(G, U_n)$ is an algebraic variety over $\mathbb{Q}_p$ and the transition maps are algebraic.

\[ H^1_f(G, U) = \{ H^1_f(G, U_n) \} \]

is the moduli space of principal bundles for $U$ in the étale topology of $\text{Spec}(\mathbb{Z}[1/S])$ that are crystalline at $p$.

If $\mathbb{Q}_T$ denotes the maximal extension of $\mathbb{Q}$ unramified outside $T$ and $G_T := \text{Gal}(\mathbb{Q}_T/\mathbb{Q})$, then $H^1_f(G, U_n)$ is naturally realized as a closed subvariety of $H^1(G_T, U_n)$. 
For the latter, there are sequences

\[ 0 \to H^1(G_T, U^{n+1 \setminus U^n}) \to H^1(G_T, U_n) \to H^1(G_T, U_{n-1}) \xrightarrow{\delta} H^2(G_T, U^{n+1 \setminus U^n}) \]

exact in a natural sense, and the algebraic structures are built up iteratively from the \( \mathbb{Q}_p \)-vector space structure on the

\[ H^i(G_T, U^{n+1 \setminus U^n}) \]

using the fact that the boundary maps \( \delta \) are algebraic. (It is non-linear in general.)
7. The map

\[ \kappa^u = \{\kappa_n^u\} : X(\mathbb{Q}) \rightarrow H^1_f(G, U) \]

is defined by associating to a point \( x \) the principal \( U \)-bundle

\[ P(x) = \pi_{1,\mathbb{Q}_p}(\bar{X}; b, x) := \text{Isom}^\otimes(F_b, F_x) \]

of tensor-compatible isomorphisms from \( F_b \) to \( F_x \), that is, the \( \mathbb{Q}_p \)-pro-unipotent étale paths from \( b \) to \( x \).

For \( n = 1 \),

\[ \kappa_1^u : X(\mathbb{Q}) \rightarrow H^1_f(G, U_1) = H^1_f(G, T_p J \otimes \mathbb{Q}_p) \]

reduces to the map from Kummer theory. But the map \( \kappa_n^u \) for \( n \geq 2 \) does not factor through the Jacobian. Hence, suggests the possibility of separating the structure of \( X(\mathbb{Q}) \) from that of \( J(\mathbb{Q}) \).
8. If one restricts $U$ to the étale site of $\mathbb{Q}_p$, there are local analogues

$$\kappa_{p,n}^u : X(\mathbb{Q}_p) \to H^1_f(G_p, U_n)$$

that can be explicitly described using non-abelian $p$-adic Hodge theory. More precisely, there is a compatible family of isomorphisms

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

to homogeneous spaces for the \textit{De Rham fundamental group}

$$U^{DR} = \pi_1^{DR}(X \otimes \mathbb{Q}_p, b)$$

of $X \otimes \mathbb{Q}_p$.

$U^{DR}$ classifies unipotent vector bundles with flat connections on $X \otimes \mathbb{Q}_p$, and $U^{DR} / F^0$ classifies principal bundles for $U^{DR}$ with compatible Hodge filtrations and crystalline structures.
Given a crystalline principal bundle $P = \text{Spec}(\mathcal{P})$ for $U$,

$$D(P) = \text{Spec}(\mathcal{P} \otimes B_{cr}^G)^p),$$

where $B_{cr}$ is Fontaine’s ring of $p$-adic periods. This is a principal $U^{DR}$ bundle.

