Mathematisches Forschungsinstitut Oberwolfach

Report No. NUMBER-OF-REPORT/2023

DOI: 10.4171/OWR/2023/NUMBER-OF-REPORT

MFO-RIMS Tandem workshop: Arithmetic Homotopy and Galois Theory

Organized by
Benjamin Collas, Kyoto
Pierre Dèbes, Villeneuve d'Ascq
Yuichiro Hoshi, Kyoto
Ariane Mézard, Paris

24 September – 29 September, 2023

Abstract. This report presents a general panorama of recent progress in the arithmetic-geometry theory of Galois and homotopy groups and its ramifications. While still relying on Grothendieck's original pillars[1], the present program has now evolved beyond the classical group-theoretic legacy *to result in an autonomous project that exploits a new geometrization of the original insight and sketches new frontiers between homotopy geometry, homology geometry, and diophantine geometry.*

This panorama "closes the loop" by including the last twenty-year progress of the Japanese arithmetic-geometry school via Ihara's program and Nakamura-Tamagawa-Mochizuki's *anabelian approach*, which brings its expertise in terms of algorithmic, combinatoric, and absolute reconstructions. These methods supplement and interact with those from the classical *arithmetic of covers and Hurwitz spaces* and *the motivic and geometric Galois representations*.

This workshop has brought together the next generation of arithmetic homotopic Galois geometers, who, with the support of senior experts, are developing new techniques and principles for the exploration of the next research frontiers.

Mathematics Subject Classification (2020): 12F12, 14G32, 14H30, 14H45 (Primary); 14F05, 55Pxx, 14F22, 14G05, 14D15, 11F70 (Secondary).

[1]That are, as presented in "Récoltes et semailles", the resolution of the discrete and the continuous, the local-to-global thinking by generization-specialization, and the quintessential intersection of arithmetic and geometry – see § 2.10 ibid.

Introduction by the Organizers

The absolute Galois group $G_{\mathbb{Q}}$ of rational numbers is the seed of number theory. Its study by homotopic and geometric means is at the heart of modern arithmetic geometry. Building on the result of previous investigations, we report on recent progress on the development of a new geometry of Galois theory and homotopy symmetries of spaces. Relying on the unexploited work of Grothendieck's descendants, this results in *a new "geometrization" of arithmetic geometry based on the homotopy insight*[2].

This workshop, together with three previous ones[3], has led to the following cross-bridging principles:

(1) The application of *classical approaches beyond their original geometric frontier* (e.g. patching, Hilbert realization, Hurwitz spaces, section conjecture);
(2) Some *enriched approaches to linear Galois representations* (e.g. local systems via analytic automorphic forms, via the derived category of perverse sheaves, and via Tannaka symmetries);
(3) The *research of an intermediate new type of arithmetic geometry* (e.g. in terms of abelian-by-central extensions, of simplicial geometry in between étale and motivic theories, of the homotopy-homology frontier);
(4) The *absolute* reconstruction of *anabelian arithmetic-geometry* in a context that goes *beyond the ring structure* (e.g. applications in Diophantine geometry, anabelian combinatorial understanding of $\widehat{GT}$ and $G_{\mathbb{Q}}$.)

In the present report, these principles are supported further by *the integration of such techniques* as p-adic Hodge theory (for (2) and (3)), the monodromy method for dynamic arithmetic (for (1)), the development of ℓ-adic Galois theory and anabelian representations (for (3) and (4)), the development of anabelian reconstruction over algebraically closed field of positive characteristic (for (3)), and the introduction of indeterminacies for the uncoupling of multiplicative and additive structures in anabelian geometry and K-theory (for (1), (3) and (4)).

Joint together, these principles and techniques further indicate the following *new research frontiers in arithmetic geometry*:

(a) *Arithmetic & rationalization:* Hurwitz-Hilbert geometry, realization-lifting-parametrization proram for covers, and rational obstruction;
(b) *Homology & homotopy:* Galois and p-adic Hodge representations, monodromy and Tannaka symmetries, the meta-abelian frontier;

---

[2] Under this form this trend takes the denomination of "Arithmetic and homotopic Galois theory" (AHGT).

[3] MFO workshop - *Homotopic and Geometric Galois Theory* (org.: B. Collas, P. Dèbes, H. Nakamura, J. Stix) in 2021; "Rencontres Arithmétiques de Caen" on *Field Arithmetic and Arithmetic Geometry* in 2019; MFO mini-workshop *Arithmetic Geometry and Symmetries around Galois and Fundamental Groups* (org.: B. Collas, P. Dèbes, M. Fried) in 2018.

(c) *New geometries:* in higher dimension and with respect to stack symmetries, over algebraically closed and finite fields, for multiplicative and additive monoids (with indeterminacies).

For a better measure of the progress of this workshop, we keep the three classical and historical approaches, that are *the arithmetic of Galois covers and Hurwitz spaces*, the *geometric and motivic Galois representations* and the *anabelian arithmetic geometry* as a structuring guide. Given the constant mutual interactions of these topics, this categorization must be read up to certain mild indeterminacies; we refer to the original reports for details.

Arithmetic of Galois covers and Hurwitz spaces. Geometry of Hurwitz spaces and concatenation within their boundary are exploited for building new rational irreducible components (Seguin). A refined version of the ring of components and splitting number are developed, which has already ramified in algebraic topology and for enumerative questions in number theory – see the work of Bianchi and Ellenberg-Venkatesh-Westerland respectively. The latter, with the systemic use of homological stability, has since established in a well-identified program of "arithmetic statistic of function fields", with, among others, applications to Malle's conjecture and the distribution of Selmer group (Westerland et al.)

Originally motivated by question from arithmetic dynamic, structural results are obtained for the monodromy group of iterated polynomials in terms of Hilbert irreducibility theorem, largeness, and arboreal representations (König, Neftin et al.). In a similar but distinct probabilistic direction, we also refer to Bary-Soroker.

The development of two in-progress projects around properties of torsion points of the jacobian of curves have been reported: one on the extension of previous results of Greenberg which, in the spirit of Ihara's program, tightly intertwines number theory and arithmetic geometry (Pries et al.), and a second, by building on previous insight of Raynaud, Tamagawa and Hoshi, on possible strategies for solving the Coleman conjecture (Takao).

Geometric and motivic Galois representations. Concerning the "homology vs homotopy" frontier, this workshop has seen *the path between linear and anabelian methods* – a path initiated in the 90's on one side with the integration of Falting's p-adic Hodge method in anabelian geometry by Mochizuki and one the other side by Kim's non-anabelian approach of Chabauty-Coleman for rational points – *to be pushed closer to a loop*[4]. At the intersection of Lawrence-Venkatesh method for the proof of the Mordell conjecture and of Chabauty-Kim theory, progress was reported on the rational obstruction to Selmer sections that exploits the whole arsenal of p-adic Hodge theory (Betts et al.). A synthetic panorama of properties of the degeneracy/toric locus of ℓ-adic local systems that build on similar approaches based on variational p-adic Hodge theory and period map was also presented

[4]This topic will be the object of a dedicated AHGT workshop in Oberwolfach, "Anabelian Geometry and Representations of Fundamental Groups" Sep. 29 - Oct. 4, 2024 (Org.: A. Cadoret, F. Pop, J. Stix, A. Topaz; ID: 2440).

