Galois Theory and Diophantine geometry

Minhyong Kim

July, 2009

Durham

Preliminary Remark

In a number of situations, Galois cohomology provides a *descent algorithm* for computing the set of rational points of a variety.

-Algorithms related to sophisticated refinements of the Hasse principle. Often associated with *simple* varieties.

-Conjectural algorithms at the boundary of simplicity; especially, abelian varieties.

-Conjectural algorithms for generic varieties?

Review of descent for elliptic curves

(E, e) elliptic curve over $\mathbb{Q}$.

$G = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

Fix a prime p (often $p = 2$).

We have

$$0 \to E[p^n] \to E(\bar{\mathbb{Q}}) \xrightarrow{p^n} E(\bar{\mathbb{Q}}) \to 0,$$

an exact sequence compatible with G-action.

This leads to an long exact sequence of Galois cohomology

$$0 \to E(\mathbb{Q})[p^n] \to E(\mathbb{Q}) \xrightarrow{p^n} E(\mathbb{Q}) \xrightarrow{\kappa_n} H^1(G, E[p^n]) \to H^1(G, E)[p^n] \to$$

and an inclusion

$$E(\mathbb{Q})/p^n \hookrightarrow H^1(G, E[p^n]).$$

The image is in fact severely constrained:

$$E(\mathbb{Q})/p^n \hookrightarrow H^1_f(G, E[p^n]) \subset H^1(G, E[p^n]).$$

The subspace $H^1_f(G, E[p^n])$ can be defined by 'local' Galois theory, and can be computed, in principle. For example, it is often realized as a computable subspace of

$$\mathrm{Hom}_N(C, E[p^n]),$$

where

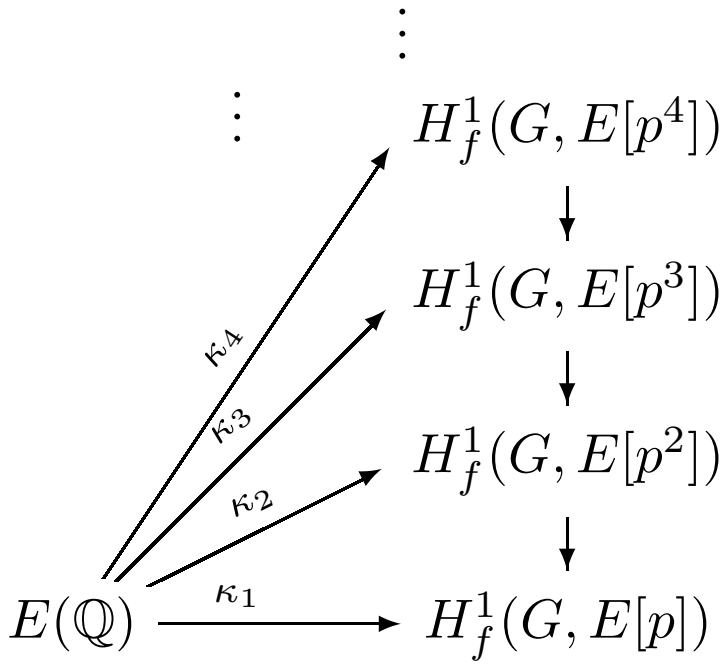
$$N = \mathrm{Gal}(F_n/\mathbb{Q})$$

for the field

$$F_n = \mathbb{Q}(E[p^n])$$

generated by the coordinates of $E[p^n]$, and C is a suitable generalized ideal class group of F_n.

The maps fit into a tower:



using which one can attempt to compute $E(\mathbb{Q})$.

There is in fact a decreasing sequence of subspaces

$$\cdots H^1_f(G, E[p])_4 \subset H^1_f(G, E[p])_3 \subset H^1_f(G, E[p])_2 \subset H^1_f(G, E[p])$$

where

$$H^1_f(G, E[p])_i \subset H^1_f(G, E[p])$$

consists of those elements that lift to $H^1_f(G, E[p^i])$. On the other hand, there is an *increasing* sequence of subsets

$$E(\mathbb{Q})_{\leq 1}/p \subset E(\mathbb{Q})_{\leq 3}/p \subset E(\mathbb{Q})_{\leq 3}/p \subset \cdots \subset \cap_i H^1_f(G, E[p])_i,$$

consisting of those classes $E(\mathbb{Q})_{\leq i}/p$ coming from the points in $E(\mathbb{Q})$ of height $\leq i$.

That

$$E(\mathbb{Q})_{\leq m}/p = H^1_f(G, E[p])_n$$

eventually is a consequence of the *finiteness of the Tate-Shafarevich group*, which implies that

$$E(\mathbb{Q}) \otimes \mathbb{Z}_p \simeq \varprojlim H^1_f(G, E[p^n]).$$

This finiteness is a key component of the conjecture of Birch and Swinnerton-Dyer.

At this point, we would have

$$E(\mathbb{Q})_{\leq m}/p = E(\mathbb{Q})/p \simeq H^1_f(G, E[p])_n$$

and be able to compute the rank of $E(\mathbb{Q})$ as well as a set of rational points generating a subspace of maximal rank. It is then straightforward to compute from these actual generators of $E(\mathbb{Q})$.

Strategy:

1. Find a computable ambient space, e.g., $H^1_f(G, E[p])$ inside which to encode points.

2. Carve out the space of actual points inside this ambient space using a conjunction of *a nested sequence of cohomological constraints* and *searching*.

A deep assertion (e.g. finiteness of Sha) provides the *termination* of this algorithm.

Non-abelian descent

(X, b), pointed projective smooth curve of genus at least 2 defined over $\mathbb{Q}$.

Approach $X(\mathbb{Q})$ along two complementary paths:

1. Motivic descent;
2. Non-abelian profinite descent.

Categorical Context

Study points $x \in X$ via homotopy classes of paths

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

as x varies. Endowed with *torsor* structure coming from action of $\pi_1(X, b)$. Also various arithmetic structures corresponding to different theories of π_1. Thus, the study of points leads to the study of variation inside a moduli space of torsors for $\pi_1(X, b)$, realized as a non-abelian cohomology space.

This variation is entirely canonical, but involves *homotopy* rather than homology, and hence, tends away from the realm of motives.

Recall that the profinite fundamental group $\pi_1^{et}(\bar{X}, b)$ is constructed from the category $Cov(\bar{X})$ of étale covers of $\bar{X}$ as the automorphism group of the fiber functor

$$F_b : Cov(\bar{X}) \rightarrow \text{Set},$$

while the space of profinite paths is defined as

$$\pi_1^{et}(\bar{X}; b, x) := Isom(F_b, F_x).$$

Similarly, the *motivic fundamental group*

$$U = \pi_1^{\mathcal{M}}(\bar{X}, b)$$

and path torsors

$$P(x) := \pi_1^{\mathcal{M}}(\bar{X}; b, x)$$

consist of various realizations constructed from fiber functors on natural Tannakian categories over $\bar{X}$.

Category

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

of unipotent $\mathbb{Q}_p$-lisse sheaves on $\bar{X}$ equipped with a fiber functor

$$F_b^{et} : \mathrm{Un}(\bar{X}, \mathbb{Q}_p) \to \mathrm{Vect}_{\mathbb{Q}_p}$$

taking a sheaf to its stalk at b. Then

$$U^{et} := \mathrm{Aut}^{\otimes}(F_b);$$

$$P^{et}(x) := \mathrm{Isom}^{\otimes}(F_b, F_x).$$

Category

$$\mathrm{Un}(X_{\mathbb{Q}_p}, DR)$$

of unipotent vector bundles with connection on $X_{\mathbb{Q}_p}$ equipped with a fiber functor

$$F_b^{DR} : \mathrm{Un}(X_{\mathbb{Q}_p}, DR) \to \mathrm{Vect}_{\mathbb{Q}_p}$$

taking a bundle to its fiber at b. Then

$$U^{DR} := \mathrm{Aut}^{\otimes}(F_b^{DR});$$

$$P^{DR}(x) := \mathrm{Isom}^{\otimes}(F_b^{DR}, F_x^{DR}).$$

These spaces also have Hodge filtrations F^* and crystalline structures, that is, an action of Frobenius coming from comparison with a crystalline fundamental group.

The classifying map: profinite version

Grothendieck's *section conjecture*:

$$X(\mathbb{Q}) \simeq H^1(G, \pi_1^{et}(\bar{X}, b))$$

via the map

$$x \mapsto [\pi_1^{et}(\bar{X}; b, x)].$$

Non-abelian analogue of the finiteness conjecture for Tate-Shafarevich groups.

The classifying map: motivic version

The *motivic fundamental group* lies between pro-finite fundamental groups and homology in complexity:

$$\begin{array}{c} \hat{\pi}_1(\bar{X}, b) \\ | \\ \pi_1^{\mathcal{M}}(\bar{X}, b) \\ | \\ H_1(\bar{X}) \end{array}$$

The motivic classifying map is defined using motivic paths

$$X(\mathbb{Q}) \to H^1_{\mathcal{M}}(G, U);$$

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

except the target space needs clarification.

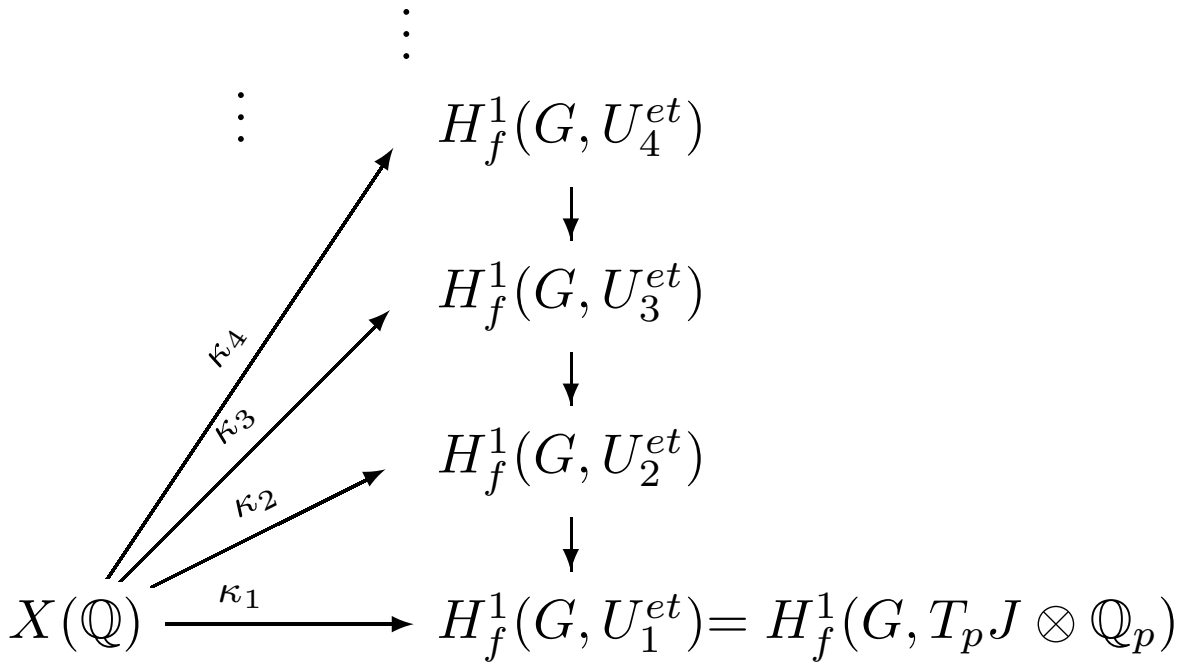
Motivic descent

The most important component of the classifying map is the $\mathbb{Q}_p$-étale realization:

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

$$x \mapsto [P^{et}(x)],$$

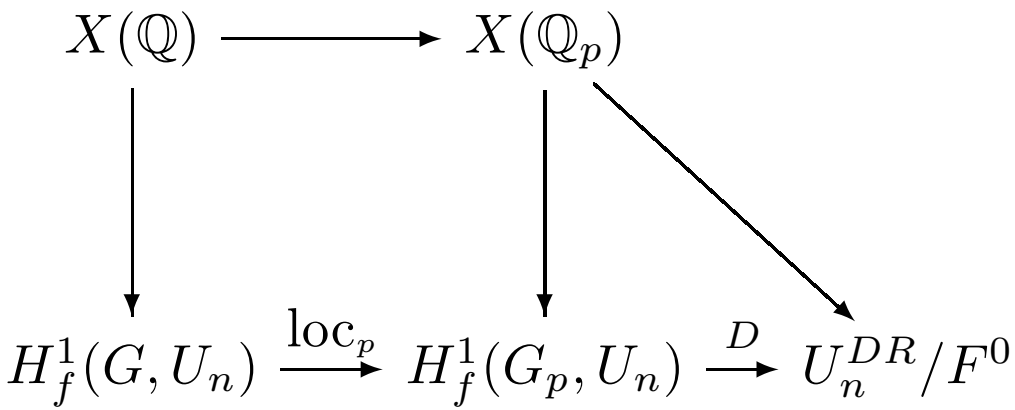
This map is actually a tower coming from the descending central series of U:



corresponding to motivic descent.

At the bottom we have the usual Tate module T_pJ of the Jacobian J of X.

The tower has other realizations that fit into commutative diagrams



where the bottom horizontal maps occur in the category of algebraic varieties, 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 $D \circ \mathrm{loc}_p$.

The De Rham/crystalline fundamental group U^{DR} is equipped with a Frobenius action and a Hodge filtration

$$U^{DR} \supset \cdots F^{-n} \supset \cdots F^{-1} \supset F^0$$

by subgroups, so that

$$U^{DR}/F^0$$

classifies torsors with compatible De Rham/crystalline structures. The map

$$X(\mathbb{Q}_p) \to U^{DR}/F^0$$

sends a point x to the set $P^{DR}(x)$ of De Rham/crystalline paths from b to x.

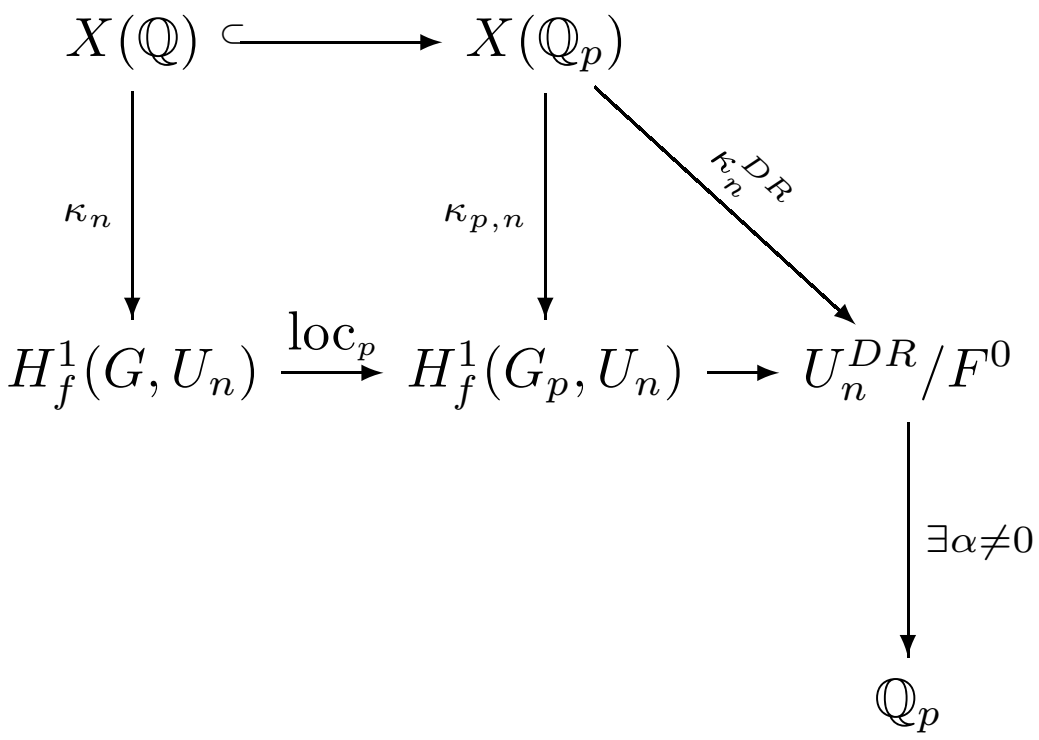
Theorem 1 *Suppose*

$$D \circ loc_p(H^1_f(G, U_n)) \subset U_n^{DR}/F^0$$

is not Zariski dense for some n. Then $X(\mathbb{Q})$ is finite.

Can use this to prove finiteness of points on some families of curves, e.g., Fermat curves.

Idea of proof: There is a non-zero algebraic function α



vanishing on $D \circ \mathrm{loc}_p[H^1_f(G, U_n)]$. Hence, $\alpha \circ \kappa_n^{DR}$ vanishes on $X(\mathbb{Q})$. But this function is a non-vanishing convergent power series on each residue disk. $\square$

The last assertion relies on an explicit computation of the map

$$X(\mathbb{Q}_p) \to U^{DR}/F^0$$

in terms of *p-adic iterated integrals*.

Furthermore,

the algebraic map

$$H^1_f(G, U_n) \xrightarrow{\mathrm{loc}_p} H^1_f(G_p, U_n) \xrightarrow{D} U^{DR}/F^0$$

can be computed in principle.

(Hypothesis H).

Assuming standard motivic conjectures, e.g., the Fontaine-Mazur conjecture on representations of geometric origin, one can effectively compute an n such that the hypothesis is satisfied. Thus, the F-M conjecture provides an explicit α such that $\alpha \circ \kappa_n^{DR}$ vanishes on $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$.

With a sufficiently accurate knowledge of α, we can compute a lower bound for the distance between the zeros of α on the residue disks of $X(\mathbb{Q}_p) = X(\mathbb{Z}_p)$. Use this to find m such that the zeros of α are separated modulo p^m, leaving us with an injection

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{Z}/p^m).$$

From this, we get an injection

$$X(\mathbb{Q}) \hookrightarrow J(\mathbb{Z}/p^m)$$

and hence, an injection

$$X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})/NJ(\mathbb{Q})$$

for $N = |J(\mathbb{Z}/p^m)|$.

Thus, we have also an injection

$$X(\mathbb{Q}) \hookrightarrow H^1_f(G, J[N]) \subset H^1(G_T, J[N]),$$

where $T = S \cup \{p\} \cup \{l \ : \ l|N\}$ with S the set of primes of bad reduction for X, and $G_T = \mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$ for the maximal extension $\mathbb{Q}_T$ of $\mathbb{Q}$ unramified outside T. Therefore, the motivic theory has provided us with an ambient space

$$H^1(G_T, J[N])$$

inside which to start the descent.

Non-abelian profinite descent

$$J[N] \simeq \pi^{et,ab}(\bar{X}, b)/N$$

is a quotient of $\pi_1^{et}(\bar{X}, b)$. Let A_i be a cofinal system of finite quotient groups of $\pi_1^{et}(\bar{X}, b)$, so that $A_0 = J[N]$ and having the property that

$$H^1(G, \pi_1^{et}(\bar{X}, b)) = \varprojlim H^1(G_i, A_i)$$

for some inverse system of restricted ramification Galois groups G_i with $G_0 = G_T$.

Eventually, we have maps

$$\begin{array}{ccccccc} \cdots & H^1(G_{i+2}, A_{i+2}) & \to & H^1(G_{i+1}, A_{i+1}) & \to & H^1(G_i, A_i) & \cdots \\ & \downarrow & & \downarrow & & \downarrow & \\ \cdots & Im_{i+2} & \hookrightarrow & Im_{i+1} & \hookrightarrow & Im_i & \cdots \end{array}$$

leading to a decreasing sequence of subsets Im_i of

$$H^1(G_T, J[N]).$$

Since we are dealing with *finite* Galois cohomology, everything is in principle computable.

Meanwhile, there is also an increasing sequence of subsets

$$\cdots X(\mathbb{Q})_{\leq i} \subset X(\mathbb{Q})_{\leq i+1} \subset X(\mathbb{Q})_{\leq i+2} \subset \cdots$$

coming from points of increasing height.

The section conjecture implies that the two nested sequence of subsets have to meet eventually, i.e.,

$$X(\mathbb{Q})_m = H^1(G_T, J[N])_n$$

for some m and n, at which point we can conclude

$$X(\mathbb{Q})_m = X(\mathbb{Q}).$$

Thus, we have a a *terminating algorithm* of *non-abelian descent.*

Completes the analogy between the section conjecture and BSD.

Main input of motivic theory, in particular, non-archimedean, non-abelian Hodge theory:

> *effective lower bound for distances between all points at one non-Archimedean place.*

Compare with usual approach to effective Mordell, where one seeks

> *effective upper bound for heights*

or equivalently,

> *an effective lower bound for the distance from one fixed point at all places.*

Remark on base-points: The original section conjecture considers the exact sequence

$$0 \to \pi_1^{et}(\bar{X}, b) \to \pi_1^{et}(X) \to G \to 0$$

and proposes that conjugacy classes of splittings for this sequence should correspond exactly to the rational points of X. Our discussion assumed that we have one rational base-point b to start with. But Ambrus Pal shows that the original section conjecture also gives an algorithm for determining the existence of a point.

That is, we have

Section conjecture+ Fontaine-Mazur conjecure+hypothesis H $\Rightarrow$ $X(\mathbb{Q})$ is computable for curves of genus ≥ 2.

(Non-)Example

Let (E, e) be the Weierstrass minimal model for an elliptic curve over $\mathbb{Q}$ of analytic rank 1.

Let $X = E \setminus \{e\}$. Assume we have an integral point $b \in X(\mathbb{Z})$ already and let

$$\log_1(z) := \int_v^z dx/y,$$

$$\log_2(z) := \int_v^z x dx/y$$

$$D(z) = \int_v^z (dx/y)(x dx/y),$$

where v is a tangential base-point at the origin.

Then the set of integral points

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

lies inside the zero set of the analytic function

$$(\log_1(b))^2(D_2(z) - (1/2)\log_1(z)\log_2(z))$$

$$-(\log_1(z))^2(D_2(b) - (1/2)\log_1(b)\log_2(b)).$$

Philosophical summary

Galois theory according to Galois proposes group theory to encode Diophantine geometry in dimension zero. (Polynomials in one variable.)

Need to extend Galois theory include categorical structures relevant to Diophantine geometry in dimension one. (Polynomials in two variables.)

Arithmetic fundamental groups, moduli space of torsors, ...