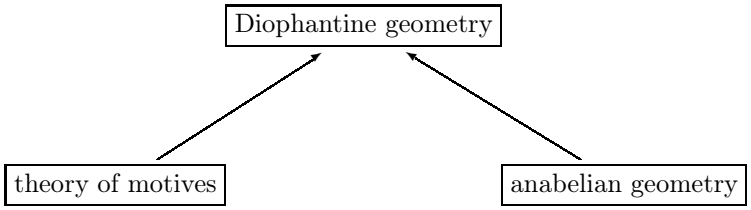
Galois Theory and Diophantine geometry

Minhyong Kim

August 5, 2009

Lecture at Cambridge workshop, July, 2009

The author must confess to having contemplated for some years a diagram of the following sort.



To a large extent, the investigations to be brought up today arise from a curious inadequacy having to do with the arrow on the left. On the one hand, it is widely acknowledged that the theory of motives finds a strong source of inspiration in Diophantine geometry, inasmuch so many of the structures, conjectures, and results therein have as model the conjecture of Birch and Swinnerton-Dyer, where the concern is with rational points on elliptic curves that can be as simple as

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

Even in the general form discovered by Deligne, Beilinson, Bloch and Kato, (see, for example, [17]) it is clear that motivic L-functions are supposed, in an ideal world, to give access to invariants in arithmetic geometry of a *Diophantine nature*. The difficulty arises when we focus on the very primitive concerns of Diophantine geometry, which might broadly be characterized as the study of maps between schemes of finite type over $\mathbb{Z}$ or $\mathbb{Q}$. One might attempt, for example, to define the points of a motive M over $\mathbb{Q}$ using a formula like

$$\mathrm{Ext}^1(\mathbb{Q}(0), M)$$

or even

$$\mathrm{RHom}(\mathbb{Q}(0), M),$$

hoping it eventually to be adequate in a large number of situations. However, even in the best of all worlds, this formula will never provide direct access to the points of a scheme, except in very special situations like $M = H_1(A)$ with A an abelian variety. This is a critical limitation of the abelian nature of motives, rendering it quite difficult to find direct applications to any mildly non-abelian Diophantine problem, say that posed by a curve of genus 2. It is worth remarking that this limitation is essentially by design, since the whole point of the motivic category is to *linearize* by increasing the number of morphisms[1]. Of course we should pause to acknowledge the role of technology that is more or less motivic in nature within two of the most celebrated Diophantine results of our times, namely the theorems of Faltings and of Wiles. But there, the idea is to constrain points on a non-abelian variety by forcing them to *parametrize* motives of a very special type. The method of achieving this is highly ingenious in each case and, therefore, underscores our concern that it is rather unlikely to be part of a general system, and certainly not of the motivic philosophy as it stands.

[1] Even then, we complain that there are not enough.

Much has been written about the meaning of anabelian geometry, with a general tendency to retreat to the realm of curves as the only firm ground on which to venture real assertions or conjectures. We as well will proceed to use X to denote a smooth projective curve of genus at least two over $\mathbb{Q}$. The basic anabelian proposal then is to replace the Ext group that appeared above by the topological space

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

the non-abelian continuous cohomology [35] of the absolute Galois group $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$ with coefficients in the profinite étale fundamental group of X. The notation will suggest that a rational basepoint $b \in X(\mathbb{Q})$ has been introduced. Many anabelian results do not require it [29], but the Diophantine issues discussed today will gain in clarity by having it at the outset, even if the resulting restriction may appear as serious to many. An immediate relation to the full set of points is established by way of a non-abelian Albanese map

$$X(\mathbb{Q}) \xrightarrow{\kappa^{na}} H^1(G, \pi_1^{et}(\bar{X}, b));$$

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

We remind ourselves that the definition of fundamental groups in the style of Grothendieck [39] typically starts from a suitable category over X, in this case that of finite étale covers of

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

that we might denote by

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

The choice of any point $y \in \bar{X}$ determines a fiber functor

$$F_y : \mathrm{Cov}(\bar{X}) \longrightarrow \text{Finite Sets},$$

using which the fundamental group is defined to be

$$\pi_1^{et}(\bar{X}, y) := Aut(F_y),$$

in the sense of invertible natural transformations familiar from category theory[2]. Given two points y and z, there is also the set of étale paths

$$\pi_1^{et}(\bar{X}; y, z) := \mathrm{Isom}(F_y, F_z)$$

from y to z that the bare definitions equip with a right action of $\pi_1^{et}(\bar{X}, y)$, turning it thereby into a torsor for the fundamental group. When y and z are rational points, the naturality of the constructions equips all objects with a compatible action of G, appearing in the non-abelian cohomology set and the definition of the map κ^{na}.

The context should make it clear that $H^1(G, \pi_1^{et}(\bar{X}, b))$ can be understood as a non-abelian Jacobian in an étale profinite realization, where the analogy might be strengthened by the interpretation of the G-action as defining a sheaf on $\mathrm{Spec}(\mathbb{Q})$ and $H^1(G, \pi_1^{et}(\bar{X}, b))$ as the moduli space of torsors for

[2]The reader unfamiliar with such notions would do well to think about the case of a functor

$$F : \mathbb{N}^{op} \to \mathcal{C}$$

whose source is the category of natural numbers with a single morphism from n to m for each pair $m \leq n$. Of course this is just a sequence

$$\to F(3) \to F(2) \to F(1) \to F(0)$$

of objects in $\mathcal{C}$, and an automorphism of F is a compatible sequence $(g_i)_{i \in \mathbb{N}}$ of automorphisms

$$g_i : F(i) \simeq F(i).$$

For a general $F : \mathcal{B} \to \mathcal{C}$, it is profitable to think of $\mathcal{B}$ as a complicated indexing set for things in $\mathcal{C}$.