(Cadoret et al.). Exploiting a special type of geometric Galois representations (of Barsotti-Tate type), report was presented on *how arithmetic invariants resulting from explicit and computational approach* lead to new geometric and arithmetic results in the p-adic Langlands program (Mézard et al.)

On the classical topic of Artin L-functions, and as motivated by potential applications of anabelian geometry to analytic number theory, some investigations were presented that reflect the use of purely group-theoretic method (Yamashita).

In the direction of étale cohomology and the structure of Massey products, and with *motivation from the embedding problem*, an extensive and solid state-of-the-art of the most recent results was presented for Galois cohomology in terms of formality and with application to Koszulity (Quick et al.) and for cohomology of curves in various geometric situations (Bleher et al.). A synthetic report was given on finitness results of Galois cohomology and Tate-Shafarevich groups, a key tool whose properties ramifies in multiple aspects of the AHGT program (Harari et al.)

Anabelian arithmetic geometry & ramifications. This workshop has been the opportunity to report on *two recent breakthroughs*: the construction, as a consequence of the anabelianity of the Grothendieck-Teichmüller group, of *a combinatorial model of* $\bar{\mathbb{Q}}$ (Tsujimura et al.), a decisive step toward the Galois-Grothendieck-Teichmüller conjecture, and *the resolution of non-singularities* (Lepage), an algebraic geometry statement originally formulated by Tamagawa, with implications in anabelian geometry, Grothendieck-Teichmüller theory, and the section conjecture.

A certain thematic group has appeared, that exploits various flavors of anabelian ℓ-adic Galois representations, in terms of purely anabelian methods (Iijima et al.), of the symmetries of spaces (applied to associators, Shiraishi or to Oda's conjecture, Philip et al.), or in relation with Deligne-Ihara's conjecture pushed from genus zero to one (Ishii).

The emergence of a new geometry of monoids with indeterminacies provides new connections between anabelian geometry, diophantine geometry and analytic number theory (Mochizuki et al.), a principle that can also be found in the reconstruction of function fields via K-theory (Topaz).

New geometric frontiers were exploited: higher homotopy and motivic rational obstructions via the simplicial homotopy method (Corwin), the nearly-abelian study of local-global properties of Galois sections (Porowski), and a reconstrution program over algebraically closed fields of positive characteristic, with in particular a new proof of Mochizuki's seminal anabelian result (Yang et al.).

A bridge between Europe and Japan. Following the Oberwolfach tradition, the workshop was opened with a few words of Prof. Klaus on behalf of MFO and of Prof. K. Ono on behalf of RIMS, both present at RIMS Kyoto. The workshop was structured over 2 sites, one in Japan and one in Germany, with a Zoom bridge for live interaction and a dedicated Discord forum for sharing video recordings of the talks, slides, and asynchronous comments. The crossover of some Japanese researchers at the MFO and of some French researchers in Japan ensured the dissemination of ideas between the two sites.

The week gathered a total of 58 participants – 25 participants at RIMS Kyoto and 33 participants at Oberwolfach Germany – around 25 one-hour long talks (5 each day). An extended break time after lunch – under the form of a "Bento" time with MFO-like random seating at RIMS – supported informal interactions and discussions during the event.

Speakers, rather than to restrict themselves to their individual work, reported on recent progress of entire subtopics. Scientific exchanges reached the next stage, where participants would send video recordings of their comments and questions on blackboard to the other site.

Poster session for Oberwolfach Leibniz Fellows. The oral presentations above were complemented with online poster sessions on the dedicated MFO-RIMS Discord forum for the OWLG fellows to introduce their research topics and latest results: (1) Assoun (Lille) uses Galois theory of skew fields for the inverse Galois problem, (2) Holzschuh (Heidelberg) develops the étale homotopy type of spaces in terms of infinity categories for a higher-dimensional result on Grothendieck's section conjecture, and (3) Shmueli (Tel Aviv) obtains probabilistic results on the residue degree and ramification of p-adic splitting field of polynomials.

A decisive opus within the AHGT project. This third opus has confirmed the dynamic initiated with the 2018 mini-workshop "Arithmetic Geometry and Symmetries around Galois and Fundamental Groups" and developed in the 2021 workshop "Homotopic and Geometric Galois Theory". A shared feeling of the participants on both sites is that *a new common culture has been built, a structured program has appeared that paves the way to future collaboration and a network of conjectures.* Following the strong support and feedback of the participants, and as part of the "Arithmetic and Homotopic Galois Theory" project (AHGT)[5], agreement has been made to meet again within the next 2 years for reporting on the latest progress of the field.

Acknowledgement: This workshop was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University, and by the CNRS-RIMS "Arithmetic and Homotopic Galois Theory" (AHGT) International Research Network. The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-2230648, "US Junior Oberwolfach Fellows".

[5]For updated information on workshops, seminars, and publications of the AHGT project, we refer to `https://ahgt.math.cnrs.fr`

Arithmetic Homotopy and Galois Theory

Table of Contents

Abstracts

On the Grothendieck-Teichmüller group via combinatorial anabelian geometry

Shota Tsujimura
(joint work with Yuichiro Hoshi, and Shinichi Mochizuki)

The Grothendieck-Teichmüller group $\widehat{GT}$, which was originally introduced by V. Drinfel'd [Dri90], is a purely combinatorial object and may be regarded as a closed subgroup of the outer automorphism group of the free profinite group of rank 2. On the other hand, it is well-known – and proved rigorously by Y. Ihara – that the absolute Galois group $G_{\mathbb{Q}} \stackrel{\text{def}}{=} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the field of rational numbers, which is a purely arithmetic object, may be embedded into $\widehat{GT}$ via the natural outer action on the étale fundamental group $\pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\})$ of the projective line minus three points.

In light of this embedding, the group $\widehat{GT}$ has been thought of as a sort of a purely combinatorial approximation of $G_{\mathbb{Q}}$. However, it is still totally unknown to which extent this approximation is strong. We report on recent progress surrounding this topic that is based on an approach via combinatorial anabelian geometry.

1. Harbater-Schneps' definition of $\widehat{GT}$

Let us first recall one of the definitions of $\widehat{GT}$, as given by D. Harbater and L. Schneps, which is known to be equal to Drinfeld's original one, cf. [HS00]. Write

$$X \stackrel{\text{def}}{=} \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}; \quad X_2 \stackrel{\text{def}}{=} X \times X \setminus \Delta,$$

where Δ denotes the diagonal divisor. Note that X_2 is isomorphic to the moduli stack $\mathcal{M}_{0,5}$ of hyperbolic curves of genus 0 over $\overline{\mathbb{Q}}$ with 5 ordered punctured points. Note also that, in light of the notion of pointed stable curves, $\mathcal{M}_{0,5}$ admits the natural compactification $\overline{\mathcal{M}}_{0,5}$ whose complement is a normal crossing divisor. In particular, $\mathcal{M}_{0,5} \subseteq \overline{\mathcal{M}}_{0,5}$, hence also X_2, admits the natural action of the symmetric group $\mathfrak{S}_5$. Then the Grothendieck-Teichmüller group

$$\widehat{GT} \subseteq \mathrm{Out}(\pi_1(X_2))$$

may be defined as a closed subgroup of $\mathrm{Out}(\pi_1(X_2))$ consisting of the elements $\sigma \in \mathrm{Out}(\pi_1(X_2))$ satisfying the following conditions:

(1) Let δ be an irreducible component of $\overline{\mathcal{M}}_{0,5} \setminus \mathcal{M}_{0,5}$; $I_\delta \subseteq \pi_1(X_2)$ an inertia subgroup associated to δ [determined up to conjugate]; $\tilde{\sigma} \in \mathrm{Aut}(\pi_1(X_2))$ a lifting of σ. Then $\tilde{\sigma}(I_\delta)$ and I_δ are conjugate.
(2) σ commutes with the natural outer action of $\mathfrak{S}_5$, i.e., $\sigma \in Z_{\mathrm{Out}(\pi_1(X_2))}(\mathfrak{S}_5)$.

