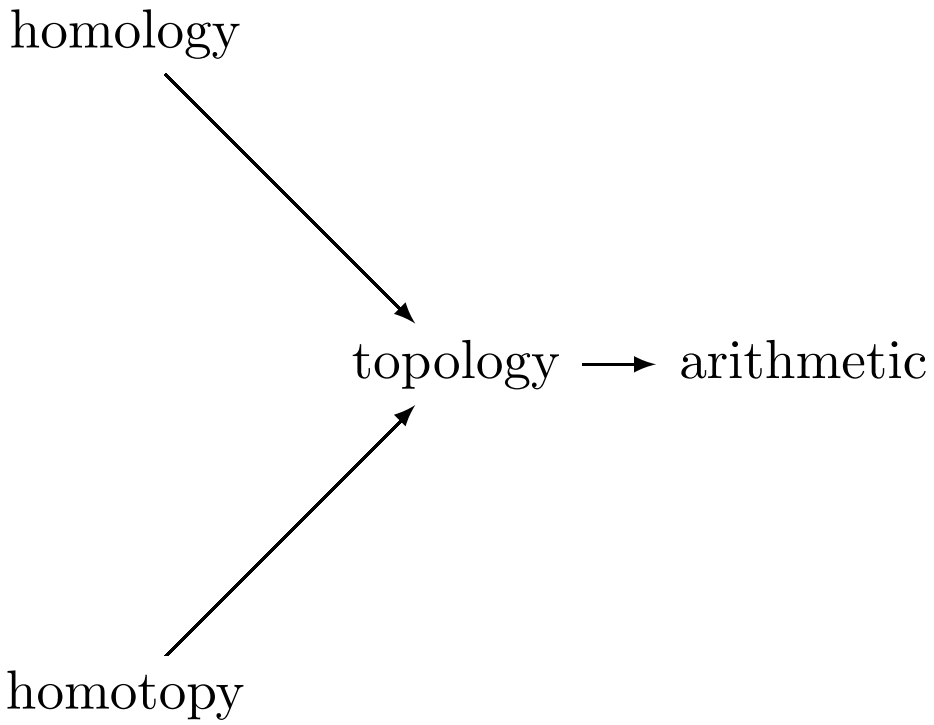
Fundamental groups and Diophantine geometry

Minhyong Kim

October 18, 2006


homology
topology
arithmetic
homotopy

Grothendieck:

arithmetic topology=arithmetic geometry

for *anabelian schemes*, in a manner analogous to *hyperbolic manifolds*.

$X/\mathbb{Q}$ compact smooth hyperbolic curve.

$\mathrm{Cov}(\bar{X})$ category of finite étale coverings of $\bar{X}$.

$b \in X(\mathbb{Q})$ rational point. Determines a fiber functor

$F_b : \mathrm{Cov}(\bar{X}) \to$ Finite Sets

$$\begin{array}{ccc} Y & & Y_b \\ \downarrow & \mapsto & \downarrow \\ X & & b \end{array}$$

$$\hat{\pi}_1(\bar{X}, b) := Aut(F_b)$$

For any other point $x \in X(\mathbb{Q})$, have the *torsor of paths*

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

All carry actions of $\Gamma := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, i.e., are Γ-equivariant torsors. Classified by continuous non-abelian cohomology set:

$$H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

That is, given a torsor P, choosing a point an element $p \in P$ and measuring its lack of Γ-invariance determines a function

$$g \in G \mapsto c(g) \in \hat{\pi}_1(\bar{X}, b)$$

characterized by

$$g(p) = pc(g)$$

Thus, we have a map

$$\hat{\kappa} : X(\mathbb{Q}) \to H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

$$x \mapsto [\hat{\pi}_1(\bar{X}; b, x)]$$

Grothendieck's section conjecture:

$\hat{\kappa}$ is a bijection.

Remarks:

- Injectivity known (Mordell-Weil $\Rightarrow$ non-abelian Mordell-Weil). Surjectivity appears very difficult.

-Grothendieck and Deligne expected the conjecture to be relevant to Diophantine geometry, especially the theorem of Faltings. Initial expectation appears to have been erroneous.

-Two separate deep problems:

(1) section conjecture itself;

(2) 'section conjecture implies Mordell conjecture.'

