Cent. Eur. J. Math. • 8(4) • 2010 • 633-645
DOI: 10.2478/s11533-010-0047-y

VERSITA

Central European Journal of **Mathematics**

Fundamental groups and Diophantine geometry

Review Article

Minhyong Kim[1*]

1 *University College London, London, UK*

Received 23 March 2010; accepted 16 June 2010

Abstract: This is a brief exposition on the uses of non-commutative fundamental groups in the study of Diophantine problems.

MSC: 14G25

Keywords: Fundamental group • Diophantine geometry

Colloquium lecture, Leeds, January 2008

To work our way towards the very canonical but rather difficult relationship between the notions appearing in the title, it is appropriate to review briefly the classical problems that make up the background of our study, and whose importance will be initially regarded as self-evident. Thus, we are given a polynomial

$$f(x_1, x_2, \ldots, x_n)$$

whose coefficients will be assumed to be in $\mathbb{Z}$ for the sake of simplicity. The set of solutions to the equation

$$f(\underline{x}) = 0$$

can be considered in any number of different environments such as

$$\mathbb{Z},\ \mathbb{Z}[1/62],\ \mathbb{Q},\ \mathbb{Z}[i],\ \mathbb{Q}[i], \ldots,\ \mathbb{Q}[i, \pi], \ldots,\ \mathbb{R},\ \mathbb{C},\ \mathbb{Q}_p,\ \mathbb{C}_p, \ldots$$

* *E-mail: minhyong.kim@ucl.ac.uk*

In recent decades, the designation of the equation as Diophantine has not been a reference to any particular property of the equation itself, but rather calls attention to our primary focus on contexts closer to the beginning of the list, although how far we might extend the scope is better left undetermined. In any case, there are famous results corresponding to different lines of demarcation, such as the one that says

$$x^n + y^n = z^n$$

has only the obvious solutions in $\mathbb{Z}$ as long as $n \geq 3$, or where

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

for a generic f of degree at least 4 has only finitely many solutions in $\mathbb{Q}(i, \pi, e)$.

Elementary *coordinate geometry* can be brought to bear on some such questions as a potent tool for describing solution sets, or least for generating solutions. A simple but already interesting case is a quadratic equation in two variables, say

$$x^2 + y^2 = 1.$$

By visualizing the real solution set as a circle, we might come upon the idea of considering the intersections with lines that pass through the specific point $(-1, 0)$, where the set-up has already encouraged us casually to refer to a solution using geometric terminology. The lines are described using equations $y = m(x + 1)$ for various m whereby algebraic substitution leads to the constraint

$$x^2 + (m(x + 1))^2 = 1$$

or

$$(1 + m^2)x^2 + 2m^2x + m^2 - 1 = 0.$$

A deeper connection to algebra comes from the observation that one solution $x = -1$ is already rational, so that whenever the slope m is rational, the other solution is also bound to be rational. As we vary m, we can generate thereby *all* the other rational solutions to the equation, for example, $(-99/101, 20/101)$ corresponding to $m = 10$. It seems that the visually compelling nature of the solution set in a sufficiently big field provides valuable insight into finding solutions in much smaller fields. Incidentally, I am sure you are aware also that this procedure leads to the famous *Pythagorean triples* involved in equations like

$$99^2 + 20^2 = 101^2.$$

The elementary elegance of the method described becomes progressively harder to retain with the increasing complexity of the problem, measured, for example, by the degree of the equation. Nevertheless, it is instructive to consider one example of degree 3:

$$x^3 + y^3 = 1729.$$

One verifies with the help of Ramanujan that $(9, 10)$ is a solution, so the case of the circle might motivate us to consider lines through it. Unfortunately, the previous argument for the rationality of intersection points fails as the associated constraint becomes cubic. But if we want to start out generating just *one* other solution, a more subtle idea is to consider the tangent line to the real curve at the point $(9, 10)$, because then, the corresponding cubic equation will have 9 as a *double* root. To spell this out, calculate the equation of the tangent line,

$$81(x - 9) + 100(y - 10) = 0$$

or

$$y = (-81/100)x + 1729/100,$$

and substitute to obtain the equation

$$x^3 + ((-81/100)x + 1729/100)^3 = 1729.$$

We have arranged for $x = 9$ to be a double root, and hence, the remaining root is forced to be rational. Even by hand, you can (tediously) work out the resulting rational point to be

$$(-24561/271, 24580/271).$$

Repeating the procedure with the points that are successively obtained thus actually provides us with infinitely many rational solutions. Here, you must pause to consider the possibility that repetition will just move us (quasi-)periodically around finitely many points, but there is a well-known theorem of Nagell and Lutz that tells us this cannot happen given the denominator of the solution at hand.