Here, by applying the first condition, we have a natural injective homomorphism $\widehat{GT} \hookrightarrow \mathrm{Out}(\pi_1(X))$ whose image coincides with the original one. Moreover, if we adopt this definition, the existence of the natural embedding

$$G_{\mathbb{Q}} \subseteq \widehat{GT}$$

follows immediately from Belyi's theorem.

2. Results via combinatorial anabelian geometry

In this section, we introduce recent results surrounding the inclusion $G_{\mathbb{Q}} \subseteq \widehat{GT}$ obtained by applying combinatorial anabelian geometry.

The first result proved by Y. Hoshi, A. Minamide, and S. Mochizuki is the following, cf. [CbGT, Corollary C]:

Theorem 1. *The equality*

$$\mathrm{Out}(\pi_1(X_2)) = \widehat{GT} \times \mathfrak{S}_5$$

holds.

In light of the above equality, one may observe that there is almost no scheme-theoretic restriction on $\widehat{GT}$. In particular, if $G_{\mathbb{Q}} = \widehat{GT}$, then this may be a really surprising phenomenon! As an application of Theorem 1, one may give a purely group-theoretic algorithm whose input data is (the underlying topological group structure of) $\pi_1(X_2)$ and whose output data are the subgroups $\widehat{GT}, \mathfrak{S}_5 \subseteq \mathrm{Out}(\pi_1(X_2))$, cf. [CbGT, Corollary C].

Next, we briefly mention *combinatorial Belyi cuspidalization* developed by the author in [Tsu20]. In general, a cuspidalization in anabelian geometry is a procedure to reconstruct, from the étale fundamental group $\pi_1(S)$ of a connected scheme S, the (outer) surjections to $\pi_1(S)$ that arise from open subschemes of S. Roughly speaking, combinatorial Belyi cuspidalization is a purely combinatorial/group-theoretic procedure – that is closely related to Belyi maps – to reconstruct, from the data $(\pi_1(X), \widehat{GT} \subseteq \mathrm{Out}(\pi_1(X)))$, the outer surjections to $\pi_1(X)$ that arise from open subschemes of X, cf. [Tsu20, Theorem A].

In the remainder, we introduce two applications of this combinatorial Belyi cuspidalization.

2.1. Galois as retract within $\widehat{GT}$.

Let p be a prime number. Recall that there exists a certain p-adic analogue

$$G_{\mathbb{Q}_p} \overset{\mathrm{def}}{=} \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subseteq \widehat{GT}_p$$

of the inclusion $G_{\mathbb{Q}} \subseteq \widehat{GT}$ defined by Y. André via the notion of tempered fundamental groups [And03]. Then the first application is the following, cf. [Tsu20, Corollary B]:

Theorem 2. *The inclusion $G_{\mathbb{Q}_p} \subseteq \widehat{GT}_p$ admits a natural retraction, i.e., there exists a natural surjection*

$$\widehat{GT}_p \twoheadrightarrow G_{\mathbb{Q}_p}$$

whose restriction to $G_{\mathbb{Q}_p}$ is the identity automorphism.

Here, we note that there exist various versions of p-adic analogue of $\widehat{GT}$ in the literatures, see [MT23, Theorem G]. However, in a recent joint work with Mochizuki, we proved that all of them are equal, see ibid.

On the other hand, it is natural to ask how small the kernel of the surjection $\widehat{GT}_p \twoheadrightarrow G_{\mathbb{Q}_p}$ is. With regard to this question, in light of various rigidity results concerning geometric tempered fundamental groups of hyperbolic curves, the author expects that this kernel is trivial, hence that the inclusion $G_{\mathbb{Q}_p} \subseteq \widehat{GT}_p$ is, in fact, bijective.

2.2. **BGT – A combinatorial model of $G_{\mathbb{Q}}$.** The second application, which is a joint work with Hoshi and Mochizuki, is the following, cf. [CbGal, Theorem C, (ii)]:

Theorem 3. *There exists a purely combinatorial/group-theoretic algorithm whose input data is (the underlying topological group structure of) $\pi_1(X_2)$ and whose output data is the conjugacy class of $G_{\mathbb{Q}}$ in $\widehat{GT}$.*

Theorem 3 may be regarded as a *conditional surjectivity* of the inclusion $G_{\mathbb{Q}} \subseteq \widehat{GT}$ in the sense that if we replace $\widehat{GT}$ by a smaller – but still combinatorially defined! – closed subgroup of $\widehat{GT}$, then this subgroup coincides with a $\widehat{GT}$-conjugate of $G_{\mathbb{Q}}$.

Note that since $\pi_1(X)$ is center-free, every $\widehat{GT}$-conjugate, or more generally $\mathrm{Out}(\pi_1(X))$-conjugate, of $G_{\mathbb{Q}}$ determines a profinite group isomorphic to $\pi_1(\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\})$. On the other hand, from the viewpoint of mono-anabelian geometry, every $\mathrm{Out}(\pi_1(X))$-conjugate of $G_{\mathbb{Q}}$ corresponds to a scheme isomorphic to $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$. In particular, Theorem 3 is equivalent to construct, in a purely combinatorial/group-theoretic way, from (the underlying topological group structure of) $\pi_1(X_2)$, a suitable set of schemes isomorphic to $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ or X.

Such a construction may be realized by the following two steps as in [AbsTopIII] § 1:

(1) *Combinatorial construction of base fields*, i.e., fields isomorphic to $\overline{\mathbb{Q}}$.
(2) *Combinatorial construction of function fields*, i.e., fields isomorphic to the function field of X.

The first step is achieved by introducing certain (combinatorially defined!) class "BGT", for "Belyi-Grothendieck-Teichmüller", of closed subgroups of $\widehat{GT}$. By a slight abuse of notation, we also write BGT for any element of the class BGT. Roughly speaking, BGT $\subseteq \widehat{GT}$ is a closed subgroup that enables us to take a "limit" of combinatorial Belyi cuspidalizations in a suitable sense. Once one obtains such a "limit", one may define the inductive limit $\overline{\mathbb{Q}}_{\mathrm{BGT}}$ of the conjugacy classes of cuspidal inertia subgroups (that do not associated to ∞) of cuspidalizations. Then, by using the subgroup $\mathfrak{S}_5 \subseteq \mathrm{Out}(\pi_1(X_2))$, cf. the discussion immediately after

Theorem 1, one may also define a field structure on the set $\overline{\mathbb{Q}}_{\mathrm{BGT}}$ isomorphic to $\overline{\mathbb{Q}}$. Here, we note that one may not exclude the possibility that a "domination relation" (used to define the "limit") between two cuspidalizations does not arise from an open immersion. In particular, *the fact that* $\overline{\mathbb{Q}}_{\mathrm{BGT}}$ *is isomorphic to* $\overline{\mathbb{Q}}$ *is a nontrivial statement.* Finally, with regard to the second step, after introducing certain abstract functions and Kummer classes of them, the function fields are constructed in a similar spirit to [AbsTopIII] §1.

