

Anabelian geometry

Grothendieck's programme: K a field, Y/K a smooth connected variety, $y \in Y(K)$ a basepoint. We have the profinite étale fundamental group $\pi_1^{\text{ét}}(Y_{\overline{K}}; y)$, endowed with a Galois action; for $z \in Y(K)$ we also have the profinite torsor of paths $\pi_1^{\text{ét}}(Y_{\overline{K}}; y, z)$, endowed with a compatible Galois action. One can study the Diophantine geometry of Y via the *non-abelian Kummer map*

$$Y(K) \rightarrow H^1(G_K, \pi_1^{\text{ét}}(Y_{\overline{K}}; y)).$$

Kim's variant: U_n/\mathbb{Q}_ℓ the n -step \mathbb{Q}_ℓ -unipotent étale fundamental group of (Y, y) . Study the Diophantine geometry of Y via the more computable non-abelian Kummer map

$$Y(K) \rightarrow H^1(G_K, U_n(\mathbb{Q}_\ell)).$$

Unipotent Kummer maps for small n

When $n = 1$ and Y is complete, $U_1 = V_\ell \text{Alb}(Y)$ is the \mathbb{Q}_ℓ -linear Tate module of the Albanese variety of Y , and the “non-abelian” Kummer map is the composite

$$Y(K) \rightarrow \text{Alb}(Y)(K) \rightarrow H^1(G_K, V_\ell \text{Alb}(Y)).$$

The non-abelian Kummer maps for $n > 1$ are thought to see more refined arithmetic information. In the particular case that $n = 2$, the non-abelian Kummer map is thought to see information related to archimedean and ℓ -adic heights.

Local heights as functions on H^1

Theorem (Balakrishnan–Dan–Cohen–Kim–Wewers, 2014)

Let E° be the complement of 0 in an elliptic curve E over a p -adic local field K , and U_2 the 2-step \mathbb{Q}_ℓ -unipotent fundamental group ($\ell \neq p$) of E° . Then the natural map $\mathbb{Q}_\ell(1) \hookrightarrow U_2$ induces a bijection on H^1 , and the composite map

$$E^\circ(K) \rightarrow H^1(G_K, U_2(\mathbb{Q}_\ell)) \xleftarrow{\sim} H^1(G_K, \mathbb{Q}_\ell(1)) \xrightarrow{\sim} \mathbb{Q}_\ell$$

is a \mathbb{Q} -valued Néron function on E with divisor $2[0]$, postcomposed with the natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_\ell$.

Generalisation to abelian varieties: setup

In place of the elliptic curve E , we will consider an abelian variety A over a local field K and a line bundle L/A , and let $L^\times = L \setminus 0$ denote the complement of the zero section. The natural abelian invariant associated to this setup is the \mathbb{Q}_ℓ -unipotent fundamental group of L^\times – this is a central extension of the \mathbb{Q}_ℓ -linear Tate module $V_\ell A$ by $\mathbb{Q}_\ell(1)$.

The role of the local height in this setup is played by the *Néron log-metric*

$$\lambda_L: L^\times(K) \rightarrow \mathbb{R},$$

namely the unique (up to additive constants) function which scales like the log of a metric on the fibres of L and such that for any/all non-zero section(s) s of L , $\lambda_L \circ s$ is a Néron function on A with divisor $\text{div}(s)$. This is even \mathbb{Q} -valued when K is non-archimedean.

Conventions

Notation

Fix (for the rest of the talk) a prime p , a finite extension K/\mathbb{Q}_p , and an algebraic closure \overline{K}/K , determining an absolute Galois group G_K .

Later, we will denote by B_{dR} , B_{st} , B_{cris} etc. the usual period rings constructed by Fontaine, and will fix a choice of p -adic logarithm, giving us an embedding $B_{\text{st}} \hookrightarrow B_{\text{dR}}$.

Generalisation to abelian varieties: the theorem

Theorem (B.)

