数理解析研究所講究録 1267 巻 2002 年 96-111

Anabelian Geometry in the Hodge-Arakelov Theory of Elliptic Curves

SHINICHI MOCHIZUKI (望月 新一)

RIMS, Kyoto University (京都大学数理解析研究所)

Abstract:

The purpose of the present manuscript is to survey some of the main ideas that appear in recent research of the author on the topic of applying *anabelian geometry* to construct a *"global multiplicative subspace"* — i.e., an analogue of the well-known (local) multiplicative subspace of the Tate module of a degenerating elliptic curve. Such a global multiplicative subspace is necessary to apply the *Hodge-Arakelov theory of elliptic curves* ([Mzk1-5]; also cf. [Mzk6], [Mzk7] for a survey of this theory) — i.e., a sort of "Hodge theory of elliptic curves" analogous to the classical *complex and p-adic* Hodge theories, but which exists in the *global arithmetic framework of Arakelov theory* — to obtain results in *diophantine geometry.* Unfortunately, since this research is still in progress, the author is not able at the present time to give a complete, polished treatment of this theory.

Contents:

Section 1: Multiplicative Subspaces and Hodge-Arakelov Theory

At a technical level, the *Hodge-Arakelov theory of elliptic curves* may in some sense be summarized as the arithmetic theory of the *theta function*

$$\Theta = \sum_{n \in \mathbb{Z}} q^{\frac{1}{2}n^2} \cdot U^n$$

and its *logarithmic derivatives* $(U \cdot \partial/\partial U)^r \Theta$. Here, we think of the elliptic curve in question as the *"complex analytic Tate curve"*

$$E \stackrel{\text{def}}{=} \mathbb{C}^\times / q^{\mathbb{Z}}$$

where $q \in \mathbb{C}^\times$ satisfies $|q| < 1$. Note that this representation of E as a quotient of $\mathbb{C}^\times$ induces a *natural exact sequence on the singular homology* of E:

$$0 \to 2\pi i \cdot \mathbb{Z} = H_1^{\text{sing}}(\mathbb{C}^\times, \mathbb{Z}) \to H_1^{\text{sing}}(E, \mathbb{Z}) \to \mathbb{Z} \to 0$$

We shall refer to the subspace $\text{Im}(2\pi i \cdot \mathbb{Z}) \subseteq H_1^{\text{sing}}(E, \mathbb{Z})$ as the *multiplicative subspace* of $H_1^{\text{sing}}(E, \mathbb{Z})$, and to the generator $1 \in \mathbb{Z}$ (well-defined up to multiplication by ± 1) of the quotient of $H_1^{\text{sing}}(E, \mathbb{Z})$ by the multiplicative subspace as the *canonical generator* of this quotient.

It is not difficult to see that the multiplicative subspace and canonical generator constitute the *essential data* necessary to represent the theta function as a series in q and U. Without this representation, it is extremely difficult to perform explicit calculations concerning Θ and its derivatives. Indeed, it is (practically) no exaggeration to state that *all the main results of Hodge-Arakelov theory are, at some level, merely formal consequences of this series representation* — i.e., of the existence of the *multiplicative subspace/canonical generator* (and its arithmetic analogues).

Since, ultimately, however, we wish to "do arithmetic," it is necessary to be able to consider the analogue of the above discussion in various arithmetic situations. The most basic arithmetic situation in which such an analogue exists is the following. Write $A \stackrel{\text{def}}{=} \mathbb{Z}[[q]] \otimes_{\mathbb{Z}} \mathbb{Q}[q^{-1}]$ (where q is an indeterminate). Write

$$E \stackrel{\text{def}}{=} \text{`}\mathbb{G}_m / q^{\mathbb{Z}}\text{'}$$

for the *Tate curve* over A. Then the structure of E as a (rigid analytic) quotient of $\mathbb{G}_m$ gives rise to an *exact sequence*

$$0 \to \boldsymbol{\mu}_d \to E[d] \to \mathbb{Z}/d\mathbb{Z} \to 0$$

involving the group scheme $E[d]$ (over A) of d-torsion points, for some integer $d \geq 1$. This exact sequence is a "q-analytic" analogue of the complex analytic exact sequence considered above. We shall refer to the image $\text{Im}(\boldsymbol{\mu}_d) \subseteq E[d]$ (respectively, generator $1 \in \mathbb{Z}/d\mathbb{Z}$, well-defined up to multiplication by ± 1) as the *multiplicative subspace* (respectively, *canonical generator*) of $E[d]$.

Since much of the Hodge-Arakelov theory of elliptic curves deals with the values of Θ and its derivatives on the d-torsion points, it is not surprising that this multiplicative subspace/canonical generator play an *important role* in Hodge-Arakelov theory, especially from the point of view of *"eliminating Gaussian poles"* (cf. [Mzk2]; [Mzk6], §1.5.1).

Note that by pulling back the objects constructed above over A, one may construct a multiplicative subspace/canonical generator for *any Tate curve over a p-adic local field*, e.g., a completion $F_{\mathfrak{p}}$ of a *number field* F at a *finite prime* $\mathfrak{p}$. Ultimately, however, to apply Hodge-Arakelov theory to diophantine geometry, it is necessary to construct a multiplicative subspace/canonical generator not just over such local fields, but *globally over a number field.* It turns out that this is a *highly nontrivial enterprise*, which requires, in an essential way, the use of *anabelian geometry*, as will be described below.

Section 2: Basepoints in Motion

In this §, we let F be a *number field* and consider an *elliptic curve* E over $\mathcal{G} \stackrel{\text{def}}{=} \text{Spec}(F)$ with *bad, multiplicative reduction* at a finite prime $\mathfrak{p}_{\mathcal{G}}$ of F. Write

$$\mathcal{N} \to \mathcal{G}$$

for the finite Galois étale covering of *trivializations* $(\mathbb{Z}/d\mathbb{Z})^2 \xrightarrow{\sim} E[d]$ of the finite étale group scheme of d-torsion points $E[d]$; denote the finite étale local system determined by $E[d]$ over $\mathcal{G}$ (respectively, $\mathcal{N}$) by $\mathcal{E}_{\mathcal{G}}$ (respectively, $\mathcal{E}_{\mathcal{N}}$). Also, for simplicity, we *assume* that $\mathcal{N}$ is *connected* (an assumption which holds, for instance, whenever d is a power of a sufficiently large prime number).