The two constructions fit into a diagram

$$
\begin{array}{ccc}
X(\mathbb{Q}_p) & \xrightarrow{\kappa_p^{na}} & H^1_f(G_p, U) \\
& \downarrow{\kappa_{\text{tr/cr}}} & D \\
& \downarrow{D} & U^{DR}/F^0 \\
& \downarrow{\kappa_{\text{tr/cr}}} & \\
& U^{DR}/F^0 & 
\end{array}
$$

whose commutativity reduces to the assertion that

$$\pi^{DR}_1(X \otimes \mathbb{Q}_p; b, x) \otimes B_{cr} \simeq \pi^{u, \mathbb{Q}_p}_1(\bar{X}; b, x) \otimes B_{cr}.$$
9. The map

\[ \kappa_{dr/cr}^u : X(\mathbb{Q}_p) \rightarrow U^{DR}/F^0 \]

is described using \( p \)-adic iterated integrals

\[ \int \alpha_1 \alpha_2 \cdots \alpha_n \]

of differential forms on \( X \), and has a highly transcendental natural:

For any residue disk \( \overline{y} \subset X(\mathbb{Q}_p) \),

\[ \kappa_{dr/cr,n}^u(\overline{y}) \subset U^{DR}_n/F^0 \]

is Zariski dense for each \( n \) and its coordinates can be described as convergent power series on the disk.
10. The local and global constructions fit into a family of commutative diagrams

\[
\begin{array}{ccc}
X(\mathbb{Q}) & \xrightarrow{} & X(\mathbb{Q}_p) \\
\downarrow & & \downarrow \\
H^1_f(G, U_n) & \xrightarrow{\text{loc}_p} & H^1_f(G_p, U_n) \\
& & \xrightarrow{D} U^{DR}_n/F^0
\end{array}
\]

where the bottom horizontal maps are algebraic, while the vertical maps are transcendental. Thus, the difficult inclusion \(X(\mathbb{Q}) \subset X(\mathbb{Q}_p)\) has been replaced by the algebraic map \(\log_p := D \circ \text{loc}_p\).
III. Diophantine Finiteness

Theorem 1 Suppose

$$\log_p(H_f^1(G, U_n)) \subset U_n^{DR}/F^0$$

is not Zariski dense for some $n$. Then $X(\mathbb{Q})$ is finite.
Idea of proof: There is a non-zero algebraic function $\phi$

$$
\begin{align*}
X(\mathbb{Q}) & \overset{\kappa_n^u}{\hookrightarrow} X(\mathbb{Q}_p) \\
H^1_f(G, U_n) & \overset{\log_p}{\longrightarrow} U^{DR}/F^0 \\
\end{align*}
$$

vanishing on $\log_p(H^1_f(G, U_n))$. Hence, $\phi \circ \kappa_{dr/cr,n}^u$ vanishes on $X(\mathbb{Q})$. But using the comparison with the De Rham realization, we see that this function is a non-vanishing convergent power series on each residue disk. $\square$
Hypothesis of the theorem expected to always hold for \( n \) sufficiently large, but difficult to prove. Key necessary (unproven) lemma is

\[ H_f^1(G, M) = 0 \]

for a motivic Galois representation \( M \) of weight > 0.

Note that Grothendieck expected

Non-abelian ‘finiteness of III’ (= \textit{section conjecture}) \(\Rightarrow\) finiteness of \( X(\mathbb{Q}) \).

Instead we have:

‘Higher abelian finiteness of III’ \(\Rightarrow\) finiteness of \( X(\mathbb{Q}) \).
Can prove the hypothesis (and hence, finiteness of points) in cases where the image of $G$ inside $\text{Aut}(H_1(\bar{X}, \mathbb{Z}_p))$ is essentially abelian. That is, when

- $X$ is affine hyperbolic of genus zero;
- $X = E \setminus \{e\}$ where $E$ is an elliptic curve with complex multiplication;
- (with John Coates) $X$ compact of genus $\geq 2$ and $J_X$ factors into abelian varieties with potential complex multiplication.

