

Galois Theory and Diophantine geometry

Minhyong Kim

Essen, February, 2010

1. Abelian preliminaries

1.1. Elliptic Curves

E/\mathbb{Q} elliptic curve. Would like to understand the structure of Mordell-Weil group

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times (\text{finite group}).$$

Still do not have an algorithm that provably works to compute r .

An algorithm that *should* work uses Galois theory of the exact sequences

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

as we run over powers of a prime p .

Eventually arrive at

$$\delta : E(\mathbb{Q}) \otimes \mathbb{Q}_p \hookrightarrow H^1(G, V_p E),$$

where

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

and

$$V_p E = \left(\varprojlim_n E[p^n] \right) \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^2.$$

This Galois cohomology group is very unwieldy, but still constitutes the basic connection between Diophantine data and Galois theory.

One improves the situation by noticing a subspace that contains the image:

$$\text{Im}(\delta) \subset H_f^1(G, V_p E) \subset H^1(G, V_p E),$$

where the \mathbb{Q}_p -Selmer group

$$H_f^1(G, V_p E)$$

is defined by Galois-theoretic local conditions on cohomology classes: Let $G_v = \text{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v)$. Then $c \in H_f^1(G, V_p E)$ if and only if

- $c_v \in H^1(G_v, V_p)$ is unramified outside a finite set of v ;

-and *De Rham* for $v = p$.

Conjecturally (BSD),

$$E(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq H_f^1(G, V_p E).$$

(Finiteness of p -part of Tate-Shafarevich group.)

There is a well-known algorithm for computing $E(\mathbb{Q})$ whose termination depends on this conjecture, the key point being that $H_f^1(G, V_p E)$ is computable in a suitable sense. (See Silverman's book, for example.)

1.2. Abelian motives

This conjecture has seen many generalizations in the theory of motives, using the fact that the local conditions make sense for classes in

$$H^1(G, M_p)$$

given *any* motivic \mathbb{Q}_p -representation M_p of G .

That is, there is a

$$H_f^1(G, M_p) \subset H^1(G, M_p),$$

defined using local conditions exactly as above.

Imprecise version:

Fontaine-Mazur conjecture says any class in

$$[E_p] \in H_f^1(G, M_p)$$

should be motivic, that is, realized by a mixed motive E fitting in an exact sequence

$$0 \rightarrow M \rightarrow E \rightarrow \mathbb{Q} \rightarrow 0.$$

Some precise versions:

Beilinson and Bloch-Kato say that when $M = H^{2i-1}(\bar{X})(i)$ for smooth projective X , then any class in

$$H_f^1(G, H^{2i-1}(\bar{X}, \mathbb{Q}_p)(i))$$

can be realized as

$$0 \rightarrow H^{2i-1}(\bar{X})(i) \rightarrow H^{2i-1}(\bar{U})(i) \rightarrow \mathbb{Q}cl(Z) \rightarrow 0$$

for some cycle Z on X homologically equivalent to zero, and $U = X \setminus Z$.

Similarly, when $r \neq \lceil (n+1)/2 \rceil$

$$K_{2r-n-1}^{(r)}(\bar{X}) \otimes \mathbb{Q}_p \simeq H_f^1(G, H^n(\bar{X}, \mathbb{Q}_p(r))).$$

Will refer to these as *standard conjectures on mixed motives*.

The statements are of the form

$$\mathrm{Ext}_{\mathrm{Mot}_{\mathbb{Z}}}^1(\mathbb{Q}, M) \otimes \mathbb{Q}_p \simeq \mathrm{Ext}_{G,f}^1(\mathbb{Q}_p, M_p),$$

together with various explicit conjectural descriptions of the motivic extensions.

Instructive also to compare with conjectures of Tate (or Hodge) type:

$$\mathrm{Hom}_{\mathrm{Mot}_{\mathbb{Z}}}(\mathbb{Q}, M) \otimes \mathbb{Q}_p \simeq \mathrm{Hom}_G(\mathbb{Q}_p, M_p).$$

1.3. Problems

Serious deficiency of the motivic formalism:

No description of

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

when X is not an abelian variety, for example, a curve of higher genus.

