Galois Theory and Diophantine geometry

Minhyong Kim

Paris, November, 2009

1. Some Examples

1.1

A typical finiteness theorem in Diophantine geometry:

Let $a, b, c, n \in \mathbb{Z}$ and $n \geq 4$. Then the equation

$$ax^n + by^n = c$$

has at most finitely many rational solutions in (x, y).

General proof due to Faltings.

Recent 'homotopical' proof (Coates and K., arXiv:0810.3354), using general structure theory of moduli spaces of torsors and some non-vanishing for L-values.

1.2

$E/\mathbb{Q}$ 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

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

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

Uses small fragment of explicit non-abelian duality and reciprocity.

2. Some Anabelian Geometry

2.1 Grothendieck in the 80's

(1) Pursuing stacks;

(2) Long march through Galois theory;

(3) Letter to Faltings.

-(3) contains the idea that certain 'anabelian' schemes should be encoded in their fundamental groups.

-(2) the idea that *arbitrary* schemes can be constructed out of anabelian ones, and hence, encoded in some structure involving non-abelian fundamental groups.

-This procedure should perhaps involve (1).

Picture should be something like this:

-X scheme.

$$X = \cup_i U_i$$

with U_i anabelian.

-

$$U_{ij} \rightarrow U_i \times_X U_j$$

with U_{ij} anabelian.

-possibly continue with further 'intersections.'

Encode X into the system of fundamental groups of the U_I's.

Basic idea: X and Y anabelian schemes, then one should have

$$\mathrm{Hom}(X, Y) \simeq \mathrm{Hom}(\pi_1(X), \pi_1(Y))/\pi_1(Y).$$

Also

$$\mathrm{Isom}(X, Y) \simeq \mathrm{Isom}(\pi_1(X), \pi_1(Y))/\pi_1(Y).$$

Latter statement proved for hyperbolic curves over number fields by Nakamura, Tamagawa, and Mochizuki.

Diophantine geometry, being the study of maps between schemes of finite type, should also be clarified through this study.

2.2 Section conjecture

For 'usual' Diophantine geometry, need to consider the exact sequence

$$0 \to \pi_1(\bar{X}) \to \pi_1(X) \to \mathrm{Gal}(\bar{F}/F) \to 0.$$

Here, X/F is a curve of genus ≥ 2 over a number field F, and $\bar{X}$ is its base-change to the algebraic closure $\bar{F}$. Given any point $x \in X(F)$, viewed as

$$x : \mathrm{Spec}(F) \to X,$$

get a splitting

$$x_* : \pi_1(\mathrm{Spec}(F)) = \mathrm{Gal}(\bar{F}/F) \to \pi_1(X).$$

Section conjecture:

$$X(F) \simeq \{\text{Splittings of sequence}\}/\text{conjugacy}.$$

A non-abelian analogue of the conjecture of Birch and Swinnerton-Dyer, which Grothendieck believed to be highly relevant to the Diophantine geometry of X.

3. The fundamental groupoid

Let $X/\mathbb{Q}$ be a compact curve.

Consider $X(\mathbb{C})$, the manifold of complex points of X.

The fundamental groupoid is made up of the path spaces

$$\pi_1(X(\mathbb{C}); a, b)$$

as the two points a and b vary over $X(\mathbb{C})$, together with the composition

$$\pi_1(X(\mathbb{C}); b, c) \times \pi_1(X(\mathbb{C}); a, b) \to \pi_1(X(\mathbb{C}); a, c)$$

obtained by concatenating paths.

The portion that originates at a fixed base-point b is comprised of the fundamental group

$$\pi_1(X(\mathbb{C}), b)$$

and the homotopy classes of paths

$$\pi_1(X(\mathbb{C}); b, x)$$

for any other point $x \in X(\mathbb{C})$.

We will focus mostly on the category of *torsors* for the group $\pi_1(X(\mathbb{C}), b)$, inside which the path spaces $\pi_1(X(\mathbb{C}); b, x)$ move.

This means that there is a group action

$$\pi_1(X(\mathbb{C}); b, x) \times \pi_1(X(\mathbb{C}), b) \longrightarrow \pi_1(X(\mathbb{C}); b, x)$$

that is simply transitive.