Geometric techniques of the same general flavor can be made considerably more sophisticated, with nice applications to varieties of simple type as might be defined by equations of low degree in a greater number of variables. But in the present lecture we wish to explain the important conceptual shift that occurred in the 1960's, whereby Diophantine problems acquired an *intrinsically* geometric nature by way of two foundational ideas of Grothendieck.

The first one, elementary in comparison to the second, associates to the polynomial $f(\underline{x})$ the ring

$$A := \mathbb{Z}[\underline{x}]/(f(\underline{x})).$$

This leads to a natural correspondence between solutions $(b_1, \ldots, b_n)$ of $f(\underline{x}) = 0$ in a ring B, and ring homomorphisms

$$A \to B$$

That is, an *arbitrary* n-tuple $\underline{b} = (b_1, \ldots, b_n)$ determines a ring homomorphism $\mathbb{Z}[\underline{x}] \to B$ that sends x_i to b_i, which factors through the quotient ring A exactly when $\underline{b}$ is a zero of $f(\underline{x})$. The spatial intuition is supposed to arise from the idea that a commutative ring R with 1 can be viewed as the ring of functions on a space, its *spectrum*

$$\mathrm{Spec}(R),$$

whose underlying set consists of the prime ideals of R. This correspondence reverses arrows reflecting the intuition that a map of spaces should pull functions backwards by composition. Thus, the solutions in B of $f(\underline{x}) = 0$ come into bijection with the set of maps

$$\mathrm{Spec}(B) \to X := \mathrm{Spec}(A),$$

conventionally denoted by

$$X(B).$$

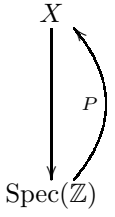
Even before considering such difficult maps, it is pleasant to note that an obvious map

$$\begin{array}{c} X \\ \downarrow \\ \mathrm{Spec}(\mathbb{Z}) \end{array}$$

corresponds to the inclusion

$$\mathbb{Z} \to A = \mathbb{Z}[\underline{x}]/(f(\underline{x}))$$

using which we think of X as a fibration over $\mathrm{Spec}(\mathbb{Z})$. Then the solutions in $\mathbb{Z}$, the elements of $X(\mathbb{Z})$, are precisely the *sections*



of the fibration. The remarkable upshot of this formulation is that the study of solutions to equations is subsumed into the study of maps whose very nature compels us to consider as the most basic in all of mathematics. This perspective is of late provenance in the theory of Diophantine equations, but still provides at this point its most fundamental justification.

The second idea involves a sophisticated construction whereby spaces like $\mathrm{Spec}(\mathbb{Q})$ or $\mathrm{Spec}(\mathbb{Z})$ are endowed with very non-trivial topologies that go beyond scheme theory (by which we mean the global theory of such spectra). We will not review the precise definitions in this summary, since it appears by now well-known that a Grothendieck topology on an object T allows open sets to be certain maps with range T from domains that are not necessarily subsets of T. On a 'usual' topological space, one could make the topology finer by allowing as open sets maps

$$U \to T$$

that are local homeomorphisms. This would allow covering spaces of T, for example, to be regarded as an 'open set.' An open covering then is a collection $\{U_i \to T\}_{i \in I}$ of such maps with the property that the union of the images is T. But this does not give anything essentially new. By definition each such $U \to T$ is a local homeomorphism, so that coverings by families of usual open subsets is co-final among all such exotic open coverings. That is to say, any covering $\{U_i \to T\}_{i \in I}$ in the generalized sense has a refinement

$$\{V_{ij} \hookrightarrow T\}$$

where each $V_{ij} \hookrightarrow T$ is an open embedding that factors through one of the U_i:

$$V_{ij} \to U_i \to T.$$

This fact induces an equivalence of categories between the category of usual sheaves and sheaves in this refined topology.