In the CM cases, need to choose $p$ to split inside the CM fields.
Idea: Construct the quotient

\[ U \longrightarrow W := U / [[U, U], [U, U]] \]

and a diagram

\[
\begin{array}{cccccc}
X(\mathbb{Z}_S) & \subset & X(\mathbb{Z}_p) & \quad & \quad & \quad & \quad \\
\kappa^u_n & & \kappa^u_{p,n} & \quad & \kappa_{\text{dr/cr},n} & \\
H^1_f(G, U_n) & \xrightarrow{\text{loc}_p} & H^1_f(G_p, U_n) & \xrightarrow{D} & U_n^{DR}/F^0 \\
& & & & \downarrow & \\
& & & & \downarrow & \\
H^1_f(G, W_n) & \xrightarrow{\text{loc}_p} & H^1_f(G_p, W_n) & \xrightarrow{D} & W_n^{DR}/F^0 & \\
\end{array}
\]
Theorem 2 (with John Coates) Suppose $J$ is isogenous to a product of abelian varieties having potential complex multiplication. Choose the prime $p$ to split in all the CM fields that occur. Then

$$\dim H_f^1(G, W_n) < \dim W_n^{DR} / F^0$$

for $n$ sufficiently large.
Outline of proof when $J_X$ is simple:

Via the exact sequences

$$0 \rightarrow H^1(G_T, W^{n+1} \setminus W^n) \rightarrow H^1(G_T, W_n) \rightarrow H^1(G_T, W_{n-1})$$

we get

$$\dim H^1_f(G, W_n) \leq \dim H^1(G_T, W_n) \leq \sum_{i=1}^{n} \dim H^1(G_T, W^{i+1} \setminus W^i).$$

reducing the problem to the study of the vector spaces $W^{i+1} \setminus W^i$ for which there are Euler characteristic formulas:

$$\dim H^0(G_T, W^{i+1} \setminus W^i) - \dim H^1(G_T, W^{i+1} \setminus W^i) + \dim H^2(G_T, W^{i+1} \setminus W^i) = -\dim [W^{i+1} \setminus W^i]^-.$$
But the $H^0$ term always, vanishes:

$$\dim H^1(G_T, W^{i+1 \setminus W^i}) = \dim [W^{i+1 \setminus W^i}]^- + \dim H^2(G_T, W^{i+1 \setminus W^i}).$$

A simple combinatorial count of elements in a Hall basis shows that

$$\sum_{i=1}^{n} \dim [W^{i+1 \setminus W^i}]^- \leq \frac{(2g-1)}{2} \frac{n^{2g}}{(2g)!} + O(n^{2g-1})$$
Similarly, on the De Rham side:

\[
\dim W_n^{DR}/F^0 = W_2/F^0 + \sum_{i=3}^{n} \dim [W^{DR,i+1}\setminus W^{DR,i}]
\]

\[
\geq (2g - 2) \frac{n^{2g}}{(2g)!} + O(n^{2g-1}).
\]

Hence, since \(g \geq 2\), we have

\[
\sum_{i=1}^{n} \dim [W^{i+1}\setminus W^{i}] < \dim W_n^{DR}/F^0.
\]

Therefore, it suffices to show that

\[
\sum_{i=1}^{n} \dim H^2(G_T, W^{i+1}\setminus W^{i}) = O(n^{2g-1}).
\]
Poitou-Tate duality eventually reduces this to the study of

$$\text{Hom}_\Gamma(M(-1), \sum_{i=1}^n [W^{i+1}\backslash W^i]^*),}$$

where

- $F$ is a field of definition for all CM and containing $\mathbb{Q}(J[p])$,
- $\Gamma = \text{Gal}(F_\infty/F)$ for the field $F_\infty = F(J[p^\infty])$ generated by the $p$-power torsion of $J$
- and

$$M = \text{Gal}(H/F_\infty)$$

is the Galois group of the $p$-Hilbert class field $H$ of $F_\infty$. 
Choosing an annihilator

\[ \mathcal{L} \in \Lambda := \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T_1, T_2, \ldots, T_{2g}]] \]

for \( M(-1) \), we need to count its zeros among the characters that appear in

\[ \sum_{i=1}^{n} [W^{i+1}\backslash W^i]^*. \]

If we denote by \( \{\psi_i\}_{i=1}^{2g} \) the characters in \( H^1(\bar{X}, \mathbb{Q}_p) \), the characters in \( [W^{i+1}\backslash W^i]^* \) are a subset of

\[ \psi_{j_1} \psi_{j_2} \psi_{j_3} \cdots \psi_{j_i}, \]

where \( j_1 < j_2 \geq j_3 \geq \cdots \geq j_i \).
A lemma of Greenberg allows us to reduce to the case where

\[ \mathcal{L} = a_0(T_1, \ldots, T_{2g-1}) + a_1(T_1, \ldots, T_{2g-1})T_{2g} + \cdots \]

\[ + a_{l-1}(T_1, \ldots, T_{2g-1})T_{2g}^{l-1} + T_{2g}^l, \]

a polynomial in the last variable.