In general, if one fixes a base-point $b \in X$, one has maps

$$X(\mathbb{Q}) \rightarrow H_f^1(G, H^{2d-1}(\bar{X}, \mathbb{Q}_p)(d));$$

$$x \mapsto [x] - [b];$$

but the image is very difficult to control.

This is due in part to factorization

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & H_f^1(G, H^{2d-1}(\bar{X}, \mathbb{Q}_p)(d)) \\ & \searrow & \nearrow \\ & J_X(\mathbb{Q}) & \end{array}$$

making it difficult to disentangle points of X from those of J_X .

However, note that

$$H^{2d-1}(\bar{X}, \mathbb{Q}_p)(d) \simeq H_1(\bar{X}, \mathbb{Q}_p).$$

2. Non-abelian Albanese maps

Homotopy provides a refinement:

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

except for the need to interpret the homotopy and construct a useful target for this map.

In any case, as we run over x , the composition action

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

will turn the path spaces into *torsors* for the fundamental group. Thus, the target should be a moduli space of torsors.

2.1. Pro-finite version

The most elementary possibility uses the category

$$\mathrm{Cov}(\bar{X})$$

of finite étale covers of $\bar{X} = X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\bar{\mathbb{Q}})$:

$$F_x : \mathrm{Cov}(\bar{X}) \rightarrow \text{Finite Sets};$$

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

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

In this case, all these objects carry compatible continuous actions of $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

2.1.1 Remark

To compute the Galois action, one constructs an inverse system

$$\tilde{\tilde{X}} := \{\bar{X}_i\}_{i \in I}$$

of finite étale covers of \bar{X} . If $b \in X(\mathbb{Q})$, the choice of a lift $\tilde{b} \in \tilde{\tilde{X}}$, determines a unique model

$$(\tilde{X}, \tilde{b}) \rightarrow (X, b)$$

defined over \mathbb{Q} . Then

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

and

$$\hat{\pi}_1(\bar{X}; b, x) \simeq \tilde{X}_x.$$

That is, the G -action can be computed on the fibers of $\tilde{X} \rightarrow X$.

2.1.2. Example

$(X, b) = (E, e)$ an elliptic curve. Then

$$(\tilde{E}, \tilde{e}) = (\{n : E \rightarrow E\}, e),$$

and

$$\hat{\pi}_1(\bar{E}, e) \simeq \hat{T}(E)$$

$$\hat{\pi}_1(\bar{E}; e, x) = \{(y_n) \mid my_{mn} = y_n, y_1 = x\}.$$

This torsor is trivial if and only if there is a G -invariant element in it, that is, a rational collection of division points. Not possible for $x \neq e$.

2.1.3. Remark

Description of \tilde{X} is essentially intractable for hyperbolic curves.

2.1.4. The section conjecture

We have thus a pro-finite étale Albanese map

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

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

to a continuous non-abelian cohomology set classifying G -equivariant torsors for $\hat{\pi}_1(\bar{X}, b)$.

Grothendieck's section conjecture:

When X is a smooth projective curve of genus ≥ 2 , then this map should be a bijection. That is, *all* G -equivariant torsors for $\hat{\pi}_1(\bar{X}, b)$ should be path torsors.

Should be viewed as a non-abelian extension of the conjecture of Birch and Swinnerton-Dyer, providing some kind of computable structure to the set of rational points.

Application to Diophantine geometry?

2.2. Motivic version

Difficult to study the profinite non-abelian Albanese map because $H^1(G, \hat{\pi}_1(\bar{X}, b))$ has very little geometric structure.

The *motivic fundamental group*

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

lies between the pro-finite fundamental group and homology:

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

Correspondingly, we have the classifying space of motivic torsors

$$H^1(G, \pi_1^M(\bar{X}, b)),$$

substantially more informative than $\text{Ext}^1(\mathbb{Q}, H_1(\bar{X}))$, but much more tractable than $H^1(G, \hat{\pi}_1(\bar{X}, b))$.

Note that we will be discussing motives only at the level of certain *realizations*, so the classifying space is also a compatible system of classifying spaces.

[However, Faltings and Hadian have ideas for working directly with mixed motives.]

The most important portion is a tower

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

arising from the \mathbb{Q}_p -pro-unipotent étale fundamental group

$$U := \pi_{1,et}^{\mathbb{Q}_p}(\bar{X}, b),$$

where p is a prime of good reduction.

