Galois Theory and Diophantine geometry ±11

Minhyong Kim

Bordeaux, January, 2010

1. Some Examples

1.1

A Diophantine finiteness theorem:

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

$$|\text{Ш}(E)[p^\infty]| < \infty$$

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

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

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

A fragment of non-abelian duality and explicit 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

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

Proved for hyperbolic curves over number fields by Nakamura, Tamagawa, and Mochizuki.

General idea: 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.

Actually connected to the termination of a *non-abelian descent algorithm.*

3. The fundamental groupoid

Let $X/\mathbb{Q}$ be a compact curve of genus ≥ 2.

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

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

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. 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

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

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.

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

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

In fact, a tower of moduli spaces and maps:

$$
\begin{array}{ccc}
 & & \vdots \\
\vdots & & H^1_f(G, U_4) \\
 & & \downarrow \\
 & & H^1_f(G, U_3) \\
 & & \downarrow \\
 & & H^1_f(G, U_2) \\
 & & \downarrow \\
X(\mathbb{Q}) & \longrightarrow & H^1_f(G, U_1)
\end{array}
$$

corresponding to the lower central series of U, refining the map at the bottom (where $U_1 = H^{et}_1(\bar{X}, \mathbb{Q}_p)$).

4.1 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:
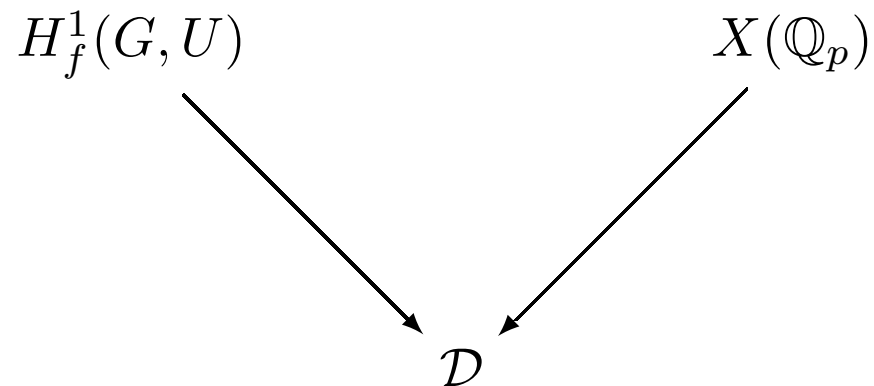
$$H^1_f(G, U)$$

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

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

$$\mathcal{D}$$

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

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

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

In fact, whenever

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

is non-dense, one gets finiteness of points.

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.

More generally, non-denseness of

$$Im(H^1_f(G, U)) \subset U^{DR}/F^0$$

follows from conjectural structure theory of mixed motives, e.g., Jannsen's vanishing conjecture.

Relation to non-abelian Iwasawa theory:

Let M be the p-ideal class group of the field F_∞ generated by $J_X[p^\infty]$ and Λ the Iwasawa algebra of $\Gamma = \mathrm{Gal}(F_\infty/F(J_X[p]))$.

Then $M/M[p^\infty]$ should admit a non-abelian algebraic L-function

$$L_M \in K_1(\Lambda_{S^*}).$$

For ρ a positive weight representation occurring in the category generated by $H^1(\bar{X}, \mathbb{Q}_p)$, we then have

$$\rho(L_M) \in K_1(End(V_\rho)) = \mathbb{Q}_p^*.$$

A *non-abelian zero* is a ρ such that $\rho(L_M) = 0$.

Then sparseness of non-abelian zeros for L_M is closely related to the non-density of $Im(H^1_f(G, U))$.