$\pi_1^{et}(\bar{X}, b)$ in the étale topos of Spec($\mathbb{Q}$). It is instructive to compare this space with the moduli space $Bun_n(X)$ of rank n vectors bundles on X for $n \geq 2$. Their study was initiated in a famous paper of André Weil [42] whose title suggests the intention of the author to regard them also as non-abelian Jacobians. Perhaps less well-known is the main motivation of the paper, which the introduction essentially states to be the study of rational points on curves of higher genus. Weil had at that point already expected non-abelian fundamental groups to intervene somehow in a proof of the Mordell conjecture, except that a reasonable arithmetic theory of π_1 was not available at the time. In order to make the connection to fields of definition, Weil proceeded to interpret the representations of the fundamental group in terms of algebraic vector bundles, whose moduli would then have the same field of definition as the curve. In this sense, the paper is very much a continuation of Weil's thesis [41], where an algebraic interpretation of the Jacobian is attempted with the same goal in mind, however with only the partial success noted by Hadamard. The spaces $Bun_n(X)$ of course fared no better, and it is perhaps sensible to ask why. One possibility was suggested by Serre [36] in his summary of Weil's mathematical contributions, where he calls attention to the lack of the geometric technology requisite to a full construction of Bun_n, which was subsequently developed only in the 60's by Mumford, Narasimhan, Seshadri, and others [27, 30]. However, even with geometric invariant theory and its relation to π_1 completed in the remarkable work of Carlos Simpson [38], there has never been any direct applications of these moduli spaces (or their cotangent bundles) to Diophantine problems. It is for this reason that the author locates the difficulty in a far more elementary source, namely, *the lack of an Albanese map to go with* Bun_n. Unless $n = 1$, there is no canonical relation[3] between Bun_n and the points on X. It is fortunate then that the étale topology manages to provide us with two valuable tools, namely, topological fundamental groups that come with fields of definition; and topological classifying spaces with extremely canonical Albanese maps. We owe this to a distinguished feature of Grothendieck's theory: the flexible use of basepoints, which are allowed to be any geometric point at all. The idea that Galois groups of a certain sort should be regarded as fundamental groups is likely to be very old, as Takagi[16] refers to Hilbert's preoccupation with Riemann surfaces as inspiration for class field theory. Indeed, it is true that that the fundamental group of a smooth variety V will be isomorphic to the Galois group $\mathrm{Gal}(k(V)^{nr}/k(V))$ of a maximal unramified extension $k(V)^{nr}$ of its function field $k(V)$. However, this isomorphism will be *canonical* only when the basepoint is taken to be a separable closure of $k(V)$ that contains $k(V)^{nr}$:

$$b : \mathrm{Spec}(k(V)^s) \to \mathrm{Spec}(k(V)^{nr}) \to \mathrm{Spec}(k(V)) \to V.$$

Within the Galois group approach, there is little room for small basepoints that come through rational points, or a study of variation. In fact, there seems to be no reasonable way to fit path spaces at all into the field picture. This could then be described as the precise ingredient missing in the arithmetic theory of fundamental groups at the time of Weil's paper. Even after the introduction of moving basepoints, appreciation of their genuine usefulness appears to have taken some time to develop. A rather common response is to pass quickly to invariants or situations where the basepoint can be safely ignored. The author for example came to appreciate the basepoint as a variable only after reading Professor Deligne's paper written in the 80's [7] as well as the papers of Hodge-theorists like Dick Hain [15].

One way to visualize path spaces is to consider a universal (pro-)cover

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

The choice of a lifting $\tilde{b} \in \tilde{\bar{X}}_b$ turns the pair into a *universal pointed covering space*. The uniqueness then allows us to descend to $\mathbb{Q}$, while the universal property determines canonical isomorphisms

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

[3] It is conceivable that the theory of Hecke correspondences can be employed to establish the link.

so that the Galois action can be interpreted using the action on fibers[4] . This is one way to see that the map κ^{na} will never send $x \neq b$ to the trivial torsor, that is, a torsor with an element fixed by G, since, by the Mordell-Weil theorem, nothing but the basepoint will lift rationally even up to the maximal abelian quotient of $\tilde{\tilde{X}}$. A change of basepoint[5] then shows that the map must in fact be injective. That is, we have arrived at the striking fact that points can really be distinguished through the associated torsors[6]. In elementary topology, one encounters already the warning that such path spaces are isomorphic, but not in a canonical fashion. The distinction may appear pedantic until one meets such enriched situations as to endow the torsors with the extra structure necessary to make them genuinely different.

The remarkable *section conjecture* of Grothendieck [14] proposes that κ^{na} is even surjective:

$$X(\mathbb{Q}) \simeq H^1(G, \pi_1^{et}(\bar{X}, b)),$$

that is,

every torsor should be a path torsor.

The reader is urged to compare this conjecture with the assertion that the map

$$\widehat{E(\mathbb{Q})} \simeq H^1_f(G, \pi_1^{et}(\bar{E}, e)),$$

from Kummer theory is supposed to be bijective for an elliptic curve (E, e). A small difference has to do with the local 'Selmer' conditions on cohomology indicated by the subscript 'f', which the complexity of the non-abelian fundamental group is supposed to render unnecessary. This is a subtle point on which the experts seem not to offer a consensus. Nevertheless, the comparison should make it clear to the newcomer that a resolution of the section conjecture is quite unlikely to be straightforward, being, as it is, a deep non-abelian incarnation of the principle that suitable conditions on a Galois-theoretic construction should force it to 'come from geometry'[7]. And then, the role of this bijection in the descent algorithm for elliptic curves might suggest a useful Diophantine context for the section conjecture [22]. Yet another reason for thinking the analogy through is a hope that the few decades worth of effort that went into the study of Selmer groups of elliptic curves might illuminate certain aspects of the section conjecture as well, even at the level of concrete technology.

*

Our main concern today is with a version of these ideas where the parallel with elliptic curves is especially compelling, in that a good deal of unity between the abelian and non-abelian realms is substantially realized. This is when the profinite fundamental group is replaced by the motivic one [7]:

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

[4]The difficult problem of coming to actual grips with this is that of constructing a cofinal system making up $\tilde{\tilde{X}}$ in a manner that makes the action maximally visible. Consider $\mathbb{G}_m$ or an elliptic curve.

[5]One needs here the elementary fact that an isomorphism of torsors

$$\pi_1(\bar{X}; b, x) \simeq \pi_1(\bar{X}; b, y)$$

is necessarily induced by a path $F_x \simeq F_y$.

[6]It is however, quite interesting to work out injectivity or its failure for quotients of fundamental groups corresponding to other natural systems, like modular towers. Alternatively, one could use the full fundamental group for a variety where the answer is much less obvious, like a moduli space of curves.

[7]This notion in abelian settings coincides roughly with 'motivic.'

The motivic fundamental group lies between the profinite π_1 and homology in complexity:

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

although it should be acknowledged right away that it is much closer to the bottom of the hierarchy. The precise meaning of 'motivic' should not worry us here more than in other semi-formal expositions on the subject, since we will regress quickly to the rather precise use of realizations. But still, some inspiration may be gather by the rather ghostly presence of a classifying space

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

of motivic torsors as well that of a motivic Albanese map

$$\kappa^M : X(\mathbb{Q}) \longrightarrow H^1_M(G, \pi_1^M(\bar{X}, b))$$

that associates to points motivic torsors

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

of paths. The astute reader will object that we are again using the points of X to parametrize motives as in the subterfuge of Parshin and Frey, to which we reply that the current family is entirely intrinsic to the curve X, and requires no particular ingenuity to consider.