Brief description of the constructions.

1. The étale site of \bar{X} defines a category

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

of locally constant unipotent \mathbb{Q}_p -sheaves on \bar{X} . A sheaf \mathcal{V} is unipotent if it can be constructed using successive extensions by the constant sheaf $[\mathbb{Q}_p]_{\bar{X}}$.

2. We have a fiber functor

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

that associates to a sheaf \mathcal{V} its stalk \mathcal{V}_b . Then

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

the tensor-compatible automorphisms of the functor. U is a pro-algebraic pro-unipotent group over \mathbb{Q}_p .

3.

$$U = U^1 \supset U^2 \supset U^3 \supset \dots$$

is the descending central series of U , and

$$U_n = U^{n+1} \setminus U$$

are the associated quotients. There is an identification

$$U_1 = H_1^{et}(\bar{X}, \mathbb{Q}_p) = V_p(J) := T_p J \otimes \mathbb{Q}_p$$

at the bottom level and exact sequences

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

for each n .

4. U has a natural action of G lifting the action on V_p , and $H^1(G, U_n)$ denotes continuous Galois cohomology with values in the points of U_n . For $n \geq 2$, this is *non-abelian cohomology*, and hence, does not have the structure of a group.

5. $H_f^1(G, U_n) \subset H^1(G, U_n)$ denotes a subset defined by local ‘Selmer’ conditions that require the classes to be

(a) unramified outside the set $T = S \cup \{p\}$, where S is the set of primes of bad reduction;

(b) and *crystalline* at p , a condition coming from p -adic Hodge theory.

6. The system

$$\cdots \rightarrow H_f^1(G, U_{n+1}) \rightarrow H_f^1(G, U_n) \rightarrow H_f^1(G, U_{n-1}) \rightarrow \cdots$$

is a pro-algebraic variety, the *Selmer variety* of X . That is, each $H_f^1(G, U_n)$ is an algebraic variety over \mathbb{Q}_p and the transition maps are algebraic.

$$H_f^1(G, U) = \{H_f^1(G, U_n)\}$$

is the moduli space of principal bundles for U in the étale topology of $\text{Spec}(\mathbb{Z}[1/S])$ that are crystalline at p .

If \mathbb{Q}_T denotes the maximal extension of \mathbb{Q} unramified outside T and $G_T := \text{Gal}(\mathbb{Q}_T/\mathbb{Q})$, then $H_f^1(G, U_n)$ is naturally realized as a closed subvariety of $H^1(G_T, U_n)$.

For the latter, there are sequences

$$0 \rightarrow H^1(G_T, U^{n+1} \setminus U^n) \rightarrow H^1(G_T, U_n) \rightarrow H^1(G_T, U_{n-1}) \xrightarrow{\delta} \\ H^2(G_T, U^{n+1} \setminus U^n)$$

exact in a natural sense, and the algebraic structures are built up iteratively from the \mathbb{Q}_p -vector space structure on the

$$H^i(G_T, U^{n+1} \setminus U^n)$$

using the fact that the boundary maps δ are algebraic. (It is non-linear in general.)

7. The map

$$\kappa^u = \{\kappa_n^u\} : X(\mathbb{Q}) \longrightarrow H_f^1(G, U)$$

is defined by associating to a point x the principal U -bundle

$$P(x) = \pi_1^{u, \mathbb{Q}_p}(\bar{X}; b, x) := \text{Isom}^{\otimes}(F_b, F_x)$$

of tensor-compatible isomorphisms from F_b to F_x , that is, the \mathbb{Q}_p -pro-unipotent étale paths from b to x .

For $n = 1$,

$$\kappa_1^u : X(\mathbb{Q}) \rightarrow H_f^1(G, U_1) = H_f^1(G, T_p J \otimes \mathbb{Q}_p)$$

reduces to the map from Kummer theory. But the map κ_n^u for $n \geq 2$ does not factor through the Jacobian. Hence, suggests the possibility of separating the structure of $X(\mathbb{Q})$ from that of $J(\mathbb{Q})$.

2.3. Remark

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

But the idea of putting points into *geometric families of structured objects* is a classical one in Diophantine geometry, as in the the Kodaira Parshin-construction, or 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 torsors $\pi_1(X; b, x)$ running over the moduli space $H_f^1(G, U)$ is an extremely primitive version of this idea.

