

Anabelian geometry, path spaces, and  
Diophantine geometry

Minhyong Kim

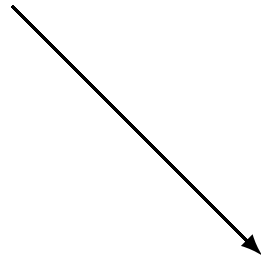
November 26, 2006

References:

The motivic fundamental group of  $\mathbf{P}^1 \setminus \{0, 1, \infty\}$  and the theorem of Siegel. *Invent. Math.* 161 (2005), no. 3

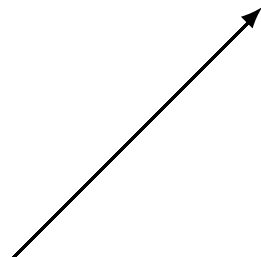
The unipotent Albanese map and Selmer varieties for curves  
<http://www.math.purdue.edu/~kimm>

homology



topology → arithmetic

homotopy



$X/\mathbb{Q}$  smooth curve with good model

$$\mathcal{X}/R$$

for  $R = \mathbb{Z}[1/S]$ ,  $S$  a finite set of primes.

$$X(R)$$

the  $R$ -points of  $X$ .

Would like to understand its structure.

Theorem of Siegel and Faltings:

$$X(R)$$

finite if  $X$  is hyperbolic, i.e., genus  $\geq 2$ , genus one minus at least one point, or genus zero minus at least three points.

For example, generic equation  $f(Z_0, Z_1, Z_2) = 0$  of degree  $\geq 4$  has only finitely many  $R$ -solutions.

Basic difficulty: \*no\* apparent sophisticated structure on  $X(R)$ .

Obviously in contrast to the case of an *elliptic curve*  $E$  where  $E(R) = E(\mathbb{Q})$  ends up being a finitely-generated abelian group, in fact, a lattice.

Abelianize  $X$ ?

Classical construction:

$$i_b : X \hookrightarrow J_X$$

where  $J_X$  is the *Jacobian* of  $X$ .

$J_X$  is a natural sub-quotient of the free abelian group generated by  $X$ . In this context,

$$i_b(x) = [x] - [b].$$

Initial construction an analytic one via Hodge theory:

$$J_X := H_1(X, \mathbb{Z}) \backslash H^0(\Omega_X)^* = H_1(X, \mathbb{Z}) \backslash H_1(X, \mathbb{C}) / F^0$$

$i_b$  depends on choice of base-point  $b$  and sends  $x$  to

$$\alpha \mapsto \int_b^x \alpha$$

Algebraic version was constructed by Weil

*in order to study  $X(R)$ .*

In fact,  $J_X$  is a projective variety defined over  $\mathbb{Q}$  and has a good model over  $R$ .  $i_b$  is defined over  $\mathbb{Q}$  if  $b \in X(\mathbb{Q})$ .

That is, we have

$$X/R \hookrightarrow J_X/R$$

underlying

$$X(\mathbb{C}) \hookrightarrow J_X(\mathbb{C})$$

Hence,

$$X(R) \hookrightarrow J_X(R)$$

Advantage is that  $J_X(R)$  is an abelian group.

Disadvantage is that  $J_X(R)$  is an abelian group.

Added structure obliterates information about  $X(R)$ . In particular,  $J_X$  usually cannot be used for proving finiteness of  $X(R)$ .

Problem is that

$$J_X \otimes \mathbb{Q} = \text{Ext}_{MM_{\mathbb{Z}}}^1(\mathbb{Q}, H_1(X))$$

so abelian nature is intrinsic to the category of *motives*.

In fact, for a general variety  $V$ , the category of motives, being of homological nature, destroys information about

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

How to remedy this?

Weil (1938), ‘Généralisation des fonctions abélienne’: *non-abelian fantasy*

-‘A text presented as analysis, whose significance is essentially algebraic, but whose motivation is arithmetic.’ (Serre)

-Discusses need to move beyond abelian objects in study of arithmetic.