References

[And03] Y. André, On a geometric description of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and a p-adic avatar of $\widehat{GT}$, *Duke Math. J.* **119** (2003), 1–39.

[Dri90] V. G. Drinfeld, On quasitriangular quasi-Hopf algebras and a group closely connected with $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Algebra i Analiz* **2** (1990), 149–181.

[HS00] D. Harbater and L. Schneps, Fundamental groups of moduli and the Grothendieck-Teichmüller group, *Trans. Amer. Math. Soc.* **352** (2000), 3117–3148.

[CbGT] Y. Hoshi, A. Minamide, and S. Mochizuki, Group-theoreticity of numerical invariants and distinguished subgroups of configuration space groups, *Kodai Math. J.* **45** (2022), 295–348.

[CbGal] Y. Hoshi, S. Mochizuki, and S. Tsujimura, Combinatorial construction of the absolute Galois group of the field of rational numbers, RIMS Preprint **1935** (December 2020).

[AbsTopIII] S. Mochizuki, Topics in absolute anabelian geometry III: Global reconstruction algorithms, *J. Math. Sci. Univ. Tokyo* **22** (2015), 939–1156.

[MT23] S. Mochizuki and S. Tsujimura, Resolution of nonsingularities, point-theoreticity, and metric-admissibility for p-adic hyperbolic curves, RIMS Preprint **1974** (June 2023).

[Tsu20] S. Tsujimura, Combinatorial Belyi cuspidalization and arithmetic subquotients of the Grothendieck-Teichmüller group, *Publ. Res. Inst. Math. Sci.* **56** (2020), 779–829.

An example of potentially Barsotti–Tate deformation ring

Ariane Mézard

Potentially Barsotti-Tate representations are a special type of geometric Galois representations which can be described by simple objects of p-adic Hodge theory on which explicit calculations can be carried out. It is therefore an ideal case for testing conjectures and highlighting new geometric structures.

The object of this note is to illustrate how the explicit and combinatorial approach leads to new conjectures and new arithmetic results in the context of p-adic Langlands program.

1. Potentially Barsotti–Tate deformation ring

1.1. **Notation.** Let p be a prime number, $K/\mathbf{Q}_p$ a finite unramified extension of degree f, $G_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$ its absolute Galois group. Let K' be the unique unramified extension of degree 2, $G_{K'} = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K')$. Let $E/\mathbf{Q}_p$ be a sufficiently large finite extension with ring of integers $\mathcal{O}$ and residue field $\mathbf{F}$. Let $\overline{\mathbf{F}}$ be an algebraic closure of $\mathbf{F}$.

Let ω_f (resp. ω_{2f}) be the Serre fundamental character of $G_{K'}$ of level f (resp. $2f$), and, for $\theta \in \mathbf{F}^*$, let $\mathrm{nr}'(\theta)$ denote the unique unramified charater of $G_{K'}$ that sends the arithmetic Frobenius to θ. We fix an irreducible Galois representation

$$\bar{\rho} : G_K \longrightarrow \mathrm{GL}_2(\mathbf{F}), \quad \bar{\rho} = \mathrm{Ind}_{G_{K'}}^{G_K} \left(\omega_{2f}^h \times \mathrm{nr}'(\theta)\right),$$

with $h \in \mathbf{Z}/(p^{2f}-1)\mathbf{Z}, p^f+1$ does not divide h, and a non-scalar tame inertial type

$$\tau = \omega_f^{\gamma} \oplus \omega_f^{\gamma'},$$

with $\gamma, \gamma' \in \mathbf{Z}/(p^f-1)\mathbf{Z}, \gamma \neq \gamma'$.

1.2. **Moduli stack and deformation ring.** To such type τ, Caraiani, Emerton, Gee and Savitt associated the moduli stack $\mathcal{Z}^{\tau}$ of potentially Barsotti–Tate Galois representations of with inertial type τ [CEGS20]. By construction, the potentially Barsotti-Tate deformation ring $R_{\bar{\rho}}^{\eta,\tau}$ of $\bar{\rho}$ with inertial type τ defined by Kisin is a versal ring to $\mathcal{Z}^{\tau}$ at $\bar{\rho}$, [Ki08].

These objects[1], $\mathcal{Z}^{\tau}$ and $R_{\bar{\rho}}^{\eta,\tau}$, play an important role in the p-adic Langlands program. Understanding the structure of the moduli stack and the geometric deformation ring is a challenging question related to many important arithmetic open problems among them the Fontaine Mazur conjecture, weight part of Serre conjecture, the Breuil-Mézard conjecture, multiplicity one conjecture or $R = T$ theorems.

The weight part of Serre conjecture, the Buzzard-Jarvis conjecture [BDJ10] and the Breuil-Mézard conjecture [BM02] have been proved by Gee and Kisin [GK14] under a genericity hypothesis on the inertial type. Kisin [Ki09] deduced new cases of the Fontaine-Mazur conjecture via a proof of the Breuil-Mézard conjecture combining a global argument with the p-adic local Langlands correspondence of Colmez [Co10] and Berger-Breuil [BB10].

In potentially Barsotti-Tate context, the Breuil-Mézard conjecture can be expressed as a numerical equality between:

- the number of irreducible components of $R_{\bar{\rho}}^{\eta,\tau}/(\pi_E)$ and
- the cardinal of the set $W(\tau, \bar{\rho})$ of common weights of $\bar{\rho}$ and τ.

1.3. **A combinatorial approach.** In a series of articles in collaboration with Caruso and David [CDM18, CDM23], we studied the deformation ring $R_{\bar{\rho}}^{\eta,\tau}$ in the non-generic case. Our calculations highlighted the importance of an associated combinatorial object $\mathbb{X}(\tau, \bar{\rho})$ associated to $\bar{\rho}$ and τ. We called $\mathbb{X}(\tau, \bar{\rho})$ the "gene" because it encodes the liftings of $\bar{\rho}$. From the gene, we deduced several algorithms determining important arithmetic objects associated to $\bar{\rho}$ and τ:

(1) the set of common weights $W(\tau, \bar{\rho})$ in [CDM23], and
(2) the equations of the Kisin variety [CDM18] associated to $\bar{\rho}$ and τ defined by Pappas and Rapoport in [PR09].

[1]These objects can be defined in a more general geometric context notably for potentially semi-stable deformations. The notation η in $R_{\bar{\rho}}^{\eta,\tau}$ refers to "potentially Barsotti-Tate" case.

Moreover the gene allowed us to formulate and to test several conjectures that we present in the following section.