Note that there is a *tautological trivialization* $(\mathbb{Z}/d\mathbb{Z})^2 \xrightarrow{\sim} E[d]$ of $E[d]$ over $\mathcal{N}$. By applying this tautological trivialization to the elements "$(1,0)$" and "$(0,1)$," respectively, we obtain — just as a matter of *"general nonsense,"* i.e., without applying any difficult results from anabelian geometry — a *submodule/generator* (of the quotient by the submodule) of $\mathcal{E}_{\mathcal{N}}$. Now, let us *choose* a prime of $\mathcal{N}$

$$\mathfrak{p}_{\circledast}$$

lying over $\mathfrak{p}_{\mathcal{G}}$ with the property that *this* submodule/generator *coincides* with the multiplicative subspace/canonical generator (cf. §1) at $\mathfrak{p}_{\mathcal{G}}$. (One verifies easily that such a $\mathfrak{p}_{\circledast}$ always *exists.*) Denote this data of submodule/generator of $\mathcal{E}_{\mathcal{N}}$ by:

$$\mathcal{L}_{\circledast,\mathcal{N}} \subseteq \mathcal{E}_{\mathcal{N}}; \quad \gamma_{\circledast,\mathcal{N}}$$

Note that although the restricted data

$$\mathcal{L}_{\circledast,\mathcal{N}}|_{\mathfrak{p}_{\circledast}}; \quad \gamma_{\circledast,\mathcal{N}}|_{\mathfrak{p}_{\circledast}}$$

is (by construction) *multiplicative/canonical* at $\mathfrak{p}_{\circledast}$, at *"most"* of the primes $\mathfrak{p}_{\mathcal{N}}$ of $\mathcal{N}$ lying over $\mathfrak{p}_{\mathcal{G}}$, the restricted data will *not* be multiplicative/canonical. Thus:

> At first glance, the goal of constructing a submodule/generator which is *"always multiplicative/canonical"* globally over all of $\mathcal{N}$ appears to be hopeless.

In fact, however, in the theory of [Mzk16], we wish to *think about things in a different way* from the "naive" approach just described.

Namely, in addition to the *original (set-theoretic) universe*

$$\circledast$$

in which we have been working up until now — which we shall also often refer to as the *"base universe"* — we would also like to consider *another distinct, independent universe* in which *"equivalent/analogous, but* **not equal***"* objects are constructed. This analogous, but distinct universe will be referred to as the *reference universe*:

$$\circledcirc$$

The analogous objects belonging to the reference universe will be denoted by a *subscript* $\circledcirc$: e.g., $\mathcal{G}_{\circledcirc}$, $\mathcal{N}_{\circledcirc}$, etc.

Then *instead* of thinking of the primes

$$\mathfrak{p}_{\mathcal{N}}$$

of $\mathcal{N}$ which lie over $\mathfrak{p}_{\mathcal{G}}$ as primes at which one is to restrict $\mathcal{L}_{\circledast,\mathcal{N}}$; $\gamma_{\circledast,\mathcal{N}}$ to see if they are canonical (i.e., multiplicative/canonical), we think of these points as *parametrizing the possible relationships between the $\mathcal{N}$ of the "original universe" and the $\mathcal{N}_{\circledcirc}$ of the "reference universe."* That is to say, assuming for the moment that there is a *canonical identification* between $\mathcal{G}$ and $\mathcal{G}_{\circledcirc}$ — a fact which is not obvious (or indeed true, without certain further assumptions — cf. Example 3.2 in §3 below), but is, in fact, a highly nontrivial consequence of the methods introduced in §3 — then $\mathfrak{p}_{\mathcal{N}}$ parametrizes *that particular relationship*

$$\text{“}\alpha[\mathfrak{p}_{\mathcal{N}}; \mathfrak{p}_{\circledcirc}]\text{”}$$

(well-defined up to an ambiguity described by the action of the *decomposition subgroup* in $\mathrm{Gal}(\mathcal{N}/\mathcal{G})$ determined by $\mathfrak{p}_{\mathcal{N}}$) between $\mathcal{N}$, $\mathcal{N}_{\circledcirc}$ that *associates the prime $\mathfrak{p}_{\mathcal{N}}$ of $\mathcal{N}$ to the prime $\mathfrak{p}_{\circledcirc}$ of $\mathcal{N}_{\circledcirc}$*. Moreover:

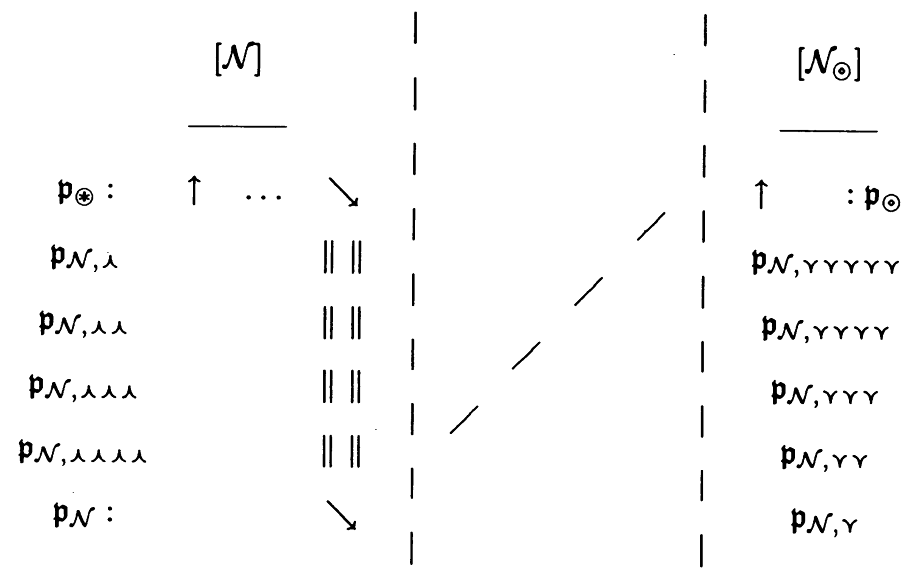
> *Relative to the relationship "$\alpha[\mathfrak{p}_{\mathcal{N}}; \mathfrak{p}_{\circledcirc}]$" parametrized by $\mathfrak{p}_{\mathcal{N}}$, the data (submodule/generator) on $\mathcal{N}_{\circledcirc}$ determined by $\mathcal{L}_{\circledast,\mathcal{N}}|_{\mathfrak{p}_{\mathcal{N}}}$; $\gamma_{\circledast,\mathcal{N}}|_{\mathfrak{p}_{\mathcal{N}}}$* **are** *multiplicative/canonical at the "basepoint" $\mathfrak{p}_{\circledcirc}$ of $\mathcal{N}_{\circledcirc}$.*