Alternatively, any choice of a path $p \in \pi_1(X(\mathbb{C}); b, x)$ determines a bijection

$$\pi_1(X(\mathbb{C}), b) \simeq \pi_1(X(\mathbb{C}); b, x)$$

$$\gamma \mapsto p \circ \gamma.$$

One version of the anabelian philosophy is to encode points into the structures $\pi_1(X(\mathbb{C}); b, x)$.

The idea of putting points into *geometric families* is a common one in Diophantine geometry, as when solutions

$$a^n + b^n = c^n$$

to the Fermat equation are encoded into the elliptic curves

$$y^2 = x(x - a^n)(x + b^n).$$

The geometry of the path torsor $\pi_1(X(\mathbb{C}); b, x)$ is an extremely canonical version of this idea.

4. Implementation: Non-archimedean completions

To distinguish rational solutions $X(\mathbb{Q})$ from arbitrary complex ones, one needs to pass to a non-archimedean *linearization*. Let S be the primes of bad reduction, $p \notin S$, and $T = S \cup \{p\}$.

Standard linearization: the group ring

$$\mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)].$$

Obtain thereby, a number of additional structures.

The group ring is a Hopf algebra with comultiplication

$$\Delta : \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \to \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \otimes \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]$$

determined by the formula

$$\Delta(g) = g \otimes g$$

for $g \in \pi_1(X(\mathbb{C}), b)$.

Inside the group ring there is the augmentation ideal

$$J \subset \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]$$

generated by elements of the form $g - 1$.

Completion:

$$A = \mathbb{Q}_p[[\pi_1(X(\mathbb{C}), b)]] := \varprojlim_n \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]/J^n,$$

whose elements can be thought of as non-commuative formal power series in elements $g - 1$, $g \in \pi_1$.

The previous co-product carries over to an algebra homomorphism

$$\Delta : A \longrightarrow A\hat{\otimes}A := \varprojlim A/J^n \otimes A/J^m,$$

turning A into a *complete Hopf algebra*.

Study of such structures originates in *rational homotopy theory*, with which we are actually concerned from a motivic point of view.

One defines the group-like elements

$$U = \{g \mid \Delta(g) = g \otimes g,\ V \in L\}.$$

The elements of the discrete fundamental group give rise to elements of U, but there are many more. For example, given $g \in \pi_1$, one can obtain elements of U using $\mathbb{Q}_p$-powers of g:

$$g^\lambda := \exp(\lambda \log(g)).$$

The group U is in fact very large, with the structure of a pro-algebraic group over $\mathbb{Q}_p$.

The natural map

$$\pi_1(X(\mathbb{C}), b) \to U$$

turns it into the $\mathbb{Q}_p$-*pro-unipotent completion* of the fundamental group.

The path torsors can be completed as well, to give

$$P(x) := \pi_1(X(\mathbb{C}); b, c) \times_{\pi_1(X(\mathbb{C}),b)} U,$$

which are torsors for U.

The most important extra structure arises when b and x are both rational points. Then U and $P(x)$ admit continuous actions of

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

The action arises from a reinterpretation of these constructions in terms of the étale topology of the scheme X.

Two important facts:

-If p is chosen large enough and the fundamental group is non-trivial, then the structure $P(x)$ completely determines the point x. That is, if

$$P(x) \simeq P(x')$$

as U-torsors with G-action, then $x = x'$.

-Can classify such structures, using a pro-algebraic moduli space

$$H^1_f(G, U),$$

describing non-abelian continuous group cohomology. The *Selmer variety* of X.

Each $P(x)$ determines an element of this space.