5. Explicit reciprocity

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

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

$$
\begin{array}{ccc}
X(\mathbb{Z}) & \longrightarrow & X(\mathbb{Z}_p) \\
\downarrow & & \downarrow \\
H^1_f(G, U_2) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_2) \\
& & \downarrow \psi \\
& & \mathbb{Q}_p.
\end{array}
$$

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

$$\log \chi_p : G_p \rightarrow \mathbb{Q}_p$$

is the logarithm of the $\mathbb{Q}_p$-cyclotomic character and x is a *global* solution, that is,

$$x : G_T \rightarrow V_p,$$

to the equation

$$dx = \log \chi_p \cup \xi_1.$$

Theorem 0.1 *ψ vanishes on the image of*

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

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:

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

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. Duality and number fields

Idea: Duality method should generalize to number fields, when appropriately formulated.

F: Number field.

S: finite set of primes of F.

$R := \mathcal{O}_F[1/S]$, the ring of S integers in F.

p: odd prime not divisible by primes in S and v a prime of F above p with $F_v = \mathbb{Q}_p$.

T: $S \cup \{w|p\}$.

$G := \mathrm{Gal}(\bar{F}/F)$. $G_T := \mathrm{Gal}(F_T/T)$.

$\mathcal{X}$: smooth curve over $\mathrm{Spec}(R)$ with good compactification. (Itself might be compact.)

X: generic fiber of $\mathcal{X}$, assumed to be hyperbolic.

$b \in X(\mathcal{O}_F[1/S])$.

Study the *tangential localization map*:

$$dloc_v(c) : T_c H^1_f(G, U) \rightarrow T_{loc_v(c)} H^1_f(G_v, U),$$

Formulae:

$$T_c H^1_f(G, W) \simeq H^1_f(G, L(c));$$

$$T_{loc_v(c)} H^1_f(G_v, U) \simeq H^1_f(G_v, L(c));$$

where L is the Lie algebra of U with Galois action twisted by the cocycle c.

For finiteness of points, suffices to show that $dloc_v(c)$ is not surjective at a generic c. Cotangent space:

$$T^*_{loc_v(c)} H^1_f(G_v, U) \simeq H^1(G_v, (L(c))^*(1))/H^1_f(G_v, (L(c))^*(1)).$$

Theorem 0.2 *Assume that for generic c there is a class $z \in H^1(G_T, (L_n(c))^*(1))$ such that $loc_w(z) = 0$ for $w \neq v$ and $loc_v(z) \notin H^1_f(G_v, (L_n(c))^*(1))$. Then*

$$loc_v : H^1_f(G, U_n) \to H^1_f(G_v, U_n)$$

is not dominant.

Proof.

By Poitou-Tate duality, we know that the images of the localization maps

$$\mathrm{loc}_T : H^1(G_T, L_n(c)) \to \oplus_{w \in T} H^1(G_w, L_n(c))$$

and

$$\mathrm{loc}_T : H^1(G_T, (L_n(c))^*(1)) \to \oplus_{w \in T} H^1(G_w, (L_n(c))^*(1))$$

are exact annihilators under the natural pairing

$$< \cdot, \cdot >: \oplus_{w \in T} H^1(G_w, L_n(c)) \times \oplus_{w \in T} H^1(G_w, (L_n(c))^*(1)) \to \mathbb{Q}_p.$$

With respect to the pairing $< \cdot, \cdot >_v$ at v, $H^1_f(G_v, L_n(c))$ and $H^1_f(G_v, (L_n(c))^*(1))$ are mutual annihilators.

Given any element $(a_w) \in \oplus_{w \in T} H^1(G_w, L_n(c))$, we have

$$< \mathrm{loc}_T(z), (a_w) > = < \mathrm{loc}_v(z), a_v >_v .$$

Hence, for any $a \in H^1_f(G, L_n(c))$, we get

$$< \mathrm{loc}_v(a), \mathrm{loc}_v(z) >_v = < \mathrm{loc}_T(a), \mathrm{loc}_T(z) > = 0.$$

Since $< \cdot, \mathrm{loc}_v(z) >$ defines a non-trivial linear functional on $H^1_f(G_v, L_n(c))$, this implies the desired results. $\square$