2. Genetic conjectures

To data $(\gamma, h) \in \mathbf{Z}/(p^f-1)\mathbf{Z} \times \mathbf{Z}/(p^{2f}-1)\mathbf{Z}$ such that $h \not\equiv 0$ modulo p^f+1 and $h-2\gamma-(\sum_{j=0}^{f-1} p^j) \not\equiv 0$ modulo p^f-1, Caruso David and the author associate[2] in [CDM18, CDM23], a combinatorial data said to be the gene in the following way, Consider the p-expansion

$$(1) \quad h-(p^f+1)\left(h-\gamma-\sum_{j=0}^{f-1} p^j\right) \equiv p^{2f-1}v_0+p^{2f-2}v_1+\cdots+pv_{2f-2}+v_{2f-1} \pmod{p^{2f}-1}$$

with $v_{j'} \in \{0,\ldots,p-1\}$ for all $j' \in \mathbf{Z}/2f\mathbf{Z}$.

The *gene* $\mathbb{X}$ associated to such a pair $(\gamma, h) \in \mathbf{Z}/(p^f-1)\mathbf{Z} \times \mathbf{Z}/(p^{2f}-1)\mathbf{Z}$ is a $\mathbf{Z}/2f\mathbf{Z}$-tuple of symbols $\mathbb{X} = \mathbb{X}(\gamma,h) = (\mathbb{X}_{j'})_{j'\in\mathbf{Z}/2f\mathbf{Z}} \in \{\mathtt{A},\mathtt{B},\mathtt{AB},\mathtt{O}\}^{\mathbf{Z}/2f\mathbf{Z}}$ which satisfies the following properties, see [CDM23, Lemma B.1.3]:

(1) if $v_{j'}=0$ and $\mathbb{X}_{j'+1}=\mathtt{O}$, then $\mathbb{X}_{j'}=\mathtt{AB}$;
(2) if $v_{j'}=0$ and $\mathbb{X}_{j'+1}\neq\mathtt{O}$, then $\mathbb{X}_{j'}=\mathtt{A}$;
(3) if $v_{j'}=1$ and $\mathbb{X}_{j'+1}=\mathtt{O}$, then $\mathbb{X}_{j'}=\mathtt{O}$;
(4) if $v_{j'}=1$ and $\mathbb{X}_{j'+1}\neq\mathtt{O}$, then $\mathbb{X}_{j'}=\mathtt{B}$;
(5) if $v_{j'}\geq 2$, then $\mathbb{X}_{j'}=\mathtt{O}$.

The gene is related to several conjectures presented succinctly in the following statement:

Conjecture 1 (Conjecture 5.1.6 [CDM18], Conjecture 3.1.2 [CDM23])**.**

(1) The deformation ring $R_{\bar\rho}^{\eta,\tau}$ depends only on $\mathbb{X}(\tau,\bar\rho)$.
(2) There is a decomposition $\mathbb{X}(\tau,\bar\rho) = \cup_{i=0}^r (\mathbb{X}_{j_i}, \mathbb{X}_{j_i+f})_{j_i\leq i\leq j_{i+1}}$ such that $R_{\bar\rho}^{\eta,\tau} = \widehat{\otimes}_{i=0}^r R_i$, where R_i is a complete local Noetherian $\mathcal{O}$-algebra depending only on $(\mathbb{X}_{j_i}, \mathbb{X}_{j_i+f})_{j_i\leq i\leq j_{i+1}}$.
(3) The formation of $R_{\bar\rho}^{\eta,\tau}$ is "independent of p".

With B. Le Hung and S. Morra ([LHMM23]), we developed a local model theory for the moduli stack $\mathcal{Z}^\tau$ of 2-dimensional non-scalar tame potentially Barsotti–Tate Galois representations of G_K. Let Gr_1 be the cover of the affine Grassmannian over $\mathbf{Z}_p$ associated to the group $\mathrm{GL}_{2/\mathbf{Z}_p}$, with loop variable $v(v+p)$ and first principal congruence level with respect to v. The main result of [LHMM23] establishes a smooth locally isomorphism between $\mathcal{Z}^\tau$ and a closed irreducible subvariety of $(\mathrm{Gr}_1)^f$ obtained as the p-saturation of explicit schemes of group theoretic nature. Our model is "really" explicit: for $p > 16+7$ and any 2-dimensional $\mathbf{F}$-representation $\bar\rho$ of G_K (without assumption of irreducibility), it allows us to determine the deformation ring $R_{\bar\rho}^{\eta,\tau}$.

[2]Note that we may assume that $\gamma' \equiv h-\gamma-\sum_{j=0}^{f-1} p^j \bmod p^f-1$ since otherwise the ring $R_{\bar\rho}^{\eta,\tau}$ is known to be zero, see [CDM23].

As a corollary, for any gene $\mathbb{X}$, we constructed a ring $R_{\mathbb{X}}$ quotient of polynomial ring over $\mathbf{Z}[t]$ modulo an ideal $I_{\mathbb{X}} \subset R_{\mathbb{X}}$ ([LHMM23]). This ring is independent of p and conjecture 1 is proved by showing that $R_{\bar\rho}^{\eta,\tau}$ is isomorphic to the completion of $R_{\mathbb{X}}/(t-p) \otimes \mathcal{O}$ at the ideal generated by t and the variables of $R_{\mathbb{X}}$, where $\mathbb{X} = \mathbb{X}(\tau, \bar\rho)$.

Theorem 1 (Theorem 5.4.16 [LHMM23])**.** *Conjecture 1 is true.*

In fact, we obtain in [LHMM23] a more general version of Theorem 1 also valid for reducible Galois representations.

3. An example

Take $f = 6$, $p > 103$, $h = p^5 - p^4 + 2p^2 + 1$ and

$$\gamma = -p^4 - p^3 + p^2 - p + 1 \text{ and } \gamma' = -p^4 - 1.$$

Then, for this explicit example, we obtain $\mathbb{X} = \mathbb{X}(\tau, \bar\rho)$ a given below:

$\mathbb{X}_0 = \mathtt{B}$	$\mathbb{X}_1 = \mathtt{A}$	$\mathbb{X}_2 = \mathtt{AB}$	$\mathbb{X}_3 = \mathtt{O}$	$\mathbb{X}_4 = \mathtt{AB}$	$\mathbb{X}_5 = \mathtt{O}$
$\mathbb{X}_6 = \mathtt{A}$	$\mathbb{X}_7 = \mathtt{B}$	$\mathbb{X}_8 = \mathtt{A}$	$\mathbb{X}_9 = \mathtt{A}$	$\mathbb{X}_{10} = \mathtt{A}$	$\mathbb{X}_{11} = \mathtt{B}$

3.1. **The Kisin variety.** By [CDM18], we can extract from $\mathbb{X}(\tau, \bar\rho)$ the explicit description of the Kisin variety associated to $\bar\rho$ and τ as a subvariety of $([x_i : y_i])_{0 \le i \le 5} \in (\mathbf{P}^1_{\mathbf{F}})^f$ given by the following equations $y_3 = 0 = y_5 = 0$, $x_0 y_1 = y_1 x_2 = x_2 y_3 = x_3 y_4 = 0$. Hence, for our explicit example, the Kisin variety associated to $\bar\rho$ and τ is the union of a projective line and a projective plane:

$$\left\{ \begin{array}{l} [x_0 : y_0] \times [1:0] \times [x_2 : y_2] \times [1:0] \times [1:0] \times [1:0] \\ \cup [0:1] \times [x_1 : y_1] \times [0:1] \times [1:0] \times [1:0] \times [1:0] \end{array}, [x_i : y_i] \in \mathbf{P}^1_{\mathbf{F}}, 0 \le i \le 2 \right\}.$$