Let A/K be an abelian variety, L^\times/A the complement of zero in a line bundle L , and U the \mathbb{Q}_ℓ -unipotent fundamental group ($\ell \neq p$) of L^\times . Then the natural map $\mathbb{Q}_\ell(1) \hookrightarrow U$ induces a bijection on H^1 , and the composite map

$$L^\times(K) \rightarrow H^1(G_K, U(\mathbb{Q}_\ell)) \xleftarrow{\sim} H^1(G_K, \mathbb{Q}_\ell(1)) \xrightarrow{\sim} \mathbb{Q}_\ell$$

takes values in \mathbb{Q} , and is the* Néron log-metric on L .

The p -adic analogue

We will define a certain natural subquotient $H_{g/e}^1(G_K, U(\mathbb{Q}_p))$ of the non-abelian Galois cohomology set $H^1(G_K, U(\mathbb{Q}_p))$, allowing us to state a p -adic analogue of the preceding theorem.

Theorem (B.)

Let A/K be an abelian variety, L^\times/A the complement of zero in a line bundle L , and let U be the \mathbb{Q}_p -unipotent fundamental group of L^\times . Then U is de Rham, the natural map $\mathbb{Q}_p(1) \hookrightarrow U$ induces a bijection on $H_{g/e}^1$, and the composite map

$$L^\times(K) \rightarrow H_{g/e}^1(G_K, U(\mathbb{Q}_p)) \xleftarrow{\sim} H_{g/e}^1(G_K, \mathbb{Q}_p(1)) \xrightarrow{\sim} \mathbb{Q}_p$$

is (well-defined and) the Néron log-metric on L .

Local (abelian) Bloch–Kato Selmer groups

- ▶ S. Bloch and K. Kato define, for any de Rham representation V of G_K on a \mathbb{Q}_p -vector space, subspaces

$$H_e^1(G_K, V) \leq H_f^1(G_K, V) \leq H_g^1(G_K, V)$$

of the Galois cohomology $H^1(G_K, V)$.

- ▶ Their dimensions are easily computable, and $H_e^1(G_K, V)$ can be studied via an “exponential” exact sequence

$$0 \rightarrow V^{G_K} \rightarrow D_{\text{cris}}^{\varphi=1}(V) \rightarrow D_{\text{dR}}(V)/D_{\text{dR}}^+(V) \rightarrow H_e^1(G_K, V) \rightarrow 0.$$

- ▶ When $V = V_p A$ is the \mathbb{Q}_p Tate module of an abelian variety A/K , these are all equal to the \mathbb{Q}_p -span of the image of the Kummer map

$$A(K) \rightarrow H^1(G_K, V_p A).$$

Local non-abelian Bloch–Kato Selmer sets

- ▶ Following Kim, we will define, for any de Rham representation U/\mathbb{Q}_p of G_K on a unipotent group, pointed subsets

$$H_e^1(G_K, U(\mathbb{Q}_p)) \subseteq H_f^1(G_K, U(\mathbb{Q}_p)) \subseteq H_g^1(G_K, U(\mathbb{Q}_p))$$

of the non-abelian Galois cohomology set $H^1(G_K, U(\mathbb{Q}_p))$.

- ▶ We will also make sense of the relative quotients, including $H_{g/e}^1(G_K, U(\mathbb{Q}_p)) = H_g^1/H_e^1$, which appears in the p -adic main theorem.
- ▶ $H_e^1(G_K, U(\mathbb{Q}_p))$ can be studied via an “exponential” exact sequence generalising the abelian sequence (see later).
- ▶ When U is the \mathbb{Q}_p pro-unipotent* fundamental group of a smooth connected variety Y/K (which is de Rham), H_g^1 contains the image of the non-abelian Kummer map

$$Y(K) \rightarrow H^1(G_K, U(\mathbb{Q}_p)).$$

Basic definitions

Definition (Galois representations on unipotent groups)

A representation of G_K on a unipotent group U/\mathbb{Q}_p is an action of G_K on U (by algebraic automorphisms) such that the action on $U(\mathbb{Q}_p)$ is continuous.

We say that U is *de Rham* (resp. *semistable*, *crystalline* etc.) just when the following equivalent conditions hold:

- ▶ $\text{Lie}(U)$ is de Rham;
- ▶ $\mathcal{O}(U)$ is ind-de Rham;
- ▶ $\dim_K(D_{\text{dR}}(U)) = \dim_{\mathbb{Q}_p}(U)$, where $D_{\text{dR}}(U)/K$ is the unipotent group representing the functor

$$D_{\text{dR}}(U)(A) := U(A \otimes_K B_{\text{dR}})^{G_K}.$$

Definition (Local non-abelian Bloch–Kato Selmer sets)

Let U/\mathbb{Q}_p be a de Rham representation of G_K on a unipotent group. We define pointed subsets

$$H_e^1(G_K, U(\mathbb{Q}_p)) \subseteq H_f^1(G_K, U(\mathbb{Q}_p)) \subseteq H_g^1(G_K, U(\mathbb{Q}_p))$$

of the non-abelian cohomology $H^1(G_K, U(\mathbb{Q}_p))$ to be the kernels

$$H_e^1(G_K, U(\mathbb{Q}_p)) := \ker \left(H^1(G_K, U(\mathbb{Q}_p)) \rightarrow H^1(G_K, U(\mathbb{B}_{\text{cris}}^{\varphi=1})) \right);$$

$$H_f^1(G_K, U(\mathbb{Q}_p)) := \ker \left(H^1(G_K, U(\mathbb{Q}_p)) \rightarrow H^1(G_K, U(\mathbb{B}_{\text{cris}})) \right);$$

$$H_g^1(G_K, U(\mathbb{Q}_p)) := \ker \left(H^1(G_K, U(\mathbb{Q}_p)) \rightarrow H^1(G_K, U(\mathbb{B}_{\text{st}})) \right).$$

One can use \mathbb{B}_{dR} in place of \mathbb{B}_{st} in the definition of H_g^1 .

Definition (Quotients of Bloch–Kato Selmer sets)

Let U/\mathbb{Q}_p be a de Rham representation of G_K on a unipotent group. We denote by $\sim_{H_e^1}$, $\sim_{H_f^1}$, $\sim_{H_g^1}$ the equivalence relations on $H^1(G_K, U(\mathbb{Q}_p))$ whose equivalence classes are the fibres of

$$H^1(G_K, U(\mathbb{Q}_p)) \rightarrow H^1(G_K, U(\mathbb{B}_{\text{cris}}^{\varphi=1}));$$

$$H^1(G_K, U(\mathbb{Q}_p)) \rightarrow H^1(G_K, U(\mathbb{B}_{\text{cris}}));$$

$$H^1(G_K, U(\mathbb{Q}_p)) \rightarrow H^1(G_K, U(\mathbb{B}_{\text{st}})).$$

We then define, for instance, the *Bloch–Kato quotient*

$$H_{g/e}^1(G_K, U(\mathbb{Q}_p)) := H_g^1(G_K, U(\mathbb{Q}_p)) / \sim_{H_e^1}.$$

Why a cosimplicial approach?

The abelian Bloch–Kato exponential for a de Rham representation V arises from tensoring it with the exact sequence

$$0 \rightarrow \mathbb{Q}_p \rightarrow B_{\text{cris}}^{\varphi=1} \rightarrow B_{\text{dR}}/B_{\text{dR}}^+ \rightarrow 0$$

and taking the long exact sequence in Galois cohomology. Equivalently, if we consider the cochain complex

$$C_e^\bullet : B_{\text{cris}}^{\varphi=1} \rightarrow B_{\text{dR}}/B_{\text{dR}}^+,$$

then the cohomology groups of the cochain $(C_e^\bullet \otimes_{\mathbb{Q}_p} V)^{G_K}$ are canonically identified as

$$H^j \left((C_e^\bullet \otimes_{\mathbb{Q}_p} V)^{G_K} \right) \cong \begin{cases} V^{G_K} & j = 0; \\ H_e^1(G_K, V) & j = 1; \\ 0 & j \geq 2. \end{cases}$$

The advantage of using cochain complexes is that we can perform analogous constructions for H_f^1 and H_g^1 . For instance, taking the cochain complex

$$C_g^\bullet : B_{\text{st}} \rightarrow B_{\text{st}}^{\oplus 2} \oplus B_{\text{dR}}/B_{\text{dR}}^+ \rightarrow B_{\text{st}},$$

the cohomology groups of the cochain $(C_g^\bullet \otimes_{\mathbb{Q}_p} V)^{G_K}$ are canonically identified as

$$H^j \left((C_g^\bullet \otimes_{\mathbb{Q}_p} V)^{G_K} \right) \cong \begin{cases} V^{G_K} & j = 0; \\ H_g^1(G_K, V) & j = 1; \\ D_{\text{cris}}^{\varphi=1}(V^*(1))^* & j = 2; \\ 0 & j \geq 3. \end{cases}$$

