Iwasawa theory and Selmer schemes I
- torsion Selmer pointed sets -

Dohyeong Kim

Seoul National University

May 11, 2022
Iwasawa theory and p-adic L-functions

Motivation: Selmer groups and elliptic curves

Let E be an elliptic curve over a number field F. For $n \geq 1$, let $E[n]$ be the group of n-division points. The Kummer map

$$\kappa \colon E(F) \to H^1(F, E[n]) \tag{1}$$

allows one to study $E(F)$ in terms of the Galois cohomology groups.
Observations:

1. It is a homomorphism between abelian groups.
2. The kernel is $nE(F)$.
3. The image satisfies 'local conditions'.

Hyperbolic curves

For hyperbolic curves, their integral/rational points are not directly approachable using Selmer groups. For simplicity let us consider the case of $X = E - \{\infty\}$, smooth over $R = \mathbb{Z}[\frac{1}{N}]$ for some $N \geq 1$.
It is known that $X(R)$ is not an abelian group. The Kummer map induces a map

$$X(R) \hookrightarrow E(\mathbb{Q}) \to H^1(\mathbb{Q}, E[n]) \tag{2}$$

which 'forgets too much'.

Nonabelian Kummer map

The Chabauty-Kim method in this case proposes to study, with a choice of a prime p, the nonabelian analogue of the Kummer map

$$\kappa_m \colon X(R) \to H^1(\mathbb{Q}, U_m) \tag{3}$$

where U_m is a unipotent algebraic group over $\mathbb{Q}_p$ with Galois action, and m denotes the class of U_m as a nilpotent group. We note:

1. If $m = 1$ then U_m is abelian.
2. The image satisfies 'local conditions'.
3. If m is sufficiently large, κ_m should capture enough information about $X(R)$. (The dimension hypothesis)

This extends to $X(F)$, when X is a smooth projective curve of genus at least two over a number field F together with a fixed F-rational base point.

Where does U_m come from?

Let Γ be any finitely presented group and k a field of characteristic zero. Fix $m \geq 1$ and consider the maps

$$\Gamma \to U(k) \tag{4}$$

where U/k is a unipotent algebraic group over k of class m. Form a category by adding morphisms as k-maps $U \to V$ subject to the obvious compatibility conditions.
There is a universal such homomorphism

$$\Gamma \to U_m(k) \tag{5}$$

which we refer to as the unipotent completion of class m. They form a projective system by functoriality.

Where does U_m come from?

If $k = \mathbb{Q}_p$, then we can consider a topological analogue by considering continuous maps

$$\widehat{\Gamma} \to U_m(\mathbb{Q}_p) \tag{6}$$

where $\widehat{\Gamma}$ is the profinite completion.
These two notions agree, a fact I learned in a paper by Hain and Matsumoto. In the arithmetic setting, we take $\Gamma = \pi_1$, the (topological) fundamental group whose profinite completion is the etale fundamental group.

Finite nonabelian coefficients?

In a sense, $U_m(\mathbb{Q}_p)$ is the nonabelian extension of

$$U_1(\mathbb{Q}_p) = \left(\varprojlim_r E[p^r] \right) \otimes_{\mathbb{Z}_P} \mathbb{Q}_p \tag{7}$$

and it is not clear how each $E[p^r]$ extends in the nonabelian context.

Integral coefficients

To have a nonabelian extension of $E[p^r]$, one could look for the unipotent completion defined over $\mathbb{Z}_p$. Taking reduction modulo powers of p, one would get finite nonabelian coefficiets.
My goal today is to explain how this can be done.

Integral unipotent completion

Adopt the convention that all Lie algebras are finitely generately over the base ring. Here is my key result:

Theorem (K-.)

If $\mathfrak{U}/\mathbb{Q}_p$ is a nilpotent Lie algebra and $C \subset \mathfrak{U}$ is a compact subset, then C is contained in a powerful Lie $\mathbb{Z}_p$-algebra $\mathfrak{u}$.