3.2. **Common weights and irreducible components.** In [CDM23], we give an algorithm to construct the set $W(\tau, \bar\rho)$ of common weighs of $\bar\rho$ and τ from $\mathbb{X}$. It is given up to torsion by some powers of the determinant by $\otimes_{i=0}^5 (\mathrm{Sym}^{r_i} \mathbf{F}^2)^{\tau_i}$ for

$$(r_i)_{0 \le i \le 5} \in \left\{ \begin{array}{cc} (1, p-1, p-2, 0, p-2, p-1), & (1, p-1, 0, p-1, p-1, p-1), \\ (0, p-1, p-2, 0, 0, 0), & (1, p-1, p-2, p-2, p-1, p-1) \end{array} \right\}.$$

By [LHMM23], we have

$$R_{\bar\rho}^{\eta,\tau} = \frac{\mathcal{O}[[Y_5, X_0, X_1, X_2, X_3]]}{(X_1 X_2 X_3 Y_5 + p(X_1 + X_2) Y_5 + p^2 X_2 X_3 + p^3)} \hat\otimes \mathcal{O}[[X_5, Y_3]]$$

where the first and second summand are respectively the rings R_0 and R_1 associated to:

$\mathbb{X}_{11} = \mathtt{B}$	$\mathbb{X}_0 = \mathtt{B}$	$\mathbb{X}_1 = \mathtt{A}$	$\mathbb{X}_2 = \mathtt{AB}$	$\mathbb{X}_3 = \mathtt{O}$
$\mathbb{X}_5 = \mathtt{O}$	$\mathbb{X}_6 = \mathtt{A}$	$\mathbb{X}_7 = \mathtt{B}$	$\mathbb{X}_8 = \mathtt{A}$	$\mathbb{X}_9 = \mathtt{A}$

$\rightsquigarrow R_0$

and to

$$\boxed{\begin{array}{ccc} \mathbb{X}_3 = \mathtt{0} & \mathbb{X}_4 = \mathtt{AB} & \mathbb{X}_5 = \mathtt{0} \\ \mathbb{X}_9 = \mathtt{A} & \mathbb{X}_{10} = \mathtt{A} & \mathbb{X}_{11} = \mathtt{B} \end{array}} \rightsquigarrow R_1$$

We immediately check that the number of irreducible components of $R_{\bar{\rho}}^{\eta,\tau}/(\pi_E)$ is 4 and is equal to the cardinal of $W(\tau, \bar{\rho})$.

References

[BB10] L. Berger, C. Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbf{Q}_p$, Astérisque 330, 2010, 155-211.

[BDJ10] K. Buzzard, F. Diamond, F. Jarvis, *On Serre's conjecture for mod ℓ Galois representations over totally real fields*, Duke Math. J. 155, 2010, 105-161.

[BM02] C. Breuil, A. Mézard, *Multiplicités modulaires et représentations de* $\mathrm{GL}_2(\mathbf{Z}_p)$ *et de* $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ *en* $\ell = p$, with an appendix by Guy Henniart, Duke Math. J. **115** (2002), 205–310.

[CEGS20] A. Caraiani, M. Emerton, T. Gee, D. Savitt, *Local geometry of moduli stacks of two dimensional Galois representations*, Proceedings of the International Colloquium on Arithmetic Geometry, TIFR Mumbai, Jan 6-10, (2020).

[CDM18] X. Caruso, A. David, A. Mézard, *Variétés de Kisin strafiées et déformations potentiellement Barsotti–Tate*, J. Inst. Math. Jussieu **17** (2018), 1019–1064.

[CDM23] ———, *Combinatorics of Serre weights in the potentially Barsotti–Tate setting*, Moscou J. Comb. Number Theory **12** (2023), 1–56.

[Co10] P. Colmez, *Série principale unitaire de* $\mathrm{GL}_2(\mathbf{Q}_p$, Astérisque 330, 2010, 213–262.

[GK14] T. Gee, M. Kisin, *The Breuil-Mézard conjecture for potentially Barsotti–Tate representations*, Forum of Mathematics, Pi, 2014.

[Ki08] M. Kisin, *Potentially semi-stable deformation rings*, J. Amer. Math. Soc. **21** (2) (2008), 513—546.

[Ki09] ———, *The Fontaine-Mazur conjecture for* GL_2, J. Amer. Math. Soc. **22** (3) (2009), 641—690.

[LHMM23] B. Le Hung, A. Mézard, S. Morra, *Local model theory for non-generic tame potentially Barsotti–Tate deformation rings*, Preprint 2023.

[PR09] G. Pappas, M. Rapoport, *Φ-modules and coefficient spaces*, Mosc. Math. J. 9, 2009, 625–663.

Galois action on cyclic Beyli curves

Rachel Pries

By Grothendieck's philosophy, the absolute Galois group of $\mathbb{Q}$ is determined by how it acts on curves that are covers of the projective line branched at $\{0, 1, \infty\}$. There are open questions about this even in the most simple case, when the cover is cyclic with prime degree. For example, consider the curve $X_k \colon y^p = x(x-1)^k$ for p prime and $1 \leq k < p-1$; it is a quotient of the Fermat curve of degree p.

We report on work in progress to reprove, and extend, some previous results of Greenberg [Gre81] and Kurihara [Ku92] on the arithmetic properties of p-torsion points of the Jacobian of certains families of curves via explicit methods on the étale homology of Fermat curves in [DPSW18].

In the first part of this report, I review a theorem of Greenberg [Gre81] and Kurihara [Ku92], about the p-torsion points of the Jacobian of X_k that are defined over the cyclotomic field $K = \mathbb{Q}(\zeta_p)$; the proof of this theorem relies on many foundational topics in algebraic number theory. In the second part of this report, I review some work of Anderson [And87] about the action of G_K on the étale homology of the Fermat curve of degree p with coefficients in $\mathbb{Z}/p\mathbb{Z}$; in earlier joint work with Davis, Stojanoska, and Wickelgren [DPSW18], we implemented and investigated this action. In future work, I will use this material to reprove and extend the result of Greenberg.

1. On arithmetic jacobian properties of a certain family of curves

In his paper, Greenberg establishes multiple results on the p-power torsion points of the Jacobian of the curve:

$$X'_a \colon y^p = x^a(1-x) \quad 1 \leq a \leq p-2$$

which is isomorphic to the curve $X_k \colon y^p = x(1-x)^k$ when $k = a^{-1}$, a quotient of a Fermat curve.