When it comes to precise definitions [20, 21], that we must (alas!) inflict upon the reader in a rapid succession of mildly technical paragraphs, the most important (Tannakian) category

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

consists of locally constant unipotent $\mathbb{Q}_p$-sheaves on $\bar{X}$, where a sheaf is unipotent if it can be constructed using successive extensions starting from the constant sheaf $[\mathbb{Q}_p]_{\bar{X}}$. As in the profinite theory, we have a fiber functor

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

that associates to a sheaf $\mathcal{V}$ its stalk $\mathcal{V}_b$, which has now acquired a linear nature. The $\mathbb{Q}_p$-pro-unipotent étale fundamental group is defined to be

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

the tensor-compatible[8] automorphisms of the fiber functor, which the linearity equips with the added structure of a pro-algebraic pro-unipotent group over $\mathbb{Q}_p$. In fact, the descending central series filtration

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

yields the finite-dimensional algebraic quotients

$$U_n = U^{n+1} \backslash U,$$

at the very bottom of which is an identification

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

[8] To see the significance of this notion, one should consider the group algebra $\mathbb{C}[G]$ of a finite group G. On the category $Rep_G(\mathbb{C})$ of G-representations on complex vector spaces, we have the fiber functor that forgets the G-action. Any unit in $\mathbb{C}[G]$ defines an automorphism of this functor, while the elements of G will then be picked out by the condition of being tensor-compatible.

with the $\mathbb{Q}_p$-Tate module of the (abelian) Jacobian J of X. The different levels are connected by exact sequences

$$0 \to U^{n+1}\backslash U^n \to U_n \to U_{n-1} \to 0$$

that add the extra term $U^{n+1}\backslash U^n$ at each stage, which, however, is a vector group that can be approached with rather conventional techniques. In fact, the G-action on U lifts the well-studied one on $V = V_p J$, and repeated commutators come together to a quotient map

$$V^{\otimes n} \longrightarrow\!\!\!\!\!\rightarrow\ U^{n+1}\backslash U^n,$$

placing the associated graded pieces into the category of motives generated by J. The inductive pattern of these exact sequences is instrumental in making the unipotent completions considerably more tractable than their profinite ancestors.

We will again denote by $H^1(G, U_n)$ continuous Galois cohomology with values in the points of U_n. For $n \geq 2$, this is still non-abelian cohomology, and hence, lacks the structure of a group. Nevertheless, the proximity to homology is evidenced in the presence of a remarkable subspace

$$H^1_f(G, U_n) \subset H^1(G, U_n)$$

defined by local 'Selmer' conditions[9] that require the classes to be

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

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

The locality of the conditions refers to their focus on the pull-back of a torsor for U to the completed fields $\mathrm{Spec}(\mathbb{Q}_l)$. For $l \notin T$, (a) requires the torsor to trivialize over an unramified extension of $\mathbb{Q}_l$, while condition (b) requires it to trivialize over Fontaine's ring B_{cr} of crystalline periods [8]. One could equivalently describe the relevant torsors as having coordinate rings that are unramified or crystalline as representations of the local Galois groups.

Quite important to our purposes is the *algebraicity* of the system

$$\cdots \to H^1_f(G, U_{n+1}) \to H^1_f(G, U_n) \to H^1_f(G, U_{n-1}) \to \cdots .$$

This is the *Selmer variety* of X. That is, each $H^1_f(G, U_n)$ is an algebraic variety over $\mathbb{Q}_p$ and the transition maps are algebraic, so that

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

is now a moduli space very similar to the ones that come up in the study of Riemann surfaces [11], in that it parametrizes crystalline principal bundles for U in the étale topology of $\mathrm{Spec}(\mathbb{Z}[1/S])$. By comparison $H^1(G, \pi_1^{et}(\bar{X}, b))$ has no apparent structure but that of a pro-finite space: the motivic context has restored some geometry[10] to the moduli spaces of interest. The algebraic structure is best understood in terms of $G_T = \mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$, where $\mathbb{Q}_T$ is the maximal extension of $\mathbb{Q}$ unramified outside T. Our moduli space $H^1_f(G, U_n)$ sits inside $H^1(G_T, U_n)$ as a subvariety defined by the additional crystalline condition. For the latter, there are sequences

$$0 \to H^1(G_T, U^{n+1}\backslash U^n) \to H^1(G_T, U_n) \to H^1(G_T, U_{n-1}) \stackrel{\delta_{n-1}}{\to}$$
$$H^2(G_T, U^{n+1}\backslash U^n)$$

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

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

[9] Starting at this point, one should take p to be a prime of good reduction for X, even though an extension of the theory to the general case should be straightforward.

[10] 'Coefficient geometry,' one might say, in contrast to Bun_n, which carries the algebraic geometry of the field of definition.

using the fact that the boundary maps δ_{n-1} are algebraic[11]. That is, $H^1(G_T, U_n)$ is inductively realized as a torsor for the vector group $H^1(G_T, U^{n+1}\backslash U^n)$ lying over the kernel of δ_{n-1}.

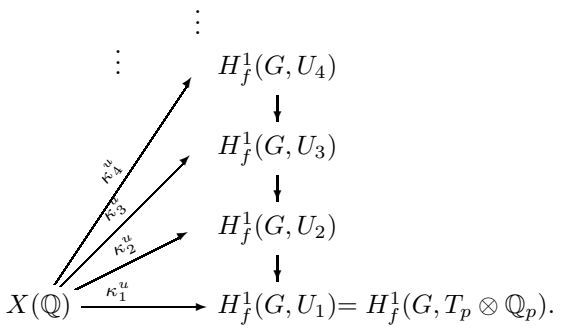
It should comes as no surprise at this point that there is a map

$$\kappa^u = \{\kappa^u_n\} : X(\mathbb{Q}) \longrightarrow H^1_f(G, U)$$

associating to a point x the principal U-bundle

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

of tensor-compatible isomorphisms from F_b to F_x, that is, the $\mathbb{Q}_p$-pro-unipotent étale paths from b to x. This map is best viewed as a tower:



For $n = 1$,

$$\kappa^u_1 : X(\mathbb{Q}) \to H^1_f(G, U_1) = H^1_f(G, T_p J \otimes \mathbb{Q}_p)$$

reduces to the map from Kummer theory. But the maps κ^u_n for $n \geq 2$, much weaker as they are than the κ^{na} discussed in the profinite context, still do not extend to cycles in any natural way, and hence, retain the possibility of separating the structure[12] of $X(\mathbb{Q})$ from that of $J_X(\mathbb{Q})$.

Restricting U to the étale site of $\mathbb{Q}_p$, there are local analogues

$$\kappa^u_{p,n} : X(\mathbb{Q}_p) \to H^1_f(G_p, U_n)$$

that can be described explicitly (and rather surprisingly) using non-abelian p-adic Hodge theory. More precisely, there is a compatible family of isomorphisms

$$D : H^1_f(G_p, U_n) \simeq U^{DR}_n / F^0$$

to homogeneous spaces for the *De Rham fundamental group*

$$U^{DR} = \pi_1^{DR}(X \otimes \mathbb{Q}_p, b)$$

of $X \otimes \mathbb{Q}_p$. Here, U^{DR} classifies unipotent vector bundles with flat connections on $X \otimes \mathbb{Q}_p$, while

$$U^{DR}/F^0$$

is a moduli space for U^{DR}-torsor that carry compatible Hodge filtrations and Frobenius actions, the latter being obtained from a comparison isomorphism[13] with the crystalline fundamental group and path torsors associated to a reduction modulo p. The advantage of the De Rham realization is its

[11] The reader is warned that it is non-linear in general.