However, in algebraic geometry, there are many maps that behave formally like local homeomorphisms without actually being so. These are the so-called *étale maps* between schemes. A nice and fairly general class of examples arise from maps

$$\mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

corresponding to maps of rings $A \to B$ where B has the form

$$A[x]/(f(x))$$

for a monic polynomial $f(x)$. The constraint we wish to impose is that the fibers of $\mathrm{Spec}(B)$ over $\mathrm{Spec}(A)$, which have the form

$$\mathrm{Spec}(k[x]/(\bar{f}(x)))$$

for residue fields k of A, should have the same number of elements, indicating an absence of ramification. For this, we need to prevent $f(x)$ from having multiple roots in any such residue field. This amounts to the condition that $f(x)$ and $f'(x)$ should not have common roots point-wise, or that the discriminant of f should be a unit in A. The obvious map

$$\mathrm{Spec}(\mathbb{C}[t][x]/(x^2 - t)) \to \mathrm{Spec}(\mathbb{C}[t]),$$

is not étale, the discriminant of $x^2 - t$ being the non-unit $4t$, while

$$\mathrm{Spec}(\mathbb{C}[t, t^{-1}][x]/(x^2 - t)) \to \mathrm{Spec}(\mathbb{C}[t, t^{-1}]),$$

is étale.

Allowing étale maps as open subsets gives a genuinely richer topology to a scheme than the Zariski topology. The connected étale coverings of $\mathrm{Spec}(\mathbb{Q})$, for example, are maps

$$\mathrm{Spec}(F)\to\mathrm{Spec}(\mathbb{Q}),$$

where F is a finite field extension of $\mathbb{Q}$. For $\mathrm{Spec}(\mathbb{Z})$, one can construct an open covering using the two maps

$$\mathrm{Spec}(\mathbb{Z}[i][1/2])\to\mathrm{Spec}(\mathbb{Z})$$

and

$$\mathrm{Spec}(\mathbb{Z}[(1+\sqrt{-7})/2][1/7])\to\mathrm{Spec}(\mathbb{Z}).$$

The (co-)homology theory associated to sheaves in the étale topology has been spectacularly applied to the arithmetic geometry of schemes in the past many decades, with results well-enough known not to require a separate survey. Less known perhaps, is that Grothendieck's exotic topologies can also lead to interesting *homotopy* groups, whose structures are only recently being probed at any depth. One such direction is the *motivic homotopy theory* of Voevodsky, about which we will say nothing. The emphasis here instead is on rather recent developments in a somewhat older homotopy theory belonging to the *étale fundamental group* and its variations. In particular, we will focus exclusively on the application of the theory to Diophantine problems.

The beginning point is surprisingly elementary, wherefrom the theory obtains a substantial portion of its charm. Let therefore X be a variety defined over $\mathbb{Q}$ and $G=\pi_1(X(\mathbb{C}),b)$ the usual topological fundamental group of the space obtained from the complex points of X. For any point $x\in X(\mathbb{C})$, we can also consider the homotopy classes of paths

$$\pi_1(X(\mathbb{C});b,x)$$

from b to x. Then $\pi_1(X(\mathbb{C});b,x)$ has the natural structure of a principal G-bundle, or a *G-torsor*, in that G naturally acts on $\pi_1(X(\mathbb{C});b,x)$ via composition of paths, and the choice of any $p\in\pi_1(X(\mathbb{C});b,x)$ induces a bijection

$$G\simeq\pi_1(X(\mathbb{C});b,x)$$

$$g\mapsto pg$$

via the action. Since this principal bundle lives on a topological point, of course it is trivial. However, we see even here that the *variation* of $\pi_1(X(\mathbb{C});b,x)$ in x is not at all trivial in general. That is to say, the triviality of the individual P_x is not different from the triviality of the fibers of even a complicated vector bundle. To be more precise on this point, choose a pointed universal covering space

$$f:(\widetilde{X(\mathbb{C})},\tilde{b})\to(X(\mathbb{C}),b).$$

Then lifting of paths determines natural bijections

$$\pi_1(X(\mathbb{C});b,x)\simeq\widetilde{X(\mathbb{C})}_x$$

between homotopy classes of paths and the fibers of the universal covering space. In fact, it is natural to *construct* $\widetilde{X(\mathbb{C})}$ as

$$\cup_x\pi_1(X(\mathbb{C});b,x)$$

topologized so that the obvious projection that takes $\pi_1(X(\mathbb{C});b,x)$ to x is a local homeomorphism. In any case, we see thereby that the principal bundles in question form the fibers of a map

$$f:(\widetilde{X(\mathbb{C})},\tilde{b})\to(X(\mathbb{C}),b)$$

that can be highly non-trivial. In fact, we will see that the lack of a *canonical* isomorphism $G \simeq \pi_1(X(\mathbb{C}); b, x)$ is the essential ingredient underlying our ability to endow $\pi_1(X(\mathbb{C}); b, x)$ with a genuinely non-trivial structure of a principal G-bundle within suitably enriched contexts.