The cochain complexes C_e^\bullet , C_f^\bullet , C_g^\bullet themselves cannot be directly be used in the non-abelian setting (as we cannot tensor a group by a vector space), so we have to tweak them slightly to find a non-abelian generalisation of the Bloch–Kato exponential.

For example, in place of C_e^\bullet , we consider the diagram

$$B_{\text{cris}}^{\varphi=1} \times B_{\text{dR}}^+ \rightrightarrows B_{\text{dR}}$$

of \mathbb{Q}_p -algebras. Taking points in U and then G_K -fixed points, we then obtain the diagram

$$D_{\text{cris}}^{\varphi=1}(U)(\mathbb{Q}_p) \times D_{\text{dR}}^+(U)(K) \rightrightarrows D_{\text{dR}}(U)(K).$$

There is an action of $D_{\text{cris}}^{\varphi=1}(U)(\mathbb{Q}_p) \times D_{\text{dR}}^+(U)(K)$ on $D_{\text{dR}}(U)(K)$ by $(x, y): z \mapsto y^{-1}zx$ – we will see later that the orbit space is canonically identified with $H_e^1(G_K, U(\mathbb{Q}_p))$.

Non-abelian analogy

In order to extend the study of local Bloch–Kato Selmer groups to the non-abelian context, we need to replace three abelian concepts with non-abelian analogues.

- ▶ In place of the cochain complexes C_*^\bullet of G_K -representations, we will use *cosimplicial \mathbb{Q}_p -algebras* B_*^\bullet with G_K -action.
- ▶ In place of the cochain complexes $(C_*^\bullet \otimes_{\mathbb{Q}_p} V)^{G_K}$, we will examine the *cosimplicial groups* $U(B_*^\bullet)^{G_K}$.
- ▶ In place of the cohomology groups of these cochain complexes, we will calculate the *cohomotopy groups/sets* of the corresponding cosimplicial groups.

Cosimplicial groups

Definition (Cosimplicial objects)

A *cosimplicial object* of a category \mathcal{C} is a covariant functor $X^\bullet: \Delta \rightarrow \mathcal{C}$ from the simplex category Δ of non-empty finite ordinals and order-preserving maps. We think of this as a collection of objects X^n together with *coface* maps d^\bullet

$$X^0 \rightrightarrows X^1 \begin{matrix} \rightrightarrows \\ \leftarrow \\ \rightarrow \end{matrix} X^2 \dots$$

and *codegeneracy* maps s^\bullet

$$X^0 \leftarrow X^1 \begin{matrix} \leftarrow \\ \rightarrow \\ \leftarrow \end{matrix} X^2 \dots$$

satisfying certain identities.

Definition (Cohomotopy groups/sets)

Let U^\bullet be a cosimplicial group

$$U^0 \rightrightarrows U^1 \begin{matrix} \rightrightarrows \\ \leftarrow \\ \rightarrow \end{matrix} U^2 \dots$$

We define the *0th cohomotopy group* $\pi^0(U^\bullet)$ to be

$$\pi^0(U^\bullet) := \{u^0 \in U^0 \mid d^0(u^0) = d^1(u^0)\} \leq U^0.$$

We also define the pointed set of *1-cocycles* to be

$$Z^1(U^\bullet) := \{u^1 \in U^1 \mid d^1(u^1) = d^2(u^1)d^0(u^1)\} \subseteq U^1$$

and the *1st cohomotopy (pointed) set* $\pi^1(U^\bullet) := Z^1(U^\bullet)/U^0$ to be the quotient of $Z^1(U^\bullet)$ by the twisted conjugation action of U^0 , given by $u^0: u^1 \mapsto d^1(u^0)^{-1}u^1d^0(u^0)$.

Definition (Cohomotopy groups/sets (cont.))

When U^\bullet is abelian, $\pi^0(U^\bullet)$ and $\pi^1(U^\bullet)$ are abelian groups, and we can define the higher cohomotopy groups $\pi^j(U^\bullet)$ to be the cohomology groups of the cochain complex

$$U^0 \rightarrow U^1 \rightarrow U^2 \dots$$

with differential $\sum_k (-1)^k d^k$.

Example (Non-abelian group cohomology)

Suppose G is a topological group acting continuously on another topological group U . Then $C^n(G, U) := \text{Map}_{\text{cts}}(G^n, U)$ can be given the structure of a cosimplicial group. Its cohomotopy $\pi^j(C^\bullet(G, U))$ is canonically identified with the group cohomology $H^j(G, U)$ for $j = 0, 1$, and for all j when U is abelian.

Long exact sequences in cohomotopy

Notation

When we assert that a sequence

$$\dots \rightarrow U^{r-1} \rightarrow U^r \xrightarrow{\cong} U^{r+1} \rightarrow U^{r+2} \rightarrow \dots$$

is *exact*, we shall mean that:

- ▶ $\dots \rightarrow U^{r-1} \rightarrow U^r$ is an exact sequence of groups (and group homomorphisms);
- ▶ $U^{r+1} \rightarrow U^{r+2} \rightarrow \dots$ is an exact sequence of pointed sets;
- ▶ there is an action of U^r on U^{r+1} whose orbits are the fibres of $U^{r+1} \rightarrow U^{r+2}$, and whose point-stabiliser is the image of $U^{r-1} \rightarrow U^r$.

Cosimplicial groups give us many ways of producing long exact sequences of groups and pointed sets. For example:

Theorem (Bousfield–Kan, 1972)

Let

$$1 \rightarrow Z^\bullet \rightarrow U^\bullet \rightarrow Q^\bullet \rightarrow 1$$

be a central extension of cosimplicial groups. Then there is a cohomotopy exact sequence

$$\begin{array}{ccccccc}
 1 & \rightarrow & \pi^0(Z^\bullet) & \rightarrow & \pi^0(U^\bullet) & \rightarrow & \pi^0(Q^\bullet) \\
 & & & & & & \downarrow \\
 & & \pi^1(Z^\bullet) & \xrightarrow{\sim} & \pi^1(U^\bullet) & \rightarrow & \pi^1(Q^\bullet) \rightarrow \pi^2(Z^\bullet)
 \end{array}$$

The cosimplicial models

Our general method for studying local Bloch–Kato Selmer sets and their quotients will be to define various cosimplicial \mathbb{Q}_p -algebras $B_e^\bullet, B_f^\bullet, B_g^\bullet, B_{g/e}^\bullet, B_{f/e}^\bullet$ with G_K -action such that, for any de Rham representation of G_K on a unipotent group U/\mathbb{Q}_p , we have a canonical identification

$$\pi^1 \left(U(B_*^\bullet)^{G_K} \right) \cong H_*^1(G_K, U(\mathbb{Q}_p)).$$

Cohomotopy of the cosimplicial Dieudonné functors

In fact, we can give a complete description of the cohomotopy groups/sets of each $U(\mathbf{B}_*^\bullet)^{G_K}$. For instance, we have

$$\pi^j \left(U(\mathbf{B}_e^\bullet)^{G_K} \right) \cong \begin{cases} U(\mathbb{Q}_p)^{G_K} & j = 0; \\ H_e^1(G_K, U(\mathbb{Q}_p)) & j = 1; \\ 0 & j \geq 2 \text{ and } U \text{ abelian;} \end{cases}$$

$$\pi^j \left(U(\mathbf{B}_{g/e}^\bullet)^{G_K} \right) \cong \begin{cases} D_{\text{cris}}^{\varphi=1}(U)(\mathbb{Q}_p) & j = 0; \\ H_{g/e}^1(G_K, U(\mathbb{Q}_p)) & j = 1; \\ D_{\text{cris}}^{\varphi=1}(U(\mathbb{Q}_p)^*(1))^* & j = 2 \text{ and } U \text{ abelian;} \\ 0 & j \geq 3 \text{ and } U \text{ abelian.} \end{cases}$$