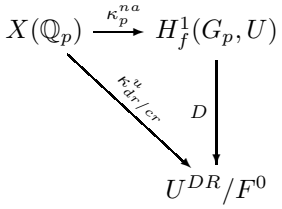
[12] It might be suggested, only half in jest, that the Jacobian, introduced by Weil to aid in the Diophantine study of a curve, has been getting in the way ever since.

[13] That is to say, if $\mathcal{X}$ denotes a smooth and proper $\mathbb{Z}_p$-model of $X \otimes \mathbb{Q}_p$, the category of unipotent vector bundles with flat connections on $X \otimes \mathbb{Q}_p$ is equivalent to the category of unipotent convergent isocystals on $\mathcal{X} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$. This comparison is the crucial ingredient in defining p-adic iterated integrals [10].

expression as a p-adic homogenous space whose form is far more transparent than that of Galois cohomology. The map D (for Dieudonné, as in the theory of p-divisible groups) associates to a crystalline principal bundle $P = \mathrm{Spec}(\mathcal{P})$ for U, the space

$$D(P) = \mathrm{Spec}([\mathcal{P} \otimes B_{cr}]^{G_p}).$$

This ends up as a U^{DR}-torsor with Frobenius action and Hodge filtration inherited from that of B_{cr}. The compatibility of the two constructions is expressed by a diagram



whose commutativity amounts to the non-abelian comparison isomorphism [31]

$$\pi_1^{DR}(X \otimes \mathbb{Q}_p; b, x) \otimes B_{cr} \simeq \pi_1^{u,\mathbb{Q}_p}(\bar{X}; b, x) \otimes B_{cr}.$$

The explicit nature of the map

$$\kappa^u_{dr/cr} : X(\mathbb{Q}_p) \to U^{DR}/F^0,$$

is a consequence of the p-adic iterated integrals[14] [10]

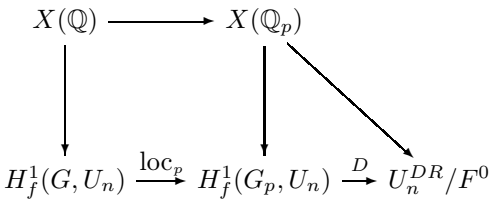
$$\int_b^z \alpha_1 \alpha_2 \cdots \alpha_n$$

that appear in its coordinates. This expression endows the map with a highly transcendental nature: for any residue disk $]y[\subset X(\mathbb{Q}_p)$,

$$\kappa^u_{dr/cr,n}(]y[) \subset U_n^{DR}/F^0$$

is Zariski dense for each n, and is made up of non-zero convergent power series that are obtained explicitly as repeated anti-derivatives starting from differential forms on X.

Finally, the local and global constructions fit into a family of commutative diagrams



where the bottom horizontal maps are algebraic and the vertical maps transcendental. Thus, the difficult inclusion $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$ has been replaced by the map[15] $\log_p := D \circ \mathrm{loc}_p$, whose algebraicity gives a glimmer of hope that the arithmetic geometry can be understood and controlled.

The following result is basic to the theory.

Theorem 1 *Suppose*

$$\log_p(H^1_f(G, U_n)) \subset U_n^{DR}/F^0$$

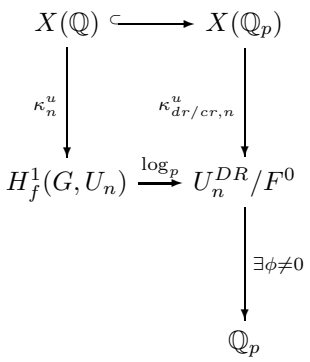
is not Zariski dense for some n. Then $X(\mathbb{Q})$ is finite[16].

[14] Special values of such integrals have attracted attention because of the connection to values of L-functions. Here we are interested primarily in the integrals themselves as analytic functions, and in their zeros.

[15] The strange notation is comes the view that D is itself a log map, according to Bloch and Kato [2].

[16] Professor Serre would object that the theorem is trivially true since $X(\mathbb{Q})$ *is* finite. The author offers no defense.

The proof of this assertion in its entirety is captured by the diagram



indicating the existence of a non-zero algebraic function ϕ vanishing on $\log_p(H^1_f(G,U_n))$. Hence, the function $\phi \circ \kappa^u_{dr/cr,n}$ on $X(\mathbb{Q}_p)$ vanishes on $X(\mathbb{Q})$. But this function is a non-vanishing convergent power series on each residue disk, which therefore can have only finitely many zeros. $\Box$.

A slightly more geometric account of the proof might point to the fact that the image of $X(\mathbb{Q}_p)$ in U^{DR}_n/F^0 is a space-filling curve, with no portion contained in a proper subspace. Hence, its intersection with any proper subvariety must be discrete. Being compact as well, it must then be finite[17]. Serge Lang once proposed a strategy for proving the Mordell conjecture by deducing it from a purely geometric hope that the complex points on a curve of higher genus might intersect a finitely generated subgroup of the Jacobian in finitely many points. While that idea turned out to be very difficult to realize, here we have a non-Archimedean analogue, wtih U^{DR}_n/F^0 playing the role of the complex Jacobian, and the Selmer variety that of the Mordell-Weil group.

The hypothesis of the theorem on non-denseness of the global Selmer variety is expected always to hold for n large, in that we should have [21]

$$\mathrm{dim} H^1_f(G,U_n) << \mathrm{dim} U^{DR}_n/F^0.$$

(Recall that the map $\log_p$ is algebraic.) Such an inequality follows, for example, from the reasonable folklore conjecture that

$$H^1_f(G,M) = 0$$

for a motivic Galois representation[18] M of weight > 0. This, in turn, might be deduced from the conjecture of Fontaine and Mazur on Galois representations of geometric origin [9], or from portions of the Bloch-Kato conjecture[19] [2]. The point is that if we recognized the elements of $H^1_f(G,M)$ themselves to be motivic, then the vanishing would follow from the existence of a weight filtration. Thus instead of the implication

> Non-abelian 'finiteness of Ш' (= *section conjecture*) $\Rightarrow$ finiteness of $X(\mathbb{Q})$.

expected by Grothendieck, we have

> 'Higher abelian finiteness of Ш' (that $H^1_f(G,M)$ is generated by motives)$\Rightarrow$ finiteness of $X(\mathbb{Q})$.

This is not the only place that our considerations revolve around pale shadows of the section conjecture. One notes for example, the critical use of the dense image of $\kappa^u_{dr/cr}$, which could itself be thought of as an 'approximate local section conjecture.'

[17] This proof, involving a straightforward interplay of denseness, non-denseness, and compactness, is a curious avatar of some ideas of Professor Deligne relating the section conjecture to Diophantine finiteness.

[18] It suffices here to take M to be among the motives generated by $H^1(X)$.

[19] We thus have reason, in the manner of physicists, to regard Theorem 1 as good news for mixed motives, in that highly non-trivial real phenomena are among the corollaries of their theory. A small counterpoint to the pessimistic view of Professor Serre.