As far as Diophantine problems are concerned, we will of course be interested in the situation where b and x are both rational points in $X(\mathbb{Q})$. As it stands, the principal bundles $\pi_1(X(\mathbb{C}); b, x)$ cannot pick out such special points as being different in any way from generic points. There are several ways to remedy this, of which the (ostensibly) easiest one to explain is the passage to the pro-finite completion. That is, define

$$G^\wedge := \varprojlim_{N \lhd G, [G:N] < \infty} G/N$$

and

$$P^\wedge := \varprojlim_{N \lhd G, [G:N] < \infty} P \times_G G/N$$

for any principal G-bundle P. Here, $P \times_G G/N$ is the pushout torsor, obtained by taking the quotient of the product $P \times G/N$ by the diagonal G-action, $g(p, x) = (pg, g^{-1}x)$.

Then the basic and remarkable fact is that $G^\wedge$ is a sheaf of groups on the étale topology of $\mathrm{Spec}(\mathbb{Q})$ while $\pi_1(X(\mathbb{C}); b, x)^\wedge$ is a principal bundle for $G^\wedge$ in this topology. This statement is demystified just a little bit by recalling that a sheaf on $\mathrm{Spec}(\mathbb{Q})$ is simply a set equipped with a continuous action of $\Gamma = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Nevertheless, it remains to see that the Galois group will indeed act on an object that arose thus out of ordinary topology.

Accounting for the action is an isomorphism

$$\pi_1(X(\mathbb{C}), b)^\wedge \simeq \pi_1^{et}(\bar{X}, b)$$

where

$$\bar{X} = X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\bar{\mathbb{Q}})$$

is X regarded as a variety over $\bar{\mathbb{Q}}$, while π_1^{et} refers to the *pro-finite étale fundamental group*. It is the latter object on which Γ will act naturally.

The definition will be reviewed after a brief return to usual topology. For a manifold M and an element $b \in M$, the fundamental group $\pi_1(M, b)$ of M with base-point b can be defined in at least two different ways avoiding direct reference to topological loops. One way is to note first that a loop l acts naturally on the fiber over b of any covering space $N \to M$ of M using the monodromy of a lifting $\tilde{l}$ of l to N:

$$l_N : N_b \simeq N_b.$$

This bijection is compatible with composition of loops on the one hand, and with maps between covering spaces, on the other. That is, $(ll')_N = l_N \circ l'_N$, and if $f : N \to P$ is a map of covering spaces, then

$$f \circ l_N = l_P \circ f$$

as maps from N_b to P_b. It is something of a surprise that the only way to give such a compatible collection of automorphisms is in fact using an element of the fundamental group. The concise way to state this is via the functor

$$F_b : \mathrm{Cov}(M) \to \mathrm{Sets}$$

that associates to each covering N its fiber N_b over b. Then the fact in question is that

$$\pi_1(M, b) \simeq \mathrm{Aut}(F_b)$$

with the Aut understood in the sense of invertible natural transformations of a functor.

Now given a variety V, we can use this approach to *define* the étale fundamental group simply by changing the category of coverings. So we let

$$\mathrm{Cov}^{et}(V)$$

be the finite étale covers of V and, for any point $b \in V$, consider the functor F_b^{et} that takes $W \to V$ to the fiber W_b. Then

$$\pi_1^{et}(V, b) := \mathrm{Aut}(F_b^{et}).$$

Similarly,

$$\pi_1^{et}(V; b, x) := \mathrm{Isom}(F_b^{et}, F_x^{et}).$$

These superb definitions have been around at least since the 1960's, but it is rather striking that variation of the base-point has not been really attended to until fairly recently. The primary impetus for a serious reassessment appears to have come from the interaction with the Hodge theory of the fundamental group.