The Jacobian $J_k = \mathrm{Jac}(X_k)$ is a principally polarized abelian variety of dimension $g = (p-1)/2$. Let $\gamma \in \mathrm{Aut}(X_k)$ be the automorphism $\gamma((x,y)) = (x, \zeta y)$, where ζ is a pth-root of unity, and consider $\pi = \gamma - 1 \in \mathrm{End}(J(X_k))$. Since

$$1 + \gamma + \cdots + \gamma^{p-1} = 0 \text{ in } \mathrm{End}(J_k)$$

one has that $\mathbb{Z}[\zeta] \subset \mathrm{End}(J_k)$, and we deduce that J_k has complex multiplication by $K = \mathbb{Q}(\zeta_p)$.

For an integer s, let $J_k[\pi^s]$ denote the kernel of π^s. Note that

$$J_k[\pi] \subset J_k[\pi^2] \subset \cdots \subset J_k[\pi^{p-1}] = J_k[p].$$

A goal is to determine the field of definition of $J_k[\pi^s]$ for each $1 \leq s \leq p-1$.

1.1. Some number fields.

Recall that $K = \mathbb{Q}(\zeta_p)$. Let $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Let $E = \mathcal{O}_K^*$ (resp. $E^+ = \mathcal{O}_{K^+}^*$) denote the group of units in $\mathcal{O}_K$ (resp. $\mathcal{O}_{K^+}$).

Let $V \subset K^*$ be the subgroup generated by $\{\pm\zeta, 1-\zeta^i \mid 1 \leq i \leq p-1\}$. Consider the cyclotomic units $C = V \cap E$ of K and the real cyclotomic units $C^+ = C \cap E^+$ of K^+.

For an integer j, consider the real cyclotomic unit $\eta_j = \zeta^{(1-j)/2}(1-\zeta^j)/(1-\zeta)$. Then C^+ is generated by $\{-1, \eta_j \mid 1 < j \leq (p-1)/2\}$.

Let L be the splitting field of $1-(1-x^p)^p$ over $\mathbb{Q}$. Let $L_{cyc^+} = K(\sqrt[p]{\eta_j})_{1<j\leq(p-1)/2}$.

1.2. Some Theorems of Greenberg.

Among the many results of Greenberg, the three in our field of interest are as follows.

Theorem 1 (Greenberg Theorems [Gre81])**.** *For the curve X_k and with the previous notations as above:*

1. *$J_k[\pi^3] \subset J_k[p](K)$.*
2. *There is an equality if and only if $(E^+/C^+)_{p-3}$ is trivial, where the subscript $p-3$ denotes the $p-3$ eigenspace for the* $\mathrm{Gal}(K/\mathbb{Q})$ *action.*
3. *The field of definition of $\oplus_{k=1}^{p-2} J_k$ is L_{cyc^+}.*

We refer to Theorem 1 ibid. for (1), and to Theorem 4 ibid for (3).

The paper [Gre81] is only 15 pages, but it uses a wide variety of techniques in arithmetic geometry and algebraic number theory.

1.3. **A plethora of arithmetic geometry and number theory techniques.** I include an outline of Greenberg's proof below. I first recall how to obtain part (1) of Theorem 1.

(1) *Weil divisors.* The p-torsion $J_k[p]$ can be described using Weil divisors.
(2) *Galois representations.* Let F be a number field and G_F its absolute Galois group. Let ρ be the Galois representation of G_F on the Tate module. Then $J[p^\infty](F) = J[\pi^s]$ if and only if s is the maximum integer such that $\rho(\sigma) \equiv 1 \bmod \pi^s$ for all $\sigma \in G_F$.
(3) One can show $J_k[\pi] = J[p](\mathbb{Q})$ using the degree 0 divisor $\eta_0 - \eta_\infty$; here η_0 is the point $(0,0)$ and η_∞ is the point at infinity on J_k.
(4) *Weil pairing.* Using the Weil pairing, Greenberg shows that $J_k[p](K) = J_k[\pi^s]$ for an odd integer s.
(5) *Norm computation.* A longer calculation with unit groups and norms shows that $s > 1$. This stage completes the proof of (1) in Theorem 1, that is $J_k[\pi^3] \subset J_k[p](K)$.

Let us sketch how to obtain parts (2) and (3) of Theorem 1.

(1) *Zeta functions and Jacobi sums.* Working with the zeta function of X_k over a finite field, Greenberg shows that the value $\rho(\sigma)$ can be expressed as the conjugate of a Jacobi sum $g(1)g(k)/g(1+k)$.
(2) *Artin map.* Using the Artin map, he computes the rank d_k over $\mathbb{Z}_p$ of the field generated by all points of p-power order over $\bar{K}$. By [Gre81, Theorem 2], one obtains that $0 \le d_k \le (p+1)/2$.
(3) Working over the local field $K_p = \mathbb{Q}_p(\zeta_p)$, Greenberg shows that $J_k[\pi^4] \subset J_k(K_p)$ if and only if p divides the Bernouilli number B_{p-3}, which can happen, e.g. when $p = 16843$.
(4) *Eigenspace decompositions.* Finally, Greenberg considers $L^{(k)}$, the field of definition of $J_k[p]$. He decomposes the Galois group of $L^{(k)}/K$ into eigenspaces for the action of $\mathrm{Gal}(K/\mathbb{Q})$.
(5) *Artin–Hasse reciprocity law, and Bauer's theorem.* The ith eigenspace determines an extension of K which equals K or $K(\sqrt[p]{\eta_j})$ where $i + j = p$. To prove this, Greenberg uses power residue symbols, the Artin–Hasse reciprocity law, and Bauer's theorem about a Galois field extension being determined by the set of primes that split completely. This stage yields parts (2) and (3).

Remark 1.

(1) *On the $\mathbb{Z}_p$-rank in (2) of Theorem 1.* One shows that $d_k < (p+1)/2$ in numerous examples.
(2) Later, Tzermias found explicit divisors that generate $J_k[\pi^2]$ and $J_k[\pi^3]$, see [Tz00].

1.4. **A p-Sylow Class group condition.** Let $(\mathrm{Cl}_K)_p$ denote the p-Sylow subgroup of the class group of K. Then $(E^+/C^+)_{p-3}$ is trivial if and only if $(\mathrm{Cl}_K)_{p,p-3}$ is trivial. Using Quillen K-groups, Kurihara proved that $(\mathrm{Cl}_K)_{p,p-3}$ is trivial for all p, see [Ku92, Corollary 3.8].

First, Lee and Szczarba proved that $K_4(\mathbb{Z}) = 0$ modulo 2 and 3 torsion. Then, Kurihara proved that $K_{2r-2}(\mathbb{Z})$ contains $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(r))$ as a summand.

When $r = 3$, this shows that $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(3)) = 0$, which implies that $(\mathrm{Cl}_K)_{p,p-3}$ is trivial.

2. Explicit Galois action via étale homology

For the Fermat curve $X : x^p + y^p = 1$ of degree p and the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, Anderson described the action of G_K on the étale homology $H_1(X; \mathbb{Z}/p\mathbb{Z})$; he proved that it factors through L/K where L is the splitting field of $1 - (1 - x^p)^p$ [And87, Section 10.5]. Anderson shows that this action is determined by an analogue of the classical gamma function. It can be analyzed by taking a logarithmic derivative and working in the module of Kähler differentials. We refer to [AI88] for similar results.