In other words:

> *By allowing, in effect, the "basepoint in question" to* **vary**, *we obtain globally canonical data in the sense that* $\mathcal{L}_{\circledast,\mathcal{N}}|_{\mathfrak{p}_{\mathcal{N}}}$; $\gamma_{\circledast,\mathcal{N}}|_{\mathfrak{p}_{\mathcal{N}}}$ *are always canonical,* **relative to the basepoint parametrized by** $\mathfrak{p}_{\mathcal{N}}$.

This is the reason why it is necesary to introduce the *"reference universe"* — i.e., in order to have an *alternative arena* in which to consider a *"distinct, independent basepoint"* (i.e., $\mathfrak{p}_{\circledcirc}$) from the "original basepoint" $\mathfrak{p}_{\circledast}$ of $\mathcal{N}$, relative to which the data in question becomes canonical. Note that once one introduces a distinct, independent reference universe, it is a *tautology* — by essentially the same reasoning as that of *"Russell's paradox"* concerning the "set of all sets" — that *all possible relationships* "$\alpha[\mathfrak{p}_{\mathcal{N}}; \mathfrak{p}_{\circledcirc}]$" between these two universes do, in fact, occur.

We refer to the *figure* below for a *pictorial representation* of the situation just described:



In this depiction, the "$\mathfrak{p}$'s" denote various *primes* in $\mathcal{N}$, $\mathcal{N}_{\circledcirc}$ lying over $\mathfrak{p}_{\mathcal{G}}$, $(\mathfrak{p}_{\mathcal{G}})_{\circledcirc}$; the arrows denote *"directions"* in $\mathcal{E}_{\mathcal{N}}$, $\mathcal{E}_{\mathcal{N}_{\circledcirc}}$; the arrow shown closest to a ":" is to be understood to represent the *multiplicative subspace* at the prime on the other side of the ":"; the area set out on the left (respectively, right) is to be taken to represent the *base universe* (respectively, *reference universe*); the diagonal dotted line between these two universes is to be taken to be the equivalence "$\alpha[\mathfrak{p}_{\mathcal{N}}; \mathfrak{p}_{\circledcirc}]$" discussed above; the "|| ||'s" are to be taken to represent *parallel transport* of arrows — which is possible since the local system $\mathcal{E}_{\mathcal{N}}$ is *trivial*, and $\mathcal{N}$ is *connected.*

On the other hand, once one introduces such a distinct, independent universe, the task of *relating events in the new universe in an orderly, consistent way to events in the old* becomes highly nontrivial. This is the role played by the introduction of ideas motivated by *anabelian geometry*, to be described below in §3, 4.

Section 3: Anabelioids and Cores

A *connected anabelioid* is simply a *Galois category* (in the classical language of [SGA1], Exposé V). In general, we will also wish to consider *arbitrary anabelioids*, which have finitely many connected components, each of which is a connected anabelioid. Thus, in the language of [SGA1], Exposé V, §9, an anabelioid is a *multi-Galois category.*

Thus, an anabelioid is a *topos* — hence, in particular, a *(1-)category* — satisfying certain properties. Moreover, the finite set of connected components of an anabelioid, as well as the connected anabelioid corresponding to each element of this set, may be *recovered entirely category-theoretically* from the original anabelioid.

Suppose that we work in a *universe* $\circledast$ in which we are given a *small category of sets* $\mathfrak{Ens}$. Let G be a *small profinite group.* Then the category

$$\mathcal{B}(G)$$

of sets in $\mathfrak{Ens}$ equipped with a *continuous G-action* is a connected anabelioid. In fact, every connected anabelioid is equivalent to $\mathcal{B}(G)$ for some G.

Another familiar example from *scheme theory* is the following. Let X be a (small) *connected locally noetherian scheme.* Denote by

$$\text{Ét}(X)$$

the *category* whose *objects* are (small) finite étale coverings of X and whose *morphisms* are X-morphisms of schemes. Then it is well-known (cf. [SGA1], Exposé V, §7) that Ét(X) is a connected *anabelioid.*

Note that since an anabelioid is a 1-category, the *"category of anabelioids"* naturally forms a *2-category*. In particular, if G and H are profinite groups, then one verifies easily that the *(1-)category of morphisms*

$$\text{Mor}(\mathcal{B}(G), \mathcal{B}(H))$$

is equivalent to the category whose *objects* are continuous homomorphisms of profinite groups $\psi : G \to H$, and whose *morphisms* from an object $\psi_1 : G \to H$ to an object $\psi_2 : G \to H$ are the elements $h \in H$ such that $\psi_2(g) = h \cdot \psi_1(g) \cdot h^{-1}$, $\forall g \in G$.

At this point, the reader might wonder *why* the author felt the need to introduce the terminology *"anabelioid,"* instead of using the term "multi-Galois category" of [SGA1]. The main reason for the introduction of this terminology is that we wish to emphasize that we would like to think of anabelioids $\mathcal{X}$ as *generalized spaces* — which is natural since they are, after all, *topoi* — whose geometry just happens to be *"completely determined by their fundamental groups"* (albeit somewhat tautologically! — cf. the preceding paragraph). This is meant to recall the notion of an *anabelian variety*, i.e., a variety whose geometry is determined by its fundamental group. The point here is that:

> *The introduction of anabelioids allows us to work with both "algebro-geometric anabelioids" (i.e., anabelioids arising as the "*Ét$(-)$*" of an (anabelian) variety) and "abstract anabelioids" (i.e., those which do not necessarily arise from an (anabelian) variety) as* **geometric objects** *on an equal footing.*

The reason that it is important to deal with "geometric objects" $\mathcal{B}(G)$ as opposed to (profinite) groups G, is that:

> *We wish to study what happens as one* **varies the basepoint** *of one of these geometric objects (cf. §2).*

That is to say, groups are determined only once one *fixes* a basepoint. Thus, it is difficult to describe what happens when one varies the basepoint solely in the language of groups.