Nevertheless, constructions of the same general nature have now become commonplace in mathematics, the best known being associated to the notion of a Tannakian category, whereby the automorphisms of suitable functors defined on agreeable categories give rise to group schemes. Here we will content ourselves with mentioning two more examples. Fix a non-Archimedean completion $\mathbb{Q}_p$ of $\mathbb{Q}$ and consider the category

$$\mathrm{Loc}^{et}(V, \mathbb{Q}_p)$$

of locally constant sheaves of finite-dimensional $\mathbb{Q}_p$-vector spaces on V considered in the étale topology. There is still a fiber functor

$$F_b^{alg} : \mathrm{Loc}^{et}(V, \mathbb{Q}_p) \to \mathrm{Vect}_{\mathbb{Q}_p},$$

now taking values in $\mathbb{Q}_p$-vector spaces, that associates to each sheaf its stalk at b. (In comparing with the previous situation, it would be useful for the audience to have some intuition for the notion that a locally constant $\mathbb{Q}_p$-sheaf is a 'linearized' version of a covering space.) Now define

$$\pi_1^{alg,\mathbb{Q}_p}(V, b) := \mathrm{Aut}^{\otimes}(F_b^{alg}),$$

the $\mathbb{Q}_p$-*pro-algebraic completion* of $\pi_1^{et}(V, b)$. The $\otimes$ in the superscript refers to the fact that the automorphisms are required to be compatible not just with the morphisms in the category, but also the tensor product structure. As the name suggests, it is a pro-algebraic group over $\mathbb{Q}_p$.

When we replace all local systems by unipotent ones, i.e., those that admit a filtration

$$L = L^0 \supset L^1 \supset \cdots L^n \supset L^{n+1} = 0$$

such that each quotient L^i/L^{i+1} is isomorphic to a direct sum of the constant sheaf $\mathbb{Q}_p$, one again gets a category $\mathrm{Un}^{et}(V, \mathbb{Q}_p)$ of the right sort to which one can restrict the previous fiber functor

$$F_b^u : \mathrm{Un}^{et}(V, \mathbb{Q}_p) \to \mathrm{Vect}_{\mathbb{Q}_p}.$$

The $\mathbb{Q}_p$-*pro-unipotent completion* [2] of the étale fundamental group is then defined as

$$\pi_1^{u,\mathbb{Q}_p}(V, b) := \mathrm{Aut}^{\otimes}(F_b^u).$$

In both settings, there are still torsors of paths

$$\pi_1^{alg,\mathbb{Q}_p}(V; b, x) := \mathrm{Isom}(F_b^{alg}, F_x^{alg})$$

and

$$\pi_1^{u,\mathbb{Q}_p}(V;b,x) := \mathrm{Isom}(F_b^u, F_x^u).$$

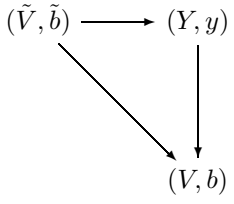
It is natural to regard such definitions with a degree of suspicion, since not having loops to visualize may make them seem entirely intractable. The situation is somewhat ameliorated through the intermediary of a universal object, which we describe in detail only for the full pro-finite étale fundamental group. Because Cov^{et} consists of *finite* covering spaces, it may not be possible to find a single universal object inside the category. However, it is possible to construct a pro-object that performs the same role. This is a compatible system

$$\tilde{V} = \{V_i\}_{i\in I}$$

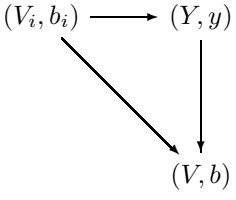
of finite étale coverings

$$V_i \to V$$

indexed by some filtered set I, having the following universal property: If we choose $\tilde{b} = (b_i) \in \tilde{V}_b$, the pair $(\tilde{V}, \tilde{b})$ is universal among pointed pro-covering spaces, in that any finite étale pointed covering $(Y, y)\to(V, b)$ fits into a unique commutative diagram



This means that there is some index i and a commutative diagram



In this situation, once again we have essentially tautological isomorphisms

$$\pi_1^{et}(V, b) \simeq \tilde{V}_b$$

and

$$\pi_1^{et}(V; b, x) \simeq \tilde{V}_x,$$

where the fibers are also projective systems of points.