Since \( M(-1) \) is \( \Lambda \)-finite-generated, another elementary estimate gives us the bound

\[ \text{Hom}_\Gamma(M(-1), \sum_{i=1}^n [W^{i+1}\setminus W^i]^*) = O(n^{2g-1}) \]

desired.
Remarks:

-In some sense, the finiteness of $X(\mathbb{Q})$ is accounted for by the ‘sparseness of zeros of $\mathcal{L}$,’ an algebraic $p$-adic $L$-function of sorts.

-Contained in the proof is a rather obvious suggestion of a non-abelian analogue that would give finiteness over $\mathbb{Q}$ for any curve of higher genus.
IV. Explicit annihilation of points: an example

A reasonable short term goal is to exhibit explicitly the $\phi$ in the proof of finiteness:

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

$$H^1_f(G, U_n) \xrightarrow{\log_p} U^{DR}/F^0$$

$$\exists \phi \neq 0$$

$$\mathbb{Q}_p$$
using the *cohomological construction* of a function \( \psi \) as below that vanishes on global classes

\[
\begin{align*}
X(\mathbb{Q}) & \to X(\mathbb{Q}_p) \\
\downarrow & \downarrow \\
H^1_f(G, U_n) & \xrightarrow{\text{loc}_p} H^1_f(G_p, U_n) \\
\downarrow & \downarrow \\
\mathbb{Q}_p & \to \mathbb{Q}_p
\end{align*}
\]

where the vanishing should be explained by a reciprocity law.
Example:

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

\[
\begin{array}{c}
X(\mathbb{Z}) \xrightarrow{\text{loc}_p} X(\mathbb{Z}_p) \\
\downarrow \quad \quad \downarrow \\
H^1_{f,\mathbb{Z}}(G, U_2) \xrightarrow{\text{loc}_p} H^1_f(G_p, U_2) \xrightarrow{D} U_2^{DR}/F^0 \\
\downarrow \quad \downarrow \quad \downarrow \\
\mathbb{Q}_p.
\end{array}
\]

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

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

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

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 3 $\psi$ vanishes on the image of

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

Proof is a simple consequence of

$$0 \to H^2(G_T, \mathbb{Q}_p(1)) \to \bigoplus_{v \in T} H^2(G_v, \mathbb{Q}_p(1)) \to \mathbb{Q}_p \to 0.$$
Explicit formula on De Rham side:

Choose a Weierstrass equation for $E$ and let

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

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 4 For any two points \( y, z \in X(\mathbb{Z}) \subset X(\mathbb{Z}_p) \), we have
\[
\log_2^2(y)(D_2(z) - \log_\alpha(z) \log_\beta(z)) = \log_2^2(z)(D_2(y) - \log_\alpha(y) \log_\beta(y)).
\]

Uses action of the multiplicative monoid \( \mathbb{Q}_p \) on \( H^1_f(G, U_2) \) covering the scalar multiplication on \( E(\mathbb{Q}) \otimes \mathbb{Q}_p \). Evaluate \( \psi \) on
\[
\log_\alpha(x) \kappa_2^u(y) - \log_\alpha(y) \kappa_2^u(x) \in H^1_f(G_p, U^3 \setminus U^2).
\]
V. Preliminary Remark

Galois theory according to Galois:

Groups encode structural properties of Diophantine geometry in dimension zero. (Polynomials in one variable.)
Consequently, Galois theory for polynomials of two-variables should propose a unified categorical framework relevant to Diophantine geometry in dimension one incorporating the known ingredients:

$L$-functions, arithmetic fundamental groups, groupoids of torsors and their moduli spaces, ...?