In spite of all such lucubrations (that fascinate the author and quite likely no one else), we must now face the plain and painful fact that an unconditional proof of the hypothesis for large n (and hence, a new proof of finiteness) can be given only in situations where the image of G inside $\mathrm{Aut}(H_1(\bar{X}, \mathbb{Z}_p))$ is *essentially abelian*. That is, when

-X is an affine hyperbolic of genus zero (say $\mathbf{P}^1 \setminus \{0, 1, \infty\}$) [20];

-$X = E \setminus \{e\}$ for an elliptic curve E with complex multiplication [23];

-(with John Coates) X is compact of genus ≥ 2 and the Jacobian J factors into abelian varieties with potential complex multiplication [3].

The first two cases require a rather obvious modification tailored to the study of integral points, while the two CM cases require p to be split inside the CM fields. Given the intermediate state of the purported application, the reason for persevering in an abstruse investigation of known results might seem obscure indeed. We will return to this point towards the end of the lecture, side-stepping the issue for now in favor of a brief sketch of the methodology, confining our attention to the third class of curves.

There is a pleasant quotient[20]

$$U \longrightarrow\!\!\!\!\!\rightarrow W := U/[[U,U],[U,U]]$$

of U that allows us to extend the key diagrams.

$$\begin{array}{ccccc}
X(\mathbb{Z}_S) & \hookrightarrow & X(\mathbb{Z}_p) & & \\
\downarrow{\scriptstyle \kappa^u_n} & & \downarrow{\scriptstyle \kappa^u_{p,n}} & \searrow^{\kappa^u_{dr/cr,n}} & \\
H^1_f(G, U_n) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_n) & \xrightarrow{D} & U_n^{DR}/F^0 \\
\downarrow & & \downarrow & & \downarrow \\
H^1_f(G, W_n) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, W_n) & \xrightarrow{D} & W_n^{DR}/F^0
\end{array}$$

The structure of W turns out to be much simpler than that of U, and we obtain the following result.

Theorem 2 (with John Coates) *Suppose J is isogenous to a product of abelian varieties having potential complex multiplication. Choose the prime p to split in all the CM fields that occur. Then*

$$dim H^1_f(G, W_n) < dim W_n^{DR}/F^0$$

for n sufficiently large.

The non-denseness of $\log_p(H^1_f(G, U))$ is an obvious corollary.

We give an outline of the proof assuming J is simple. Since

$$\mathrm{dim} H^1_f(G, W_n) \leq \mathrm{dim} H^1(G_T, W_n),$$

it suffices to estimate the dimension of cohomology with restricted ramification. Via the exact sequences

$$0 \to H^1(G_T, W^{n+1} \backslash W^n) \to H^1(G_T, W_n) \to H^1(G_T, W_{n-1})$$

the estimate can be reduced to a sum of abelian ones:

$$\mathrm{dim} H^1(G_T, W_n) \leq \sum_{i=1}^{n} \mathrm{dim} H^1(G_T, W^{i+1} \backslash W^i).$$

[20]For $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, such quotients came up in the process of isolating (simple-)polylogarithms [1].

The linear representations $W^{i+1}\backslash W^i$ come with Euler characteristic formulas[21] [28]:

$$\dim H^0(G_T, W^{i+1}\backslash W^i) - \dim H^1(G_T, W^{i+1}\backslash W^i)$$

$$+\dim H^2(G_T, W^{i+1}\backslash W^i) = -\dim[W^{i+1}\backslash W^i]^-.$$

out of which the H^0 term always vanishes, leaving

$$\dim H^1(G_T, W^{i+1}\backslash W^i) = \dim[W^{i+1}\backslash W^i]^- + \dim H^2(G_T, W^{i+1}\backslash W^i).$$

The comparison with the topological fundamental group of $X(\mathbb{C})$ reveals U to be the unipotent completion of a free group on $2g$ generators modulo a single relation. This fact can applied to construct a Hall basis for the Lie algebra of W [33], from which we get an elementary estimate

$$\sum_{i=1}^{n} \dim[W^{i+1}\backslash W^i]^- \leq [(2g-1)/2]\frac{n^{2g}}{(2g)!} + O(n^{2g-1}).$$

Similarly, on the De Rham side the dimension

$$\dim W_n^{DR}/F^0 = W_2/F^0 + \sum_{i=3}^{n} \dim[W^{DR,i+1}\backslash W^{DR,i}]$$

can easily be bounded below by

$$(2g-2)\frac{n^{2g}}{(2g)!} + O(n^{2g-1}).$$

Hence, since $g \geq 2$, we have

$$\sum_{i=1}^{n} \dim[W^{i+1}\backslash W^i]^- << \dim W_n^{DR}/F^0.$$

Therefore, it remains to show that

$$\sum_{i=1}^{n} \dim H^2(G_T, W^{i+1}\backslash W^i) = O(n^{2g-1}).$$

Standard arguments with Poitou-Tate duality[22] [28] eventually reduces the problem to the study of

$$\mathrm{Hom}_\Gamma[M(-1), \sum_{i=1}^{n}[W^{i+1}\backslash W^i]^*],$$

where

-F contains $\mathbb{Q}(J[p])$ and is a field of definition for all the complex multiplication;

-$\Gamma = \mathrm{Gal}(F_\infty/F)$ for the field

$$F_\infty = F(J[p^\infty])$$

generated by the p-power torsion of J;

-and

$$M = \mathrm{Gal}(H/F_\infty)$$

is the Galois group of the p-Hilbert class field H of F_∞.

[21] The minus sign in the superscript refers to the negative eigenspace of complex conjugation. This has roughly half the dimension of the total space, and ends up unduly important to our estimates.

[22] which switches the focus from H^2 to H^1 at the cost of dealing with some insignificant local terms

Choosing an annihilator[23]

$$\mathcal{L} \in \Lambda := \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T_1, T_2, \ldots, T_{2g}]]$$

for $M(-1)$ in the Iwasawa algebra, we need to count its zeros among the characters that appear in

$$\sum_{i=1}^{n} [W^{i+1} \backslash W^i]^*.$$

If$\{\psi_i\}_{i=1}^{2g}$ are the characters that make up $H^1(\bar{X}, \mathbb{Q}_p)$, the characters in $[W^{i+1}\backslash W^i]^*$ are a subset of

$$\psi_{j_1}\psi_{j_2}\psi_{j_3}\cdots\psi_{j_i},$$

where $j_1 < j_2 \geq j_3 \geq \cdots \geq j_i$. After a change of variables, a lemma of Greenberg [13] allows us to assume a form

$$\mathcal{L} = a_0(T_1, \ldots, T_{2g-1}) + a_1(T_1, \ldots, T_{2g-1})T_{2g} + \cdots$$
$$+a_{l-1}(T_1, \ldots, T_{2g-1})T_{2g}^{l-1} + T_{2g}^{l},$$

a polynomial in T_{2g}. We can estimate the number of zeros by considering instead the $2g-1$ polynomials obtained by fixing the index j_1, and counting their zeros among the set of $\psi_{j_2}\psi_{j_3}\cdots\psi_{j_i}$ with $j_2 \geq j_3 \geq \cdots \geq j_i$. As i runs from 1 to n, the multi-indices in the exponents of

$$\psi_1^{m_1}\psi_2^{m_2}\cdots\psi_{2g}^{m_{2g}}$$

that occur are among the integer points in a simplex of side length $n-1$ in a space of dimension $2g$. But then, since the coefficients a_i depend only on the projection of these integer points to a simplex of one smaller dimension, and the number of zeros lying above each such point is at most l, the total number of zeros is $O(n^{2g-1})$. Since $M(-1)$ is $\Lambda-$finitely-generated, we deduce the bound

$$\mathrm{Hom}_\Gamma[M(-1), \sum_{i=1}^{n} [W^{i+1}\backslash W^i]^*] = O(n^{2g-1})$$

desired. □

We have now set up the first genuine occasion to motivate our constructions. The annihilator $\mathcal{L}$ is a version of an *algebraic p-adic L-function* controlling the situation. It is therefore of non-trivial interest that the sparseness of its zeros is responsible for the finiteness of points. The parallel with the case of elliptic curves [5, 18, 26, 34] might be seen clearly by comparing the implications

non-vanishing of $L \Rightarrow$ control of Selmer groups $\Rightarrow$ finiteness of points

familiar from the arithmetic of elliptic curves to the one given:

sparseness of L-zeros $\Rightarrow$ control of Selmer *varieties* $\Rightarrow$ finiteness of points.

As promised, the motivic fundamental group has provided a natural thread linking abelian and non-abelian Diophantine problems.

We remark that the non-CM case could proceed along the same lines, except that the group Γ and hence, the corresponding Iwasawa algebra is non-abelian. But the fact remains that the estimate

$$\mathrm{dim}\mathrm{Hom}_\Lambda(M, \oplus_{i=1}^{n} W^{i+1}\backslash W^i) = O(n^{2g-1})$$

is sufficient for the analogue of Theorem 2, and hence, for the finiteness of points. The representation $W^{i+1}\backslash W^i$ is a subquotient of the more familiar one

$$(\Lambda^2 V_p) \otimes (\mathrm{Sym}^{i-2} V_p)$$

[23] provided by a theorem of Greenberg [12]

and the difference in dimensions is likely to count for very little in the coarse estimates. It might therefore be easier to work with

$$\mathrm{Hom}_\Lambda[M, \oplus_{i=1}^{n-2}(\Lambda^2 V_p) \otimes (\mathrm{Sym}^i V_p)].$$

Otmar Venjakob [40] has shown that M is locally torsion, so that a generating set $\{m_1, m_2, \ldots, m_d\}$ for M determines for each i a non-commutative power series $f_i \in \Lambda$ annihilating m_i. We must then count the *non-abelian zeros*[24] of f_i, that is, the representations containing vectors annihilated by f_i among the irreducible factors of $\oplus_{i=1}^{n-2}(\Lambda^2 V_p) \otimes (\mathrm{Sym}^i V_p)$.

John Coates has stressed the role played by the ideal class group M in this picture, which is a priori smaller than the Iwasawa module relevant to elliptic curves. The reason that ramification at p can be ignored for now is that the local contribution at p is also of lower order as a function of n. For the Diophantine geometry of abelian fundamental groups, however, the option of passing to large n is absent. One is tempted to offer this as a kind of explanation for the infinitely many rational points that can live on an elliptic curve.

*

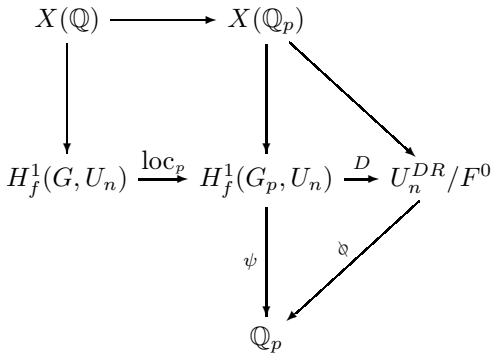
Some preliminary evidence at present suggests another reason to pursue a π_1 approach to finiteness [24]. This is the possibility that the function ϕ occurring in the proof of theorem 1 can be made explicit, leading to analytic defining equations for

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p).$$

For one thing, the map

$$\log_p : H^1_f(G, U_n) \to U_n^{DR}/F^0$$

occurs in the category of algebraic varieties over $\mathbb{Q}_p$, and is therefore amenable (in principle) to computation [6, 32]. Whenever the map itself can be presented, the computation of the image is then a matter of applying standard algorithms. A genuinely *feasible* approach, however, should be effected by the *cohomological construction* of a function ψ as below that vanishes on global classes.



That is, once we have ψ, we can put

$$\phi = \psi \circ D^{-1},$$

a function whose precise computation might be regarded as a 'non-abelian explicit reciprocity law.' The vanishing itself should be explained by a local-to-global reciprocity, as in the work of Kolyvagin, Rubin, and Kato on the conjecture of Birch and Swinnerton-Dyer [26, 34, 18].

[24] As noted by Mahesh Kakde, it would be nice to know enough to formulate this in terms of a characteristic element $f \in K_1(\Lambda_{S^*})$ for M, whereby the count will be of irreducible representations $\rho : \Gamma \to N$ for which $f(\rho) = 0$ [4].

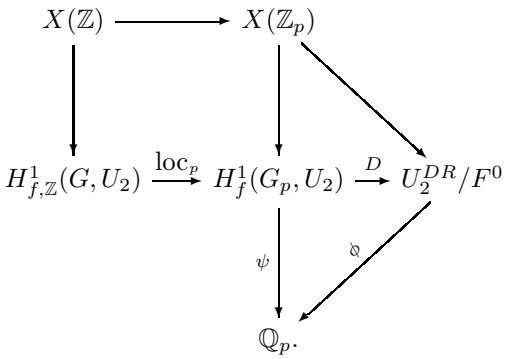
These speculations are best given substance with an example, albeit in an affine setting. Let $X = E \setminus \{e\}$, where E is an elliptic curve of rank 1 with $Ш(E)[p^\infty] = 0$. The significance of the hypotheses is that the $\mathbb{Q}_p$ localization map is bijective on points,

$$loc_p : E(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq H^1_f(G_p, V_p(E)),$$

and the second cohomology with restricted ramification vanishes:

$$H^2(G_T, V_p(E)) = 0.$$

We will construct a diagram:



using just the first non-abelian level U_2 of the unipotent fundamental group. We have introduced here a refined Selmer variety $H^1_{f,\mathbb{Z}}(G, U_2)$ consisting of classes that are actually trivial at all places $l \neq p$. It is a relatively straightforward matter to show that the integral points land in this subspace [25].

The relevant structure now is a Heisenberg group

$$0 \to \mathbb{Q}_p(1) \to U_2 \to V_p \to 0,$$

that we will analyze in terms of the corresponding extension of Lie algebras

$$0 \to \mathbb{Q}_p(1) \to L_2 \to V_p \to 0.$$

Conveniently, at this level, the Galois action on L_2 splits[25]:

$$L_2 = V_p \oplus \mathbb{Q}_p(1),$$

provided we use a tangential base-point at the missing point e. With the identification[26] of U_2 and L_2, non-abelian cochains can be thought of as maps

$$\xi : G_p \longrightarrow L_2$$

and expressed in terms of components $\xi = (\xi_1, \xi_2)$ with respect to the decomposition. The cocycle condition in these coordinates reads[27]

$$d\xi_1 = 0, \qquad d\xi_2 = (-1/2)[\xi_1, \xi_1].$$

[25] This uses the multiplication by $[-1]$, as in Mumford's theory of theta functions.

[26] For unipotent groups, the power series for the log map stops after finitely many terms, defining an algebraic isomorphism. The group then can be thought of as the Lie algebra itself with a twisted binary operation given by the Baker-Campbell-Hausdorff formula [37].

[27] In his book on gerbes, Breen emphasizes the importance of a familiarity with the 'calculus of cochains.' Indeed, the typical number-theorist will be quite anxious about non-closed cochains like ξ_2. Unfortunately, they are as unavoidable as the components of connection forms in non-abelian gauge theory, which obey complicated equations even when the connections themselves are closed in a suitable sense.

Define

$$\psi(\xi) := [\mathrm{loc}_p(x), \xi_1] - 2\log\chi_p \cup \xi_2 \in H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

where

$$\log\chi_p : G_p \to \mathbb{Q}_p$$

is the logarithm of the $\mathbb{Q}_p$-cyclotomic character and x is a *global* solution, to the equation

$$dx = \log\chi_p \cup \xi_1.$$

The equation makes sense on G_T since both χ_p and ξ_1 have natural extensions to global classes, while the non-trivial existence of the global solution

$$x : G_T \to V_p$$

is guaranteed by the aforementioned vanishing of H^2. One checks readily that $\psi(\xi)$ is indeed a 2-cocycle whose class is independent of the choice of x.

Theorem 3 *ψ vanishes on the image of*

$$loc_p : H^1_{f,\mathbb{Z}}(G, U_2) \to H^1_f(G_p, U_2).$$

The proof is a simple consequence of the standard reciprocity sequence

$$0 \to H^2(G_T, \mathbb{Q}_p(1)) \to \oplus_{v\in T} H^2(G_v, \mathbb{Q}_p(1)) \to \mathbb{Q}_p \to 0.$$

The point is that if ξ is global then so is $\psi(\xi)$. But this class has been constructed to vanish at all places $l \neq p$. Hence, it must also vanish at p.

An explicit formula on the De Rham side in this case is rather easily obtained. Choose a Weierstrass equation for E and let

$$\alpha = dx/y, \quad \beta = xdx/y.$$

Define

$$\log_\alpha(z) := \int_b^z \alpha, \quad \log_\beta(z) := \int_b^z \beta,$$

$$D_2(z) := \int_b^z \alpha\beta,$$

via (iterated) Coleman integration.

Corollary 4 *For any two points $y, z \in X(\mathbb{Z}) \subset X(\mathbb{Z}_p)$, we have*

$$\log^2_\alpha(y)(D_2(z) - \log_\alpha(z)\log_\beta(z)) = \log^2_\alpha(z)(D_2(y) - \log_\alpha(y)\log_\beta(y)).$$

The proof uses an action of the multiplicative monoid $\mathbb{Q}_p$ on $H^1_f(G, U_2)$ that covers the scalar multiplication on $E(\mathbb{Q}) \otimes \mathbb{Q}_p$. That is,

$$\lambda \cdot (\xi_1, \xi_2) = (\lambda\xi_1, \lambda^2\xi_2).$$

Evaluating ψ on the class

$$\log_\alpha(x)\kappa^u_2(y) - \log_\alpha(y)\kappa^u_2(x) \in H^1_f(G_p, U^3\backslash U^2)$$

leads directly to the formula displayed. The harmonious form of the resulting constraint is perhaps an excuse for some general optimism. Of course, as it stands, the formula is useful only if there is a point y of infinite order already at hand. One can then look for the other integrals points in the zero set of the function

$$D_2(z) - \log_\alpha(z)\log_\beta(z) - \left(\frac{D_2(y) - \log_\alpha(y)\log_\beta(y)}{\log^2_\alpha(y)}\right)\log^2_\alpha(z)$$

in the coordinate z.

The *meaning* of the construction given is not yet clear to the author, even as some tentative avenues of interpretation are opening up quite recently. If the analogy with the abelian case is to be taken seriously, ψ should be a small fragment of *non-abelian duality* in Galois cohomology[28]. For the abelian quotient, one has the usual duality

$$H^1(G_p, V) \times H^1(G_p, V^*(1)) \longrightarrow H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$$

with respect to which $H^1_f(G_p, V)$ and $H^1_f(G_p, V^*(1))$ are mutual annihilators. We take the view that

$$H^1(G_p, V^*(1))/H^1_f(G_p, V^*(1))$$

is thereby a systematic source of functions on $H^1_f(G_p, V)$, which can then be used to annihilate global classes when the function itself comes from a suitable class[29] in $H^1(G, V^*(1))$. After a minimal amount of non-commutativity has been introduced, our ψ is exactly such a global function on the local cohomology $H^1_f(G_p, U_2)$ that ends up thereby *annihilating the Selmer variety*. The main difficulty is that we know not yet a suitable space in which ψ lives. Allowing ourselves a further flight of fancy, the elusive function in general might eventually be the subject of an Iwawasa theory rising out of a landscape radically more non-abelian and non-linear than we have dared to dream of thus far [19].

*

It has been remarked that the title of this lecture was chosen to be maximally ambiguous. Notice, however, that Galois theory in dimension zero, according to Galois, proposes groups as structures encoding the Diophantine geometry of equations in one variable. The proper subject of Galois theory in dimension one should then be a unified network of structures relevant to the Diophantine geometry of polynomials in two variables. Included therein one may find the arithmetic fundamental groups, motivic L-functions of weight one, and moduli spaces of torsors that have already proved their scattered usefulness to the trade[30]. The picture as a whole is blatantly far from clear, coherent, or complete at this stage [31].

References

[1] Beilinson, A.; Deligne, P. Interprétation motivique de la conjecture de Zagier reliant polylogarithmes et régulateurs. Motives (Seattle, WA, 1991), 97–121, Proc. Sympos. Pure Math., 55, Part 2, Amer. Math. Soc., Providence, RI, 1994.

[28] Kazuya Kato's immediate reaction to the idea of non-abelian duality was that it should have an 'automorphic' nature. Such a suggestion might be highly relevant if the *reductive completion* of fundamental groups could somehow be employed in an arithmetic setting. For the unipotent completions under discussion, the author's inclination is to look for duality that is a relatively straightforward lift of the abelian phenomenon.

[29] The author is not competent to review here the laborious procedure for producing such classes as was developed in the work of Kolyvagin and Kato. The guiding concept in the abelian case is that of a *zeta element*.

[30] The section conjecture says the set of points on a curve of higher genus *is* a moduli space of torsors. One might take this to be a categorical structure that generalizes the abelian groups that come up in elliptic curves.

[31] It has been an enduring source of amazement to the author that true number-theorists employ philosophies that never work in practice as planned at the outset. The numerous subtle twists and turns that one may find, for example, in the beautiful theorems of Richard Taylor, that adhere nevertheless to the overall form of a grand plan, are hallmarks of the kind of artistry that a mere generalist could never aspire to. It is essentially for this reason that the author has avoided thus far the question of applying the techniques of this paper to varieties of higher dimension, for example, those with a strong degree of hyperbolicity. A theory whose end product is a single function applies immediately only in dimension one. It is not inconceivable that an arsenal of clever tricks will strengthen the machinery shown here to make it more broadly serviceable. A robust strategy that makes minimal demands on the user's ingenuity, however, should expect the requisite structures to evolve as one climbs up the dimension ladder, perhaps in a manner reminiscent of Grothendieck's *poursuite*.

[2] Bloch, Spencer; Kato, Kazuya L-functions and Tamagawa numbers of motives. The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math., 86, Birkhäuser Boston, Boston, MA, 1990.

[3] Coates, John; Kim, Minhyong Selmer varieties for curves with CM Jacobians. Available at the mathematics archive, arXiv:0810.3354 .

[4] Coates, John; Fukaya, Takako; Kato, Kazuya; Sujatha, Ramdorai; Venjakob, Otmar The GL_2 main conjecture for elliptic curves without complex multiplication. Publ. Math. Inst. Hautes Études Sci. No. 101 (2005), 163–208.

[5] Coates, J.; Wiles, A. On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39 (1977), no. 3, 223–251.

[6] Coleman, Robert F. Effective Chabauty. Duke Math. J. 52 (1985), no. 3, 765–770.

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

[8] Fontaine, Jean-Marc Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate. Ann. of Math. (2) 115 (1982), no. 3, 529–577.

[9] Fontaine, Jean-Marc; Mazur, Barry Geometric Galois representations. Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[10] Furusho, Hidekazu p-adic multiple zeta values. I. p-adic multiple polylogarithms and the p-adic KZ equation. Invent. Math. 155 (2004), no. 2, 253–286.

[11] Goldman, William M.; Millson, John J. The deformation theory of representations of fundamental groups of compact Kähler manifolds. Inst. Hautes Études Sci. Publ. Math. No. 67 (1988), 43–96.

[12] Greenberg, Ralph The Iwasawa invariants of Γ-extensions of a fixed number field. Amer. J. Math. 95 (1973), 204–214.

[13] Greenberg, Ralph On the structure of certain Galois groups. Invent. Math. 47 (1978), no. 1, 85–99.

[14] Grothendieck, Alexander Brief an G. Faltings. London Math. Soc. Lecture Note Ser., 242, Geometric Galois actions, 1, 49–58, Cambridge Univ. Press, Cambridge, 1997.

[15] Hain, Richard M. The de Rham homotopy theory of complex algebraic varieties. I. K-Theory 1 (1987), no. 3, 271–324.

[16] Iyanaga, Shokichi Memories of Professor Teiji Takagi [1875–1960]. Class field theory—its centenary and prospect (Tokyo, 1998), 1–11, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

[17] Motives. Proceedings of the AMS-IMS-SIAM Joint Summer Research Conference held at the University of Washington, Seattle, Washington, July 20–August 2, 1991. Edited by Uwe Jannsen, Steven Kleiman and Jean-Pierre Serre. Proceedings of Symposia in Pure Mathematics, 55, Part 1. American Mathematical Society, Providence, RI, 1994. xiv+747 pp. ISBN: 0-8218-1636-5

[18] Kato, Kazuya p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques. III. Astérisque No. 295 (2004), ix, 117–290.

[19] Kato, Kazuya Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. I. Arithmetic algebraic geometry (Trento, 1991), 50–163, Lecture Notes in Math., 1553, Springer, Berlin, 1993.

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

[21] Kim, Minhyong The unipotent Albanese map and Selmer varieties for curves. Publ. Res. Inst. Math. Sci. 45 (2009), no. 1, 89–133. (Proceedings of special semester on arithmetic geometry, Fall, 2006.)

[22] Kim, Minhyong Remark on fundamental groups and effective Diophantine methods for hyperbolic curves. To be published in Serge Lang memorial volume. Available at mathematics archive, arXiv:0708.1115.

[23] Kim, Minhyong p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication. Preprint (2007). Available at mathematics archive: arXiv:0710.5290

[24] Kim, Minhyong Massey products for elliptic curves of rank 1. Preprint (2009) arXiv:0901.4668. To be published in J. Amer. Math. Soc.

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

[26] Kolyvagin, Victor A. On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves. Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), 429–436, Math. Soc. Japan, Tokyo, 1991.

[27] Mumford, David; Fogarty, John Geometric invariant theory. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete, 34. Springer-Verlag, Berlin, 1982. xii+220 pp.

[28] Milne, J. S. Arithmetic duality theorems. Perspectives in Mathematics, 1. Academic Press, Inc., Boston, MA, 1986.

[29] Nakamura, Hiroaki; Tamagawa, Akio; Mochizuki, Shinichi The Grothendieck conjecture on the fundamental groups of algebraic curves [translation of Su-gaku 50 (1998), no. 2, 113–129; MR1648427 (2000e:14038)]. Sugaku Expositions. Sugaku Expositions 14 (2001), no. 1, 31–53.

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

[31] Olsson, Martin The bar construction and affine stacks. Preprint. Available at http://math.berkeley.edu/ molsson/.

[32] Poonen, Bjorn Computing rational points on curves. Number theory for the millennium, III (Urbana, IL, 2000), 149–172, A K Peters, Natick, MA, 2002.

[33] Reutenauer, Christophe Free Lie algebras. London Mathematical Society Monographs. New Series, 7. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1993.

[34] Rubin, Karl The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent. Math. 103 (1991), no. 1, 25–68.

[35] Serre, Jean-Pierre Galois cohomology. Translated from the French by Patrick Ion and revised by the author. Springer-Verlag, Berlin, 1997. x+210 pp.

[36] Serre, Jean-Pierre André Weil 6 May 1906-6 August 1998 Biographical Memoirs of Fellows of the Royal Society, Vol. 45, (Nov., 1999), pp. 521–529

[37] Serre, Jean-Pierre Lie algebras and Lie groups. 1964 lectures given at Harvard University. Second edition. Lecture Notes in Mathematics, 1500. Springer-Verlag, Berlin, 1992. viii+168 pp.

[38] Simpson, Carlos T. Higgs bundles and local systems. Inst. Hautes Études Sci. Publ. Math. No. 75 (1992), 5–95.

[39] Szamuely, Tamas *Galois Groups and Fundamental Groups*. Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, 2009.

[40] Venjakob, Otmar On the Iwasawa theory of p-adic Lie extensions. Compositio Math. 138 (2003), no. 1, 1–54.

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

[42] Weil, André Généralisation des fonctions abéliennes. J. Math Pur. Appl. 17 (1938), no. 9, 47–87.

Department of Mathematics, University College London, Gower Street, London, WC1E 6BT, United Kingdom and The Korea Institute for Advanced Study, Hoegiro 87, Dongdaemun-gu, Seoul 130-722, Korea