When $V = \bar{X}$ for a variety X defined over $\mathbb{Q}$ and the base-point b is in $X(\mathbb{Q})$, then the entire pro-system

$$\tilde{\bar{X}} \to \bar{X}$$

comes from a system

$$\tilde{X} \to X$$

defined over $\mathbb{Q}$ and we can choose $\tilde{b} \in \tilde{\tilde{X}}$ as well to come from a rational point $\tilde{b} \in \tilde{X}(\mathbb{Q})$. The isomorphisms

$$\pi_1^{et}(\tilde{\tilde{X}}; b, x) \simeq \tilde{\tilde{X}}_x$$

then are compatible with the action of Γ. The sheaves on $\mathrm{Spec}(\mathbb{Q})$ obtained thereby have also a harmonious description in terms of the map corresponding to a rational point. The point is that the map

$$\tilde{X} \to X$$

is a pro-sheaf of sets in the étale topology of X. Then given any point

$$x : \mathrm{Spec}(\mathbb{Q}) \to X,$$

we get the sheaf

$$x^*(\tilde{X})$$

on $\mathrm{Spec}(\mathbb{Q})$, which is nothing but $\pi_1^{et}(\tilde{\tilde{X}}; b, x)$.

We illustrate this construction with the example of $(\bar{E}, 0)$, an elliptic curve with origin over $\mathbb{Q}$. Let

$$E_n \to E$$

be the covering space given by E itself with the multiplication map

$$[n] : E \to E.$$

Then the system

$$(\tilde{\tilde{E}}, \tilde{0}) := \{(\bar{E}_n, 0)\}_n \longrightarrow (\bar{E}, 0)$$

is a universal pointed covering space. Thus, for $(\bar{E}, 0)$,

$$\pi_1^{et}(\bar{E}, 0) \simeq \hat{T}(E)$$

and an element of the fundamental group is just a compatible collection of torsion points of E. That is to say, the Galois action on $\pi_1^{et}(\bar{E}, 0)$ is the well-known action on the Tate module of E. Similarly,

$$\pi_1^{et}(\bar{E}; 0, x) \simeq \tilde{\tilde{E}}_x$$

consists of compatible systems of division points of x.

A notable fact that emerges from this description is that if we take into account the Galois action, it is no longer possible to trivialize the torsor in general, even point-wise. That is, there will often be no isomorphism between $\pi_1^{et}(\bar{X}, b)$ and $\pi_1^{et}(\bar{X}; b, x)$, reflecting the fact that the étale topology has a very rich structure even on a point. In the case of $(E, 0)$, if there were an isomorphism

$$\pi_1^{et}(\bar{E}, 0) \simeq \pi_1^{et}(\bar{E}; 0, x)$$

then there would be a Galois invariant element of

$$\pi_1^{et}(\bar{E}; 0, x) \simeq \tilde{\tilde{E}}_x.$$

In particular, for any n, there would be a rational point x_n such that $nx_n = x$, which is not possible for $x \neq 0$ by a theorem of Mordell.

To summarize, given a variety $X/\mathbb{Q}$ with a fixed rational point $b \in X(\mathbb{Q})$, we are associating to each other point $x \in X(\mathbb{Q})$ a principal bundle $\pi_1^{et}(\bar{X}; b, x)$ for $\pi_1^{et}(\bar{X}, b)$ on the étale topology of $\mathrm{Spec}(\mathbb{Q})$. This information can be organized using a standard classifying space of sorts for principal bundles. That is, given a principal bundle T, one can choose a point

$$t \in T$$

and examine the action of Γ on that point. For each $g \in \Gamma$, $g(t)$ will be related to t by an element $l_g \in \pi_1^{et}(\bar{X}, b)$, that is,

$$g(t) = tl_g.$$

The map

$$g \mapsto l_g$$

obtained thereby is a 1-cocycle

$$c_t : \Gamma \to \pi_1^{et}(\bar{X}, b),$$

that is, a continuous map that satisfies

$$c_t(g_1 g_2) = c(g_1) g_1(c(g_2)).$$

If we denote the set of such cocycles by

$$Z^1(\Gamma, \pi_1^{et}(\bar{X}, b)),$$

then $\pi_1^{et}(\bar{X}, b)$ acts on it according to

$$lc(g) := g(l^{-1})c(g)l$$

and a different choice of $s \in T$ will lead to a cocycle c_s lying in the same orbit as c_t. Denote by

$$H^1(\Gamma, \pi_1^{et}(\bar{X}, b)) := \pi_1^{et}(\bar{X}, b) \backslash Z^1(\Gamma, \pi_1^{et}(\bar{X}, b))$$

the orbit set, so that the torsor T determines a class

$$[T] = [c_t] \in H^1(\Gamma, \pi_1^{et}(\bar{X}, b)).$$

This cohomology set in fact classifies such torsors so that we have defined a map

$$\begin{aligned} X(\mathbb{Q}) &\longrightarrow H^1(\Gamma, \pi_1^{et}(\bar{X}, b)) \\ x &\longmapsto [\pi_1^{et}(\bar{X}; b, x)] \end{aligned}$$

to a classifying space that can be thought of as an *étale period map*. In his famous letter to Faltings, Grothendieck formulated the hope of studying Diophantine problems using this map. (He did not express matters using torsors, but rather, splittings of a certain canonical sequence of fundamental groups, in order to better harmonize the discussion with his general program of *anabelian geometry*.)