3. 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:

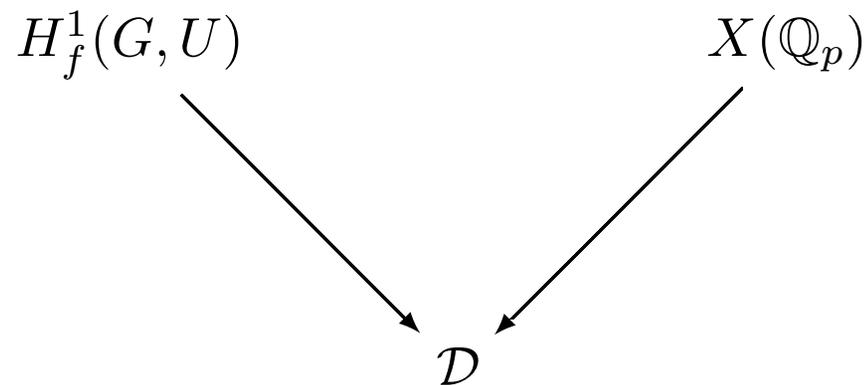
$$H_f^1(G, U)$$

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 $H_f^1(G, U)$ maps to an algebraic subspace, while $X(\mathbb{Q}_p)$ maps to a (locally) *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 $X_{\mathbb{Q}_p}$ that classifies unipotent vector bundles with flat connections, and the map

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

is a *holonomy map* expressed using p -adic iterated integrals.

There is actually a commutative diagram

$$\begin{array}{ccccc}
 X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & & \\
 \downarrow & & \downarrow & \searrow & \\
 H_f^1(G, U_n) & \xrightarrow{\text{loc}_p} & H_f^1(G_p, U_n) & \xrightarrow{\cong} & U_n^{DR}/F^0
 \end{array}$$

$H_f^1(G, U)$: moduli space of U -torsors on $\text{Spec}(\mathbb{Z}[1/T])$ that are crystalline at p .

$H_f^1(G_p, U_n)$: moduli space of crystalline U -torsors on $\text{Spec}(\mathbb{Q}_p)$.

U/F^0 : moduli space of U^{DR} torsors with compatible action of Frobenius and reduction of structure group to F^0 .

3.1 Some results

Theorem 0.1 *If the map*

$$H_f^1(G, U_n) \rightarrow D_n = U_n^{DR} / F^0$$

is not dominant for some n , then $X(\mathbb{Q})$ is finite.

Proof: Inside D_n ,

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

is discrete and compact. \square

1. The ‘standard motivic conjectures’ (e.g. Fontaine-Mazur), imply that $H_f^1(G, U_n) \rightarrow D_n$ is non-dense for $n \gg 0$.

2. Can prove non-denseness unconditionally when

$$\text{Im}(G) \subset \text{Aut}(H_1(\bar{X}, \mathbb{Q}_p))$$

is essentially abelian:

- (a) Genus zero minus three points;
- (b) Genus one CM minus one point;
- (c) Genus ≥ 2 with potentially CM Jacobian (joint with J. Coates).

3. Some non-abelian cases of genus $g \geq 2$ at the boundary of Chabauty's method, that is, when $\text{rank} J_X(\mathbb{Q}) = g$. In this case, sometimes get precise formula describing

$$\overline{\text{Im}(H_f^1(G, U_n))} \subset D_n.$$

3.1.1 Remarks

1. Grothendieck seems to have thought section conjecture \Rightarrow finiteness.

2.(c) In this proof, the dimensions of

$$H_f^1(G, U_n)$$

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.

3. In fact, effectively computing defining equations for

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

seems in principle possible because of the algebraicity of the localization map.

This can be used to show:

Section conjecture + standard conjecture on mixed motives
 \Rightarrow Terminating algorithm for finding all rational points on
a curve of genus ≥ 2 .

In this implication, the role of the section conjecture is exactly analogous to the finiteness of III, in that it leads to the termination of a non-abelian descent algorithm.

On the other hand, the unipotent Albanese map together with the standard conjectures enables us, in principle, to find an effective N such that

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{Z}_p) \rightarrow X(\mathbb{Z}/p^N)$$

is an injection. This, in turn, will yield an effective M such that the map

$$X(\mathbb{Q}) \rightarrow H^1(G_T, H_1(\bar{X}, \mathbb{Z}/M))$$

is injective, allowing us to begin a descent algorithm.