Construction of Bloch–Kato algebras

The cosimplicial algebras required to make this work are all built from standard period rings. For example, the diagram

$$B_{\text{cris}}^{\varphi=1} \times B_{\text{dR}}^+ \rightrightarrows B_{\text{dR}}$$

(which we saw earlier) is a semi-cosimplicial \mathbb{Q}_p -algebra (that is, a cosimplicial algebra without codegeneracy maps). B_e^\bullet is then the universal cosimplicial \mathbb{Q}_p -algebra mapping to this semi-cosimplicial algebra (the cosimplicial algebra cogenerated by it). Concretely, this has terms

$$B_e^n = B_{\text{cris}}^{\varphi=1} \times B_{\text{dR}}^+ \times B_{\text{dR}}^n.$$

Construction of the non-abelian Bloch–Kato exponential (cont.)

It remains to show that the image of \exp is exactly $H_e^1(G_K, U(\mathbb{Q}_p))$. The exact sequence shows that the image is exactly the kernel of

$$H^1(G_K, U(\mathbb{Q}_p)) \rightarrow H^1(G_K, U(B_{\text{cris}}^{\varphi=1})) \times H^1(G_K, U(B_{\text{dR}}^+)),$$

which certainly is contained in $H_e^1(G_K, U(\mathbb{Q}_p))$.

It is then not too hard to prove that in fact the kernel is exactly $H_e^1(G_K, U(\mathbb{Q}_p))$, using the fact that the map

$$H^1(G_K, U(B_{\text{dR}}^+)) \rightarrow H^1(G_K, U(B_{\text{dR}}))$$

has trivial kernel (we omit the diagram-chase in the interests of brevity). This establishes the desired exact sequence, and hence the description of the cohomotopy of $U(B_e^\bullet)^{G_K}$. \square

Lemma

Let

$$1 \rightarrow Z \rightarrow U \rightarrow Q \rightarrow 1$$

be a central extension of de Rham representations of G_K on unipotent groups over \mathbb{Q}_p . Then there is an exact sequence

$$\begin{array}{c} 1 \longrightarrow D_{\text{cris}}^{\varphi=1}(Z)(\mathbb{Q}_p) \xrightarrow{z} D_{\text{cris}}^{\varphi=1}(U)(\mathbb{Q}_p) \longrightarrow D_{\text{cris}}^{\varphi=1}(Q)(\mathbb{Q}_p) \\ \left. \begin{array}{l} \longrightarrow H_{g/e}^1(G_K, Z(\mathbb{Q}_p)) \xrightarrow{\sim} H_{g/e}^1(G_K, U(\mathbb{Q}_p)) \longrightarrow H_{g/e}^1(G_K, Q(\mathbb{Q}_p)) \\ \longrightarrow D_{\text{cris}}^{\varphi=1}(Z(\mathbb{Q}_p)^*(1))^* \end{array} \right\} \end{array}$$

Proof of lemma.

From the construction of $B_{g/e}^\bullet$ (out of B_{st}), it follows that

$$1 \rightarrow Z(B_{g/e}^\bullet)^{G_K} \rightarrow U(B_{g/e}^\bullet)^{G_K} \rightarrow Q(B_{g/e}^\bullet)^{G_K} \rightarrow 1$$

is a central extension of cosimplicial groups. The desired exact sequence is then the cohomotopy exact sequence for these cosimplicial groups. □

If, as in the main theorem, U/\mathbb{Q}_p is the \mathbb{Q}_p -unipotent fundamental group of $L^\times = L \setminus 0$, where L is a line bundle on an abelian variety A/K , then U is a central extension

$$1 \rightarrow \mathbb{Q}_p(1) \rightarrow U \rightarrow V_p A \rightarrow 1.$$

Applying the preceding lemma shows that $\mathbb{Q}_p(1) \hookrightarrow U$ induces a bijection on $H_{g/e}^1$, so that $H_{g/e}^1(G_K, U(\mathbb{Q}_p)) \cong \mathbb{Q}_p$.

Showing that the $H_{g/e}^1$ -valued non-abelian Kummer map is then identified with the Néron log-metric requires some extra work, but is largely straightforward.