Wish to pursue (2) and the general question of the section conjecture's relevance to Diophantine geometry.

Concentrate on analogy to Birch and Swinnerton-Dyer:

For (E, e) an elliptic curve,

$$\hat{\kappa} : \widehat{E(\mathbb{Q})} \to H^1_f(\Gamma, \hat{\pi}_1(\bar{E}, e))$$

is a bijection.

Grothendieck's conjecture is a *higher-genus non-abelian* analogue.

In the abelian case, the target is a *Selmer group* that can be

(a) computed (in principle) ← Cremona's algorithms;

(b) controlled (occasionally) ← method of Kolyvagin and Kato;

(a) involves descent and searching for points in order of height.

(b) involves critically technology of *motives*: L-functions, Iwasawa theory, duality, Hodge theory, ...

Non-abelian analogues?

Some beginnings...

Basic tool: Motivic fundamental group U^M.

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

$$|$$

$$U^M$$

$$|$$

$$H_1(\bar{X})_{\mathbb{Q}}$$

Many different components, of which our interest will primarily be in p-adic realization.

Over $\mathbb{C}$, can take discrete group $\pi_1(X(\mathbb{C}), b)$ and consider $\mathbb{Q}$-unipotent completion,

$$\pi_1 \otimes \mathbb{Q}$$

defined as the group-like elements in completed Hopf algebra

$$\varprojlim_n \mathbb{Q}[\pi_1]/I^n$$

where $I \subset \mathbb{Q}[\pi_1]$ is the augmentation ideal.

Also, view as Tannaka dual to category

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

of unipotent $\mathbb{Q}$-local systems on $X(\mathbb{C})$.

That is,

$$\pi_1(X(\mathbb{C}), b) \otimes \mathbb{Q} = Aut^{\otimes}(F_b)$$

where

$$F_b : \mathrm{Un}(X(\mathbb{C}), \mathbb{Q}) \mapsto Vect_{\mathbb{Q}}$$

$$\mathcal{L} \mapsto \mathcal{L}_b$$

Well-known machinery extends this definition to many different settings including étale, De Rham, and crystalline. Just need the right category to play role of $\mathrm{Un}(X(\mathbb{C}), \mathbb{Q})$.

Étale realization:

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

is the category of unipotent $\mathbb{Q}_p$-lisse sheaves on $\bar{X}_{et}$ and

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

where

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

$$\mathcal{L} \mapsto \mathcal{L}_b$$

De Rham realization:

$$\mathrm{Un}^{dr}(X \otimes \mathbb{Q}_p)$$

category of of unipotent vector bundles with flat connection on $X \otimes \mathbb{Q}_p$.

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

$$F_b : \mathrm{Un}^{dr}(X \otimes \mathbb{Q}_p) \to \mathrm{Vect}_{\mathbb{Q}_p}$$

$$(V, \nabla) \mapsto V_b$$

Crystalline realization: p prime of good reduction and $Y = X \mathrm{mod}\ p$. $\bar{b} \in Y(\mathbb{F}_p)$.

$$\mathrm{Un}^{cr}(Y)$$

is then the category of unipotent over-convergent isocrystals, thought of as connections on $X \otimes \mathbb{Q}_p$.

$$U^{cr} := Aut^{\otimes}(F_{\bar{b}})$$

$$F_{\bar{b}} : \mathrm{Un}^{cr}(Y) \rightarrow \mathrm{Vect}_{\mathbb{Q}_p}$$

$$(V, \nabla) \mapsto V(]\bar{b}[)^{\nabla=0}$$

In all realizations, also have path spaces

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

for points $x \in X$ which are torsors for U. Can study their variation as x varies. In contrast to pro-finite theory, variation has an analytic structure, rendering it easier to study.

All the groups and torsors carry extra structures. Most importantly, action of $\Gamma = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on U^{et} and $P^{et}(x)$. These structures are compatible under comparison isomorphisms.

Taken together, they constitute the *motivic fundamental group* U^M and motivic path torsors $P^M(x)$.

In various settings need to consider finite-dimensional quotients

$$U_n = (U)^n \backslash U$$

where the descending central series on U is given by $U^1 = U$, $U^{n+1} = [U, U^n]$. Get thereby an inductive structure

$$0 \to U^{n+1} \backslash U^n \to U_{n+1} \to U_n \to 0$$

that is important for reducing the study of U^M to vector groups, i.e., $(U^M)^{n+1} \backslash (U^M)^n$.

We have

Non-abelian Selmer variety

$$H^1_f(\Gamma, U^{et})$$

classifying torsors for U^{et} with compatible Γ-action.

Continuous cohomology with values in $\mathbb{Q}_p$-points of U^{et}. Contrary to pro-finite case, have natural local conditions requiring that torsors be unramified outside the set of primes of bad reduction and crystalline at p indicated by subscript f.

These have natural structure of pro-algebraic varieties over $\mathbb{Q}_p$ built up inductively from the case of $U^{n+1} \backslash U^n$.

We have

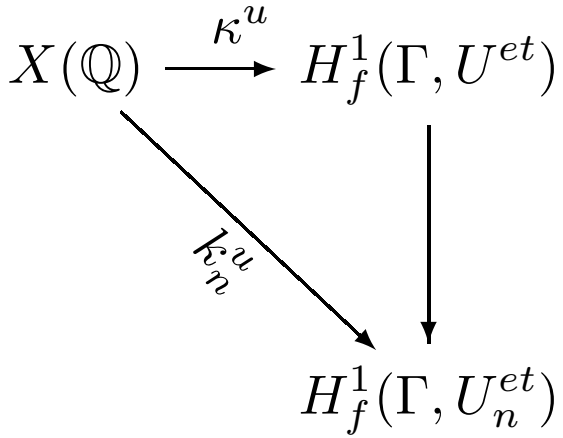
the unipotent Kummer map

$$\kappa^u : X(\mathbb{Q}) \to H^1_f(\Gamma, U^{et})$$

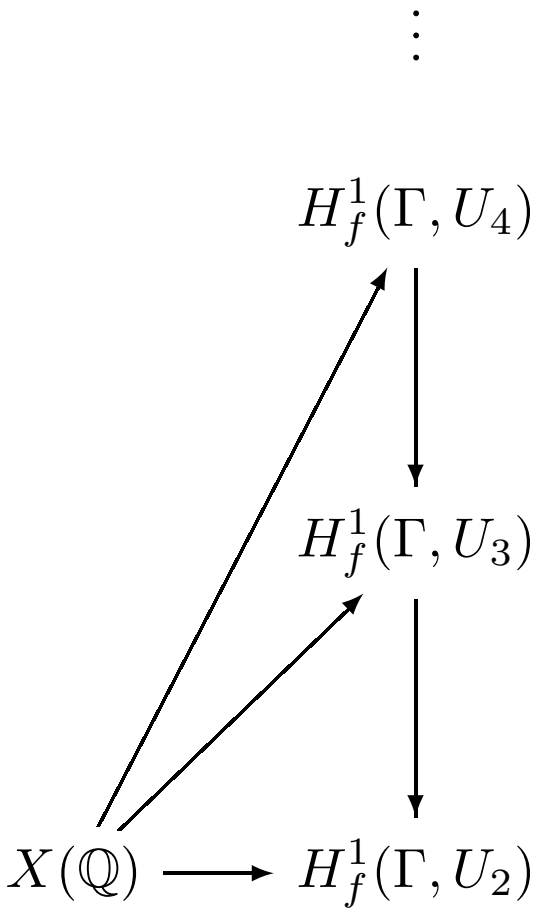
defined in the natural way:

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

and the ones κ^u_n at finite level by composing

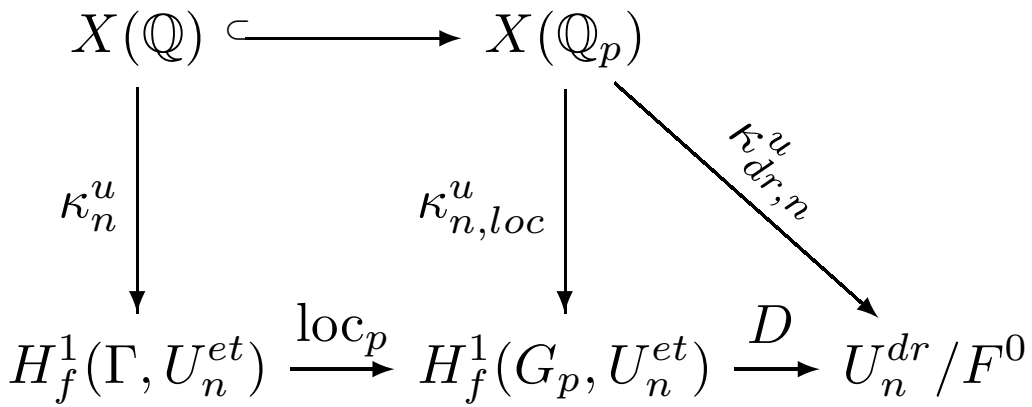


The varieties and maps fit naturally into a tower



Bottom map is usual one coming from Kummer theory on the Jacobian of X.

Application of Selmer variety comes from the diagram:



Here,

$$U_n^{dr}/F^0$$

is a classifying space for De Rham/crystalline torsors.

$$\kappa_{dr,n}^u(x) = P_n^{dr}(x)(\simeq P_n^{cr}(x))$$

a kind of p-adic period domain.

The map D associates to a crystalline U^{et}-torsor $T = \mathrm{Spec}(\mathcal{T})$, the U^{dr}-torsor

$$D(T) = \mathrm{Spec}([\mathcal{T} \otimes B_{cr}]^{G_p})$$

Commutativity of triangle comes from non-abelian p-adic comparison isomorphism (Shiho, Vologodsky, Olsson, Faltings)

$$D(\pi^{et}(\bar{X}; b, x)) = \pi^{dr}(X \otimes \mathbb{Q}_p; b, x)$$

Remarks:

-There is an affine analogue related to local and global integral points. In fact, will incorporate that version into the discussion without introducing additional notation. For $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ the coordinates of κ^u_{dr} are p-adic multiple polylogarithms.

-Image of κ^u_{dr} is *Zariski dense*.

-Underlying picture is

$$X(\mathbb{Q}) \rightarrow \text{`classifying space for motivic torsors}'$$

$$x \mapsto P^M(x)$$

Goal: Control the image

$$\mathrm{Im}_n[H^1_f(\Gamma, U^{et}_n)]$$

of global Selmer variety inside U^{dr}_n/F^0.

In fact, would like to show

$$\text{`CT(n)':} \qquad \mathrm{Im}_n[H^1_f(\Gamma, U_n^{et})] \text{ is } \textit{not} \text{ Zariski dense}$$

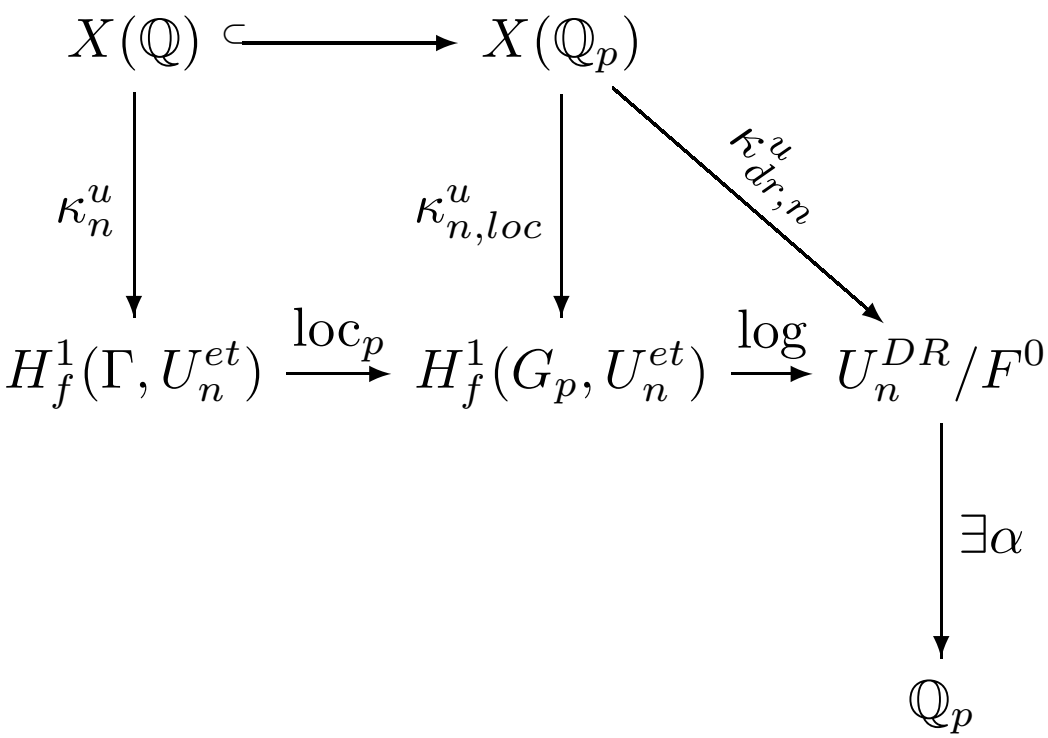
for some n. This statement CT(n) implies that