However, a key problem is to find a precise general formula for a function that vanishes on $\overline{Im(H_f^1(G, U_n))}$ as a consequence of a *non-abelian explicit reciprocity law*.

4. Tangential localization

Now X is defined over a number field F and $v|p$ is a prime of local degree 1 ($[F_v : \mathbb{Q}_p] = 1$).

Study the *tangential localization map*:

$$d\text{loc}_v(c) : T_c H_f^1(G, U) \rightarrow T_{\text{loc}_v(c)} H_f^1(G_v, U)$$

at a point $c \in H_f^1(G, U)$.

Formulae:

$$T_c H_f^1(G, U) \simeq H_f^1(G, L(c));$$

$$T_{\text{loc}_v(c)} H_f^1(G_v, U) \simeq H_f^1(G_v, L(c));$$

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

For non-denseness, suffices to show that $d\text{loc}_v(c)$ is not surjective at generic points c .

Can formulate a criterion in terms of the cotangent space:

$$T_{\text{loc}_v(c)}^* H_f^1(G_v, U) \simeq H^1(G_v, (L(c))^*(1)) / H_f^1(G_v, (L(c))^*(1))$$

coming from local Tate duality.

Theorem 0.2 *Assume that for generic c there is a class*

$$z \in H^1(G_T, (L_n(c))^*(1))$$

such that $\text{loc}_w(z) = 0$ for $w \neq v$ and

$$\text{loc}_v(z) \notin H_f^1(G_v, (L_n(c))^*(1)).$$

Then

$$\text{loc}_v : H_f^1(G, U_n) \rightarrow H_f^1(G_v, U_n)$$

is not dominant.

Proof.

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

$$\text{loc}_T : H^1(G_T, L_n(c)) \rightarrow \bigoplus_{w \in T} H^1(G_w, L_n(c))$$

and

$$\text{loc}_T : H^1(G_T, (L_n(c))^*(1)) \rightarrow \bigoplus_{w \in T} H^1(G_w, (L_n(c))^*(1))$$

are exact annihilators under the natural pairing

$$\langle \cdot, \cdot \rangle : \bigoplus_{w \in T} H^1(G_w, L_n(c)) \times \bigoplus_{w \in T} H^1(G_w, (L_n(c))^*(1)) \rightarrow \mathbb{Q}_p.$$

With respect to the pairing $\langle \cdot, \cdot \rangle_v$ at v , $H_f^1(G_v, L_n(c))$ and $H_f^1(G_v, (L_n(c))^*(1))$ are mutual annihilators.

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

$$\langle \text{loc}_T(z), (a_w) \rangle = \langle \text{loc}_v(z), a_v \rangle_v .$$

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

$$\langle \text{loc}_v(a), \text{loc}_v(z) \rangle_v = \langle \text{loc}_T(a), \text{loc}_T(z) \rangle = 0.$$

Since $\langle \cdot, \text{loc}_v(z) \rangle$ defines a non-trivial linear functional on $H_f^1(G_v, L_n(c))$, this implies the desired results. \square

Such a class z could be viewed as giving a *linearized equation* for the image of $H_f^1(G, U_n)$ is a neighborhood of $\text{loc}_v(c)$.

Can use this to show finiteness of integral points on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ over totally real fields, for example. [Also proved by Hadian using different methods.]

In any case, brings into focus the importance of studying *duality in families*.

5. Non-linear example

E/\mathbb{Q} elliptic curve with

$$\text{rank}E(\mathbb{Q}) = 1,$$

integral j -invariant, and

$$|\text{III}(E)[p^\infty]| < \infty$$

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,

$$d\omega = \left(\int_b^z \beta \right) \alpha.$$

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.

6. Question

Galois theory for polynomials $f(x, y)$?

7. Some references

- Selmer varieties for curves with CM Jacobians. (with John Coates).
- Massey products for elliptic curves of rank 1.
- p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication.
- The unipotent Albanese map and Selmer varieties for curves.
- A remark on fundamental groups and effective Diophantine methods for hyperbolic curves.
- The motivic fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel.