Foundations of the nonabelian method of Chabauty

Minhyong Kim and Martin Lüdtke

Contents

1. Introduction and apologies

What follows is a somewhat disorganised collection of lecture notes explaining the first author's motivations and mode of thinking about the so-called 'nonabelian method of Chabauty'. The title is somewhat misleading in that there is no attempt to lay out foundational methods in a systematic way and certainly no attempt at providing proofs. Rather, the intention was to capture the *foundational ideas*. It is well-known that in mathematics, a good deal of hard work is necessary to make ideas effective and useful. From this point of view, the content of these notes is likely to represent nothing but vague laziness. Nonetheless, for a student completely new to these ideas, it is hoped that it might provide a rough guide to an area that the authors find interesting.

Non-abelian Selmer schemes were initially developed from around 2000 to 2004 [**Kim05, Kim09**]. Afterwards, M.K. struggled with various vague directions for making the techniques more powerful and tractable. This meant firstly that one should end up with an algorithm for completely computing the rational points on

a curve of genus at least two, even if it relies on conjectures in the manner of the theory of elliptic curves. Secondly, it was expected that a precise framework of 'non-abelian BSD' would emerge. Thirdly, ideas from geometric gauge theory were to play an important role.

As it stands, laziness has turned all these grandiose thoughts into an unfinished project. For M.K., if some young mathematician reading these notes finds ideas therein rich enough to inspire them to take the project forward into something deep and interesting, of course it would be extremely gratifying.

2. Arithmetic of algebraic curves

Diophantine geometry is concerned with maps

$$U \longrightarrow V$$

between schemes that are absolutely finitely-generated. This means U and V are both finite unions of schemes of the form $\mathrm{Spec}(R)$, where R is isomorphic to a quotient ring of a polynomial ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ over the integers. Obviously, this will involve coming to grips with the geometry of U and V in their own right, which is itself quite a difficult task. Already, when $U = \mathrm{Spec}(\mathcal{O}_F)$, where F is an algebraic number field, the topology ends up being quite elaborate, involving at least the machinery of class field theory to begin to understand. As usual in mathematics (and science in general), one goes on to study the interaction between such objects even in the absence of a complete understanding of the objects themselves.

In fact, we will confine our attention to smooth algebraic curves of genus g defined over $\mathbb{Q}$, which we will attempt to consistently denote by X. A large part of the reason is that one author (M.K.) has not worked seriously on any other class of schemes. The reader will notes that $\mathbb{Q}$ is not absolutely of finite type and hence, neither is X. However, they are simple limits associated to diagrams of the form

$$\begin{array}{ccc} X & \hookrightarrow & \mathcal{X}_N \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{Q}) & \hookrightarrow & \mathrm{Spec}(\mathbb{Z}[1/N]), \end{array}$$

and tradition dictates that there is a certain simplicity in allowing such limits into the zoology of interest. The restriction to the field $\mathbb{Q}$ is almost certainly unnecessary in the long run [**Dog20**], but most of the existing work took place in this context, so we will stick to it for conceptual simplicity.

Thus, when we try to express the associated problems in elementary terms, X might be given by a polynomial equation

$$f(x, y) = 0$$

of degree d with rational coefficients, where

$$g = (d-1)(d-2)/2.$$

(We are assuming for this that the corresponding homogeneous equation has no singularities.) Diophantine geometry studies the set $X(\mathbb{Q})$ of rational solutions from a geometric point of view. It is probably well known by now that the structure is quite different in the three cases:

$g = 0$: spherical geometry (positive curvature);
$g = 1$: flat geometry (zero curvature);

$g \geq 2$: hyperbolic geometry (negative curvature).

The geometry listed in parentheses refers to one given by the so-called *uniformisation theorem*, whereby the universal covering space admits a constant curvature metric compatible with the complex structure. The relevance of this metric to the arithmetic structure is not at all a straightforward matter to understand, even while much of the research on the arithmetic geometry of curves has been informed by this connection, albeit indirectly.

We go on to a brief summary of what is known.

2.1. Genus zero curves. Even now, after millennia of studying these problems, it is a bit of an embarrassment to number theory that the case $g = 0$ is the only one that is completely understood. For $g = 0$, techniques like *local-to-global methods* or generation of solutions via intersection theory reduce the question to class field theory and algebraic geometry. It should be appreciated that the interaction between these two areas in the resolution of genus zero equations is already an indication of the depth of arithmetic geometry.

The idea is to study $\mathbb{Q}$-solutions by considering the geometry of solutions in various completions, namely the local fields

$$\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \ldots, \mathbb{Q}_{691}, \ldots$$

Local-to-global methods allow us to "globalise". For example, the equation

$$37x^2 + 59y^2 - 67 = 0$$

has a $\mathbb{Q}$-solution if and only if it has a solution in each of $\mathbb{R}$, $\mathbb{Q}_2$, $\mathbb{Q}_{37}$, $\mathbb{Q}_{59}$, $\mathbb{Q}_{67}$. More generally,

$$ax^2 + by^2 = c$$

with a, b, c integral, square-free, and pairwise coprime has a rational solution if and only if it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for $p = 2$ and all p dividing abc. This is a criterion that can be effectively implemented. That is, there is a method based on local class field theory that enables one to determine whether or not such quadratic equations over $\mathbb{Q}_p$ have a solution. That is, the equation has a solution in $\mathbb{Q}_p$ if and only if

$$(-1, abc)_p = (a, b)_p (a, -c)_p (b, -c)_p,$$

where $(x, y)_p \in \{\pm 1\}$ is the *Hilbert symbol*, for which there is an explicit formula **[Ser78]**. The possibility of globalising the information, that is, deducing the existence of a $\mathbb{Q}$-solution from all these local solutions, is called the *Hasse principle*.

If the existence of a solution is guaranteed, it can be found by an exhaustive search. This is a curious aspect of certain algorithms. Swinnerton-Dyer asserted quite strongly to M.K. once that he doesn't regard such a thing as an algorithm. M.K. disagrees: the current algorithms for computing the Mordell–Weil basis for an elliptic curve (which we will review later) have no a priori bound. The only problem with an exhaustive search is if one is ignorant of the existence, in which case one indeed does not know when to stop.

For this problem, there is an alternative theorem of Holzer that says if a solution exists, then there is a solution $(x, y) = (p/r, q/r)$ such that

$$|p| \leq \sqrt{|bc|}, \quad |q| \leq \sqrt{|ac|}, \text{and} \quad |r| \leq \sqrt{|ab|}.$$

This gives a bound, albeit exponential in size, on the length of the exhaustive search. (Here, we are using the jargon of complexity theory, whereby an algorithm

of 'exponential' complexity refers to one whose running time is a polynomial in the exponential of the length of the input. In our case, the length of the input can be taken as the log of $|abc|$.)

From one solution, there is a method for parametrising all others, sometimes called *the method of sweeping lines*, that consists of searching for intersection points between the curve and all lines passing through the given point. The best known case is certainly the circle equation $x^2 + y^2 = 1$, for which the solution $(-1, 0)$ allows us to generate all others via the formula

$$\Big(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\Big), \quad t \in \mathbb{Q}.$$

Such a formula should convey the sense in which the rational solutions are completely understood for equations of genus zero. The reader who has never tried this before should also work this all out for the equation

$$3x^2 + 5y^2 = 167.$$

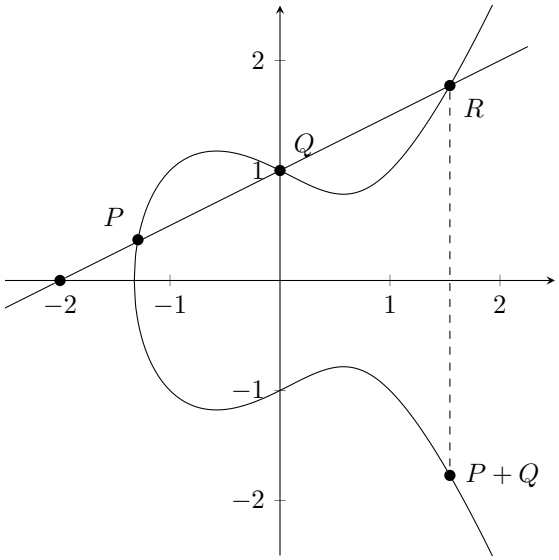
2.2. Genus one curves. When $g = 1$ (for example if X is given by a polynomial equation $f(x, y) = 0$ of degree $d = 3$), the cases where $X(\mathbb{Q})$ is

- empty;
- non-empty finite;
- infinite

are all possible. Crucially, the Hasse principle fails. For example the curve defined by the equation

$$3x^2 + 4y^2 + 5 = 0$$

has points in all completions $\mathbb{Q}_v$, but no rational points. For now, we will ignore the thorny question of existence. In fact, in contrast to the genus zero case, even when we are already given a point in $X(\mathbb{Q})$, it is difficult to describe the full set. Analogous ideas in this setting will lead to the use of a fixed $O \in X(\mathbb{Q})$ as the origin for an abelian group structure on $X(\mathbb{Q})$ constructed via the chord-and-tangent method:



Mordell's Theorem states that the group $X(\mathbb{Q})$ is finitely generated, so it has the form

$$X(\mathbb{Q}) \simeq X(\mathbb{Q})_{\mathrm{tor}} \times \mathbb{Z}^r,$$

where $r \geq 0$ is called the *rank* of the curve and $X(\mathbb{Q})_{\mathrm{tor}}$ is a finite, effectively computable abelian group.

Computing $X(\mathbb{Q})_{\mathrm{tor}}$ is a straightforward matter dealt with in elementary courses. If all else fails, there is the Nagell–Lutz theorem, which writes the curve in the form

$$X \coloneqq \{y^2 = x^2 + ax + b\} \cup \{\infty\}$$

with $a, b \in \mathbb{Z}$ and states that if $(x, y) \in X(\mathbb{Q})_{\mathrm{tor}}$, then x, y are integral and we have the divisibility relation

$$y \mid (4a^3 + 27b^2).$$

This allows us to enumerate the possibilities. (There is a slight subtlety: Given a candidate point (x, y), how might one check for sure that it is torsion?)

However, the algorithmic computation of the rank and a full set of generators for $X(\mathbb{Q})$ is very difficult, and is the subject of the conjecture of Birch and Swinnerton-Dyer. Note that a set of generators for the group is essentially the same starting point as a single point for genus zero curves, in that this is the input that leads to all points via a straightforward geometric method. In practice, this problem is quite often computationally feasible. For example, for

$$y^2 = x^3 - 2,$$

the programme Sage will give you $r = 1$ and the point $P = (3, 5)$ as generator. In fact, the algorithm *uses* the BSD conjecture, in that the termination of the algorithm relies on the finiteness of a p-primary portion of the Tate–Shafarevich group for some p. If you haven't spent much time working with such programmes, this is a good time to start. Using it, it is easy to compute the group law, so that the first few multiples of P are given as follows:

$$\begin{aligned} P &= (3, 5), \\ 2P &= (129/100, -383/1000), \\ 3P &= (164323/29241, -66234835/5000211), \\ 4P &= (2340922881/58675600, 113259286337279/449455096000). \end{aligned}$$

It is also amusing to list the denominators of the x-coordinates of nP for $1 \leq n \leq 25$ and observe a parabolic shape appear as the envelope of the numbers:

Finally, we remark that the problem of determining the existence of a point on a curve of genus one can by and large be absorbed into the theory of elliptic curves. This is because any curve of genus one is in fact a *principal bundle* for an elliptic curve, namely its Jacobian, and we need to know if this bundle is trivial. We will be discussing principal bundles in greater detail below.

2.3. Curves of higher genus. Our main concern in these lectures are in fact curves of genus $g \geq 2$, for example given by a polynomial equation $f(x, y) = 0$ of degree $d \geq 4$. For such curves, $X(\mathbb{Q})$ is always finite. This is the statement of the Mordell conjecture, which was proven by Faltings. However, it is *very* difficult to compute the set $X(\mathbb{Q})$, as the example of the Fermat equation,

$$x^n + y^n = 1, \quad n \geq 4,$$

shows. Sometimes it is very easy, such as

$$x^4 + y^4 = -1,$$

which does not have any solutions in the real numbers. However, when there is no obvious local reason for non-existence (e.g., when there is already one known solution), then it is hard to know when you have the full list. For example,

$$y^3 = x^6 + 23x^5 + 37x^4 + 691x^3 - 631204x^2 + 5169373941$$

obviously has the solution $(1, 1729)$, but are there any others?

The effective Mordell problem is:

Find a terminating algorithm: $X \mapsto X(\mathbb{Q})$

that lists the full set of rational solutions when a curve X is provided as input. The *Effective Mordell conjecture* (Szpiro, Vojta, ABC, ...) is one approach to making this precise by way of (archimedean) height inequalities. That is, it proposes that you can give a priori bounds on the size of numerators and denominators of solutions.

The rest of these notes will describe an alternative approach to the effective Mordell problem using the (non-archimedean) arithmetic geometry of principal bundles. Principal bundles are well-known in differential geometry as fibre bundles

$$P \longrightarrow M$$

over a manifold M whose fibres are isomorphic to a Lie group R. More precisely, R acts on P on the right

$$P \times R \longrightarrow P$$

via bundle automorphisms in such a way that the choice of any point $x \in P_m$ in a fibre above a point m induces an isomorphism

$$R \simeq P_m;$$

$$r \mapsto xr.$$

The natural examples are frame bundles consisting of bases for tangent bundles.

In algebraic geometry, the same kind of objects are called *torsors*, terminology originating in French. They have been used already extensively in number theory since the 1950's in the form of Galois cohomology. However, it's only with non-abelian problems that the geometric view of their classification starts to assume importance, as we will explain in the next sections. The key concept is that of an arithmetic principal bundle, which is just a principal bundle on an arithmetic scheme. A confusing point is that even on schemes whose underlying space is a point, e.g., Spec($\mathbb{Q}$), principal bundles can be highly non-trivial. This is just a reflection of the paucity of the set underlying a scheme when compared to the full structure of the scheme itself. In fact, such a phenomenon is already present in 'ordinary' geometry, since any two manifolds of dimension greater than zero

have exactly the same set-theoretic structure as the interval $[0,1]$. Geometry and classification clearly rely on more than the underlying set.

3. Arithmetic principal bundles

We shall give a general description of arithmetic principal bundles in the étale topology, a fundamental tool in the nonabelian method of Chabauty. For now, it might be useful to fix a field K of characteristic zero and its absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$. The group G_K is a topological group with open subgroups given by $\mathrm{Gal}(\overline{K}/L)$ for finite field extensions L/K in $\overline{K}$.

Definition 3.1. A *group over* K is a topological group R with a continuous action of G_K by group automorphisms:

$$G_K \times R \longrightarrow R.$$

In an abstract framework, one can view R as a family of groups over the space $\mathrm{Spec}(K)$, but we will somewhat avoid that formalism for the sake of concreteness. (We are living in an age where groups are regarded as concrete while Grothendieck topologies are (still) not.)

Example 3.2. Let A be an algebraic group defined over K, e.g., GL_n or an abelian variety. Then $A(\overline{K})$ with the discrete topology is a group over K.

Example 3.3. The group

$$\mathbb{Z}_p(1) \coloneqq \varprojlim \mu_{p^n},$$

where $\mu_{p^n} \subseteq \overline{K}$ is the group of p^n-th roots of unity, is a group over K. It is the Tate module of the group $\mathbb{G}_m$. Thus, elements of $\mathbb{Z}_p(1)$ are given by tuples $(\zeta_n)_n$ where

$$\zeta_n^{p^n} = 1, \quad \zeta_{nm}^{p^m} = \zeta_n.$$

As a topological group, there is an isomorphism

$$\mathbb{Z}_p(1) \simeq \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z},$$

but there is a continuous action of G_K on the left hand side.

Definition 3.4. A *principal R-bundle* over K is a topological space P with compatible continuous actions of G_K (from the left) and R (from the right and simply transitive):

$$\begin{aligned} P \times R &\longrightarrow P; \\ G_K \times P &\longrightarrow P; \\ g(zr) = g(z)g(r) &\quad \text{for } g \in G_K, z \in P, r \in R. \end{aligned}$$

Note that P is *trivial*, i.e. isomorphic to R, exactly when there is a fixed point $z \in P^{G_K}$. This is because in that case, the action induces a isomorphism

$$R \cong z \times R \cong P$$

compatible with all structures.

Example 3.5. Given any $x \in K^*$, we get a principal $\mathbb{Z}_p(1)$-bundle over K

$$P(x) \coloneqq \{(y_n)_n : y_n^{p^n} = x,\ y_{nm}^{p^m} = y_n\}.$$

The bundle $P(x)$ is trivial if and only if x admits a p^n-th root in K for all n. For example, when $K = \mathbb{C}$, then $P(x)$ is always trivial. When $K = \mathbb{Q}$, then $P(x)$ is

trivial if and only if $x = 1$ or p is odd and $x = -1$. For $K = \mathbb{R}$ and p odd, $P(x)$ is trivial for all x. For $K = \mathbb{R}$ and $p = 2$, the bundle $P(x)$ is trivial if and only if $x > 0$. This collection of cases should convey the sense in which principal bundles can encode highly non-trivial arithmetic information.

We will encounter many variations on this example in the following. For now, we note that for a principal R-bundle over K, if we choose $z \in P$, this determines a continuous function $c_P \colon G_K \to R$ via

$$g(z) = z c_P(g).$$

It is straightforward to check that the function satisfies the "cocycle condition"

$$c_P(g_1 g_2) = c_P(g_1)\, g_1(c_P(g_2)),$$

defining the set

$$Z^1(G_K, R).$$

We get a well-defined class in non-abelian cohomology

$$[c_P] \in R\backslash Z^1(G_K, R) =: H^1(G_K, R) =: H^1(K, R),$$

where the R-action is defined by

$$c^r(g) = r c(g) g(r^{-1}).$$

We get thereby a bijection

$$\left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{principal } R\text{-bundles over } K \end{array} \right\} \cong H^1(G_K, R).$$

Our main concern is the geometry of such non-abelian cohomology spaces in various forms. We will also denote it by $H^1(K, R)$.

The most important example for us is when R is a unipotent fundamental group of an algebraic curve. In this case, R will have a very complicated K-structure, i.e., G_K-action. Some more classes that we will not be discussing here in spite of their importance are:

- R consists of the $\bar{K}$-points of an algebraic group A over K. In the case of an abelian variety, $H^1(K, A(\bar{K}))$ is sometimes called the *Weil–Châtelet group* of A. As mentioned above, a curve C of genus one is a principal bundle for its Jacobian J, which is an elliptic curve, and defines a class in $[C] \in H^1(K, J(\bar{K}))$.
- R is the holonomy group of a specific local system on a curve (Lawrence and Venkatesh).
- R is a reductive group with a trivial K-structure, in which case

  $$H^1(G_K, R) = R\backslash \operatorname{Hom}(G_K, R).$$

  Principal bundles are just Galois representations, ubiquitous and highly important in number theory. The H^1 here often takes the form of the limit of analytic moduli spaces of Galois representations.

When $K = \mathbb{Q}$, there are completions $\mathbb{Q}_v$ and injections

$$G_v = \operatorname{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v) \subseteq G \coloneqq \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),$$

giving rise to the localisation map

$$\operatorname{loc} \colon H^1(\mathbb{Q}, R) \longrightarrow \prod_v H^1(\mathbb{Q}_v, R)$$

and an associated local-to-global problem. In fact, a wide range of problems in number theory rely on the study of its image. The general principle is that the local-to-global problem is easier to study for principal bundles than for points. That is, as difficult as the localisation map in cohomology might be, it is much easier than the naive inclusion

$$X(\mathbb{Q}) \hookrightarrow \prod_v X(\mathbb{Q}_v).$$

3.1. Elliptic curves. The utility of arithmetic principal bundles in the theory of elliptic curves is well-known, although they aren't often discussed in this language. Importantly, the moduli spaces there have a simple enough structure that the geometric view is not really necessary for arithmetic applications. We give a brief summary from a point of view close to our present concerns.

Let E be an elliptic curve over $\mathbb{Q}$. We let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on the exact sequence

$$0 \longrightarrow E(\overline{\mathbb{Q}})[p] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{p} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

to generate the long exact sequence

$$0 \longrightarrow E(\mathbb{Q})[p] \longrightarrow E(\mathbb{Q}) \xrightarrow{p} E(\mathbb{Q})$$

$$\longrightarrow H^1(\mathbb{Q}, E[p]) \longrightarrow H^1(\mathbb{Q}, E) \xrightarrow{p} H^1(\mathbb{Q}, E),$$

From this, we get the inclusion (Kummer map)

$$E(\mathbb{Q})/pE(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E[p]).$$

A central problem in the theory of elliptic curves is the identification of the image

$$\mathrm{Im}\big(E(\mathbb{Q})/pE(\mathbb{Q})\big) \subseteq H^1(\mathbb{Q}, E[p]),$$

where the codomain is a simple example of a moduli space of principal bundles. Of course, in this case, it's just an $\mathbb{F}_p$-vector space (albeit, a very large one). The general goal is to understand this inclusion well enough to render $E(\mathbb{Q})/pE(\mathbb{Q})$ computable. That is, we would like to produce a set of elements $B \subset E(\mathbb{Q})$ whose classes mod $pE(\mathbb{Q})$ generate the group. We remark that computing a set of generators for $E(\mathbb{Q})/pE(\mathbb{Q})$ in this sense leads easily to a set of generators for $E(\mathbb{Q})$ itself. Therefore, the Diophantine geometry of elliptic curves is more or less reduced to the study of the image of the Kummer map. We would therefore like to describe it as carefully as possible. The tradition in number theory is to approach this problem via various restrictions that the classes in the image must satisfy.

An essential restriction comes from the p-Selmer group

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \subseteq H^1(\mathbb{Q}, E[p]),$$

defined to be the classes in $H^1(\mathbb{Q}, E[p])$ that locally come from points. This is useful because the local version of this problem can be solved. To give a more precise definition of the Selmer group, consider the following diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & E(\mathbb{Q})/pE(\mathbb{Q}) & \hookrightarrow & H^1(\mathbb{Q}, E[p]) \\ & & \downarrow{\scriptstyle \mathrm{loc}_v} & & \downarrow{\scriptstyle \mathrm{loc}_v} \\ 0 & \longrightarrow & E(\mathbb{Q}_v)/pE(\mathbb{Q}_v) & \hookrightarrow & H^1(\mathbb{Q}_v, E[p]). \end{array}$$

Definition 3.6. The *p-Selmer group* $\mathrm{Sel}(\mathbb{Q}, E[p]) \subseteq H^1(\mathbb{Q}, E[p])$ is defined as

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \coloneqq \bigcap_v \mathrm{loc}_v^{-1}\Big(\mathrm{Im}\big(E(\mathbb{Q}_v)/pE(\mathbb{Q}_v)\big)\Big).$$

In other words, these are the global cohomology classes that locally lie inside the image of the Kummer map. The key point is that the p-Selmer group is a finite-dimensional $\mathbb{F}_p$-vector space that is effectively computable and this already gives us a bound on the Mordell–Weil group of E. That is, the rank of $E(\mathbb{Q})$ must be bounded by the dimension of the p-Selmer group. This is then refined by way of the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & E(\mathbb{Q})/p^nE(\mathbb{Q}) & \hookrightarrow & H^1(\mathbb{Q}, E[p^n]) \\ & & \downarrow{\scriptstyle \mathrm{loc}_v} & & \downarrow{\scriptstyle \mathrm{loc}_v} \\ 0 & \longrightarrow & E(\mathbb{Q}_v)/p^nE(\mathbb{Q}_v) & \hookrightarrow & H^1(\mathbb{Q}_v, E[p^n]). \end{array}$$

for increasing values of n, which are compatible for these values. Thus, we get a sequence of Selmer groups

$$\mathrm{Sel}(\mathbb{Q}, E[p^n]) \coloneqq \bigcap_v \mathrm{loc}_v^{-1}\Big(\mathrm{Im}\big(E(\mathbb{Q}_v)/p^nE(\mathbb{Q}_v)\big)\Big) \subset H^1(\mathbb{Q}, E[p^n]),$$

which form an inverse system compatible with quotients of the Mordell–Weil group:

$$\begin{array}{ccccccccc} \ldots & \longrightarrow & E(\mathbb{Q})/p^{n+1}E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q})/p^nE(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q})/p^{n-1}E(\mathbb{Q}) & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & \mathrm{Sel}(\mathbb{Q}, E[p^{n+1}]) & \longrightarrow & \mathrm{Sel}(\mathbb{Q}, E[p^n]) & \longrightarrow & \mathrm{Sel}(\mathbb{Q}, E[p^{n-1}]) & \longrightarrow & \ldots \end{array}$$

In particular, if we map all these Selmer groups down to $\mathrm{Sel}(\mathbb{Q}, E[p])$, we get a decreasing sequence

$$\ldots \subseteq \mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^{n+1}])\big) \subseteq \mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^n]) \subseteq \ldots \subseteq \mathrm{Sel}(\mathbb{Q}, E[p]).$$

In view of the previous diagram, these must all contain $\mathrm{Im}\big(E(\mathbb{Q})/pE(\mathbb{Q})\big)$.

Conjecture 3.7 (BSD, Tate–Shafarevich)**.**

$$\mathrm{Im}\big(E(\mathbb{Q})/pE(\mathbb{Q})\big) = \bigcap_{n=1}^{\infty} \mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^n]\big) \subseteq \mathrm{Sel}(\mathbb{Q}, E[p]).$$

Of course this implies that

$$\mathrm{Im}\big(E(\mathbb{Q})/pE(\mathbb{Q})\big) = \mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^N])\big) \subseteq \mathrm{Sel}(\mathbb{Q}, E[p])$$

at some finite level p^N at which point $\mathrm{Im}\big(E(\mathbb{Q})/pE(\mathbb{Q})\big)$ is regarded as being computed. This is because $\mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^N])\big)$ is computable via methods of algebraic number theory.

There is a conditional algorithm for finding the N above via an exhaustive search once we are guaranteed of its existence. We include the decreasing sequence above into a large one

$$\ldots \subseteq E(\mathbb{Q})_{\leq n}/pE(\mathbb{Q}) \subseteq E(\mathbb{Q})_{\leq n+1}/pE(\mathbb{Q}) \subseteq \ldots \subseteq E(\mathbb{Q})/pE(\mathbb{Q})$$

$$\ldots \subseteq \mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^{n+1}])\big) \subseteq \mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^n]) \subseteq \ldots \subseteq \mathrm{Sel}(\mathbb{Q}, E[p])$$

involving the increasing sequence

$$\ldots \subseteq E(\mathbb{Q})_{\leq n}/pE(\mathbb{Q}) \subseteq E(\mathbb{Q})_{\leq n+1}/pE(\mathbb{Q}) \subseteq \ldots \subseteq E(\mathbb{Q})/pE(\mathbb{Q})$$

where

$$E(\mathbb{Q})_{\leq n}/pE(\mathbb{Q})$$

denotes the image mod $pE(\mathbb{Q})$ of the points $E(\mathbb{Q})_{\leq n}$ of height $\leq n$. In particular, this is a computable set. The conjecture above implies that

$$E(\mathbb{Q})_{\leq N}/pE(\mathbb{Q}) = \mathrm{Im}\big(\mathrm{Sel}(\mathbb{Q}, E[p^N])$$

for N sufficiently large, and that at this point, we will have

$$E(\mathbb{Q})_{\leq N}/pE(\mathbb{Q}) = E(\mathbb{Q})/pE(\mathbb{Q}).$$

That is, we will have computed a full set of points that cover $E(\mathbb{Q})$ mod p. It is easy to go from here to a full set of generators of $E(\mathbb{Q})$. A main goal of BSD is to remove the conditional aspect of this algorithm.

3.2. The non-abelian case: a quick synopsis. A major theme of these lectures is the possibility of extending the discussion on elliptic curves to curves of higher genus. We focus on the sequence of maps

$$\ldots \longrightarrow E[p^3] \xrightarrow{p} E[p^2] \xrightarrow{p} E[p]$$

of which we take the inverse limit to get the p-adic Tate module of E:

$$T_pE \coloneqq \varprojlim E[p^n].$$

This is a free $\mathbb{Z}_p$-module of rank 2. The previous finite boundary maps can be packaged into

$$j\colon E(\mathbb{Q}) \longrightarrow \varprojlim H^1(\mathbb{Q}, E[p^n]) = H^1(\mathbb{Q}, T_pE).$$

The key point is that

$$T_pE \simeq \pi_1^p(\bar{E}, O),$$

where $\pi_1^p(\bar{X}, b)$ refers to the pro-p completion of the fundamental group $\pi_1(X(\mathbb{C}), b)$ of the topological space defined by the complex points of a variety X. The map j can be thought of as

$$x \mapsto \pi_1^p(\bar{E}; O, x),$$

where the last object is the pro-p completion of the homotopy classes of paths $\pi_1(E(\mathbb{C}); O, x)$ from O to x. We will review later the reason for these identifications.

The following is a fundamental fact of arithmetic homotopy:

Fact 3.8. If X is a variety defined over $\mathbb{Q}$ and $b, x \in X(\mathbb{Q})$, then

$$\pi_1^p(\bar{X}, b) \quad \text{and} \quad \pi_1^p(\bar{X}; b, x)$$

admit compatible actions of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Here, the compatibility refers to the action

$$\pi_1^p(\bar{X}; b, x) \times \pi_1^p(\bar{X}, b) \longrightarrow \pi_1^p(\bar{X}; b, x),$$

that turns $\pi_1^p(\bar{X}; b, x)$ into a principal $\pi_1^p(\bar{X}, b)$-bundle. That is the triples

$$(G_{\mathbb{Q}}, \pi_1^p(\bar{X}, b), \pi_1^p(\bar{X}; b, x))$$

are important concrete examples of (G_K, R, P) from the general definitions.

This can then be used to extend Kummer theory to general X, whereby we get a map

$$j\colon X(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, \pi_1^p(\bar{X}, b))$$

given by

$$x \mapsto [\pi_1^p(\bar{X}; b, x)].$$

For each prime v, we have local versions

$$j\colon X(\mathbb{Q}_v) \longrightarrow H^1(\mathbb{Q}_v, \pi_1^p(\bar{X}, b))$$

which turn out to be far more computable than the global map. The global and local maps fit into the following localisation diagram:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & \prod_v X(\mathbb{Q}_v) \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \prod_v j_v} \\ H^1(\mathbb{Q}, \pi_1^p(\bar{X}, b)) & \xrightarrow{\text{loc}} & \prod_v H^1(\mathbb{Q}_v, \pi_1^p(\bar{X}, b)). \end{array}$$

As in the elliptic curve case, our interest is in the interaction between the images of loc and $\prod_v j_v$. Actual applications use the variant

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & \prod_{v\in S} X(\mathbb{Q}_v) \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \prod_v j_v} \\ H^1(\mathbb{Q}, U(\bar{X}, b)) & \xrightarrow{\text{loc}} & \prod_{v\in S} H^1(\mathbb{Q}_v, U(\bar{X}, b)). \end{array}$$

where S is a suitable finite collection of primes and

$$U(\bar{X}, b) = `\pi_1^p(\bar{X}, b) \otimes \mathbb{Q}_p'$$

is the *$\mathbb{Q}_p$-pro-unipotent completion* of $\pi_1^p(\bar{X}, b)$. The effect is that the moduli spaces become pro-algebraic schemes over $\mathbb{Q}_p$ and the lower row of this diagram an algebraic map. That is, the key object of study is

$$H^1_f(\mathbb{Q}, U(\bar{X}, b)),$$

the *Selmer scheme* of X, defined to be the subfunctor of $H^1(\mathbb{Q}, U(\bar{X}, b))$ satisfying local conditions at all (or most) v. These are conditions like "unramified at most primes", "crystalline at p", and often a few extra conditions. A concrete goal will be to find an algebraic function

$$\alpha\colon \prod_{v\in S} H^1(\mathbb{Q}_v, U(\bar{X}, b)) \to \mathbb{Q}$$

vanishing on the image of the localisation map. Then

$$\alpha \circ \prod_v j_v$$

gives a defining equation for $X(\mathbb{Q})$ inside $\prod_{v\in S} X(\mathbb{Q}_v)$. Standard structural conjectures on mixed motives (generalised BSD) imply that there exist many functions α as above (which in turn implies Faltings' Theorem). To make this concretely computable, we take the projection

$$\mathrm{pr}_p\colon \prod_{v\in S} X(\mathbb{Q}_v) \longrightarrow X(\mathbb{Q}_p)$$

and try to compute

$$\bigcap_\alpha \mathrm{pr}_p\big(Z(\alpha \circ \prod_v j_v)\big) \subseteq X(\mathbb{Q}_p).$$

Conjecture 3.9 (Non-Archimedean effective Mordell Conjecture)**.**

I. $\bigcap_\alpha \mathrm{pr}_p\big(Z(\alpha \circ \prod_v j_v)\big) = X(\mathbb{Q})$

II. This set is effectively computable.

Remarks 3.10.

1. As soon as there is one α with α_p non-trivial, $\mathrm{pr}_p\big(Z(\alpha \circ \prod_v j_v)\big)$ is finite.
2. There is a (highly reliable) conjectural mechanism for producing infinitely many algebraically independent α.
3. This conjecture is closely related to Grothendieck's section conjecture [**Sch97**]: Rather, the main diagram and the section conjecture give an effective method of computing $X(\mathbb{Q})$.

Later on, we will describe the methods used to construct these moduli spaces and functions. But we will first illustrate their utility by way of some examples.

4. Computing rational points: Some examples

There is an obvious modification of the discussion in the previous section that deals with integral points on affine curves. The first example will take place in the affine setting since the formulas are very concrete. For $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, Dan-Cohen and Wewers [**DCW16**] have shown that

$$X(\mathbb{Z}[1/2]) = \{2, -1, 1/2\} \subseteq \{D_2(z) = 0\} \cap \{D_4(z) = 0\},$$

where

$$\begin{aligned} D_2(z) &= \ell_2(z) + \tfrac{1}{2}\log(z)\log(1-z), \\ D_4(z) &= \zeta(3)\ell_4(z) + \tfrac{8}{7}\left[\log^3(2)/24 + \ell_4(1/2)/\log(2)\right]\log(z)\ell_3(z) \\ &\quad + \left[\tfrac{4}{21}\left(\log^3(2)/24 + \ell_4(1/2)/\log(2)\right) + \zeta(3)/24\right]\log^3(z)\log(1-z), \end{aligned}$$

and

$$\ell_k(z) = \sum_{n=1}^{\infty} \frac{z^k}{n^k}.$$

Numerically, the inclusion appears to be an equality.

There are also some qualitative results:

Theorem 4.1 (Coates and Kim [**CK10**]). *The curve defined by*

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

for $n \geq 4$ has only finitely many rational points.

There is a remarkable result on modular curves by Balakrishnan, Dogra, Müller, Tuitmann, Vonk [**BDM$^+$19**]. They study the curve

$$X_s^+(N) = X(N)/C_s^+(N),$$

where $X(N)$ is the compactification of the moduli space of pairs

$$(E, \phi\colon E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2),$$

and $C_s^+(N) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normaliser of a split Cartan subgroup. Bilu–Parent–Rebolledo [**BPR13**] had shown that $X_s^+(p)(\mathbb{Q})$ consists entirely of cusps and CM points for all primes $p > 7$, $p \neq 13$. They called $p = 13$ the "cursed level".

Theorem 4.2 ([**BDM$^+$19**]). *The modular curve*

$$X_s^+(13)$$

has exactly 7 rational points, consisting of the cusp and 6 CM points.

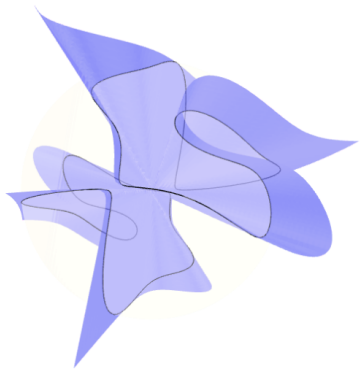


FIGURE 1. The cursed curve, plotted using SageMath by Sachi Hashimoto

The cursed curve $X_s^+(13)$ is explicitly given by the equation

$$y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z \\ - 32x^2z^2 - 40xyz‘2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0.$$

The theorem states that

$$(1:1:1),\ (1:1:2),\ (0:0:1), (-3:3:2),\ (1:1:0),\ (0:2:1),\ (-1:1:0)$$

is a complete list of its rational points.

This concludes an important chapter of a conjecture of Serre from the 1970s which postulates that there is an absolute constant A such that

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[p])$$

is surjective for all non-CM elliptic curves $E/\mathbb{Q}$ and primes $p > A$.

5. Some speculations on rational points and critical points

This section, which represents a high degree of wishful thinking, should not be taken too seriously.

We would like to think of

$$H^1(G, U(\bar{X}, b)) \longrightarrow \prod_v H^1(G_v, U(\bar{X}, b))$$

as being like

$$\mathbb{S}(M, G) \subseteq \mathcal{A}(M, G),$$

the space of solutions to a set of Euler–Lagrange equations on a space of connections. In particular, functions cutting out the image of localisation should be thought of as "classical equations of motion" for gauge fields. When X is smooth and projective, then $X(\mathbb{Q}) = X(\mathbb{Z})$, and we are actually interested in

$$\mathrm{Im}\big(H^1(G_S, U)\big) \cap \prod_{v \in S} H^1_f(G_v, U) \subseteq \prod_{v \in S} H^1(G_v, U),$$

where

$$H^1_f(G_v, U) \subseteq H^1(G_v, U)$$

is a subvariety defined by some integral or Hodge-theoretic conditions. Here, S is a finite set of primes including the primes of bad reduction and p. In order to apply symplectic techniques, replace U by

$$T^*(1)U \coloneqq (\operatorname{Lie} U)^*(1) \rtimes U.$$

Then

$$\prod_{v\in S} H^1(G_v, T^*(1)U)$$

is a symplectic variety and

$$\operatorname{Im}\big(H^1(G_S,U)\big) \quad \text{and} \quad \prod_{v\in S} H^1_f(G_v,U) \subseteq \prod_{v\in S} H^1(G_v,U)$$

are Lagrangian subvarieties. Thus, the (derived) intersection

$$\mathcal{D}_S(X) \coloneqq \operatorname{Im}\big(H^1(G_S,U)\big) \cap \prod_{v\in S} H^1_f(G_v,U) \subseteq \prod_{v\in S} H^1(G_v,U)$$

has a $[-1]$-shifted symplectic structure. Zariski-locally, it is the critical set of a function [**BBJ19**].

We have a diagram as follows:

$$\begin{array}{ccccc} X(\mathbb{Z}) & \longrightarrow & j_S^{-1}(\mathcal{D}_S(X)) & \hookrightarrow & \prod_{v\in S} X(\mathbb{Q}_v) \\ \downarrow{\scriptstyle j^g} & & \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle j_S} \\ H^1_f(G_S, T^*(1)U) & \xrightarrow{\operatorname{loc}_S} & \mathcal{D}_S(X) & \hookrightarrow & \prod_{v\in S} H^1(G_v, T^*(1)U) \end{array}$$

From this point of view, the global points can be obtained by pulling back "Euler–Lagrange equations" via a period map, establishing a connection between the study of Diophantine equations and Fermat's principle of least action [**Kim18**].

6. Covering spaces and fundamental groups

Most of the remainder of these lectures will be concerned with conveying some intuition for dealing with arithmetic fundamental groups and homotopy classes of paths. In many senses, it requires us only to think a bit carefully about the constructions of elementary algebraic topology and how they may be formulated in a way that makes sense for arithmetic schemes. We will give a few proofs of elementary facts. This will appear to the reader to be somewhat arbitrary and imbalanced, since much harder facts will not be proved. For the most part, the authors would like to believe that the elementary proofs capture the essence of the harder proofs except for the intervention of more elaborate objects. On the other hand, we admit that it is also just another manifestation of laziness. In any case, we start with a brief review.

6.1. Universal covering spaces. Let M be a locally contractible path-connected topological space.

Definition 6.1. A *covering space* $M' \to M$ is a locally trivial fibre bundle with discrete fibres, i.e. there is a discrete set F and an open covering $M = \bigcup U_i$ for

which we have a commutative diagram

$$\begin{array}{ccc} M'_{U_i} & \xrightarrow{\sim} & F \times U_i \\ & \searrow \quad \swarrow & \\ & U_i & \end{array}$$

for each i.

Definition 6.2. A *universal covering space*

$$\pi \colon \tilde{M} \longrightarrow M$$

is a covering space with $\tilde{M}$ path-connected and simply connected.

Here is an elementary fact that is surprisingly important to remember: A universal covering space is not universal in the categorical sense. For any other covering space $M' \to M$, there is a commutative diagram

$$\begin{array}{ccc} \tilde{M} & \overset{\exists}{\dashrightarrow} & M' \\ & \overset{\pi}{\searrow} & \downarrow \\ & & M. \end{array}$$

However, the diagram is *not unique*: There is no initial object in the category of covering spaces.

To remedy the situation, we consider instead *pointed* covering spaces. Having chosen a base point $b \in M$, a pointed covering space is a map

$$(M', b') \to (M, b).$$

Now we choose a point $\tilde{b} \in \tilde{M}_b$. Then the pair $(\tilde{M}_b, \tilde{b})$ is indeed an initial object in the category of pointed universal covering spaces:

$$\begin{array}{ccc} (\tilde{M}, \tilde{b}) & \overset{\exists!}{\dashrightarrow} & (M', b') \\ & \overset{\pi}{\searrow} & \downarrow \\ & & (M, b). \end{array}$$

Note that the choice of a different $\tilde{c} \in \tilde{M}_b$ will give another initial object $(\tilde{M}, \tilde{c})$ which is uniquely isomorphic to $(\tilde{M}, \tilde{b})$.

6.2. Fibre functors. Many readers will have seen fundamental groups defined via fibre functors. What follows is a brief explanation of how to work with such definitions by examining them carefully in topology.

Consider the functor

$$\begin{aligned} F_b \colon \mathrm{Cov}(M) &\longrightarrow \mathrm{Sets} \\ M' &\longmapsto M'_b, \end{aligned}$$

and its automorphism group

$$\mathrm{Aut}(F_b).$$

By the definition of a natural transformation, an element γ of this group is a compatible sequence of bijections

$$\gamma_{M'} \colon M'_b \cong M'_b$$

for all covering spaces $M' \to M$. The required compatibility is with respect to maps of covering spaces, i.e. if $f\colon M'_1 \to M'_2$ is a map of covering spaces, then the diagram

$$\begin{array}{ccc} M'_{1,b} & \xrightarrow{\gamma_{M'_1}} & M'_{1,b} \\ \big\downarrow f & & \big\downarrow f \\ M'_{2,b} & \xrightarrow{\gamma_{M'_2}} & M'_{2,b} \end{array}$$

commutes:

$$f \circ \gamma_{M'_1} = \gamma_{M'_2} \circ f.$$

The choice of $\tilde{b} \in \tilde{M}_b$ determines a map

$$\begin{aligned} \mathrm{Aut}(F_b) &\longrightarrow \tilde{M}_b \\ \gamma &\longmapsto \gamma_{\tilde{M}}(\tilde{b}). \end{aligned}$$

Proposition 6.3. *This map is a bijection*

$$\mathrm{Aut}(F_b) \cong \tilde{M}_b.$$

Proof. To show injectivity, consider an element $\gamma \in \mathrm{Aut}(F_b)$. For any covering space $M' \to M$ and any $b' \in M'_b$, there is a unique map $f\colon (\tilde{M}, \tilde{b}) \to (M', b')$. Thus,

$$\gamma_{M'}(b') = \gamma_{M'}(f(\tilde{b})) = f(\gamma_{\tilde{M}}(\tilde{b})),$$

so the action of γ on M'_b is determined by $\gamma_{\tilde{M}}(\tilde{b})$.

On the other hand, given $y \in \tilde{M}_b$, we would like to define γ such that $\gamma_{\tilde{M}}(\tilde{b}) = y$. The point is that there is only one way to do it in a way that is compatible with maps of covering spaces, and this gives us $\gamma_{M'}$ for every $M' \to M$. Given any $b' \in M'_b$, there is a unique $f_{b'}\colon (\tilde{M}, \tilde{b}) \to (M', b')$. Define

$$\gamma_{M'}(b') = \gamma_{M'}(f_{b'}(\tilde{b})) = f_{b'}(\gamma_{\tilde{M}}(\tilde{b})) \coloneqq f_{b'}(y).$$

The compatibility comes from the commutative triangles

$$\begin{array}{ccc} (\tilde{M}, \tilde{b}) & \xrightarrow{f_{b'}} & (M', b') \\ & \searrow^{f_{h(b')}} & \big\downarrow h \\ & & (M'', h(b')) \end{array}$$

for every map of covering spaces $h\colon M' \to M''$, which imply

$$h(\gamma_{M'}(b')) = h(f_{b'}(y)) = f_{h(b')}(y) = \gamma_{M''}(h(b')). \qquad \square$$

An identical proof gives us:

Proposition 6.4. *For two points $b, x \in M$, the choice of $\tilde{b} \in \tilde{M}_b$ determines a bijection*

$$\mathrm{Isom}(F_b, F_x) \cong \tilde{M}_x.$$

That is, an element $p \in \mathrm{Isom}(F_b, F_x)$ is determined by $p_{\tilde{M}}(\tilde{b})$, and any $y \in \tilde{M}_x$ determines such a p. $\square$

Note that $\mathrm{Isom}(F_b, F_x)$ is a principal bundle for $\mathrm{Aut}(F_b)$. It is an easy exercise to describe the action of $\tilde{M}_b$ on $\tilde{M}_x$.

6.3. Homotopy classes of paths. Consider the usual definition of $\pi_1(M; b, x)$ using homotopy classes of paths. There is a classical isomorphism

$$\pi_1(M; b, x) \cong \mathrm{Isom}(F_b, F_x)$$

defined via path lifting. That is, a path $p\colon I = [0,1] \to M$ such that $p(0) = b$ and $p(1) = x$ acts on the fibres of a covering $M' \to M$ via the unique lifting diagram

$$\begin{array}{ccc} & & (M', b') \\ & \overset{\exists!\, p'}{\nearrow} & \big\downarrow \\ (I, 0) & \xrightarrow{\quad p \quad} & (M, b), \end{array}$$

i.e. via the rule $p \cdot b' = p'(1)$. The endpoint $p'(1)$ depends only on the homotopy class of p because of the discreteness of the fibres. If $f\colon (M'_1, b'_1) \to (M'_2, b'_2)$ is a map of pointed covering spaces, then $f \circ p'_1 = p'_2$ by uniqueness. Thus, path lifting defines a compatible collection of isomorphisms

$$p_{M'}\colon M'_b \cong M'_x$$

In particular, loops based at b will act compatibly on all fibres M'_b. The easiest way to see that this gives an isomorphism

$$\pi_1(M; b, x) \cong \mathrm{Isom}(F_b, F_x)$$

uses the universal covering $\pi\colon \tilde{M} \to M$ again. Namely, denote by $\tilde{p}$ the lifting of p to $\tilde{M}$ such that $\tilde{p}(0) = \tilde{b}$. In that case we get:

Proposition 6.5. *The map $p \mapsto \tilde{p}(1)$ defines a bijection*

$$\pi_1(M; b, x) \cong \tilde{M}_x.$$

The inverse is given by mapping $y \in \tilde{M}_x$ to the homotopy class $[\pi \circ p_y]$, where p_y is any path in $\tilde{M}$ from $\tilde{b}$ to y. The homotopy class is independent of p_y since $\tilde{M}$ is simply connected. However, this map clearly factors through

$$\pi_1(M; b, x) \longrightarrow \mathrm{Isom}(F_b, F_x) \cong \tilde{M}_x,$$

proving that the first map is also an isomorphism.

In other words, the choice of base points gives us an expression

$$\tilde{M} = \bigcup_{x \in M} \pi_1(M; b, x).$$

The fibres of $\tilde{M} \to M$ give us a concrete model of path spaces, which generalises to situations where physical paths are missing.

To summarise, we have the bijections

$$\pi_1(M; b, x) \cong \mathrm{Isom}(F_b, F_x) \cong \tilde{M}_x,$$

and the second two objects generalise to other settings.

7. The Tannakian formalism

We review the Tannakian formalism starting with a simple example. Let G be a finite group and denote by

$$\mathrm{Rep}_k^G$$

the category of finite-dimensional representations of G on k-vector spaces.

Definition 7.1. A *pointed representation* is a pair (V, v) of a representation V and a vector $v \in V$.

Proposition 7.2. *The left-regular pointed representation*

$$(k[G], 1)$$

is the universal pointed representation of G.

Given any pointed representation (V, v), the unique map $(k[G], 1) \to (V, v)$ sends g to gv.

Let

$$F\colon \mathrm{Rep}_k^G \longrightarrow \mathrm{Vect}_k$$

be the forgetful functor to k-vector spaces. Consider the endomorphisms

$$\mathrm{End}(F)$$

of F. An element $a \in \mathrm{End}(F)$ is a compatible sequence of linear transformations $a_V\colon V \to V$ as V runs over representations of G. Compatibility means that for any map $\phi\colon V \to W$ of representations, the following square commutes:

$$\begin{array}{ccc} V & \xrightarrow{a_V} & V \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ W & \xrightarrow{a_W} & W. \end{array}$$

Proposition 7.3. *The map*

$$a \mapsto a_{k[G]}(1)$$

defines an isomorphism $\mathrm{End}(F) \cong k[G]$.

There is an augmentation map $e^*\colon k[G] \to k$, and the diagonal map $G \to G \times G$, $g \mapsto (g, g)$ induces the comultiplication map

$$\Delta\colon k[G] \longrightarrow k[G \times G] \simeq k[G] \otimes k[G].$$

Given representations V and W, the tensor product $V \otimes_k W$ is initially a representation of $k[G] \otimes k[G]$, which is turned into a representation of $k[G]$ via Δ.

Proposition 7.4. *The group G itself can be recovered as the group-like elements of $k[G]$, i.e. $a \in k[G]$ such that $e^*(a) = 1$ and*

$$\Delta(a) = a \otimes a.$$

Proposition 7.5. *The group G is isomorphic to $\mathrm{Aut}^{\otimes}(F)$, the tensor-compatible automorphisms of the forgetful functor F from Rep_k^G to Vect_k.*

Here, an element $f \in \mathrm{Aut}(F)$ is *tensor-compatible* if $f_{V \otimes W} = f_V \otimes f_W$.

If we let

$$A = \mathrm{Hom}_k(k[G], k),$$

then the map

$$\Delta^*\colon A \otimes A \cong \mathrm{Hom}(k[G] \otimes k[G], k) \longrightarrow A$$

gives A the structure of a commutative k-algebra. Of course, we have a natural embedding

$$G \hookrightarrow \mathrm{Hom}_k(A, k)$$

given by evaluation: $g \mapsto (f \mapsto f(g))$.

Corollary 7.6.

$$G = \mathrm{Spec}(A)(k) = \mathrm{Hom}_{k\text{-alg}}(A, k).$$

8. Arithmetic fundamental groups

We now consider an arithmetic setting as follows:

K: a number field or a finite extension of $\mathbb{Q}_p$;

X: a smooth curve over K;

$\bar{X}$: the base change of X to $\overline{K}$;

$b, x \in X(K)$ rational points.

The rational points b, x are sometimes viewed as geometric points:

$$\mathrm{Spec}(\overline{K}) \longrightarrow \bar{X} \longrightarrow X.$$

In the local case, let $\mathcal{X}$ be a smooth scheme over $\mathcal{O}_K$ with good compactification and generic fibre X, and let Y be the special fibre of $\mathcal{X}$ over $k = \mathcal{O}_K/\mathfrak{m}_K$.

8.1. Profinite étale fundamental groups. We now introduce the profinite étale fundamental group. A reference is Szamuely's book **[Sza09]**.

Denote by

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

the category of finite étale covering spaces of $\bar{X}$. There is a fibre functor

$$F_b \colon \mathrm{Cov}(\bar{X}) \longrightarrow \mathrm{FinSet},$$
$$(Y \to \bar{X}) \longmapsto Y_b.$$

Define

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

Proposition 8.1. *There is a 'universal' pro-étale cover*

$$\tilde{\bar{X}} = (\bar{X}_i)_i \longrightarrow \bar{X}$$

with the property that we get a diagram

$$\begin{array}{ccc} \tilde{\bar{X}} & \overset{\exists}{\dashrightarrow} & Y \\ & \searrow & \downarrow \\ & & \bar{X} \end{array}$$

for any finite étale cover $Y \to \bar{X}$.

The arrow $\tilde{\bar{X}} \to Y$ is an element of $\varinjlim_i \mathrm{Hom}(\bar{X}_i, Y)$.

Pick a 'point' $\tilde{b} \in \tilde{\bar{X}}$, by which we mean a compatible sequence of points $b_i \in \bar{X}_{i,b}$. Then $(\tilde{\bar{X}}, \tilde{b})$ is a universal pointed pro-étale cover:

Proposition 8.2. *We get a diagram*

$$\begin{array}{ccc} (\tilde{\bar{X}}, \tilde{b}) & \overset{\exists!}{\dashrightarrow} & (Y, b_Y) \\ & \searrow & \downarrow \\ & & (\bar{X}, b) \end{array}$$

for any pointed finite étale cover $(Y, b_Y) \to (\bar{X}, b)$.

Furthermore, we have the following:

Proposition 8.3. *The cover $(\widetilde{\bar{X}}, \tilde{b})$ is defined over K. That is, there is a unique cover*

$$(\widetilde{X}, \tilde{b}) \longrightarrow (X, b)$$

with $\tilde{b}$ rational, whose base change to $\overline{K}$ is $(\widetilde{\bar{X}}, \tilde{b})$.

Be warned that in spite of the notation, $\widetilde{X} \to X$ is not the universal cover of X. The universal cover of X is

$$\widetilde{\bar{X}} \longrightarrow \bar{X} \longrightarrow X.$$

The cover $\widetilde{X} \to X$ is a K-model of the universal cover of $\bar{X}$.

Example 8.4. A K-model of the universal pro-étale covering of $(\mathbb{G}_m, 1)$ is given by

$$\widetilde{\mathbb{G}_m} = (\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m)_n$$

with basepoint 1.

Example 8.5. For an elliptic curve E/K with base point $O \in E(K)$, a K-model of the universal pro-étale covering of (E, O) is given by

$$\widetilde{E} = (E \xrightarrow{n} E)_n$$

with basepoint O.

Theorem 8.6. *The map*

$$\gamma \mapsto (\gamma_{\bar{X}_i}(b_i)) \in \widetilde{\bar{X}}_x = \widetilde{X}_x(\overline{K})$$

induces a G_K-equivariant isomorphism

$$\hat{\pi}_1(\bar{X}; b, x) \simeq \widetilde{\bar{X}}_x = \widetilde{X}_x(\overline{K}).$$

This isomorphism gives a concrete way of "computing" the action of $\mathrm{Gal}(\overline{K}/K)$ on $\hat{\pi}_1(\bar{X}; b, x)$. The formal definition of the action on the left is given as follows. For $g \in G_K$ and $p \in \hat{\pi}_1(\bar{X}; b, x)$, the element $g(p)$ associates to $X' \to \bar{X}$ the lower arrow that makes the diagram commute:

$$\begin{array}{ccc} g^*(X')_b & \xrightarrow{p_{g^*(X')}} & g^*(X')_x \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ X'_b & \xrightarrow{g(p)} & X'_x, \end{array}$$

that is,

$$g(p)_{X'} = g \circ p_{g^*(X')} \circ g^{-1}.$$

The theorem allows us to largely forget this and focus on the naive action on the fibres. However, this is somewhat misleading in that to apply this theorem, we must first have constructed the K-model

$$(\widetilde{X}, \tilde{b}) \longrightarrow (X, b).$$

Example 8.7 (Continuation of Example 8.4)**.** For $(X, b) = (\mathbb{G}_m, 1)$ we have canonical isomorphisms for the fundamental group and path space

$$\hat{\pi}_1(\overline{\mathbb{G}}_m, 1) = (\widetilde{\mathbb{G}_m})_1 = \hat{\mathbb{Z}}(1),$$
$$\hat{\pi}_1(\overline{\mathbb{G}}_m; 1, x) = (\widetilde{\mathbb{G}_m})_x = (x^{1/n})_n.$$

Example 8.8 (Continuation of Example 8.5)**.** For $(X, b) = (E, O)$ an elliptic curve, we have

$$\hat{\pi}_1(\overline{E}, O) = (\widetilde{E})_O = \widehat{T}(E),$$
$$\hat{\pi}_1(\overline{E}; O, x) = \widetilde{E}_x = \Big(\frac{1}{n}x\Big)_n.$$

There is a general construction as follows: If $P \to M$ is a principal G-bundle and G (left-)acts continuously on a set A, then we can form the associated bundle

$$P \times_G A \coloneqq [P \times A]/G,$$

where G acts on the product as $(p, a)g = (pg, g^{-1}a)$. This is a fibre bundle over M with fibre A which varies according to the variation of P. When $\rho\colon G \to H$ is a group homomorphism, this construction $P \times_G H$ gives a principal H-bundle.

The cover

$$\widetilde{\bar{X}} \to \bar{X}$$

is a principal $\hat{\pi}_1(\bar{X}, b)$-bundle. The cover

$$\widetilde{\bar{X}}^{(p)} = \widetilde{\bar{X}} \times_{\hat{\pi}_1(\bar{X},b)} \hat{\pi}_1^{(p)}(\bar{X}, b),$$

which is a principal $\hat{\pi}_1^{(p)}(\bar{X}, b)$-bundle, is the universal pro-p étale cover. In general, we might try to study the G_K-action on $\hat{\pi}_1(\bar{X}; b, x)$ via fibres of suitable quotient coverings like this. For example, if X is a modular curve, then the tower

$$X_{\mathrm{Mod}} \longrightarrow X$$

of modular curves, corresponds to the "modular quotient group" of $\hat{\pi}_1(\bar{X}, b)$.

Given a continuous $\mathbb{Q}_p$-representation V of $\hat{\pi}_1(\bar{X}, b)$, we get a locally constant sheaf of $\mathbb{Q}_p$-vector spaces

$$\widetilde{\bar{X}} \times_{\hat{\pi}_1(\bar{X},b)} V,$$

giving a functor

$$\mathrm{Rep}^{\mathbb{Q}_p}_{\hat{\pi}_1(\bar{X},b)} \longrightarrow \mathrm{Loc}^{\mathbb{Q}_p}(\bar{X})$$

which is inverse to the fibre functor

$$F_b\colon \mathcal{L} \mapsto \mathcal{L}_b.$$

This is a version of the "vector bundle associated to a principal G-bundle and a linear representation of G", familiar from usual geometry. However, to do this carefully in this case, you need to construct the correspondence with finite coefficients first and then consider projective systems. (This is where the continuity is needed.)

8.2. Unipotent fundamental groups. We now introduce unipotent fundamental groups, obtained by linearising categories. A reference is [**Del89**].

Let

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

be the category of unipotent $\mathbb{Q}_p$-locally constant sheaves on the étale site of $\bar{X}$.

Definition 8.9. A local system $\mathcal{F}$ is *unipotent* if it admits a filtration

$$\mathcal{F} = \mathcal{F}^0 \supset \mathcal{F}^1 \supset \ldots \supset \mathcal{F}^n = 0$$

such that

$$\mathcal{F}^i/\mathcal{F}^{i+1} \simeq (\mathbb{Q}_p)^{r_i}_{\bar{X}}$$

for each i. With this notation, we say $\mathcal{F}$ has *index of unipotency* $\leq n$.

THEOREM 8.10. *There is a universal pointed pro-object in* $\mathrm{Un}(\bar{X}, \mathbb{Q}_p)$. *This is a projective system*

$$(\mathcal{E}, v) = ((\mathcal{E}_n, v_n))_n$$

with $v_n \in (\mathcal{E}_n)_b$ *such that for any* $\mathcal{F} \in \mathrm{Un}(\bar{X}, \mathbb{Q}_p)$ *and* $w \in \mathcal{F}_b$, *there is a unique map*

$$f\colon (\mathcal{E}, v) \longrightarrow (\mathcal{F}, w).$$

Here,

$$\mathrm{Hom}((E, v), (F, w)) = \varinjlim \mathrm{Hom}((E_n, v_n), (F, w)).$$

The $\mathcal{E}_n$ as above corresponds to the representation

$$\mathcal{E}_{n,b} = E_n \coloneqq (\mathbb{Z}_p[\![\hat{\pi}_1(\bar{X}, b)]\!]/I^{n+1}) \otimes \mathbb{Q}_p,$$

where $I \subseteq \mathbb{Z}_p[\![\hat{\pi}_1(\bar{X}, b)]\!]$ is the augmentation ideal, and $v_n = 1$. We put

$$E = \varprojlim_n E_n = \varprojlim (\mathbb{Z}_p[\![\hat{\pi}_1(\bar{X}, b)]\!]/I^{n+1}) \otimes \mathbb{Q}_p.$$

We think of this as non-commutative power series in $\gamma - 1$, where γ are topological generators of $\hat{\pi}_1(\bar{X}, b)$. It contains elements like

$$\gamma^a = \exp(a \log(\gamma))$$

for $a \in \mathbb{Q}_p$.

The pointed local system $(\mathcal{E}_n, v_n)$ is universal among unipotent local systems of index of unipotency $\leq n$. Thus we get unique compatible system of maps

$$\mathcal{E}_{m+n} \to \mathcal{E}_m \otimes \mathcal{E}_n$$

that send v_{m+n} to $v_m \otimes v_n$. These come together to a map

$$\Delta\colon \mathcal{E} \longrightarrow \mathcal{E}\hat{\otimes}\mathcal{E}.$$

Using the fibre functor

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

we now define

$$U^{\text{ét}} \coloneqq U(\bar{X}, b) \coloneqq \mathrm{Aut}^{\otimes}(F_b),$$
$$P^{\text{ét}}(x) \coloneqq P(\bar{X}; b, x) \coloneqq \mathrm{Isom}^{\otimes}(F_b, F_x).$$

Lemma 8.11. *There is a canonical isomorphism*

$$\mathrm{End}(F_b) \cong \mathcal{E}_b.$$

THEOREM 8.12. *The pro-algebraic group* $U(\bar{X}, b)$ *is isomorphic to the group-like elements in* $\mathcal{E}_b$, *while* $P(\bar{X}; b, x)$ *is given by the group-like elements in* $\mathcal{E}_x$.

There is a sloppiness in the statement that we will not dwell on. We should be referring in all this to the $\mathbb{Q}_p$-points of $U(\bar{X}, b)$ rather than the group itself. To remedy this, we can transport the discussion to one over an arbitrary $\mathbb{Q}_p$-algebra and make the corresponding statement for the functor of points.

In fact, the lower central series

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

is compatible with the filtration by I^n, so that $U_n = U/U^{n+1}$ are the group-like elements in E_n.

Put

$$\mathcal{A} = \mathrm{Hom}(\mathcal{E}, \mathbb{Q}_p) = \varinjlim \mathrm{Hom}(\mathcal{E}_n, \mathbb{Q}_p).$$

Then $\mathcal{A}$ is a sheaf of $\mathbb{Q}_p$-algebras via Δ^*.

Corollary 8.13. *There are canonical isomorphisms*

$$U(\bar{X}, b) = \mathrm{Spec}(\mathcal{A}_b),$$
$$P(\bar{X}; b, x) = \mathrm{Spec}(\mathcal{A}_x).$$

Remarks 8.14. Some remarks on Galois actions:

(1) The action on $P(\bar{X}; b, x)$ is induced by the action on $\mathcal{E}_x$.

(2) The action on $\mathcal{E}_x$ uses $\tilde{\bar{X}} \otimes_{\hat{\pi}_1(\bar{X},b)} E$.