Some remarks:

1. Being powerful means $[\mathfrak{u}, \mathfrak{u}] \subset 2p \cdot \mathfrak{u}$.
2. The proof is by elementary induction on the class of $\mathfrak{U}$.
3. The nilpotency is strictly necessary.

Integral unipotent completion

Let $\widehat{\Gamma}$ be the profinite completion of a finitely generated group Γ and

$$\gamma_m \colon \widehat{\Gamma} \to U_m(\mathbb{Q}_p) \tag{8}$$

be the universal homomorphism. The log induces a bijection

$$L \colon U_m(\mathbb{Q}_p) \to \mathfrak{U}_m \tag{9}$$

where $\mathfrak{U}_m$ is the Lie algebra. By continuity, $L \circ \gamma_m$ has compact image and is contained in a minimal powerful Lie $\mathbb{Z}_p$-algebra.
Call it the nilpotent envelop, denoted by $\mathfrak{u}_m$.

Application

An immediate application is the map

$$X(R) \to H^1(F, \mathfrak{u}_m/p^r\mathfrak{u}_m) \tag{10}$$

with finite nonabelian coefficients.

graded analogue

As a variation, consider

$$C = \bigoplus_{1 \le j \le m} \left(\Gamma^j / \Gamma^{j+1} \right) \otimes_{\mathbb{Z}} \mathbb{Z}_p \tag{11}$$

where Γ^j is the central series $\Gamma^1 = \Gamma$, $\Gamma^2 = [\Gamma, \Gamma]$, $\Gamma^3 = [\Gamma^2, \Gamma]$, and so on. Let $\mathfrak{u}_m$ be the powerful envelop of C inside $C \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then, $\mathfrak{u}_m$ is a *graded* Lie $\mathbb{Z}_p$-algebra.

the advantage of graded analogue

In the graded analogue, we have the endomorphism

$$\langle p \rangle (x_i)_i \mapsto (p^i x_i)_i \tag{12}$$

which is a Lie-homomorphism.
This idea goes back to K. Sakugawa. I think he was the first to notice and use graded objects. My contribution is to supply graded objects of arbitrary class by taking suitable envelops.

torsion Selmer pointed sets

Let $\mathfrak{u}_m$ be obtained from the etale fundamental group of a hyperbolic curve defined over a number field F. The pointed sets

$$H^1(F, \mathfrak{u}_m/p^r\mathfrak{u}_m) \tag{13}$$

together with maps between them induced by $\langle p \rangle$ form a non-abelian analogue of the family

$$H^1(F, E[p^r]) \tag{14}$$

when E/F is an elliptic curve.

Sakugawa's Theorem and its extension

In this setting, we obtain an extension of Sakugawa's theorem. For simplicity, we do not consider 'twisting by finite order characters'. Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension. Put $\Gamma_n := \mathrm{Gal}(F_\infty/F_n)$. The theorem involves the restriction maps

$$H^1_f(F_n, \mathfrak{u}_m/p^r\mathfrak{u}_m) \to H^1_f(F_\infty, \mathfrak{u}_m/p^r\mathfrak{u}_m)^{\Gamma_n} \tag{15}$$

and the theorem extends Mazur's control theorem of the case $m = 1$. We need a notion that extends the cokernel.

Sakugawa's Theorem and its extension

Instead of looking at cokernels, we ask whether the image of

$$H^1_f(F_n, \mathfrak{u}_m/p^r\mathfrak{u}_m) \to H^1_f(F_\infty, \mathfrak{u}_m/p^r\mathfrak{u}_m)^{\Gamma_n} \tag{16}$$

is contained in the image of

$$\langle p^M \rangle \colon H^1_f(F_\infty, \mathfrak{u}_m/p^r\mathfrak{u}_m)^{\Gamma_n} \longrightarrow H^1_f(F_\infty, \mathfrak{u}_m/p^r\mathfrak{u}_m)^{\Gamma_n} \tag{17}$$

for some large M.

Theorem (K-.)

The desired M can be chosen independently of $(r, n) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$.

Proof.

Identical to Sakugawa's proof when $m < p$. □

Thank You!