$$\mathrm{Im}_n[H^1_f(\Gamma, U_n^{et})] \cap \mathrm{Im}_n[X(\mathbb{Q}_p)]$$

is finite, and hence, that

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

is finite.



$\alpha|\mathrm{Im}_n[H_f^1(\Gamma, U_n^{et})] = 0$

$\alpha|\mathrm{Im}_n[X(\mathbb{Q}_p)] \neq 0$

Historical remark: In Weil's 1938 paper on vector bundles, he speculates about application of 'non-abelian' mathematics to number theory, including π_1 and vector bundles.

$CT(n)$ appears quite hard in general. Easiest case is when $\text{rank}(J_X(\mathbb{Q})) < g$. Then $CT(2)$ is true, corresponding to *method of Chabauty*.

Otherwise, can prove:

-$CT(n)$ for $n >> 0$ when X has genus zero (with at least three points at infinity).

-$CT(3)$ for elliptic curves of rank 1 minus origin. Need slightly modified Selmer variety (with Tamagawa).

-Can deduce $CT(n)$ for $n >> 0$ in general from other difficult conjectures, in fact, motivic 'higher' abelian analogues of section conjectures.

(Bloch-Kato) If $V/\mathbb{Q}$ is a smooth projective variety. Then

$$ch_{n,r} : K^{(r)}_{2r-n-1}(V) \otimes \mathbb{Q}_p \to H^1_g(\Gamma, H^n(\bar{V}, \mathbb{Q}_p(r)))$$

is surjective.

(Fontaine-Mazur) If $V/\mathbb{Q}$ is a smooth projective variety. Then

$$\text{Mixed Motives} \to H^1_g(\Gamma, H^n(\bar{V}, \mathbb{Q}_p(r)))$$

is surjective.

Apply to $H^n(\bar{X}^n, \mathbb{Q}_p(n+1))$.

Then either of these implies CT(n) for n large, and hence, finiteness.

Sketch of proof (in the compact case): dimension estimate based on inductive structure

$$0 \to U^{n+1} \backslash U^n \to U_{n+1} \to U_n \to 0$$

that gives rise to

$$0 \to H^1_f(\Gamma, U^{n+1} \backslash U^n) \to H^1_f(\Gamma, U_{n+1}) \to H^1_f(\Gamma, U_n)$$

and explicit computation of dimension of U_n^{dr}/F^0.

Principle: Both local and global dimension grow with n, but global dimension grows more slowly.

S primes of bad reduction. $T = S \cup \{p\}$.

$Sh^1_n := Ker[H^1(\Gamma_T, (U^{n+1} \backslash U^n)^*(1)) \rightarrow \oplus_{v \in T} H^1(G_v, (U^{n+1} \backslash U^n)^*(1))]$

Either B-K or F-M imply

$$Sh^1_n = 0$$

for $n >> 0$ so by Poitou-Tate duality

$$Sh^2_n := Ker[H^2(\Gamma_T, U^{n+1} \backslash U^n) \rightarrow \oplus_{v \in T}\, H^2(G_v, U^{n+1} \backslash U^n)]$$

also vanishes.

Hence, dimension of

$$H^2(\Gamma_T, U^{n+1} \backslash U^n)$$

is bounded by local dimensions. Can show sum of local dimensions is bounded by

$$|T|(n + (2g-2)^2 n(n-1)/2))g^n$$

using weight-monodromy filtration (for $l \neq p$) and Hodge-Tate decomposition (at p).

But we have Euler characteristic formula

$$\dim H^1(\Gamma_T, U^{n+1}\backslash U^n) - \dim H^2(\Gamma_T, U^{n+1}\backslash U^n)$$

$$= (U^{n+1}\backslash U^n)^- = \frac{1}{2}\dim(U^{n+1}\backslash U^n)$$

for n odd.

Meanwhile, the dimensions $r_n = \dim U^{n+1}\backslash U^n$ are calculated by a recursive formula

$$\Sigma_{i|n} i r_i = (g + \sqrt{g^2-1})^n + (g - \sqrt{g^2-1})^n$$

so

$$r_n \approx (g + \sqrt{g^2-1})^n / n$$

Also,

$$\dim F^0[(U^{dr})^{n+1}\backslash (U^{dr})^n] \leq g^n$$

To summarize: $H^1(\Gamma_T, U^{n+1}\backslash U^n)$ grows like at most

$$\frac{(g+\sqrt{g^2-1})^n}{n}$$

for n even, and

$$\frac{(g+\sqrt{g^2-1})^n}{2n}$$

for n odd, while $(U^{dr})^{n+1}\backslash(U^{dr})^n/F^0$ grows consistently like

$$\frac{(g+\sqrt{g^2-1})^n}{n}$$

Therefore, get

$$\dim H^1(\Gamma_T, U_n^{et}) < U_n^{dr}/F^0$$

for $n >> 0$, and thus,

$$D \circ (\mathrm{loc}_p(H^1(\Gamma_T, U_n^{et}))) \subset U_n^{dr}/F^0$$

is non-dense.

Can view:

B-K $\Rightarrow$ Mordell conjecture

as a substitute for

'Section conjecture $\Rightarrow$ Mordell conjecture.'

However, real motivation comes from the vague idea:

> B-K, section conjecture + $\epsilon \Rightarrow$ an effective Mordell conjecture for curves already having one point.

Here, 'effective Mordell' means

> *The set of rational points is computable.*

Sketch: Assuming B-K, can compute l such that

$$H^1_f(\Gamma, U_l^{et}) \to U_l^{dr}/F^0$$

has non-dense image. Furthermore, can (in principle) compute this map. Thereby, explicitly find α such that $\alpha \circ \kappa_l^u | X(\mathbb{Q}_p)$ vanishes on the global points.

How well do we need to know α? So that 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. Thereby, we get a injection

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

[ϵ] The non-abelian congruence Mordell-Weil property:

'Can find $n = n(m)$ and $N = N(m)$ such that the map

$$X(\mathbb{Z}/p^m) \to H^1(G_p, \hat{\pi}_1(\bar{X}, b)_{(n)}[p^N])$$

$$x \mapsto \hat{\pi}_1(\bar{X}; b, x)_{(n)}[p^N]$$

is injective.'

Here, $\hat{\pi}_1(\bar{X}; b)_{(n)}$ is the quotient of the pro-finite fundamental group via the n-th level of the derived series, and the bracket refers to the maximal p^N-torsion quotient.

Such an injection is implicit in Mochizuki. Explicit form is currently under investigation by Hoshi.

This leads to an injection

$$X(\mathbb{Q}) \hookrightarrow H^1(\Gamma_T, \hat{\pi}_1(\bar{X}; b, x)_{(n)}[p^N])$$

Let F_i be a cofinal system of finite quotient groups of $\hat{\pi}(\bar{X}; b)$, so that

$$H^1(\Gamma, \hat{\pi}(\bar{X}; b)) = \varprojlim H^1(\Gamma_i, F_i)$$

for some restricted ramification Galois groups Γ_i.

Eventually, we have maps

$$\begin{array}{ccccccc} \cdots & H^1(\Gamma_{i+2}, F_{i+2}) & \to & H^1(\Gamma_{i+1}, F_{i+1}) & \to & H^1(\Gamma_i, F_i) & \cdots \\ & \downarrow & & \downarrow & & \downarrow & \\ \cdots & Im_{i+2} & \hookrightarrow & Im_{i+1} & \hookrightarrow & Im_i & \cdots \end{array}$$

leading to a decreasing of subsets Im_i of

$$H^1(\Gamma_T, \hat{\pi}_1(\bar{X}; b, x)_{(n)}[p^N])$$

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.

Section conjecture implies that the two nested sequence of subsets have to eventually meet, giving a *terminating algorithm* of *non-abelian descent*.

Essentially 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.*