-Initiates study of vector bundles in this context to generalize the Jacobian.

-Homological nature of the Jacobian is emphasized and footnote contains allusion to importance of non-abelian  $\pi_1$ .

From current day perspective, moduli of semi-stable bundles corresponds to the theory of *reductive completions* of  $\pi_1$ .

However, at the time of Weil, no serious *arithmetic theory* of  $\pi_1$ .

Grothendieck (60's): Pro-finite  $\pi_1$ .

$V$  variety.

$\text{Cov}(V)$  category of finite étale coverings of  $V$ .

$b : \text{Spec}(K) \rightarrow V$  geometric point.

Determines a fiber functor

$F_b : \text{Cov}(V) \rightarrow \text{Finite Sets}$

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

$$\hat{\pi}_1(V, b) := \text{Aut}(F_b)$$

Remarks:

-Isomorphic to a Galois group, but *not canonically*.

-Galois group case corresponds to  $b$  a separable closure of generic point:

$$b : \text{Spec}(\overline{K(V)}) \rightarrow V$$

-Significantly, definition allows ‘small’ base-points naturally, as well as variation in  $x$ .

Applications slow to come in the manner envisaged by Weil, that is, over number fields.

Used for Diophantine problems over *finite fields* via the Weil conjectures, in a *horizontal* rather than *vertical* direction.

$V/S$  scheme with geometrically connected fibers.  $s \in S$  a geometric point.  $V_s$  fiber over  $s$ .  $b \in V_s$  geometric point.

Then

$$\begin{array}{ccccccc} \hat{\pi}_1(V_s, b) & \longrightarrow & \hat{\pi}_1(V, b) & \longrightarrow & \hat{\pi}_1(S, s) & \longrightarrow & 0 \\ \uparrow & & & & \uparrow & & \\ \text{vertical} & & & & \text{horizontal} & & \end{array}$$

In Weil conjecture, study action of  $\hat{\pi}_1(S, s)$  on homology of  $V_s$ .

But even here, naturality of small base-point was useful.

Substantive Diophantine work on the vertical fundamental group starts again with Grothendieck in the 80's.

In essence, involves considering the whole *fundamental groupoid* coming from

$$\hat{\pi}_1(V; b_1, b_2) := \text{Isom}(F_{b_1}, F_{b_2})$$

for varying points  $b_1, b_2$  together with composition

$$\hat{\pi}_1(V; b_2, b_3) \times \hat{\pi}_1(V; b_1, b_2) \rightarrow \hat{\pi}_1(V; b_1, b_3)$$

In fact, already sufficient to consider

$$\hat{\pi}_1(V; b, v)$$

for fixed  $b$  and varying  $v$  as *torsors* for

$$\hat{\pi}_1(V, b)$$

$$\hat{\pi}_1(V; b, v) \times \hat{\pi}_1(V, b) \rightarrow \hat{\pi}_1(V; b, v)$$

Return to the case of a compact hyperbolic curve  $X/\mathbb{Q}$ . Then  $\hat{\pi}_1(\bar{X}, b)$  and  $\hat{\pi}_1(\bar{X}; b, x)$  for  $b, x \in X(\mathbb{Q})$  carry actions of the Galois group

$$\Gamma := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

Difficult arithmetic analogues of Hodge structure.

Partially understood only in special cases, say

$X = \mathbf{A}^1 \setminus \{0\}$  (cyclotomic character);

$X = E$  an elliptic curve (voluminous literature);

or  $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$  (Ihara's theory).

In any case,  $\hat{\pi}_1(\bar{X}; b, x)$  are now  $\Gamma$ -equivariant torsors for  $\hat{\pi}_1(\bar{X}, b)$  classified by non-abelian continuous cohomology set

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

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

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

characterized by

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

Thus, we have a map

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

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

*Grothendieck's section conjecture:*

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

Remarks:

-In original formulation,  $H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$  is in bijection with splittings of exact sequence

$$0 \rightarrow \hat{\pi}_1(\bar{X}, b) \rightarrow \hat{\pi}_1(X, b) \rightarrow \Gamma \rightarrow 0$$

and conjecture says every splitting is geometric. In this form, part of *anabelian geometry*.

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

-Many maps in arithmetic geometry of nature

‘scheme-theoretic objects  $\rightarrow$  Galois-theoretic objects.’

Suitable surjectivity statement key issue in problems of central interest. (Conjectures of Birch and Swinnerton-Dyer, Beilinson, Bloch-Kato.)

-Grothendieck and Deligne expected the section 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 explore (2), again allowing  $X$  to be non-compact.

Main ingredient is the *motivic* fundamental group  $U^M$  (Deligne).

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

|

$$U^M$$

|

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

$U^M$  consists of ‘realizations’ that are pro-unipotent pro-algebraic groups. Definition of each obtained by replacing the Galois category of coverings  $\text{Cov}(\bar{X})$  with various *Tannakian* categories. Results in an easier structure than  $\hat{\pi}_1(\bar{X}, b)$ .

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

$$U^B = \pi_1 \otimes \mathbb{Q}$$

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,

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

where

$$F_b : \text{Un}(X(\mathbb{C}), \mathbb{Q}) \mapsto \text{Vect}_{\mathbb{Q}}$$

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

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

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

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

where

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

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

De Rham realization:

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

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

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

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

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

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

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

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

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

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

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

In all realizations, also have path spaces

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

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  $\Gamma = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  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

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

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

The basic tool for studying points is a map

$$\kappa^M : x \mapsto [P^M(x)]$$

from  $X$  to a *classifying space*

$\mathcal{D}$

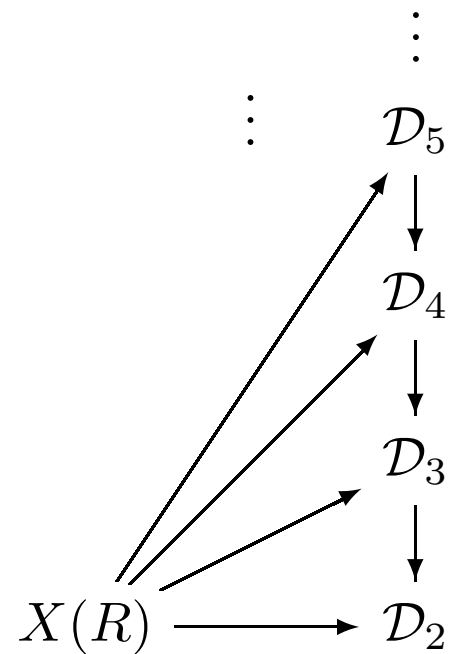
for motivic torsors.

Considerably easier than

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

but refines Albanese maps.

In fact, they constitute a tower:



where the bottom map consists of Albanese maps in various realizations.

Over  $\mathbb{C}$ , map *higher Albanese maps*

$$\kappa_n^B : X(\mathbb{C}) \rightarrow L_n \setminus U_n^B \otimes \mathbb{C}/F^0$$

defined by Hain. Coordinates given by *iterated integrals*

$$x \mapsto \int_b^x \alpha_1 \alpha_2 \cdots \alpha_i$$

Over  $\mathbb{Q}_p$ , have  $p$ -adic unipotent Albanese maps

$$\kappa_n^{dr/cr} : X(\mathbb{Z}_p) \rightarrow U_n^{dr} / F^0$$

defined using  $p$ -adic iterated integrals.

For example, when  $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$  components of  $\kappa_n^{dr/cr}$  consist of  $p$ -adic multiple polylogarithms (Furusho).

These are the local Archimedean and non-Archimedean components of  $\kappa^M$  that give explicit form to the maps

$$x \mapsto [P^B(x)]$$

and

$$x \mapsto [P^{dr}(x) \simeq P^{cr}(\bar{x})]$$

Global component:

$$\kappa_n^{et, glob} : X(R) \rightarrow H_f^1(\Gamma, U_n^{et})$$

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

with target in unipotent Selmer variety

$$H_f^1(\Gamma, U_n^{et})$$

Continuous non-abelian cohomology generalizing pro- $p$  Selmer groups

$$H_f^1(\Gamma, T_p J_X \otimes \mathbb{Q}_p)$$

occurring in BSD conjecture. Subscript refers to natural local conditions on cohomology classes.

Has the natural structure of an affine algebraic variety.

But *not* abelian groups for  $n > 2$ . Hence preserves more of the structure of  $X(R)$ .

Remark: Factorization at bottom level.

$$\begin{array}{ccc} X(R) & \xrightarrow{\kappa_2^{et, glob}} & H_f^1(\Gamma, U_2^{et}) \\ & \searrow & \nearrow \\ & J_X(R) & \end{array}$$

To use these constructions for Diophantine geometry, have to combine into one big diagram.

$$\begin{array}{ccccc}
 X(R) & \hookrightarrow & X(\mathbb{Z}_p) & & \\
 \downarrow \kappa_n^{et, glob} & & \downarrow \kappa_n^{et, loc} & \searrow \kappa_n^{dr/cr} & \\
 H_f^1(\Gamma, U_n^{et}) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, U_n^{et}) & \xrightarrow{D} & U_n^{dr} / F^0
 \end{array}$$

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

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

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

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

## Proposition

$$X(\mathbb{Z}_p) \xrightarrow{\kappa_n^{dr/cr}} U_n^{dr} / F^0$$

has Zariski dense image.

## Proposition

When  $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ , the image of

$$H_f^1(\Gamma, U_n^{et}) \xrightarrow{\text{loc}_p} H_f^1(G_p, U_n^{et}) \xrightarrow{D} U_n^{dr} / F^0$$

is *not* Zariski dense for  $n \gg 0$ .

Idea: As  $n$  grows, both local and global dimension grows, but global dimension grows more slowly than local dimension.

## Corollary

$X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$  has finitely many  $\mathbb{Z}[1/S]$  points.

$$\begin{array}{ccccc}
X(R) & \hookrightarrow & X(\mathbb{Z}_p) & & \\
\downarrow \kappa_n^{et, glob} & & \downarrow \kappa_n^{et, loc} & \searrow \kappa_n^{dr/cr} & \\
H_f^1(\Gamma, U_n^{et}) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, U_n^{et}) & \xrightarrow{D} & U_n^{DR}/F^0 \\
& & & & \downarrow \exists \alpha \\
& & & & \mathbb{Q}_p
\end{array}$$

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

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

Even in general, whenever we can find  $n$  such that

$$H_f^1(\Gamma, U_n^{et}) \xrightarrow{\text{loc}_p} H_f^1(G_p, U_n^{et}) \xrightarrow{D} U_n^{dr} / F^0$$

has non-dense image, can prove finiteness of  $X(R)$ .

Appears to be a good framework for  $\pi_1$ -proof of Diophantine finiteness.

-Classical case,  $n = 2$  works when

$$\text{rank} J_X(R) < \dim T_e J_X$$

Method of Chabauty.

- $n = 3$  works for  $X = E \setminus \{e\}$  when  $(E, e)$  is an elliptic curve of Mordell-weil rank 1. (Joint work with Tamagawa.)

-Predicted to work in general by

*standard conjectures on mixed motives*

such as conjecture of Bloch and Kato on surjectivity of  $p$ -adic Chern class map.

Bloch-Kato  $\Rightarrow$  Mordell.

viewed as substitute for

Section conjecture  $\Rightarrow$  Mordell.

Note that many ingredients predicted by Weil's non-abelian fantasy have appeared in rather concrete form.

However, unipotent completion rather than reductive completion.

Bloch-Kato+section conjecture provides an effective algorithm for computing all rational points via *non-abelian descent*.

Key point is

Section conjecture  $\Rightarrow$  Termination of non-abelian descent