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

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

4.1 Construction

The cohomology here is defined as a quotient space

$$H^1(G,U) = Z^1(G,U)/U,$$

where $Z^1(G,U)$ consists of the continuous functions

$$c : G \to U$$

satisfying the 'cocycle condition'

$$c(\sigma_1\sigma_2) = c(\sigma_1)\sigma_1(c(\sigma_2)),$$

and $u \in U$ acts on such functions by

$$(u \cdot c)(\sigma) = u^{-1}c(\sigma)\sigma(u).$$

A torsor P gives rise to such a function when we choose an element $t \in P$. Then for any $\sigma \in G$, we have

$$\sigma(t) = tu_\sigma$$

for some unique $u_\sigma \in U$. It is easily checked that the function

$$\sigma \mapsto u_\sigma$$

satisfies the cocycle condition, and that the corresponding class in $H^1(G, U)$ is independent of the choice of t.

$$H^1_f(G, U) \subset H^1(G, U)$$

is a subspace defined by a collection of 'local conditions' reflecting the natural geometry of the scheme. Namely, the torsor should be trivial at all primes $l \notin T$ and *crystalline* at p.

4.2 The nature of Diophantine finiteness

There is another natural geometric family containing the rational points, namely, the p-adic points $X(\mathbb{Q}_p)$, which has a non-archimedean analytic structure.

Thereby, the $\mathbb{Q}$-points $X(\mathbb{Q})$ become embedded in two *entirely canonical families* having, however, very different natures:

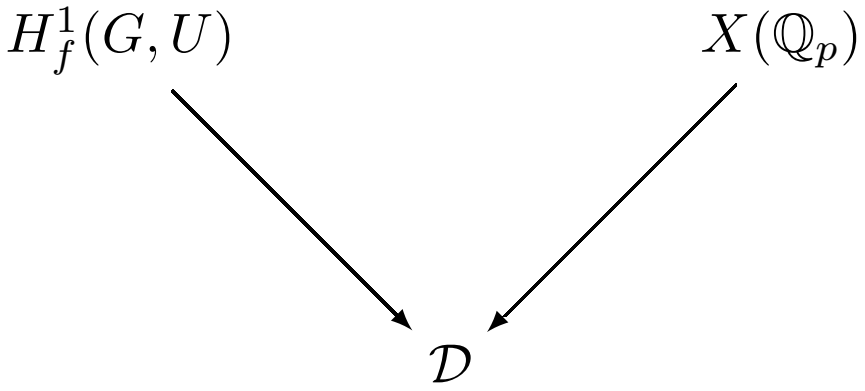
$$H^1_f(G, U)$$

and

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

There is severe tension between the two families when X itself is sufficiently complex, more precisely, when $\pi_1(X(\mathbb{C}), b)$ is *non-abelian*.

This tension is brought out by mapping both families into a large p-adic symmetric space



constructed using *p-adic Hodge theory*.

It emerges that the key difference between the two maps is that $H^1_f(G,U)$ maps to an algebraic subspace, while $X(\mathbb{Q}_p)$ maps to a *space-filling curve*.

The ambient symmetric space $\mathcal{D}$ is in fact a homogeneous space

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

for the *De Rham fundamental group* of $X_{\mathbb{Q}_p}$, and the map

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

is expressed using p-adic iterated integrals.

4.2.2 Example

For the equation

$$ax^n + by^n = c$$

the fundamental group is non-abelian exactly when $n \geq 4$.

In this case, with a careful selection of p, one can show that

$$Im(H^1_f(G, U)) \cap Im(X(\mathbb{Q}_p))$$

is finite, and deduce from this the finiteness of points.

An important technical ingredient is *multi-variable Iwasawa theory* (joint work with John Coates), which shows that the image of $H^1_f(G, U)$ is a proper subspace.

In this proof, the dimensions of

$$H^1_f(G, U_n)$$

are controlled using Iwasawa theory. Specifically, one needs to show *sparseness of zeros* for an algebraic p-adic L-function associated to X.

That is, we have the implications

> Sparseness of L-zeros $\Rightarrow$ control of Selmer varieties $\Rightarrow$ finiteness of points.

in a manner entirely analogous to the theory of elliptic curves.

5. Duality

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

Hence, we get

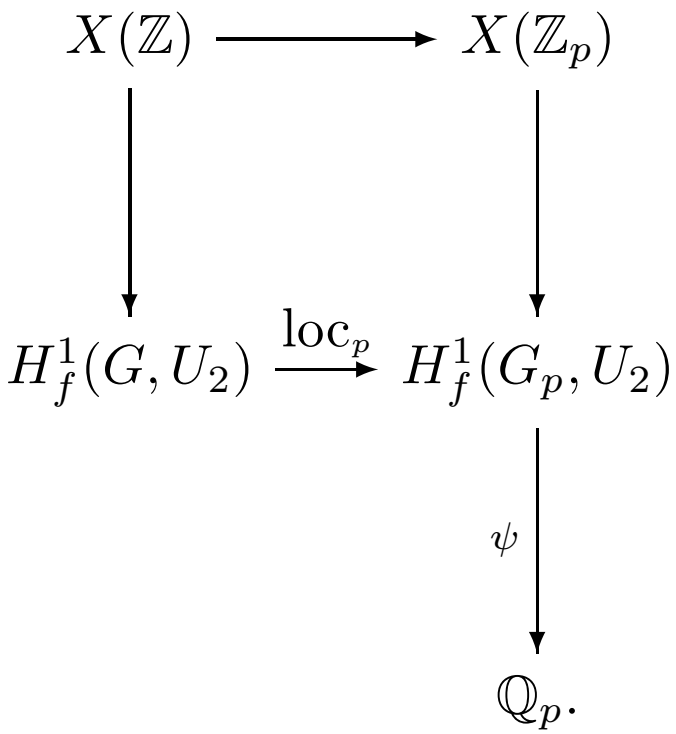
$$loc_p : E(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq H^1_f(G_p, V_p(E))$$

and

$$H^2(G_T, V_p(E)) = 0,$$

where $T = S \cup \{p\}$ and S is the set of primes of bad reduction.

We will construct a map ψ



that annihilates the global points by annihilating the image of the Selmer variety.

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

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

Define

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

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 0.1 *ψ vanishes on the image of*

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

where

$$H^1_{f,\mathbb{Z}}(G, U_2) \subset H^1_f(G, U_2)$$

consists of the classes that vanish *at all $l \neq p$.*

Proof is a simple consequence of the reciprocity sequence:

$$0 \to H^2(G_T, \mathbb{Q}_p(1)) \to \oplus_{v \in T} H^2(G_v, \mathbb{Q}_p(1)) \to \mathbb{Q}_p \to 0.$$

Hence, illustrates some elements of *non-abelian duality.*

Easy to check that for the class

$$k(x) = H^1_f(G_p, \mathbb{Q}_p(1)) \subset H^1_f(G_p, U_2)$$

of a number $x \in \mathbb{Z}_p^\times$, we have $\psi(k(x)) = \pm \log \chi_p(rec(x))$, and hence, that ψ is not identically zero.

An explicit evaluation of ψ using p-adic Hodge theory yields the formula from the introduction.

5.1 Speculation

Both the structure theory of the Selmer variety and the duality should admit a deeper homotopical interpretation.

The group U is a locally constant sheaf on $V = \mathrm{Spec}(\mathbb{Z}[1/T])$. There is an associated simplicial presheaf $K(U,1)$ on the étale site of V and the associated simplicial set of morphisms

$$RHom(V, K(U,1)).$$

On the other hand, if $V_l = \mathrm{Spec}(\mathbb{Q}_l)$ for $l \in T$, we have the map

$$j_l : V_l \to V,$$

giving us the sheaf $j_l^*(U)$ and the associated simplicial sets

$$RHom(V_l, K(j_l^* U, 1)).$$

Similarly, we have

$$RHom(V_l, K([j_l^* U](B_{cr}), 1)),$$

for Fontaine's ring of crystalline periods B_{cr}.

Then one should study the fibers of the maps

$$RHom(V, K(U,1)) \to \coprod_l RHom(V_l, K(U(j_l^* U, 1))$$

and

$$RHom(V, K(U,1)) \to \coprod_l RHom(V_l, K([j_l^* U](B_{cr}), 1))$$

in some manner involving non-abelian p-adic L-functions.

6. Discussion: Diophantine geometry and Galois theory

An outstanding problem of Diophantine geometry is to develop a Galois theory for polynomials of two variables.

Classical Galois theory studies the Diophantine geometry of polynomials in one variable using *group theory*.

What are the relevant structures for two variables?