(3) The action on $\tilde{\bar{X}}_x$ is given by a cocycle

$$c_x \colon G_K \longrightarrow \hat{\pi}(\bar{X}, b).$$

That is, choose $\tilde{x} \in \tilde{\bar{X}}$. Then c_x is defined by

$$g(\tilde{x}) = \tilde{x} c_x(g)$$

and satisfies $c_x(g_1 g_2) = c(g_1) \cdot g_1 c(g_2)$. Then $\mathcal{E}_x$ can be identified with E where the action is twisted:

$$g_x v = c_x(g) g v.$$

The following are some basic structural facts. The map

$$g \mapsto [g - 1]$$

induces an isomorphism

$$H_1(\bar{X}, \mathbb{Q}_p) = \hat{\pi}_1(\bar{X}, b)^{\mathrm{ab}} \otimes \mathbb{Q}_p \cong I/I^2.$$

The multiplication map

$$(I/I^2)^{\otimes n} \longrightarrow I^n/I^{n+1}$$

induces an isomorphism

$$H_1^{\otimes n}/K_n \simeq I^n/I^{n+1}$$

where $T_n \coloneqq H_1^{\otimes n}/K_n \simeq (R^n)^*$, and $R^n \subset (H^1)^{\otimes n}$ is defined inductively as follows.

$$R^0 = \mathbb{Q}_p,$$
$$R^1 = H^1,$$
$$R^2 = \mathrm{Ker}(H^1 \otimes H^1 \xrightarrow{\gamma_1 := \cup} H^2).$$

We will have $R^{n+1} \subset R^n \otimes H^1$. Define the map γ_n inductively as

$$\gamma_n \colon R^n \otimes H^1 \to R^{n-1} \otimes H^1 \otimes H^1 \to R^{n-1} \otimes H^2,$$

and define

$$R^{n+1} = \mathrm{Ker}(\gamma_n).$$

This comes from a different tautological construction [**AIK15, Fal07, Fal12**]. We have an isomorphism

$$\mathrm{Ext}^1_{\bar{X}}((\mathbb{Q}_p)_{\bar{X}}, (H_1(\bar{X}))_{\bar{X}}) \simeq H^1(\bar{X}) \otimes H_1(\bar{X}) = \mathrm{Hom}(H_1, H_1).$$

So there is an extension

$$0 \longrightarrow H_1(\bar{X}) \longrightarrow \mathcal{E}_1 \longrightarrow \mathbb{Q}_p \longrightarrow 0$$

corresponding to the identity map on the right. Now we get an exact sequence

$$\begin{array}{l} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathrm{Hom}_{\bar{X}}(H_1,\mathbb{Q}_p) \\ \hookrightarrow \mathrm{Ext}^1_{\bar{X}}(\mathbb{Q}_p,\mathbb{Q}_p) \longrightarrow \mathrm{Ext}^1_{\bar{X}}(\mathcal{E}_1,\mathbb{Q}_p) \longrightarrow \mathrm{Ext}^1_{\bar{X}}(H_1,\mathbb{Q}_p) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathrm{Ext}^2_{\bar{X}}(\mathbb{Q}_p,\mathbb{Q}_p). \end{array}$$

This can be written as

$$H^1 \xrightarrow{\delta} H^1 \longrightarrow \mathrm{Ext}^1_{\bar{X}}(\mathcal{E}_1,\mathbb{Q}_p) \longrightarrow H^1 \otimes H^1 \xrightarrow{\delta} H^2,$$

which induces the isomorphism

$$\mathrm{Ext}^1_{\bar{X}}(\mathcal{E}_1,\mathbb{Q}_p) \cong R^2 \cong T_2^*.$$

Hence,

$$\mathrm{Ext}^1_{\bar{X}}(\mathcal{E}_1,T_2) \cong \mathrm{Hom}(T_2,T_2,)$$

so that there is an extension

$$0 \longrightarrow T_2 \longrightarrow \mathcal{E}_2 \longrightarrow \mathcal{E}_1 \longrightarrow 0$$

corresponding to the identity on the right. One continues in this way and the universal property can also be proved in a tautological manner. The idea is as follows: When the index of unipotency is 1, we have a constant sheaf $V_{\bar{X}} \to \bar{X}$. Of course, there is a unique map

$$f_1 \colon [\mathbb{Q}_p]_{\bar{X}} \longrightarrow V_{\bar{X}}$$

that takes $1 \in \mathbb{Q}_p = [\mathbb{Q}_p]_{\bar{X},b}$ to any fixed $v \in V = V_{\bar{X},b}$. Now suppose you have

$$0 \longrightarrow W \longrightarrow \mathcal{F} \longrightarrow V \longrightarrow 0$$

with V and W constant. We would like to construct a lift f_2 as below

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_1 & \longrightarrow & \mathcal{E}_1 & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\ & & \downarrow & & \vdots{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \\ 0 & \longrightarrow & W & \longrightarrow & \mathcal{F} & \longrightarrow & V & \longrightarrow & 0. \end{array}$$

The idea is to pull back by f_1 to get

$$0 \longrightarrow W \longrightarrow f_1^*\mathcal{F} \longrightarrow \mathbb{Q}_p \longrightarrow 0.$$

We would like to show that this comes from $\mathcal{E}_1$ via a push-out along a map $\phi \colon T_1 \to W$. But this extension is a class

$$c \in \mathrm{Ext}^1_{\bar{X}}(\mathbb{Q}_p,W) = H^1 \otimes W.$$

Meanwhile, $\mathcal{E}_1$ corresponds to the class

$$I = \sum_i b^i \otimes b_i \in \mathrm{Ext}^1(\mathbb{Q}_p,H_1) = H^1 \otimes H_1,$$

where $\{b_i\}$ is a basis for H_1 and $\{b^i\}$ is the dual basis. Write $c = \sum_i b^i \otimes w_i$, and define ϕ to be the linear map that takes b_i to w_i.

8.3. De Rham fundamental groups. We now introduce de Rham fundamental groups. Let us fix the following notation:

F: a finite extension of $\mathbb{Q}_p$

X: a smooth curve over F

$\bar{X}$: the basechange of X to $\bar{F}$

$b, x \in X(F)$: rational points, viewed sometimes as geometric points

$$\mathrm{Spec}(\bar{F}) \to \bar{X} \to X$$

$\mathcal{X}$: a smooth scheme over $\mathcal{O}_F$, the valuation ring of F, with good compactification and generic fibre X

Y: the special fibre of $\mathcal{X}$ over the residue field $k = \mathcal{O}_F/\mathfrak{m}_F$.

The de Rham version is similar to the étale case [**Hai87a, AIK15, Kim09**]. The relevant category is

$$\mathrm{Un}^{\mathrm{DR}}(X) \subset \mathrm{Loc}^{\mathrm{DR}}(X),$$

the category of unipotent vector bundles with (flat) connection, a full subcategory of all bundles with flat connection. There are fibre functors

$$F_b \colon \mathrm{Un}^{\mathrm{DR}}(X) \longrightarrow \mathrm{Vect}_F,$$
$$(V, \nabla) \longmapsto V_b,$$

and the objects of interest are

$$U^{\mathrm{DR}} \coloneqq U^{\mathrm{DR}}(X, b) \coloneqq \mathrm{Aut}^{\otimes}(F_b),$$

and

$$P^{\mathrm{DR}}(x) \coloneqq U^{\mathrm{DR}}(X; b, x) \coloneqq \mathrm{Isom}^{\otimes}(F_b, F_x).$$

They can be constructed using universal objects which in turn admit a tautological construction [**AIK15**] using

$$\mathrm{Ext}^i_{\mathrm{Loc}^{\mathrm{DR}}(X)}((V, \nabla), (W, \nabla)) \simeq H^i_{\mathrm{DR}}(X, (V, \nabla)^* \otimes (W, \nabla)),$$

where

$$H^i_{\mathrm{DR}}(X, (V, \nabla)) = H^i(X_{\mathrm{Zar}}, V \to V \otimes_{\mathcal{O}_X} \Omega_X).$$

In particular, the universal object $\mathcal{E}^{\mathrm{DR}}$ is a projective system of objects

$$(\mathcal{E}^{\mathrm{DR}}_n, \nabla_n)$$

which fit together as

$$0 \longrightarrow T^{\mathrm{DR}}_n \otimes \mathcal{O}_X \longrightarrow \mathcal{E}^{\mathrm{DR}}_n \longrightarrow \mathcal{E}^{\mathrm{DR}}_{n-1} \longrightarrow 0.$$

Here, T^{DR}_n is a quotient of $(H^{\mathrm{DR}}_1)^{\otimes n}$ as in the étale case.

After choosing an element $1 \in \mathcal{E}^{\mathrm{DR}}_b$, we get the universal property:

Proposition 8.15. *Given any object (V, ∇_V) in $\mathrm{Un}^{\mathrm{DR}}(X)$ together with an element $v \in V_b$ (the fibre at b), there exists a unique morphism $\phi \colon (\mathcal{E}^{\mathrm{DR}}, \nabla) \to (V, \nabla_V)$ such that $1 \in \mathcal{E}^{\mathrm{DR}}_b \mapsto v$.*

Corollary 8.16. *There is a canonical isomorphism*

$$\mathrm{End}(F_b) \cong \mathcal{E}^{\mathrm{DR}}_b.$$

Theorem 8.17. *The pro-algebraic group $U^{\mathrm{DR}}(X, b)$ is isomorphic to the group-like elements in $\mathcal{E}_b$, while $P^{\mathrm{DR}}(X; b, x)$ is isomorphic to the group-like elements in $\mathcal{E}_x$.*

The universal property gives rise to a map of pro-objects in $\mathrm{Un}^{\mathrm{DR}}(X)$

$$\Delta\colon (\mathcal{E}^{\mathrm{DR}},\nabla)\longrightarrow(\mathcal{E}^{\mathrm{DR}},\nabla)\hat{\otimes}(\mathcal{E}^{\mathrm{DR}},\nabla)$$

which takes 1 to $1\otimes 1$. Let $\mathcal{A}^{\mathrm{DR}}=(\mathcal{E}^{\mathrm{DR}})^*$ be the dual (ind-)bundle. Then Δ^* gives

$$\mathcal{A}^{\mathrm{DR}}_x=\mathrm{Hom}(\mathcal{E}^{\mathrm{DR}}_x,F)$$

the structure of a commutative algebra, and we have

$$P^{\mathrm{DR}}(x)=\mathrm{Spec}(\mathcal{A}^{\mathrm{DR}}_x).$$

8.3.1. *The Hodge filtration.* For this section, we will assume for simplicity that X is projective. Otherwise one must consider logarithmic connections on the compactification. The universal bundle $\mathcal{E}^{\mathrm{DR}}$ carries a Hodge filtration [**Hai87a, Woj93, Vol03, Had11, Kim09**]. This is the unique decreasing filtration $\mathcal{F}^i$, $i\leq 0$ of $\mathcal{E}^{\mathrm{DR}}$ satisfying the following conditions:

(1) Griffiths transversality: $\nabla(\mathcal{F}^i)\subset\mathcal{F}^{i-1}\otimes\Omega_X$;
(2) The induced filtration on T^{DR}_n coincides with the constant one coming from (co)homology;
(3) $1\in F^0\mathcal{E}^{\mathrm{DR}}_b$.

There is an induced Hodge filtration with non-negative degrees on $\mathcal{A}^{\mathrm{DR}}$ and $F^1\mathcal{A}^{\mathrm{DR}}$ is an ideal. One defines $F^0P^{\mathrm{DR}}(x)$ to be the zero set of $F^1\mathcal{A}^{\mathrm{DR}}_x$. It is a torsor for F^0U^{DR}, which is a subgroup of U^{DR}. This is an aspect of the fact that the action of U^{DR} on $P^{\mathrm{DR}}(x)$ is compatible with the Hodge filtration. Namely, the action map

$$P^{\mathrm{DR}}(x)\times U^{\mathrm{DR}}\longrightarrow P^{\mathrm{DR}}(x)$$

corresponds to a co-action map

$$\mathcal{A}^{\mathrm{DR}}_x\longrightarrow\mathcal{A}^{\mathrm{DR}}_x\otimes\mathcal{A}^{\mathrm{DR}}_b,$$

and this is compatible with the Hodge filtration.

The choice of a point $p\in F^0P^{\mathrm{DR}}(x)$ gives an algebra homomorphism $\mathcal{A}^{\mathrm{DR}}_x\to F$ which kills $F^1\mathcal{A}^{\mathrm{DR}}_x$, which is hence a map of Hodge structures. Thus, we get an isomorphism

$$\mathcal{A}^{\mathrm{DR}}_x\cong\mathcal{A}^{\mathrm{DR}}_b$$

that is compatible with the Hodge filtration. A dimension count then shows that

$$F^1\mathcal{A}^{\mathrm{DR}}_x\cong F^1\mathcal{A}^{\mathrm{DR}}_b,$$

and hence

$$\mathcal{A}^{\mathrm{DR}}_x/F^1\mathcal{A}^{\mathrm{DR}}_x\cong\mathcal{A}^{\mathrm{DR}}_b/F^1\mathcal{A}^{\mathrm{DR}}_b,$$

giving us

$$F^0U^{\mathrm{DR}}\cong F^0P^{\mathrm{DR}}(x).$$

8.3.2. *Crystalline structures.* In addition to the Hodge filtration, de Rham fundamental group also carries a crystalline structure. The (k-linear) Frobenius ϕ of the special fibre Y acts on the category $\mathrm{Un}^{\mathrm{DR}}(X)$ [**Del89, Bes02**]. Write $\mathcal{X}=\bigcup_i U_i$ such that U_i is affine and a smooth lift of $U_i\otimes k$. Choose local lifts ϕ_i on U_i of the Frobenius on $U_i\otimes k$. Then, given a bundle with connection (V,∇), we consider the local pullbacks $(\phi_i^*(V|_{U_i}),\phi_i^*(\nabla))$. The connection allows us to patch these together canonically to give us $\phi^*(V,\nabla)$.

In particular, the Frobenius ϕ defines an isomorphism

$$(\mathcal{E}^{\mathrm{DR}},\nabla,1)\longrightarrow(\phi^*\mathcal{E}^{\mathrm{DR}},\phi^*\nabla,\phi^*1).$$

We get compatible actions on $U^{\mathrm{DR}}(X,b)$ and $P^{\mathrm{DR}}(X;b,x)$. On T_n, it agrees with the action induced by the isomorphism

$$H^1_{\mathrm{DR}}(X) \cong H^1_{\mathrm{crys}}(Y).$$

Hence, the eigenvalues are the same as the ones coming from étale cohomology.

THEOREM 8.18. *There is a unique Frobenius-invariant element $p^{\mathrm{cr}}_{b,x}$ in $P^{\mathrm{DR}}(X;b,x)$.*

Lemma 8.19. *The Lang map $L(\phi)\colon U^{\mathrm{DR}} \to U^{\mathrm{DR}}$ that sends u to $u\phi(u)^{-1}$ is a bijection. In particular, the identity is the only element fixed by ϕ.*

PROOF. The eigenvalues of ϕ on $T^{\mathrm{DR}}_n = U^{\mathrm{DR},n}/U^{\mathrm{DR},n+1}$ are all different from 1. □

PROOF OF THEOREM 8.18. Choose $p \in P^{\mathrm{DR}}(X;b,x)$. Then there is a unique $u \in U^{\mathrm{DR}}$ such that $\phi(p) = pu$. Write $u = v\phi(v)^{-1}$, this is possible by Lemma 8.19. Then

$$\phi(pv) = pv.$$

Uniqueness comes from the fact that if p is fixed, no pu will be fixed for $u \neq 1$. □

It is better to think in terms of *crystalline fundamental groups*: Given a point $y \in Y(k)$, define on $\mathrm{Un}^{\mathrm{DR}}(X)$ the fibre functor

$$(V,\nabla) \mapsto V(]y[)^{\nabla=0},$$

the flat sections of V over the tube $]y[$, the analytic space of points that reduce to y. Then for $x, x' \in]y[$, the Frobenius-invariant element $p^{\mathrm{cr}}_{x,x'}$ is given by the diagram

$$\begin{array}{ccc} & V(]y[)^{\nabla=0} & \\ \swarrow^{\cong} & & \searrow^{\cong} \\ V_x & & V_{x'}. \end{array}$$

This is supplemented by an isomorphism

$$p^{\mathrm{cr}}_{y,y'}\colon V(]y[)^{\nabla=0} \cong V(]y'[)^{\nabla=0}$$

for $y, y' \in Y(k)$, called *Coleman integration* **[Bes02]**. The computation of this is Kedlaya's theory.

8.3.3. *De Rham moduli space.* The space of torsors for U^{DR} that have compatible Frobenius and Hodge filtration are classified by

$$U^{\mathrm{DR}}/F^0.$$

The bijection is given as follows. Given a torsor T, there exists a unique Frobenius-invariant element t^{cr}. Choose $t^H \in F^0T$ and write

$$t^H = t^{\mathrm{cr}}u^{\mathrm{cr}}_T.$$

The element u^{cr}_T is independent of the choice of t^H up to multiplication by F^0U^{DR} on the right, giving us a well-defined element

$$[u^{\mathrm{cr}}_T] \in U^{\mathrm{DR}}/F^0.$$

8.3.4. *Explicit description.* We will give an explicit description of the de Rham fundamental group for X affine [**Kim09**]. We first choose

$$\alpha_1, \alpha_2, \ldots, \alpha_m,$$

global algebraic differential forms representing a basis of $H^1_{\mathrm{DR}}(X)$. Thus, $m = 2g + s - 1$, where s is the number of missing points. Consider the algebra

$$F\langle A_1, \ldots, A_m\rangle$$

generated by the (non-commuting) symbols $A_1, A_2, \ldots, A_m$. Thus, it is the tensor algebra of the F-vector space generated by the A_i. Let I be the augmentation ideal. The algebra $F\langle A_1, \ldots, A_m\rangle$ has a natural comultiplication map Δ with values $\Delta(A_i) = A_i \otimes 1 + 1 \otimes A_i$. Now let

$$E_n = F\langle A_1, \ldots, A_m\rangle / I^{n+1}$$

and take the completion

$$E \coloneqq \varprojlim_n F\langle A_1, \ldots, A_m\rangle / I^n.$$

The comultiplication Δ extends naturally to a comultiplication $E \to E\hat{\otimes}E$.

Let $\mathcal{E}$ be the pro-unipotent pro-vector bundle $E \otimes \mathcal{O}_X$ with the connection $\nabla_{\mathcal{E}}$ determined by

$$\nabla_{\mathcal{E}} f = df - \sum_i A_i f \alpha_i$$

for sections $f\colon X \to E$. There is the distinguished element $1 \in \mathcal{E}_b = E$.

THEOREM 8.20. *There is a unique isomorphism*

$$(\mathcal{E}, \nabla_{\mathcal{E}}, 1) \cong (\mathcal{E}^{\mathrm{DR}}, \nabla, 1).$$

It is compatible with the comultiplication on either side.

The theorem is an easy consequence of the following:

Lemma 8.21. *Let (V, ∇) be a unipotent bundle with flat connection on X of rank r. Then there exist strictly upper-triangular matrices N_i such that*

$$(V, \nabla) \simeq (\mathcal{O}_X^r, d + \sum_i \alpha_i N_i).$$

The isomorphism

$$\begin{array}{ccc} & \mathcal{E}(]y[)^{\nabla=0} & \\ \swarrow^{\cong} & & \searrow^{\cong} \\ \mathcal{E}_b & & \mathcal{E}_x. \end{array}$$

for b and x in the same tube $]y[$ can be constructed locally by solving differential equations. Let

$$f = \sum_w f_w [w]$$

be a section of $\mathcal{E}$, where $[w]$ are words in the A_i, and $f(b) = 1$. Then the flatness condition is

$$df = \sum_w \sum_i f_w \alpha_i [A_i w],$$

that is

$$df_{A_i w} = f_w \alpha_i$$

for all w and i. We solve this iteratively:

$$f_{A_i}(z) = \int_b^z \alpha_i.$$

This can be constructed as a power series with initial condition $f_{A_i}(x) = 0$. We continue with

$$f_{A_j A_i}(z) = \int_b^z f_{A_i} \alpha_j,$$

and so on. Thus, the components of f become iterated integrals. Having solved the equation with initial condition 1, we get $p^{\mathrm{cr}}_{b,x}$ for $v \in \mathcal{E}^{\mathrm{DR}}_b$ by

$$p^{\mathrm{cr}}_{b,x}(v) = f(x)v.$$

For general x, the components of $p^{\mathrm{cr}}_{b,x}$ give the *definition* of iterated integrals.

The shuffle identities for iterated integrals,

$$\int_b^x \omega_1 \cdots \omega_k \int_b^x \omega_{k+1} \cdots \omega_n = \sum_\sigma \int_b^x \omega_{\sigma(1)} \cdots \omega_{\sigma(n)},$$

with the sum running over $(k, n-k)$-shuffles of $\{1, 2 \ldots, n\}$, follow from the group-like nature of $p^{\mathrm{cr}}_{b,x}$.

Another way to say this is that

$$\mathcal{A}^{\mathrm{DR}}_x = F[\phi_w],$$

the vector space generated by ϕ_w such that $\phi_w[w'] = \delta_{ww'}$. The algebra structure is given by

$$\phi_w \phi_{w'} = \sum_\sigma \phi_{\sigma(ww')}$$

where again the σ run over shuffles. The iterated integral identity is the fact that

$$p^{\mathrm{cr}}_{b,x} \colon \mathcal{A}^{\mathrm{DR}}_x \longrightarrow F$$

is an algebra homomorphism.

THEOREM 8.22. *The map*

$$j^{\mathrm{DR}} \colon X(F) \longrightarrow U^{\mathrm{DR}}/F^0$$

which sends x to the element $(p^{\mathrm{cr}}_{b,x})^{-1} p^H_{b,x}$ representing the path torsor $P^{\mathrm{DR}}(x)$, has the property that $j^{\mathrm{DR}}(]y[)$ is Zariski dense for each $y \in Y(k)$.

The idea is to show that all iterated integrals are algebraically independent using transcendental methods. Hence, as we increase n, the coordinates of the map $j^{\mathrm{DR}} \colon X(F) \to U^{\mathrm{DR}}/F^0$ keep giving genuinely new analytic functions.

9. Geometry of non-abelian cohomology

9.1. Non-abelian cohomology functors. Fix the following notation:

$X/\mathbb{Q}$: a smooth curve,
p: a prime of good reduction,
$U = U(\bar{X}, b)$, the $\mathbb{Q}_p$-prounipotent étale fundamental group,
$U_n = U/U^{n+1}$ the nth quotient of the lower central series,

G: either the group $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ or $G_T = \mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$, where $\mathbb{Q}_T$ is the maximal extension of $\mathbb{Q}$ unramified outside a finite set T of primes. We assume that T contains ∞, p, and all primes of bad reduction.

Following **[Kim05]**, we define a functor of $\mathbb{Q}_p$-algebras

$$R \mapsto H^1(G, U_n(R)) \coloneqq U_n(R)\backslash Z^1(G, U_n(R)).$$

The H^1 refers to continuous cohomology: Z^1 denotes the continuous functions $f\colon G \to U(R)$ such that

$$f(g_1 g_2) = f(g_1)\, g_1(f(g_2))$$

on which $U_n(R)$ acts via

$$f^u(g) = uf(g)g(u^{-1}).$$

The G-action on $U_n(R)$ is defined by identifying

$$U_n \underset{\log}{\cong} L_n \coloneqq \mathrm{Lie}(U_n).$$

In fact, it is often good to think of U_n as being L_n with group law defined by the Baker–Campbell–Hausdorff formula:

$$X \cdot Y = X + Y + \tfrac{1}{2}[X,Y] + \tfrac{1}{12}[X,[X,Y]] - \tfrac{1}{12}[Y,[Y,X]] + \dots,$$

the formula for $\log(\exp(X)\exp(Y))$. Then $U_n(R) = L_n \otimes R$. The topology on $U_n(R)$ is defined by using

$$U_n \cong \mathbb{A}^N,$$

which gives

$$U_n(R) \cong R^N.$$

We give R^N the inductive limit topology of finite-dimensional $\mathbb{Q}_p$-subspaces. (This definition works also for all affine schemes.)

On the abelian pieces U^n/U^{n+1}, the same definition of H^1 applies, but we can also define H^2.

Proposition 9.1. *For $i = 1, 2$, we have a canonical isomorphism*

$$H^i(G, U^n/U^{n+1}(R)) \cong H^i(G, U^n(\mathbb{Q}_p)/U^{n+1}(\mathbb{Q}_p)) \otimes R.$$

That is, the functor of R can be represented by the finite-dimensional $\mathbb{Q}_p$-vector space $H^i(G, U^n(\mathbb{Q}_p)/U^{n+1}(\mathbb{Q}_p))$.

Theorem 9.2. *The functor*

$$R \mapsto H^1(G, U_n(R))$$

is represented by an affine $\mathbb{Q}_p$-scheme of finite type.

The scheme represents principal U_n-bundles with continuous G-action: The R-points are principal $(U_n)_R$-bundles

$$P \longrightarrow \mathrm{Spec}(R)$$

with functorial continuous action of G on $P(S)$ for any R-algebra S.

Proof of Theorem 9.2. The proof is by induction on n using the exact sequence

$$0 \longrightarrow H^1(G, U^n/U^{n+1}(R)) \longrightarrow H^1(G, U_n(R)) \longrightarrow H^1(G, U_{n-1}(R)) \xrightarrow{\delta} H^2(G, U^n/U^{n+1}(R)).$$

That is, once $H^1(G, U_{n-1})$ is representable, δ is a map of schemes. The exact sequence means that $H^1(G, U_n)$ defines an $H^1(G, U^n/U^{n+1})$-torsor over $\mathrm{Ker}(\delta)$, which then must by represented by

$$\mathrm{Ker}(\delta) \times H^1(G, U^n/U^{n+1}). \qquad \square$$

In the local case, we define also

$$R \mapsto H^1(G_p, U_n(B_{\mathrm{cris}} \otimes R))$$

with Fontaine's period ring B_{cris}, and

$$H^1_f(G_p, U_n) = \mathrm{Ker}\big(H^1(G_p, U_n) \to H^1(G_p, U_n(B_{\mathrm{cris}}))\big),$$

which is a subscheme by induction on n:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G_p, U^n/U^{n+1}) & \longrightarrow & H^1(G_p, U_n) & \longrightarrow & H^1(G_p, U_{n-1}) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1(G_p, U^n/U^{n+1}(B_{\mathrm{cris}})) & \longrightarrow & H^1(G_p, U_n(B_{\mathrm{cris}})) & \longrightarrow & H^1({}_pG, U_{n-1}(B_{\mathrm{cris}})) \end{array}$$

The scheme $H^1_f(G_p, U_n)$ represents torsors that have a G_p-invariant point in $U_n(B_{\mathrm{cris}})$. We call them *crystalline torsors*.

We have the localisation map

$$\mathrm{loc}_p \colon H^1(G_T, U_n) \longrightarrow H^1(G_p, U_n),$$

which we use to define

$$H^1_f(G_T, U_n) \coloneqq \mathrm{loc}_p^{-1}(H^1_f(G_p, U_n)).$$

Thus, we get a diagram

$$\begin{array}{ccc} X(\mathbb{Z}) & \hookrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H^1_f(G_T, U_n) & \longrightarrow & H^1_f(G_p, U_n). \end{array}$$

Here, we are being imprecise in that the integral points belong to a model $\mathcal{X}$ of X, which we suppress for the sake of notational simplicity. The bottom arrow is a map of schemes since it represents a map of functors. It is a *computable replacement* for $X(\mathbb{Z}) \subset X(\mathbb{Z}_p)$.

The reason $X(\mathbb{Z}_p)$ maps to $H^1_f \subset H^1$ is because of the non-abelian p-adic Hodge theory isomorphism

$$P^{\text{ét}}_n(x)(B_{\mathrm{cris}}) \cong P^{\mathrm{DR}}(x)(B_{\mathrm{cris}}) \cong B^N_{\mathrm{cris}}$$

for $x \in X(\mathbb{Z}_p)$. The first isomorphism respects all structures, while the second is Galois equivariant, showing the existence of an invariant point.

9.2. Étale-de Rham comparison. Given a crystalline torsor $P = \mathrm{Spec}(\mathcal{O}(P))$ for U, then

$$\mathsf{D}(P) \coloneqq \mathrm{Spec}([\mathcal{O}(P) \otimes B_{\mathrm{cris}}]^{G_p})$$

is a torsor for U^{DR} with Hodge filtration and Frobenius structure [**Kim05, Kim12b, Kim09**], and those are classified by U^{DR}/F^0, as discussed in Section 8.3.3. This is an application of the *Dieudonné functor*.

Lemma 9.3. *The functor $P \mapsto \mathsf{D}(P)$ defines an isomorphism*

$$H^1_f(G_p, U) \cong U^{\mathrm{DR}}/F^0.$$

An inverse is constructed using the fundamental exact sequence of p-adic Hodge theory:

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_{\mathrm{cris}}^{\phi=1} \oplus B_{\mathrm{DR}}^{+} \longrightarrow B_{\mathrm{DR}} \longrightarrow 0.$$

From this we get

$$U(B_{\mathrm{DR}})/U(B_{\mathrm{DR}}^{+}) \longrightarrow H^1(G_p, U) \longrightarrow H^1(G_p, U(B_{\mathrm{cris}}^{\phi=1})).$$

The left term is the $\mathbb{Q}_p$-points of U^{DR}/F^0. We get an equality between

$$H^1_e(G_p, U) = \mathrm{Ker}[H^1(G_p, U) \longrightarrow H^1(G_p, U(B_{\mathrm{cris}}^{\phi=1}))]$$

and

$$H^1_f(G_p, U) = \mathrm{Ker}[H^1(G_p, U) \longrightarrow H^1(G_p, U(B_{\mathrm{cris}}))].$$

10. The fundamental diagram

Reference: **[Kim05]**

From here on, we assume that X is a smooth proper curve of genus ≥ 2. We will focus on the base field $\mathbb{Q}$, even though Netan Dogra has generalised all the arguments to number fields **[Dog20]**. The following diagram is fundamental in non-abelian Chabauty theory:

$$\begin{array}{ccccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) & & \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j_p} & \searrow^{j^{\mathrm{DR}}} & \\ H^1_f(G_T, U_n) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_n) & \xrightarrow[\cong]{\mathsf{D}} & U^{\mathrm{DR}}/F^0. \end{array}$$

Conjecture (A). *The image of loc_p is non-dense for $n \gg 0$.*

Theorem 10.1. *Assuming the conjecture, $X(\mathbb{Q})$ is finite.*

Proof. By assumption, there is an algebraic function $\alpha \neq 0$ that vanishes on $\mathsf{D}(\mathrm{loc}_p(H^1_f(G_T, U_n)))$. Hence

$$\alpha \circ j^{\mathrm{DR}}|_{X(\mathbb{Q})} = 0.$$

But $\alpha \circ j^{\mathrm{DR}}$ is a non-zero convergent power series on each tube $]y[\subseteq X(\mathbb{Z}_p) = X(\mathbb{Q}_p)$ for $y \in Y(\mathbb{F}_p)$. So the zero set is finite. □

Definition 10.2 (**[BDCKW18]**). For $n \geq 1$, define

$$\begin{aligned} X(\mathbb{Q}_p)_n &\coloneqq \bigcap_{\alpha \circ \mathsf{D} \circ \mathrm{loc}_p = 0} Z(\alpha \circ j^{\mathrm{DR}}) \\ &= (j^{\mathrm{DR}})^{-1}\big(\overline{\mathsf{D}(\mathrm{loc}_p(H^1_f(G_T, U_n)))}\big). \end{aligned}$$

Since the diagrams are compatible over n, we get a decreasing filtration:

$$X(\mathbb{Q}_p) \supset X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q}_p)_2 \supset X(\mathbb{Q}_p)_3 \supset X(\mathbb{Q}_p)_4 \supset \dots$$

The set of rational points $X(\mathbb{Q})$ is contained in $X(\mathbb{Q}_p)_n$ for all n. Note that Conjecture (A) actually implies that $X(\mathbb{Q}_p)_n$ is finite for $n \gg 0$.

Conjecture (B).

$$\bigcap_n X(\mathbb{Q}_p)_n = X(\mathbb{Q}).$$

Conjecture (C). *The sets $X(\mathbb{Q}_p)_n$ are computable and Conjecture 3.9 is computationally verifiable.*

The key problem is to find defining equations for

$$\mathrm{loc}_p(H^1_f(G_T, U_n)) \subset H^1_f(G_p, U_n).$$

One might very speculatively ask if there are *canonical* equations related to nonabelian L-functions. For example, is there a canonical trivialisation

$$R\Gamma_c(G_T, U) \sim^{\mathcal{L}} 0$$

is a suitable homotopy category? This should be similar to the annihilation of Selmer groups by p-adic L-functions [**CK10**] or Iwasawa's theorem on the image of global units in local units of cyclotomic fields [**CS06**].

10.1. Refined nonabelian Chabauty. We shall describe a variant of the fundamental diagram for affine curves which is due to Betts–Dogra [**BD19**]. Assume that $Y = X \setminus D$ where $X/\mathbb{Q}$ is a smooth proper curve (of any genus) and D is a reduced divisor of points at infinity. We assume that Y is *hyperbolic*, i.e.

$$\chi(Y) \coloneqq 2 - 2g - r < 0,$$

where g is the genus and $r = \#D(\overline{\mathbb{Q}})$ is the number of points at infinity. Thus, $Y_{\overline{\mathbb{Q}}}$ is either

(1) $\mathbb{P}^1$ minus at least three points;
(2) a genus one curve minus at least one point;
(3) a higher genus curve with arbitrarily many points removed.

In the affine case we are interested in integral points rather than rational points. More precisely, let S be a finite set of primes and let $\mathbb{Z}_S$ be the ring of *S-integers*, i.e. the subring of $\mathbb{Q}$ consisting of rational numbers whose denominators are only divisible by primes from S. Assume that we have a regular S-integral model $\mathcal{Y} = \mathcal{X} \setminus \mathcal{D}$ for $Y = X \setminus D$, by which we mean that $\mathcal{Y}$ is presented as the complement of a horizontal divisor $\mathcal{D}$ in a flat proper regular $\mathbb{Z}_S$-scheme $\mathcal{X}$.

Theorem 10.3 (Faltings, Siegel). *The number of S-integral points of $\mathcal{Y}$ is finite:*

$$\#\mathcal{Y}(\mathbb{Z}_S) < \infty.$$

Let $p \notin S$ be a prime of good reduction. Assume that we are given an S-integral base point b of Y. This is either an S-integral point of $\mathcal{Y}$ or a *tangential base point*, i.e. a nowhere vanishing section of the tangent bundle at an S-integral point at infinity. As before, $U = U(\overline{Y}, b)$ denotes the $\mathbb{Q}_p$-prounipotent étale fundamental group, and U_n denotes the nth quotient of its lower central series. For any other

S-integral point $y \in \mathcal{Y}(\mathbb{Z}_S)$, we have a principal U_n-bundle $P_n(y) \coloneqq P_n(\overline{Y}; b, y)$ with continuous $G_{\mathbb{Q}}$-action. This defines the non-abelian Kummer map

$$j_S \colon \mathcal{Y}(\mathbb{Z}_S) \to H^1(G_{\mathbb{Q}}, U_n),$$

given by $y \mapsto [P_n(y)]$. The S-integrality of y ensures that we land in a subset defined by local conditions which we now describe.

For any prime ℓ, we have a commutative diagram of the global and local non-abelian Kummer maps:

$$\begin{array}{ccc} \mathcal{Y}(\mathbb{Z}_S) & \hookrightarrow & Y(\mathbb{Q}_\ell) \\ \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle j_\ell} \\ H^1(G_{\mathbb{Q}}, U_n) & \xrightarrow{\mathrm{loc}_\ell} & H^1(G_\ell, U_n). \end{array}$$

Here, $Y(\mathbb{Q}_\ell)$ can be replaced with $\mathcal{Y}(\mathbb{Z}_\ell)$ for $\ell \notin S$. As in the projective case, the local cohomology set $H^1(G_\ell, U_n)$ is the set of $\mathbb{Q}_p$-points of an affine $\mathbb{Q}_p$-scheme of finite type.

Definition 10.4 (Betts–Dogra)**.** A cohomology class $\xi \in H^1(G_{\mathbb{Q}}, U_n)$ is *locally geometric* (with respect to $\mathcal{Y}/\mathbb{Z}_S$) if for all primes ℓ (including p), the localisation $\mathrm{loc}_\ell(\xi)$ is contained in

$$\begin{cases} j_\ell(\mathcal{Y}(\mathbb{Z}_\ell))^{\mathrm{Zar}}, & \text{if } \ell \notin S, \\ j_\ell(Y(\mathbb{Q}_\ell))^{\mathrm{Zar}}, & \text{if } \ell \in S, \end{cases}$$

where $(-)^{\mathrm{Zar}}$ denotes Zariski closure inside $H^1(G_\ell, U_n)$. The *refined Selmer scheme* $\mathrm{Sel}^{\mathrm{min}}_{S,U_n}(\mathcal{Y})$ represents the subfunctor of $R \mapsto H^1(G_{\mathbb{Q}}, U_n(R))$ given by locally geometric cohomology classes.

The refined Selmer scheme is an affine $\mathbb{Q}_p$-scheme of finite type. The compatibility of local and global Kummer maps ensures that j_S maps S-integral points into $\mathrm{Sel}^{\mathrm{min}}_{S,U_n}(\mathcal{Y})$.

The local Kummer map j_ℓ can be described quite explicitly in many cases.

- If $\ell \notin S \cup \{p\}$, then $j_\ell(\mathcal{Y}(\mathbb{Z}_\ell))$ is finite [**KT08**]. If moreover ℓ is of good reduction for $\mathcal{Y}$, then $j_\ell(\mathcal{Y}(\mathbb{Z}_\ell)) \subseteq \{*\}$ contains at most the trivial point. (If the base point b is tangential, it can happen that $\mathcal{Y}$ does not admit any $\mathbb{Z}_\ell$-integral points, in which case $j_\ell(\mathcal{Y}(\mathbb{Z}_\ell))$ is empty.)
- For $\ell \in S$, the dimension of $j_\ell(Y(\mathbb{Q}_\ell))^{\mathrm{Zar}}$ is at most 1. The point $j_\ell(y)$ depends only on the image of y on the stable reduction graph of Y [**BD19**].
- If $\ell = p$, then the assumption that $p \notin S$ is a prime of good reduction implies that $j_\ell(\mathcal{Y}(\mathbb{Z}_p))^{\mathrm{Zar}}$, if not empty, equals $H^1_f(G_p, U_n)$, the subscheme of crystalline cohomology classes [**Kim09**].

The fundamental diagram for the refined Selmer scheme looks as follows:

$$\begin{array}{ccccc} \mathcal{Y}(\mathbb{Z}_S) & \hookrightarrow & \mathcal{Y}(\mathbb{Z}_p) & & \\ \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle j_p} & \searrow^{j^{\mathrm{DR}}} & \\ \mathrm{Sel}^{\mathrm{min}}_{S,U_n}(\mathcal{Y}) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_n) & \xrightarrow[\cong]{\mathsf{D}} & U^{\mathrm{DR}}/F^0. \end{array}$$

As in the projective case we conjecture:

Conjecture (A'). *The image of* loc_p *is non-dense for* $n \gg 0$.

If loc_p is non-dense for some n, then we obtain an algebraic function $\alpha \neq 0$ on U^{DR}/F^0 vanishing on $\mathsf{D}(\mathrm{loc}_p(\mathrm{Sel}^{\mathrm{min}}_{S,U_n}(\mathcal{Y})))$. Its pullback to $\mathcal{Y}(\mathbb{Z}_p)$ along j^{DR} is then given by a non-zero convergent power series on each tube $]y[\subseteq \mathcal{Y}(\mathbb{Z}_p)$ for $y \in \mathcal{Y}(\mathbb{F}_p)$, and its finite vanishing locus contains $\mathcal{Y}(\mathbb{Z}_S)$.

Definition 10.5. For $n \geq 1$, define

$$\mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,n} \coloneqq \bigcap_{\alpha \circ \mathsf{D} \circ \mathrm{loc}_p = 0} Z(\alpha \circ j^{\mathrm{DR}}).$$

For increasing n, the vanishing loci $\mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,n}$ form a decreasing sequence of subsets of $\mathcal{Y}(\mathbb{Z}_p)$:

$$\mathcal{Y}(\mathbb{Z}_p) \supset \mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,1} \supset \mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,2} \supset \mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,3} \supset \dots,$$

all of which contain the set of S-integral points $\mathcal{Y}(\mathbb{Z}_S)$. The finiteness of $\mathcal{Y}(\mathbb{Z}_S)$ would thus be implied by Conjecture (A'). We conjecture moreover that for sufficiently large n, the refined nonabelian Chabauty method yields precisely the set of $\mathbb{Z}_S$-integral points:

Conjecture (B').

$$\bigcap_{n=1}^{\infty} \mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,n} = \mathcal{Y}(\mathbb{Z}_S).$$

The refined nonabelian Chabauty method can be made effective in some cases. The best-studied example is $\mathcal{Y} = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. For the thrice-punctured line, Conjecture (A') was shown in [**Kim05**], even without the local geometricity condition at primes contained in S. Explicit equations for the loci $\mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,n}$ have been obtained in a number of cases. The case $2 \notin S$ is somewhat trivial since $\mathcal{Y}(\mathbb{F}_2) = \mathbb{P}^1(\mathbb{F}_2) \setminus \{0, 1, \infty\} = \emptyset$, so that the local geometricity condition at 2 is unsatisfiable and all $\mathcal{Y}(\mathbb{Z}_p)^{\mathrm{min}}_{S,n}$ are empty, thus correctly detecting the emptiness of $\mathcal{Y}(\mathbb{Z}_S)$. In nontrivial cases, the obtained equations are given in terms of the p-adic polylogarithm $\ell_k(z)$, which is given near zero by

$$\ell_k(z) = \sum_{n=1}^{\infty} \frac{z^k}{n^k}.$$

The following results were obtained by a project group at the Arizona Winter School 2020 [**BBK+21**]:

- $S = \{2\}$. Here we have
$$\mathcal{Y}(\mathbb{Z}[1/2]) \subseteq S_3.\big(\{\log(z) = 0\} \cap \{\ell_2(z) = 0\}\big),$$
where $S_3.(-)$ denotes the closure under the two operations $z \mapsto 1/z$ and $z \mapsto 1 - z$. Conjecture (B') has been verified numerically for primes $p < 10^5$. This is a refinement of results of Dan-Cohen–Wewers [**DCW15**].
- $S = \{2, q\}$ for odd primes q. Here we have
$$\mathcal{Y}(\mathbb{Z}[1/2q]) \subseteq S_3.\big\{a_{2,q}\,\ell_2(z) = a_{q,2}\,\ell_2(1 - z)\big\},$$
for certain p-adic constants $a_{2,q}, a_{q,2} \in \mathbb{Q}_p$ which are related by the identity $a_{2,q} + a_{q,2} = \log(2)\log(q)$. There is an algorithm for expressing these constants as $\mathbb{Q}$-linear combinations of p-adic polylogarithms, which is implemented in SAGE [**KLS21**]. Conjecture (B') is proved for $p = 3$ if $q > 3$

is a Mersenne or Fermat prime or (by numerical verification) if q is one of the following primes:

$$19,\ 37,\ 53,\ 107,\ 109,\ 163,\ 181,\ 199,\ 269,\ 271,\ 379,$$
$$431,\ 433,\ 487,\ 523,\ 541,\ 577,\ 593,\ 631,\ 701,\ 739,$$
$$757,\ 809,\ 811,\ 829,\ 863,\ 883,\ 919,\ 937,\ 971,\ 991.$$

Moreover, upcoming work of Betts–Kumpitsch–Lüdtke, refining calculations of Corwin–Dan-Cohen [**CDC20**], shows that for $S = \{2\}$ we have

$$\mathcal{Y}(\mathbb{Z}[1/2]) \subseteq S_3.\big(\{\log(z) = 0\} \cap \bigcap_{k\geq 2 \text{ even}} \{\ell_k(z) = 0\}\big).$$

Conjecture (B') is proved to hold for all odd primes p by showing that we have $\mathcal{Y}(\mathbb{Z}_p)^{\min}_{\{2\},n} = \mathcal{Y}(\mathbb{Z}[1/2])$ whenever $n \geq p-3$.

*

It is hoped that the patient reader will have attained by now some overall sense of Selmer schemes and their applications. The remaining lectures cover a collection of complementary topics on Diophantine applications of non-abelian fundamental groups. The exposition will be brief and even more superficial than the previous sections.

11. Effectivity and the section conjecture

Reference: [**Kim12a**].

We return to the setting where $X/\mathbb{Q}$ is a smooth proper curve of genus ≥ 2 and $U = U(\bar{X}, b)$ is its $\mathbb{Q}_p$-prounipotent étale fundamental group. Assume the following:

(1) The map
$$H^1_f(G_T, U_n) \longrightarrow U_n^{\mathrm{DR}}/F^0$$
can be effectively computed.

(2) Using (1), we can compute an effective lower bound for the p-adic distances between the points in $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$.

Thus, we get an effective M such that $X(\mathbb{Q}) \to X(\mathbb{Z}/p^M)$ is injective. Using this, we get an effective N, for example $N = |J(\mathbb{Z}/p^M)|$, where J is the Jacobian of X, such that
$$X(\mathbb{Q}) \subset J(\mathbb{Q}) \subset J(\mathbb{Z})/NJ(\mathbb{Z}) \hookrightarrow H^1(G_S, J[N])$$
is injective, where S is the set of all places of bad reduction and the primes dividing pN.

(3) Grothendieck's section conjecture [**Gro97**]:
$$X(\mathbb{Q}) \cong H^1(G_{\mathbb{Q}}, \hat{\pi}_1(\bar{X}, b)).$$

Note that for elliptic curves, one conjectures
$$E(\mathbb{Q}) \otimes \mathbb{Z}_p \cong H^1_f(G_{\mathbb{Q}}, \hat{\pi}_1(\bar{E}, b)^{(p)}).$$

Let n be larger than N and all the primes in S. We use the following notation:

- $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $G_n = \hat{\pi}_1(\mathrm{Spec}(\mathbb{Z}[1/n!]))$

- $\Delta = \hat{\pi}_1(\bar{X}, b)$, and K_n is the intersection of all open subgroups of index $\leq n$. (There are only finitely many, and K_n is normal.)
- $\Delta(n) = \Delta/K_n$. Thus, the prime divisors of the order of any element in $\Delta(n)$ are $\leq n$.
- Denote by $\pi(n)$ the quotient of $\hat{\pi}_1(X, b)$ by K_n, so that we have a pushout diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta & \longrightarrow & \hat{\pi}_1(X,b) & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \| & & \\ 0 & \longrightarrow & \Delta(n) & \longrightarrow & \pi(n) & \longrightarrow & G & \longrightarrow & 0. \end{array}$$

There is a pullback diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta(n) & \longrightarrow & \pi(n) & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Delta(n) & \longrightarrow & \hat{\pi}_1(\mathfrak{X}_n, b)/K_n & \longrightarrow & G_n & \longrightarrow & 0 \end{array}$$

where $\mathfrak{X}_n$ is a smooth projective model for X over $\mathrm{Spec}(\mathbb{Z}[1/n!])$. Hence, any point $x \in X(\mathbb{Q})$ defines a class in $H^1(G_n, \Delta(n))$.

We have a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & H^1(G, \Delta) \\ \downarrow & & \downarrow \\ H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G, \Delta(n)) \end{array}$$

and hence and sequence of subsets

$$H^1(G, \Delta)_n$$

consisting of classes whose images in $H^1(G, \Delta(n))$ come from $H^1(G_n, \Delta(n))$. Thus, we have diagrams

$$\begin{array}{ccc} H^1(G, \Delta)_n & \hookrightarrow & H^1(G, \Delta) \\ \downarrow & & \downarrow \\ H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G, \Delta(n)) \\ \downarrow & & \\ H^1(G_S, J[N]) & \hookrightarrow & H^1(G_n, J[N]) \end{array}$$

and

$$\begin{array}{ccccc} & & & & H^1(G_{n+1}, \Delta(n+1)) \\ & & & & \downarrow \\ & & H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G_{n+1}, \Delta(n)) \\ & & \downarrow & & \downarrow \\ H^1(G_S, J[N]) & \hookrightarrow & H^1(G_n, J[N]) & \hookrightarrow & H^1(G_{n+1}, J[N]). \end{array}$$

Using this, we can define a decreasing sequence of subsets

$$H^1(G_S, J[N])_{n+1} \subset H^1(G_S, J[N])_n$$

consisting of those classes whose images in $H^1(G_i, J[N])$ lift to $H^1(G_i, \Delta(i))$ for all $i \leq n$, i larger than $n_0 = \sup(N, p \in S)$.

Meanwhile, there is an increasing sequence of subsets $X(\mathbb{Q})_n$ of points whose heights are $\leq n$, all of which occur in the "non-abelian descent sequence":

$$\begin{aligned} \ldots \subset X(\mathbb{Q})_n \subset & X(\mathbb{Q})_{n+1} \subset X(\mathbb{Q})_{n+2} \subset \ldots \\ \ldots \subset H^1(G_S, J[N])_{n+2} \subset & H^1(G_S, J[N])_{n+1} \subset H^1(G_S, J[N])_n \subset \ldots \end{aligned}$$

Using the section conjecture, we have

$$X(\mathbb{Q})_n = H^1(G_S, J[N])_n$$

for n sufficiently large, and $X(\mathbb{Q})_n = X(\mathbb{Q})$ at that point.

To check this, note that the section conjecture implies that the inclusions

$$X(\mathbb{Q}) \subset H^1(G, \Delta)_n \subset H^1(G, \Delta)$$

are all equalities. From the diagrams

$$\begin{array}{ccc} H^1(G, \Delta)_n & = & H^1(G, \Delta) \\ \downarrow & & \downarrow \\ H^1(G_n, \Delta(n)) & \hookrightarrow & H^1(G, \Delta(n)) \end{array}$$

we have maps

$$H^1(G, \Delta) \longrightarrow H^1(G_n, \Delta(n))$$

and

$$H^1(G, \Delta) = \varprojlim H^1(G, \Delta(n)) = \varprojlim H^1(G_n, \Delta(n)).$$

Suppose

$$c \in H^1(G_S, J[N])_n$$

for all n. Then the set $H^1(G_n, \Delta(n))_c$ of classes that lift c is non-empty for all n, and hence

$$X(\mathbb{Q})_c = H^1(G, \Delta)_c = \varprojlim H^1(G_n, \Delta(n))_c$$

is non-empty. This shows that

$$\bigcap_n H^1(G_S, J[N])_n = X(\mathbb{Q}).$$

Since all sets are finite, we must have

$$X(\mathbb{Q}) = H^1(G_S, J[N])_n$$

for some n.