Next, we introduce some terminology, as follows: A morphism of connected anabelioids

$$\mathcal{X} \to \mathcal{Y}$$

is *finite étale* if it is equivalent to a morphism of the form $\mathcal{B}(H) \to \mathcal{B}(G)$, induced by applying "$\mathcal{B}(-)$" to the natural injection of an *open subgroup* H of G into G. A morphism of anabelioids is *finite étale* if the induced morphisms from the various connected components of the domain to the various connected components of the range are all finite étale. A finite étale morphism of anabelioids is a *covering* if it induces a surjection on connected components. A profinite group G is *slim* if the centralizer $Z_G(H)$ of any open subgroup $H \subseteq G$ in G is trivial. An anabelioid $\mathcal{X}$ is *slim* if the fundamental group $\pi_1(\mathcal{X}_i)$ of every connected component $\mathcal{X}_i$ of $\mathcal{X}$ is slim. A 2-category is *slim* if the automorphism group of every 1-arrow in the 2-category is trivial.

In general, if $\mathcal{C}$ is a *slim 2-category*, we shall write

$$|\mathcal{C}|$$

for the *associated* 1*-category* whose *objects* are objects of $\mathcal{C}$ and whose *morphisms* are *isomorphism classes* of morphisms of $\mathcal{C}$.

Finite étale morphisms of anabelioids are easiest to understand when the anabelioids in question are *slim*. Indeed, let $\mathcal{X}$ be a *slim* anabelioid. Write

$$\mathfrak{Et}(\mathcal{X})$$

for the 2-category whose *objects* are finite étale morphisms $\mathcal{Y} \to \mathcal{X}$ and whose *morphisms* are finite étale arrows $\mathcal{Y}_1 \to \mathcal{Y}_2$ over $\mathcal{X}$. Then the 2-category $\mathfrak{Et}(\mathcal{X})$ is *slim*. Moreover, if we write $\text{Ét}(\mathcal{X}) \stackrel{\text{def}}{=} |\mathfrak{Et}(\mathcal{X})|$, then the functor

$$\begin{aligned} \mathfrak{F}_{\mathcal{X}} : \mathcal{X} &\to \text{Ét}(\mathcal{X}) \\ S &\mapsto (\mathcal{X}_S \to \mathcal{X}) \end{aligned}$$

(where S is an object of $\mathcal{X}$; $\mathcal{X}_S$ denotes the category whose objects are arrows $T \to S$ in $\mathcal{X}$, and whose morphisms between $T \to S$ and $T' \to S$ are S-morphisms $T \to T'$; $\mathcal{X}_S \to \mathcal{X}$ is the natural "forgetful functor") is an *equivalence*.

Next, let us write

$$\mathfrak{Loc}(\mathcal{X})$$

for the 2*-category* whose *objects* are anabelioids $\mathcal{Y}$ that admit a finite étale morphism to $\mathcal{X}$, and whose *morphisms* are finite étale morphisms $\mathcal{Y}_1 \to \mathcal{Y}_2$ (that do not necessarily lie over $\mathcal{X}$!). Then it follows from the assumption that $\mathcal{X}$ is slim that $\mathfrak{Loc}(\mathcal{X})$ is also *slim*. Write:

$$\text{Loc}(\mathcal{X}) \stackrel{\text{def}}{=} |\mathfrak{Loc}(\mathcal{X})|$$

Perhaps the most fundamental notion underlying the theory of [Mzk16] is that of a "core." We shall say that a slim anabelioid $\mathcal{X}$ is a *core* if $\mathcal{X}$ is a *terminal object* in the (1-)category $\text{Loc}(\mathcal{X})$.

Here we make the important observation that the *definability of* $\mathfrak{Loc}(\mathcal{X})$ is one of the most *fundamental differences* between the theory of finite étale coverings of *anabelioids* as presented in the present manuscript and the theory of finite étale coverings from the point of view of *"Galois categories,"* as given in [SGA1]. Indeed, from the point of view of the theory of [SGA1], it is only possible to consider "$\text{Ét}(\mathcal{X})$" — i.e., finite étale coverings and morphisms that *always lie over* $\mathcal{X}$. That is to say, in the context of the theory of [SGA1], it is not possible to consider diagrams such as:

$$\begin{array}{ccc} & \mathcal{Z} & \\ \swarrow & & \searrow \\ \mathcal{X} & & \mathcal{Y} \end{array}$$

(where the arrows are finite étale) that do *not necessarily lie over any specific geometric object*, as is necessary for the definition of $\mathfrak{Loc}(\mathcal{X})$. We shall refer to such a diagram as a *correspondence* or *isogeny* between $\mathcal{X}$ and $\mathcal{Y}$.

Here, we wish to emphasize that the reason that cores play a *key role* in the theory of [Mzk16] is that:

(Up to renaming) cores have essentially **only one basepoint**.

Indeed, this is essentially a formal consequence of the definition of a core. The reason that this property of "having essentially only one basepoint" is important is that it means that even if we consider (cf. the discussion of §2) *distinct copies* of a core that belong to *distinct, independent universes*, we may still identify their basepoints without fear of confusion or inconsistencies — such as *"Russell's paradox"* concerning the "set of all sets." That is to say, cores allow us to "navigate between universes" without "getting lost." We refer to this phenomenon as *"anabelian navigation."*

Moreover, even for (slim) anabelioids that are *not* cores, we may still perform a sort of anabelian navigation by "measuring the distance of such anabelioids from a core." Thus, even though for such non-cores, it is not possible to *completely* identify basepoints of copies of the object belonging to distinct, independent universes without confusion (as in the case of cores), we can nevertheless identify basepoints of copies of such non-cores *up to a controllable ambiguity* (cf. the "$\alpha[\mathfrak{p}_{\mathcal{N}}; \mathfrak{p}_{\odot}]$'s" of §2), which is often sufficient for applications that we have in mind.

Finally, we close this § by presenting some *examples of cores* (and non-cores), all of which are of *central* importance in the theory of [Mzk16]. Since these examples involve schemes, in order to discuss them in an orderly fashion, it is necessary to have a definition of "Loc$(-)$" for schemes, as well. Let X be a *connected noetherian regular scheme.* Then let us write

$$\mathrm{Loc}(X)$$

for the *(1-)category* whose *objects* are schemes Y that admit a finite étale morphism to X, and whose *morphisms* are finite étale morphisms $Y_1 \to Y_2$ (that do not necessarily lie over X!).

Example 3.1. Number Fields. Perhaps the most *basic example* of a core is the (slim) anabelioid

$$\mathcal{X} \stackrel{\mathrm{def}}{=} \text{Ét}(\mathbb{Q})$$

(where $\mathbb{Q}$ is the rational number field; and $\text{Ét}(\mathbb{Q}) \stackrel{\mathrm{def}}{=} \text{Ét}(\text{Spec}(\mathbb{Q}))$). That $\mathcal{X}$ is a core follows formally from: (i) the fact that $\text{Spec}(\mathbb{Q})$ is a terminal object in $\text{Loc}(\mathbb{Q})$; (ii) the theorem of Neukirch-Uchida-Iwasawa-Ikeda (cf. [NSW], Chapter XII, §2) on the *anabelian nature* of number fields. Note, on the other hand, that if F is a *number field* (i.e., finite extension of $\mathbb{Q}$) which is not equal to $\mathbb{Q}$, then

$$\text{Ét}(F)$$

is *not* a core. Indeed, this follows (via the theorem of Neukirch-Uchida-Iwasawa-Ikeda) from the easily verified fact that $\text{Spec}(F)$ is *not* a terminal object in the category $\text{Loc}(F)$.

Example 3.2. Non-arithmetic Hyperbolic Curves. Let K be a *field of characteristic* 0. Let X_K be a *hyperbolic curve* over K (i.e., the complement of a divisor of degree r in a smooth, proper, geometrically connected curve of genus g over K, such that $2g-2+r > 0$). In fact, more generally, one may take X_K to be a *hyperbolic orbicurve* over K (i.e., the quotient *in the sense of stacks* of a hyperbolic curve by the action of finite group, where we assume that the finite group acts *freely* on a dense open subscheme of the curve). Also, we assume that we have been given an *algebraic closure* $\overline{K}$ of K and write $X_{\overline{K}} \stackrel{\mathrm{def}}{=} X_K \otimes_K \overline{K}$.

We will say that X_K is a *geometric core* (cf. the term "hyperbolic core" of [Mzk11], §3) if $X_{\overline{K}}$ is a *terminal object* in $\text{Loc}(X_{\overline{K}})$ (where, in the case of orbicurves, we allow the objects of $\text{Loc}(X_{\overline{K}})$ to be orbicurves that admit a finite étale morphism to $X_{\overline{K}}$). We will say that X_K is *arithmetic* (cf. [Mzk11], §2) if it is *isogenous* to a Shimura curve (i.e., some finite étale covering of X_K is isomorphic to a finite étale covering of a Shimura curve). As is shown in [Mzk11], §3, if X_K is *non-arithmetic*, then there exists a hyperbolic orbicurve Z_K together with a finite étale morphism $X_K \to Z_K$ such that Z_K is a *geometric core*. Moreover, (cf. [Mzk11], Theorem B) in the case of hyperbolic curves of type (g,r), where $2g-2+r \geq 3$, a *general* curve of that type is a *geometric core*.

Suppose that X_K is a *geometric core*; and that K is a *number field* which is a *minimal field of definition* for X_K. Then it follows formally from the *theorem of Neukirch-Uchida-Iwasawa-Ikeda* (cf. Example 3.1), together with the *"Grothendieck Conjecture for algebraic curves"* (cf. [Tama]; [Mzk13]; [Mzk15]) that the *(slim) anabelioid*

$$\text{Ét}(X_K)$$

is a *core*.

Example 3.3. Arithmetic Hyperbolic Curves. On the other hand, an *arithmetic curve* X_K (notation as in the last paragraph of Example 3.2) is *never* *a geometric core.* For instance, consider the hyperbolic orbicurve X_K given by the *moduli stack of "hemi-elliptic orbicurves"* (i.e., orbicurves obtained by forming the quotient (in the sense of stacks) of an elliptic curve by the action of ± 1). Then the existence of the well-known *Hecke correspondences* on X_K shows that $X_{\overline{K}}$ is "far from being" a terminal object in $\mathrm{Loc}(X_{\overline{K}})$. Thus, in particular, the *(slim) anabelioid*

$$\acute{\mathrm{E}}\mathrm{t}(X_K)$$

will *never* be a core in this case.

Section 4: Holomorphic Structures and Commensurable Terminality

Sometimes, when considering the extent to which an anabelioid is a core, it is natural not to consider *all* finite étale morphisms (as in the definition of $\mathfrak{Loc}(-)$), but instead to *restrict* our attention to finite étale morphisms that *preserve some auxiliary structure.* In some sense, the two main *motivating examples* of this phenomenon are the following:

Example 4.1. Complex Holomorphic Structures. Let X be a *hyperbolic orbicurve* (cf. Example 3.2) over the field of complex numbers $\mathbb{C}$. Write X^{an} for the *associated Riemann surface* (or one-dimensional complex analytic stack). Then we may consider the *"complex analytic analogue"*

$$\mathcal{X} \stackrel{\mathrm{def}}{=} \acute{\mathrm{E}}\mathrm{t}^{\mathrm{an}}(X^{\mathrm{an}})$$

of $\acute{\mathrm{E}}\mathrm{t}(X)$, namely, the *category of local systems* (in the complex topology) on X^{an}. Just as in the case of anabelioids, one may consider finite étale coverings of $\mathcal{X}$, hence also the category:

$$\mathrm{Loc}(\mathcal{X})$$

On the other hand, it is easy to see that this category is "too big" to be of interest. Instead, it is more natural to do the following: The well-known *uniformization* of X^{an} by the *upper half plane* determines a homomorphism of the (usual topological) fundamental group $\pi_1^{\mathrm{top}}(X^{\mathrm{an}})$ of X^{an} into $PSL_2(\mathbb{R})$. This homomorphism determines a *local system of $PSL_2(\mathbb{R})$-torsors* on X^{an}, hence an object $Q_{\mathcal{X}} \in \mathcal{X}$. Then, if we regard finite étale coverings $\mathcal{Y} \to \mathcal{X}$ as always being *equipped with the auxiliary structure* $Q_{\mathcal{Y}}$ determined by pulling back $Q_{\mathcal{X}}$ to $\mathcal{Y}$ and then define $\mathfrak{Loc}^{\mathfrak{hol}}(\mathcal{X})$ to be the 2-category whose objects are such $(\mathcal{Y}, Q_{\mathcal{Y}})$ and whose morphisms $(\mathcal{Y}_1, Q_{\mathcal{Y}_1}) \to (\mathcal{Y}_2, Q_{\mathcal{Y}_2})$ are finite étale morphisms $\mathcal{Y}_1 \to \mathcal{Y}_2$ for which the pull-back of $Q_{\mathcal{Y}_2}$ is isomorphic to $Q_{\mathcal{Y}_1}$, then we obtain a slim 2-category $\mathfrak{Loc}^{\mathfrak{hol}}(\mathcal{X})$ whose associated 1-category

$$\mathrm{Loc}^{\mathrm{hol}}(\mathcal{X})$$

is easily seen to be isomorphic to $\mathrm{Loc}(X)$ (since the morphisms of $\mathrm{Loc}^{\mathrm{hol}}(\mathcal{X})$ always arise from *complex analytic morphisms* of Riemann surfaces, which may be *algebrized*). In particular, X is a *geometric core* if and only if $\mathcal{X}$ is a *terminal object* in $\mathrm{Loc}^{\mathrm{hol}}(\mathcal{X})$.

Example 4.2. ***p*-adic Holomorphic Structures.** The analogue of Example 3.1 for $\mathbb{Q}_p$ does not hold, since the (naive) analogue of the theorem of Neukirch-Uchida-Iwasawa-Ikeda does not hold for finite extensions of $\mathbb{Q}_p$. On the other hand, if K is a finite extension of $\mathbb{Q}_p$, then its absolute Galois group G_K has a natural action on $\mathbb{C}_p$ (the p-adic completion of the algebraic closure of $\mathbb{Q}_p$ under consideration). Moreover, although (unlike the case of number fields) it is not necessarily the case that an *arbitrary* isomorphism $G_{K_1} \xrightarrow{\sim} G_{K_2}$ (where K_1, K_2 are finite extensions of $\mathbb{Q}_p$) arises from a field isomorphism $K_1 \xrightarrow{\sim} K_2$, it *is* necessarily the case that such an isomorphism $G_{K_1} \xrightarrow{\sim} G_{K_2}$ arises from a field isomorphism *if* $G_{K_1} \xrightarrow{\sim} G_{K_2}$ is *compatible* with the natural actions of both sides on $\mathbb{C}_p$ (cf. the theory of [Mzk14]). Thus, if one thinks of $\mathbb{C}_p$ as determining a (pro-ind-)object Q_K in $\mathrm{\acute{E}t}(K)$, and defines the morphisms of

$$\mathfrak{Loc}^{\mathfrak{hol}}(\mathbb{Q}_p)$$

to be morphisms $\mathrm{\acute{E}t}(K_1) \to \mathrm{\acute{E}t}(K_2)$ of $\mathfrak{Loc}(\mathbb{Q}_p)$ for which the pull-back of Q_{K_2} is isomorphic to Q_{K_1}, then $\mathrm{\acute{E}t}(\mathbb{Q}_p)$ determines a *terminal object* in $\mathfrak{Loc}^{\mathfrak{hol}}(\mathbb{Q}_p)$.

The above two examples motivate the *following approach*: Let $\mathcal{Q}$ be a *slim anabelioid*. Define a *$\mathcal{Q}$-holomorphic structure* on a slim anabelioid $\mathcal{X}$ to be a *morphism* $\mathcal{X} \to \mathcal{Q}$. We will refer to a slim anabelioid equipped with a $\mathcal{Q}$-holomorphic structure as a *$\mathcal{Q}$-anabelioid*. A *$\mathcal{Q}$-holomorphic morphism* (or "$\mathcal{Q}$-morphism" for short) between $\mathcal{Q}$-anabelioids is a morphism of anabelioids compatible with the $\mathcal{Q}$-holomorphic structures. Then we obtain a *2-category*

$$\mathfrak{Loc}_{\mathcal{Q}}(\mathcal{X})$$

whose *objects* are $\mathcal{Q}$-anabelioids that admit a $\mathcal{Q}$-holomorphic finite étale morphism to $\mathcal{X}$, and whose *morphisms* are arbitrary finite étale $\mathcal{Q}$-morphisms (that do not necessarily lie over $\mathcal{X}$!).

Thus, instead of considering whether or not $\mathcal{X}$ is a(n) *(absolute) core* (as in §3), one may instead consider whether or not $\mathcal{X}$ is a *$\mathcal{Q}$-core*, i.e., determines a terminal object in $\mathrm{Loc}_{\mathcal{Q}}(\mathcal{X}) \stackrel{\mathrm{def}}{=} |\mathfrak{Loc}_{\mathcal{Q}}(\mathcal{X})|$. Just as cores "have essentially only one basepoint":

> *If $\mathcal{X}$ is a $\mathcal{Q}$-core, then every basepoint of $\mathcal{Q}$ determines an essentially* **unique** *(up to renaming) basepoint of $\mathcal{X}$ (so long as the $\mathcal{Q}$-holomorphic structures involved are held fixed).*

Thus, the theory of *"$\mathcal{Q}$-holomorphic structures"* gives rise to a sort of "relative version" of theory of cores discussed in §3.

Next, we introduce some terminology, as follows. A *closed subgroup $H \subseteq G$* of a profinite group G will be called *commensurably terminal* if the *commensurator*

$$C_G(H) \stackrel{\mathrm{def}}{=} \{g \in G \mid (g \cdot H \cdot g^{-1}) \bigcap H \text{ has finite index in } H,\, g \cdot H \cdot g^{-1}\}$$

of H in G is equal to H itself. An arbitrary morphism of connected anabelioids $\mathcal{X} \to \mathcal{Y}$ will be called a *π_1-monomorphism* (respectively, *π_1-epimorphism*) if the induced morphism on fundamental groups $\pi_1(\mathcal{X}) \to \pi_1(\mathcal{Y})$ is injective (respectively, surjective). A π_1-monomorphism $\mathcal{X} \to \mathcal{Y}$ of connected anabelioids will be called *commensurably terminal* if the induced morphism on fundamental groups $\pi_1(\mathcal{X}) \to \pi_1(\mathcal{Y})$ is commensurably terminal.

Now it is an easy, formal consequence of the definitions that:

> *Suppose that $\mathcal{X}$ is a $\mathcal{Q}$-anabelioid with the property that the morphism $\mathcal{X} \to \mathcal{Q}$ defining the $\mathcal{Q}$-holomorphic structure is a π_1-monomorphism. Then $\mathcal{X}$ is a $\mathcal{Q}$-***core** *if and only if $\mathcal{X} \to \mathcal{Q}$ is* **commensurably terminal**.

This observation allows to construct many *interesting explicit examples of $\mathcal{Q}$-cores*, as follows:

Example 4.3. p-adic Local Fields Revisited. Let F be a *number field*, with *absolute Galois group G_F*. Let $\mathfrak{p}$ be a *finite prime* of F, with associated *decomposition subgroup $G_{\mathfrak{p}} \subseteq G_F$*. Then the closed subgroup $G_{\mathfrak{p}} \subseteq G_F$ is *commensurably terminal* (cf. [NSW], Corollary 12.1.3). In particular, in Example 4.2, instead of considering the "holomorphic structure" determined by the action on $\mathbb{C}_p$, we could have considered instead the *$\mathbb{Q}$-holomorphic structure* on $\text{Ét}(\mathbb{Q}_p)$, i.e., the holomorphic structure determined by the morphism

$$\text{Ét}(\mathbb{Q}_p) \to \mathcal{Q} \stackrel{\mathrm{def}}{=} \text{Ét}(\mathbb{Q})$$

(arising from the morphism of schemes $\mathrm{Spec}(\mathbb{Q}_p) \to \mathrm{Spec}(\mathbb{Q})$). Then $\text{Ét}(\mathbb{Q}_p)$ determines a *$\mathcal{Q}$-core*, i.e., a terminal object in $\mathrm{Loc}_{\mathcal{Q}}(\text{Ét}(\mathbb{Q}_p))$.

Example 4.4. Hyperbolic Orbicurves over p-adic Local Fields. Let X_K be a *hyperbolic orbicurve* (cf. Example 3.2) over a field K which is a finite extension of $\mathbb{Q}_p$. Set $\mathcal{Q} \stackrel{\mathrm{def}}{=} \acute{\mathrm{E}}\mathrm{t}(\mathbb{Q})$, and equip $\mathcal{X} \stackrel{\mathrm{def}}{=} \acute{\mathrm{E}}\mathrm{t}(X_K)$ with the $\mathcal{Q}$-holomorphic structure $\mathcal{X} \to \mathcal{Q}$ determined by the morphism of schemes $X_K \to \mathrm{Spec}(\mathbb{Q})$. Then if X_K is a *geometric core* and K is a *minimal extension of* $\mathbb{Q}_p$ over which X_K is defined, then it follows (cf. Example 3.2; [Mzk15]) that $\mathcal{X}$ determines a $\mathcal{Q}$-*core* in $\mathrm{Loc}_{\mathcal{Q}}(\mathcal{X})$.

Example 4.5. Inertia Groups of Marked Points. Let $\widehat{\Pi}_{g,r}$ be the *profinite completion* of the fundamental group of a *topological surface of genus g with r punctures*, where $2g - 2 + r > 0$. Suppose that $r > 0$, and let

$$I \subseteq \widehat{\Pi}_{g,r}$$

be the *inertia group* associated to one of the punctures. Then it is an easy exercise to show that $I \subseteq \widehat{\Pi}_{g,r}$ is *commensurably terminal.*

Example 4.6. Graphs of Groups. Suppose that we are given a (finite, connected) *graph of (profinite) groups* $\mathcal{G}$. That is to say, we are given a *finite connected graph* Γ, together with, for each *vertex* v (respectively, *edge* e) of Γ a *profinite group* Π_v (respectively, Π_e), and, for each vertex v that *abuts* to an edge e, a *continuous injective homomorphism* $\Pi_e \to \Pi_v$. Denote by

$$\Pi_{\mathcal{G}}$$

the *profinite fundamental group* associated to this graph of profinite groups. Then we obtain natural injections $\Pi_e \hookrightarrow \Pi_{\mathcal{G}}$, $\Pi_v \hookrightarrow \Pi_{\mathcal{G}}$ (well-defined up to composition with an inner automorphism of $\Pi_{\mathcal{G}}$).

Now let Δ be a *connected subgraph* of Γ. Then "restricting" $\mathcal{G}$ to Δ gives rise to a graph of groups $\mathcal{G}_\Delta$. If we then denote the associated "$\Pi_{\mathcal{G}_\Delta}$" by Π_Δ, then we obtain a natural continuous homomorphism $\Pi_\Delta \to \Pi_{\mathcal{G}}$. Then by constructing various "finite ramified coverings" of $\mathcal{G}$ by *gluing together compatible systems of coverings at the various edges and vertices*, one verifies easily that:

(i) The homomorphism $\Pi_\Delta \to \Pi_{\mathcal{G}}$ is *injective*.

(ii) Suppose that for each vertex v of Δ, their exists an *infinite closed subgroup* $N \subseteq \Pi_v$ with the property that for every edge e that meets v, and every $g \in \Pi_v$, we have $\Pi_e \bigcap (g \cdot N \cdot g^{-1}) = \{1\}$. Then Π_Δ is *commensurably terminal* in $\Pi_{\mathcal{G}}$. In particular, for every vertex v of Δ, Π_v is *commensurably terminal* in $\Pi_{\mathcal{G}}$.

The hypotheses of (ii) are satisfied, for instance, when all the $\Pi_e = \{1\}$ and all the Π_v are *infinite*.

Example 4.7. Stable Curves and Graphic Automorphisms. Let K be an *algebraically closed field of characteristic* 0. Let X be a *stable hyperbolic curve* of type (g, r) over K — i.e., the complement of the divisor of marked points in a pointed stable curve of type (g, r) over K. Then to X, one may associate a natural *graph of groups* $\mathcal{G}_X$ as follows: The underlying graph Γ_X of $\mathcal{G}_X$ is the *dual graph* of X. That is to say, the vertices (respectively, edges) of Γ_X are the irreducible components (respectively, nodes) of X, and an edge abuts to a vertex if and only if the corresponding node is contained in the corresponding irreducible component. If v (respectively, e) is a *vertex* (respectively, *edge*) of Γ_X, then we associate to it the profinite group Π_v (respectively, Π_e) given by the algebraic fundamental group of the irreducible component (respectively, inertia group ($\cong \widehat{\mathbb{Z}}$) of the node) corresponding to v (respectively, e); the inclusions $\Pi_e \hookrightarrow \Pi_v$ are the natural ones. Note that the profinite fundamental group Π_X associated to $\mathcal{G}_X$ may be identified with the algebraic fundamental group of X, hence is (noncanonically) isomorphic to $\widehat{\Pi}_{g,r}$ (cf. Example 4.5).

One verifies easily that all of the Π_e, Π_v are *commensurably terminal* in Π_X (cf. Examples 4.5, 4.6). Denote by

$$\mathrm{Out}_\Gamma(\Pi_X) \subseteq \mathrm{Out}(\Pi_X) \stackrel{\mathrm{def}}{=} \mathrm{Aut}(\Pi_X)/\mathrm{Inn}(\Pi_X)$$

the subgroup of *graphic outer automorphisms* of Π_X. Here, an automorphism $\alpha : \Pi_X \xrightarrow{\sim} \Pi_X$ is *graphic* if there exists an automorphism $\alpha_\Gamma : \Gamma_X \xrightarrow{\sim} \Gamma_X$ such that: (i) for every vertex v (respectively, edge e) of Γ_X, $\alpha(\Pi_v)$ (respectively, $\alpha(\Pi_e)$) is equal to a conjugate of $\Pi_{\alpha_\Gamma(v)}$ (respectively, $\Pi_{\alpha_\Gamma(e)}$); (ii) the resulting outer isomorphism $\Pi_v \xrightarrow{\sim} \Pi_{\alpha_\Gamma(v)}$ preserves the conjugacy classes of the inertia groups associated to the punctures of X that lie on v, $\alpha_\Gamma(v)$, respectively. Then it is not difficult to show by an argument involving *"weights"* as in [Mzk13], §1 – 5, that:

$\mathrm{Out}_\Gamma(\Pi_X)$ is *commensurably terminal* in $\mathrm{Out}(\Pi_X)$.

One may regard this fact as a sort of *anabelian analogue* of the well-known "linear algebra fact" that *the subgroup of upper triangular matrices in $GL_n(\widehat{\mathbb{Z}})$ is commensurably terminal in $GL_n(\widehat{\mathbb{Z}})$.*

Bibliography

zk1] S. Mochizuki, *The Hodge-Arakelov Theory of Elliptic Curves: Global Discretization of Local Hodge Theories*, RIMS Preprint Nos. 1255, 1256 (October 1999).

zk2] S. Mochizuki, *The Scheme-Theoretic Theta Convolution*, RIMS Preprint No. 1257 (October 1999).

SHINICHI MOCHIZUKI (RIMS, KYOTO UNIVERSITY)

[Mzk3] S. Mochizuki, *Connections and Related Integral Structures on the Universal Extension of an Elliptic Curve*, RIMS Preprint No. 1279 (May 2000).

[Mzk4] S. Mochizuki, *The Galois-Theoretic Kodaira-Spencer Morphism of an Elliptic Curve*, RIMS Preprint No. 1287 (July 2000).

[Mzk5] S. Mochizuki, *The Hodge-Arakelov Theory of Elliptic Curves in Positive Characteristic*, RIMS Preprint No. 1298 (October 2000).

[Mzk6] S. Mochizuki, A Survey of the Hodge-Arakelov Theory of Elliptic Curves I, to appear in *"Moduli of Profinite Aspects of Arithmetic Covers,"* an AMS research volume edited by M. Fried.

[Mzk7] S. Mochizuki, *A Survey of the Hodge-Arakelov Theory of Elliptic Curves II*, manuscript.

[Mzk9] S. Mochizuki, A Theory of Ordinary p-adic Curves, *Publ. of RIMS* **32** (1996), pp. 957-1151.

[Mzk10] S. Mochizuki, *Foundations of p-adic Teichmüller Theory*, AMS/IP Studies in Advanced Mathematics **11**, American Mathematical Society/International Press (1999).

[Mzk11] S. Mochizuki, Correspondences on Hyperbolic Curves, *Journ. Pure Appl. Algebra* **131** (1998), pp. 227-244.

[Mzk12] S. Mochizuki, The Geometry of the Compactification of the Hurwitz Scheme, *Publ. of RIMS* **31** (1995), pp. 355-441.

[Mzk13] S. Mochizuki, The Profinite Grothendieck Conjecture for Closed Hyperbolic Curves over Number Fields, *J. Math. Sci., Univ. Tokyo* **3** (1996), pp. 571-627.

[Mzk14] S. Mochizuki, A Version of the Grothendieck Conjecture for p-adic Local Fields, *The International Journal of Math.* **8** (1997), pp. 499-506.

[Mzk15] S. Mochizuki, The Local Pro-p Anabelian Geometry of Curves, *Invent. Math.* **138** (1999), pp. 319-423.

[Mzk16] S. Mochizuki, *Global Anabelian Geometry in the Hodge-Arakelov Theory of Elliptic Curves*, manuscript in preparation.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, *Grundlehren der Mathematischen Wissenschaften* **323**, Springer-Verlag (2000).

[SGA1] *Revêtement étales et groupe fondamental*, Séminaire de Géometrie Algébrique du Bois Marie 1960-1961 (SGA1), dirigé par A. Grothendieck, augmenté de deux exposés de M. Raynaud, *Lecture Notes in Mathematics* **224**, Springer-Verlag (1971).

[Tama] A. Tamagawa, The Grothendieck Conjecture for Affine Curves, *Compositio Math.* **109** (1997), pp. 135-194.