Unfortunately, it seems at present that the set $H^1(\Gamma, \pi_1^{et}(\bar{X}, b))$ has too little structure to study in a comprehensible manner. It should be obvious, meanwhile, that an entirely analogous construction can be carried out with $\pi_1^{alg,\mathbb{Q}_p}(\bar{X}, b)$ or with $\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)$. For reasons that are somewhat technical to discuss in a short survey, $\pi_1^{alg,\mathbb{Q}_p}(\bar{X}, b)$ does not afford much advantage at present over $\pi_1^{et}(\bar{X}, b)$. The unipotent completion, on the other hand, has been exploited to a certain extent in the study of Diophantine sets. The key difference from the other cases has to do with the relative ease of accessing information about

$$H^1(\Gamma, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)),$$

or rather, a slight improvement of this set. Let S be the set of primes of bad reduction for X, and denote by $X(\mathbb{Z}_S)$ the set of points in the ring $\mathbb{Z}_S$ of S-integers, where the integrality is defined in terms of a suitably good model. (Note that if X is compact, then the integral points are the same as rational points.) Choose a prime $p \notin S$. The first point of note is that the map

$$X(\mathbb{Q}) \to H^1(\Gamma, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)), \qquad x \mapsto [\pi_1^{u,\mathbb{Q}_p}(\bar{X}; b, x)],$$

when restricted to the integral points, factors through a natural subspace corresponding to local conditions satisfied by the torsors $[\pi_1^{u,\mathbb{Q}_p}(\bar{X}; b, x)]$, such as being unramified away from the primes of bad reduction and p, and having a 'crystalline' nature at p. This last condition arises from the *p-adic Hodge theory* of the non-Archimedean variety

$$X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\mathbb{Q}_p)$$

that exerts a useful influence on $\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)$. In fact, these conditions are meaningless for $H^1(\Gamma, \pi_1^{et}(\bar{X}, b))$ and quite difficult to analyze for $H^1(\Gamma, \pi_1^{alg,\mathbb{Q}_p}(\bar{X}, b))$. The advantage of considering them in the unipotent setting is that the subspace $H^1_f(\Gamma, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b))$ becomes canonically equipped with the structure of a pro-algebraic variety. In fact, for various quotients $[\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n$ of $\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)$ modulo its descending central series, the sets

$$H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

have natural structures of affine algebraic varieties over $\mathbb{Q}_p$ that fit into a tower:

$$\begin{array}{ccc}
 & \vdots & \\
\vdots & & \\
 & H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_4) & \\
 & \downarrow & \\
 & H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_3) & \\
 & \downarrow & \\
 & H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_2) & \\
 & \downarrow & \\
X(\mathbb{Z}_S) & \longrightarrow & H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_1)
\end{array}$$

refining the map at the bottom (which has a classical interpretation in Kummer theory). The discussion can be repeated verbatim for the sets

$$H^1_f(\Gamma_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

of local Galois cohomology for the group $\Gamma_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p, \mathbb{Q}_p)$. This local space also admits a map from $X(\mathbb{Z}_p)$ that fits into a commutative diagram

$$\begin{array}{ccc}
X(\mathbb{Z}_S) & \longrightarrow & X(\mathbb{Z}_p) \\
\downarrow & & \downarrow \\
H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) & \longrightarrow & H^1_f(\Gamma_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)
\end{array}$$

It comes furthermore with an analytic description

$$H^1_f(\Gamma_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) \simeq [\pi_1^{DR}(X_{\mathbb{Q}_p}, b)]_n / F^0$$

provided by *p-adic Hodge theory* and the *De Rham fundamental group* $\pi_1^{DR}(X_{\mathbb{Q}_p}, b)$ together with its Hodge filtration $F^\bullet$. Thus, eventually, our diagram becomes

$$\begin{array}{ccc} X(\mathbb{Z}_S) & \longrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) & \longrightarrow & [\pi_1^{DR}(X_{\mathbb{Q}_p}, b)]_n / F^0 \end{array}$$

the effect of which is that we have replaced the difficult inclusion

$$X(\mathbb{Z}_S) \hookrightarrow X(\mathbb{Z}_p)$$

with

$$H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) \to [\pi_1^{DR}(X_{\mathbb{Q}_p}, b)]_n / F^0,$$

an algebraic map between $\mathbb{Q}_p$-varieties, whose image is therefore computable in principle.