12. Remark on non-abelian reciprocity

Reference: [**Kim16**]

Our discussion started with curves of genus zero and the Hasse principle. Of course this is not a strategy that works for any but the most simple varieties. However, one might try to refine the Hasse principle. That is, given a variety X over a number field F, we might try to describe the inclusion

$$X(F) \subset X(\mathbb{A}_F).$$

For $\mathbb{G}_m$, this is partially achieved by the reciprocity map

$$\mathbb{G}_m(F) \hookrightarrow \mathbb{G}_m(\mathbb{A}_F) \xrightarrow{\text{rec}} \text{Gal}(\bar{F}/F)^{\text{ab}}$$

and Artin's reciprocity law

$$\mathbb{G}_m(F) \subset \text{rec}^{-1}(0),$$

interpreted thereby as a result of Diophantine geometry. That is, it states that the global points of $\mathbb{G}_m$ are cut out by an equation inside the adelic points, albeit with values in a group.

For an affine conic

$$C\colon ax^2 + by^2 = c$$

described by a class $\chi \in H^1(\text{Gal}(\bar{F}/F), \pm 1)$, one can replace this by

$$C(F) \hookrightarrow C(\mathbb{A}_F) \longrightarrow \text{Hom}(H^1(\text{Gal}(\bar{F}/F), \mathbb{Q}/\mathbb{Z}(\chi)), \mathbb{Q}/\mathbb{Z}).$$

It turns out that there is a *non-abelian class field theory* with coefficients in a fairly general variety X over a number field F generalising CFT with coefficients in $\mathbb{G}_m$ and giving a partial answer to the problem of refining the Hasse principle. This consists (with some simplifications) of a filtration

$$X(\mathbb{A}_F) = X(\mathbb{A}_F)_1 \supset X(\mathbb{A}_F)_2 \supset X(\mathbb{A}_F)_3 \supset \dots$$

and a sequence of maps

$$\text{rec}_n\colon X(\mathbb{A}_F)_n \longrightarrow \mathfrak{G}_n(X)$$

to a sequence of groups $\mathfrak{G}_n(X)$ such that

$$X(\mathbb{A}_F)_{n+1} = \text{rec}_n^{-1}(0).$$

Thus, the sets form a diagram as follows:

$$\begin{array}{ccccccccc}
\dots & \subset & \text{rec}_3^{-1}(0) & \subset & \text{rec}_2^{-1}(0) & \subset & \text{rec}_1^{-1}(0) & \subset & X(\mathbb{A}_F) \\
 & & \| & & \| & & \| & & \| \\
\dots & \subset & X(\mathbb{A}_F)_4 & \subset & X(\mathbb{A}_F)_3 & \subset & X(\mathbb{A}_F)_2 & \subset & X(\mathbb{A}_F)_1 \\
 & & \downarrow{\scriptstyle \text{rec}_4} & & \downarrow{\scriptstyle \text{rec}_3} & & \downarrow{\scriptstyle \text{rec}_2} & & \downarrow{\scriptstyle \text{rec}_1} \\
\dots & & \mathfrak{G}_4(X) & & \mathfrak{G}_3(X) & & \mathfrak{G}_2(X) & & \mathfrak{G}_1(X).
\end{array}$$

Put

$$X(\mathbb{A}_F)_\infty \coloneqq \bigcap_{n=1}^{\infty} X(\mathbb{A}_F)_n.$$

Theorem 12.1 (Non-abelian reciprocity).

$$X(F) \subset X(\mathbb{A}_F)_\infty.$$

When $F = \mathbb{Q}$, for a fixed p, we can define

$$X(\mathbb{Q}_p)_n \coloneqq \mathrm{pr}_p(X(\mathbb{A}_{\mathbb{Q}})_n) \subset X(\mathbb{Q}_p).$$

Conjecture 12.2. *Suppose X is a smooth projective curve of genus ≥ 2. Then*

$$X(\mathbb{Q}) = X(\mathbb{Q}_p)_\infty = \bigcap_{n=1}^{\infty} X(\mathbb{Q}_p)_n.$$

It remains to be seen if the reciprocity maps can be made computable so as to be applicable to the resolution of Diophantine problems.

13. Diophantine principal bundles: a little history

We interject a few remarks on the history of non-abelian constructions in Diophantine geometry, which seem still not to be very well-known.

For a smooth projective curve $X/\mathbb{Q}$ of genus $g \geq 1$, Weil **[Wei29]** constructed in 1929 an embedding

$$j\colon X \hookrightarrow J_X,$$

where J_X is an abelian variety of dimension g. That is, within the framework of analytic geometry,

$$J_X(\mathbb{C}) = \mathbb{C}^g/\Lambda = H^0(X(\mathbb{C}), \Omega^1_{X(\mathbb{C})})^*/H_1(X, \mathbb{Z}).$$

and map j is defined over $\mathbb{C}$ by fixing a basepoint b setting

$$j(x)(\alpha) = \int_b^x \alpha \bmod H_1(X, \mathbb{Z})$$

for $\alpha \in H^0(X(\mathbb{C}), \Omega^1_{X(\mathbb{C})})$. The Hodge-theoretic description in some form certainly goes back to the 19th century and the work of Abel and Jacobi. But Weil's point was that J_X is also a projective algebraic variety defined over $\mathbb{Q}$, and if $b \in X(\mathbb{Q})$, then the map j is also defined over $\mathbb{Q}$. The reason is that J_X is a moduli space of line bundles of degree 0 on X and

$$j(x) = \mathcal{O}(x) \otimes \mathcal{O}(-b).$$

The main application is that we get an embedding of rational points

$$j\colon X(\mathbb{Q}) \hookrightarrow J_X(\mathbb{Q}).$$

Weil also proved that $J_X(\mathbb{Q})$ is a finitely generated abelian group, and hoped, without success, that this could be somehow used to study $X(\mathbb{Q})$.

In the 1938 paper "Généralisation des fonctions abéliennes", Weil **[Wei38]** studied

$$\mathrm{Bun}_X(\mathrm{GL}_n) = \mathrm{GL}_n(K(X))\backslash \mathrm{GL}_n(\mathbb{A}_{K(X)})/\prod_x \mathrm{GL}_n(\widehat{\mathcal{O}}_x)$$

as a "non-abelian Jacobian". He proved a number of foundational theorems, including the fact that vector bundles of degree zero admit flat connections, beginning non-abelian Hodge theory. His paper was very influential in geometry, leading to the celebrated paper of Narasimhan and Seshadri **[NS65]** that proved the isomorphism

$$\mathrm{Bun}_X(\mathrm{GL}_n)_0^{\mathrm{st}} \simeq H^1(X, U(n))^{\mathrm{irr}}$$

between moduli spaces of stable bundles and unitary representations of the fundamental group. This was extended by Donaldson [**Don83**], influencing his groundbreaking work on four-manifolds and gauge theory, and by Simpson [**Sim92**] to

$$\mathrm{Higgs}_X(\mathrm{GL}_n) \simeq H^1(X, \mathrm{GL}_n).$$

However, as pointed out by Serre in an obituary for Weil, the paper was

> "*a text presented as analysis, whose significance is essentially algebraic, but whose motivation is arithmetic*"

To this day, there have been no direct applications of algebro-geometric moduli spaces of non-abelian bundles to Diophantine geometry.

Much of the work described in this paper makes progress by examining the original analytic Hodge theory of the Jacobian and reinterpreting the maps in terms of mixed Hodge structures.

$$X(\mathbb{C}) \longrightarrow J_X(\mathbb{C}) \simeq \mathrm{Ext}^1_{\mathrm{MHS},\mathbb{Z}}(\mathbb{Z}, H_1(X(\mathbb{C}), \mathbb{Z})).$$

This naturally suggests an arithmetic realisation:

$$X(\mathbb{Q}) \longrightarrow J_X(\mathbb{Q}) \otimes \mathbb{Z}_p \simeq \mathrm{Ext}^1_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),f}(\mathbb{Z}_p, H_1^{\text{ét}}(\bar{X}, \mathbb{Z}_p)),$$

where the map is well-defined via Kummer theory but the isomorphism is conjectural. Critically, we have the interpretation

$$H_1 = \pi_1^{\mathrm{ab}},$$

suggesting the possibility of extending the construction to non-abelian homotopy and moduli spaces of non-abelian structures. This is what was carried out in the following settings:

- over $\mathbb{C}$: Hain's higher Albanese varieties [**Hai87b**];
- over $\mathbb{Q}_p$: p-adic period spaces;
- over global fields: Selmer schemes and variants.

14. Why Diophantine geometry?

Finitely-generated rings of the form

$$R \simeq \mathbb{Z}[x_1, x_2, \ldots, x_n]/I,$$

which could be, e.g,

$$R = \mathbb{Z}[\pi, 1/\pi, e, 1/691, \zeta(3)],$$

should be thought of as number systems with *intrinsic discreteness*. Scheme theory provides the conceptual tools to view them as rings of functions on a space. Do such spaces occur in nature? This is a difficult question, but they appear to be fundamental building blocks in a way similar to (but harder than) the simplices or cells of algebraic or combinatorial topology. However, note that the approach is dual to topology, in that it is the functions that have an underlying discrete skeleton. Functions represent measurement, you might say, which are then proposed to be discrete at some fundamental level.

Once arithmetic schemes become a subject of study, it is unavoidable to study maps between them and hence, Diophantine geometry. It is interesting that discrete approximations to spaces become a natural consequence. Any compact manifold M,

for example, has an underlying arithmetic scheme. This is because the Nash–Tognoli theorem [**Nas52, Tog76**] allows us to realise it as a real algebraic set, which then is just

$$M = X(\mathbb{R})$$

for an arithmetic scheme X. (Of course there is a choice of X involved.) Whenever we write $\mathbb{R} = \varinjlim R_i$ as a limit of absolutely finitely-generated rings

$$\cdots \subset R_{i-1} \subset R_i \subset R_{i+1} \subset \cdots \subset \mathbb{R},$$

we get the sequence of inclusions

$$\cdots \subset X(R_{i-1}) \subset X(R_i) \subset X(R_{i+1}) \subset \cdots \subset X(\mathbb{R}) = M.$$

Because Diophantine geometry is still in such a primitive state of development, the situations where one understands the $X(R_i)$ are extremely rare. This is one reason it's hard to judge at present if a filtration like this might be useful.

References

[AIK15] Fabrizio Andreatta, Adrian Iovita, and Minhyong Kim, *A p-adic nonabelian criterion for good reduction of curves*, Duke Mathematical Journal **164** (2015), no. 13, 2597 – 2642.

[BBJ19] Christopher Brav, Vittoria Bussi, and Dominic Joyce, *A Darboux theorem for derived schemes with shifted symplectic structure*, J. Am. Math. Soc. **32** (2019), no. 2, 399–443.

[BBK+21] Alex J. Best, L. Alexander Betts, Theresa Kumpitsch, Martin Lüdtke, Angus W. McAndrew, Lie Qian, Elie Studnia, and Yujie Xu, *Refined Selmer equations for the thrice-punctured line in depth two*, 2021.

[BD19] L. Alexander Betts and Netan Dogra, *The local theory of unipotent Kummer maps and refined Selmer schemes*, 2019.

[BDCKW18] Jennifer S. Balakrishnan, Ishai Dan-Cohen, Minhyong Kim, and Stefan Wewers, *A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves*, Math. Ann. **372** (2018), no. 1-2, 369–428. MR 3856816

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty–Kim for the split Cartan modular curve of level 13*, Ann. Math. (2) **189** (2019), no. 3, 885–944.

[Bes02] Amnon Besser, *Coleman integration using the Tannakian formalism*, Math. Ann. **322** (2002), no. 1, 19–48. MR 1883387

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier **63** (2013), no. 3, 957–984.

[CDC20] David Corwin and Ishai Dan-Cohen, *The polylog quotient and the Goncharov quotient in computational Chabauty-Kim theory I*, International Journal of Number Theory **16** (2020), 1859–1905.

[CK10] John Coates and Minhyong Kim, *Selmer varieties for curves with CM Jacobians*, Kyoto Journal of Mathematics **50** (2010), no. 4, 827 – 852.

[CS06] J. Coates and R. Sujatha, *Cyclotomic fields and zeta values*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006. MR 2256969

[DCW15] Ishai Dan-Cohen and Stefan Wewers, *Explicit Chabauty–Kim theory for the thrice punctured line in depth 2*, Proceedings of the London Mathematical Society **110** (2015), no. 1, 133–171.

[DCW16] ———, *Mixed Tate motives and the unit equation*, International Mathematics Research Notices. IMRN (2016), no. 17, 5291–5354. MR 3556439

[Del89] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 79–297. MR 1012168

[Dog20] Netan Dogra, *Unlikely intersections and the Chabauty–Kim method over number fields*, 2020.

[Don83] S. K. Donaldson, *An application of gauge theory to four-dimensional topology*, J. Differential Geom. **18** (1983), no. 2, 279–315. MR 710056

[Fal07] Gerd Faltings, *Mathematics around Kim's new proof of Siegel's theorem*, Diophantine geometry, CRM Series, vol. 4, Ed. Norm., Pisa, 2007, pp. 173–188. MR 2349654

[Fal12] ———, *The motivic logarithm for curves*, The arithmetic of fundamental groups—PIA 2010, Contrib. Math. Comput. Sci., vol. 2, Springer, Heidelberg, 2012, pp. 107–125. MR 3220516

[Gro97] Alexander Grothendieck, *Brief an G. Faltings*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, With an English translation on pp. 285–293, pp. 49–58. MR 1483108

[Had11] Majid Hadian, *Motivic fundamental groups and integral points*, Duke Math. J. **160** (2011), no. 3, 503–565. MR 2852368

[Hai87a] Richard M. Hain, *The de Rham homotopy theory of complex algebraic varieties. II*, K-Theory **1** (1987), no. 5, 481–497. MR 934453

[Hai87b] ———, *Higher Albanese manifolds*, Hodge theory (Sant Cugat, 1985), Lecture Notes in Math., vol. 1246, Springer, Berlin, 1987, pp. 84–91. MR 894044

[Kim05] Minhyong Kim, *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656. MR 2181717

[Kim09] ———, *The unipotent Albanese map and Selmer varieties for curves*, Kyoto University. Research Institute for Mathematical Sciences. Publications **45** (2009), no. 1, 89–133. MR 2512779

[Kim12a] ———, *Remark on fundamental groups and effective Diophantine methods for hyperbolic curves*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 355–368. MR 2867924

[Kim12b] ———, *Tangential localization for Selmer varieties*, Duke Math. J. **161** (2012), no. 2, 173–199. MR 2876929

[Kim16] ———, *Diophantine geometry and non-abelian reciprocity laws I*, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, 2016, pp. 311–334. MR 3629655

[Kim18] ———, *Arithmetic gauge theory: A brief introduction*, Modern Phys. Lett. A **33** (2018), 1859–1905.

[KLS21] Theresa Kumpitsch, Martin Lüdtke, and Elie Studnia, *`dcw_coefficients`: SAGE code for computing Dan-Cohen–Wewers coefficients*, 2021.

[KT08] Minhyong Kim and Akio Tamagawa, *The l-component of the unipotent Albanese map*, Math. Ann. **340** (2008), no. 1, 223–235. MR 2349775

[Nas52] John Nash, *Real algebraic manifolds*, Ann. of Math. (2) **56** (1952), 405–421.

[NS65] M. S. Narasimhan and C. S. Seshadri, *Stable and unitary vector bundles on a compact Riemann surface*, Ann. Math. (2) **82** (1965), 540–567 (English).

[Sch97] Pierre (ed.) Schneps, Leila; Lochak, *Geometric galois actions 1*, London Mathematical Society Lecture Notes, vol. 242, Cambridge University Press, Cambridge, 1997.

[Ser78] Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer Verlag, 1978.

[Sim92] Carlos T. Simpson, *Higgs bundles and local systems*, Inst. Hautes Études Sci. Publ. Math. (1992), no. 75, 5–95. MR 1179076

[Sza09] Tamás Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge, 2009. MR 2548205

[Tog76] Alberto Tognoli, *Su una congettura di Nash*, Annali delia Scuola Normale Superiore di Pisa **27** (1976), no. 1, 167–185.

[Vol03] Vadim Vologodsky, *Hodge structure on the fundamental group and its application to p-adic integration*, Mosc. Math. J. **3** (2003), no. 1, 205–247, 260. MR 1996809

[Wei29] André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315. MR 1555278

[Wei38] André Weil, *Généralisation des fonctions abéliennes*, J. Math. Pures Appl. (9) **17** (1938), 47–87 (French).

[Woj93] Zdzisław Wojtkowiak, *Cosimplicial objects in algebraic geometry*, Algebraic K-theory and algebraic topology (Lake Louise, AB, 1991), NATO Adv. Sci. Inst. Ser.

C: Math. Phys. Sci., vol. 407, Kluwer Acad. Publ., Dordrecht, 1993, pp. 287–327. MR 1367304