It is reasonable to state a theorem [5]:

Theorem 1.

Let X be a curve and suppose

$$\dim H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) < \dim \pi_1^{DR}(X_{\mathbb{Q}_p}, b)_n / F^0$$

for some n. Then $X(\mathbb{Z}_S)$ is finite.

The proof of the theorem is contained in the following diagram:

$$\begin{array}{ccc} X(\mathbb{Z}_S) & \longrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) & \longrightarrow & [\pi_1^{DR}(X_{\mathbb{Q}_p}, b)]_n / F^0 \\ & & \downarrow{\scriptstyle \alpha \neq 0} \\ & & \mathbb{Q}_p \end{array}$$

The assumption on dimensions implies that the image of $H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$ inside $\pi_1^{DR}(X_{\mathbb{Q}_p}, b)_n / F^0$ is not Zariski dense, and hence, is killed by some non-zero function α. However, when the function is pulled back to $X(\mathbb{Z}_p)$ it turns out to be a non-zero linear combination of *p-adic iterated integrals* [3]

$$\int_b^x \beta_1 \beta_2 \cdots \beta_m$$

of differential forms β_i on X. This description is the really useful technical input from p-adic Hodge theory. The point is that such a function can be expanded as a non-vanishing convergent power series on each p-adic disk in $X(\mathbb{Z}_p)$, and

hence, has only finitely many zeros. The commutativity of the diagram is then enough to imply that the function vanishes on $X(\mathbb{Z}_S)$, yielding for us its finiteness.

Some amount of progress has accrued to the program of *non-abelian Diophantine geometry* by way of this theorem, such as new proofs of Diophantine finiteness for hyperbolic curves whose homology admit Galois action that are essentially abelian, that is, curves of genus zero, or curves of positive genus with CM Jacobians [1, 4, 6]. Furthermore, standard conjectures from the theory of mixed motives imply [5] that the inequality in the hypothesis should always hold on hyperbolic curves, insofar one climbs sufficiently high up on the tower ($n >> 0$). One hopes (perhaps in vain) that the milieu of investigation is rich enough to include eventually a broader range of applications, such as a structural understanding of the relationship between Diophantine finiteness and hyperbolicity, and a 'non-abelian extension' of the main ideas surrounding the conjecture of Birch and Swinnerton-Dyer [7].

In the meanwhile, it is rather interesting to note the key role played by moduli spaces of principal bundles on $\mathrm{Spec}(\mathbb{Q})$ such as

$$H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n).$$

The situation is an appropriate non-abelian complement to the classical use of the Jacobian of a curve, and the occurrence of related moduli spaces in the Langlands' program. It appears to have been André Weil who first foresaw such possibilities in a remarkable paper of the 1930's [8], even with no knowledge of the étale topology. This is a point of considerable historical interest that will be elaborated upon in a separate lecture.

References

[1] Coates J., Kim M., Selmer varieties for curves with CM Jacobians, preprint available at http://arxiv.org/abs/0810.3354

[2] Deligne P., Le groupe fondamental de la droite projective moins trois points, In: Galois groups over $\mathbb{Q}$, Berkeley, 1987, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989, 79–297

[3] Furusho H., p-adic multiple zeta values. I: p-adic multiple polylogarithms and the p-adic KZ equation, Invent. Math., 2004, 155(2), 253–286

[4] Kim M., The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel, Invent. Math., 2005, 161(3), 629–656

[5] Kim M., The unipotent Albanese map and Selmer varieties for curves, Publ. Res. Inst. Math. Sci., 2009, 45(1), 89–133

[6] Kim M., p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication, Ann. of Math., (in press), preprint available at http://arxiv.org/abs/0710.5290

[7] Kim M., Tamagawa A., The ℓ-component of the unipotent Albanese map, Math. Ann., 2008, 340(1), 223–235

[8] Weil A., Généralisation des fonctions abéliennes, J. Math. Pures Appl., 1938, 17(9), 47–87