In [DPSW18, Theorem 1.1], the authors found an explicit formula for the action of each $\sigma \in \mathrm{Gal}(L/K)$ on $H_1(X; \mathbb{Z}/p\mathbb{Z})$, when p satisfies Vandiver's conjecture. This proof uses Kummer maps and motivic homology. We refer to [AHGT21] for an overview of this work.

This talk was an announcement of work that will appear in a future paper. In this paper, I will use the material in Section 2 to reprove and extend the Theorem in Section 1 about the field of definition of $J_k[\pi^s]$; specifically, I reprove the theorem for $s = 3$ and extend it for $s = 5$.

The main point is that the proof does not need most of the results in algebraic number theory listed in Section 1. Instead, it is possible to: first identify the kernel of π^s with a subspace of the homology of J_k with coefficients in $\mathbb{Z}/p\mathbb{Z}$; and second to use the explicit formulas for the action found in [DPSW18, Theorem 1.1] to determine the subgroup of the absolute Galois group G_K that fixes that subspace. Stay tuned!

Acknowledgement. This research was supported in part by NSF grant DMS-22-00418.

References

[And87] G. W. Anderson, *Torsion points on Fermat Jacobians, roots of circular units and relative singular homology*, Duke Math. J. **54** (1987), no. 2, 501–561.

[AI88] G. Anderson and Y. Ihara. Pro-l branched coverings of $\mathbf{P}^1$ and higher circular l-units. *Ann. of Math. (2)*, 128(2):271–293, 1988.

[DPSW18] R. Davis, R. Pries, V. Stojanoska, and K. Wickelgren, *The Galois action and cohomology of a relative homology group of Fermat curves*, J. Algebra **505** (2018), 33–69.

[Gre81] R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. **42** (1980/81), no. 3, 345–359.

[Ku92] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbf{Z}$, Compositio Math. **81** (1992), no. 2, 223–236.
[AHGT21] R. Pries, *Galois action on the étale fundamental group of the Fermat curve*, in "Homotopic and Geometric Galois Theory" (B. Collas, P. Dèbes, H. Nakamura, J. Stix Ed.) Oberwolfach Rep. **18** (2021), no. 1, pp. 663–744.
[Tz00] P. Tzermias, *Explicit rational functions on Fermat curves and a theorem of Greenberg*, Compositio Math. **122** (2000), no. 3, 337–345.

On the geometric outer monodromy representation associated to the moduli stack of hyperbolic curves

Yu Iijima

We give a panorama of recent progress on some properties of geometric and non-geometric universal outer monodromy representations for the moduli stack of hyperbolic curves in their pro-Σ and pro-l versions. This includes results on the universal fixed field including a conjecture due to Oda, see [Tak12, §0], on the congruence subgroup problem, see [Iva06, §1], and on the geometric version of the Grothendieck conjecture for hyperbolic curves via the combinatorial anabelian geometry.

Throughout this report, we consider Σ a nonempty set of prime numbers, we fix l a prime number, (g, r) a pair of nonnegative integers such that $2g-2+r$ is a positive integer, and we take k a field of characteristic zero, with $\overline{k}$ an algebraically closure of k. We shall denote by $\mathcal{P}$ the set of all prime numbers.

1. The geometric outer monodromy representation associated to the moduli stack of hyperbolic curves

The moduli stack $\mathcal{M}_{g,r}$ of r-pointed smooth proper curves of genus g over k whose r marked points are equipped with an ordering comes with an universal curve $\mathcal{C}_{g,r} \to \mathcal{M}_{g,r}$ over $\mathcal{M}_{g,r}$. This provides an exact sequence of profinite groups

$$1 \longrightarrow \mathit{\Pi}_{g,r} \longrightarrow \pi_1(\mathcal{C}_{g,r}) \longrightarrow \pi_1(\mathcal{M}_{g,r}) \longrightarrow 1 \tag{1}$$

where $\mathit{\Pi}_{g,r}$ denotes the étale fundamental group of a geometric fiber of $\mathcal{C}_{g,r} \to \mathcal{M}_{g,r}$ (which is the hyperbolic curve obtained by removing r distinct points from a smooth proper curve of genus g over $\overline{k}$).

We further write $\mathit{\Gamma}_{g,r}$ for the étale fundamental group of $\mathcal{M}_{g,r} \otimes_k \overline{k}$, $\mathit{\Pi}^{\Sigma}_{g,r}$ for the maximal pro-Σ quotient of $\mathit{\Pi}_{g,r}$, and $\mathit{\Pi}^{\Sigma}_{g}$ for the quotient of $\mathit{\Pi}^{\Sigma}_{g,r}$ determined by the smooth compactification of the geometric fiber of $\mathcal{C}_{g,r} \to \mathcal{M}_{g,r}$.

Definition 1. With the notations above, we shall write

$$\rho^{\Sigma}_{g,r} \colon \pi_1(\mathcal{M}_{g,r}) \longrightarrow \mathrm{Out}(\mathit{\Pi}^{\Sigma}_{g,r}) \text{ and } \rho^{\Sigma\text{-geo}}_{g,r} \colon \mathit{\Gamma}_{g,r} \longrightarrow \mathrm{Out}(\mathit{\Pi}^{\Sigma}_{g,r})$$

for the outer action determined by the exact sequence (1) and for the restriction of $\rho^{\Sigma}_{g,r}$ to $\mathit{\Gamma}_{g,r}$ respectively. We shall refer to $\rho^{\Sigma}_{g,r}$ as the *universal pro-Σ outer monodromy representation* associated to $\mathcal{M}_{g,r}$, and $\rho^{\Sigma\text{-geo}}_{g,r}$ as the *geometric pro-Σ outer monodromy representation* associated to $\mathcal{M}_{g,r}$.

Note that $\mathcal{M}_{0,3}$, and $\mathcal{C}_{0,3}$ is naturally isomorphic to $\operatorname{Spec} k$, and $T := \mathbb{P}^1_k \setminus \{0, 1, \infty\}$, respectively. In particular, $\rho^{\Sigma}_{0,3}$ may be identified with the pro-Σ outer Galois representation associated to T. Thus, we shall write also $\rho^{\Sigma}_T := \rho^{\Sigma}_{0,3}$.

Remark 1. Write $\mathrm{MCG}_{g,r}$ for the mapping class group of an r-pointed Riemann surface of genus g whose r marked points are equipped with an ordering, and $\Pi^{\mathrm{disc}}_{g,r}$ for the topological fundamental group of an r-punctured Riemann surface of genus g. Then $\Gamma_{g,r}$ is naturally isomorphic to the profinite completion of $\mathrm{MCG}_{g,r}$, and the natural faithful outer representation $\mathrm{MCG}_{g,r} \hookrightarrow \mathrm{Out}(\Pi^{\mathrm{disc}}_{g,r})$ fits into a commutative diagram of groups

$$\begin{tikzcd} \mathrm{MCG}_{g,r} \arrow[r, hook] \arrow[d, hook] & \mathrm{Out}(\Pi^{\mathrm{disc}}_{g,r}) \arrow[d, hook] \\ \Gamma_{g,r} \arrow[r, "\rho^{\Sigma\text{-geo}}_{g,r}"'] & \mathrm{Out}(\Pi^{\Sigma}_{g,r}), \end{tikzcd}$$

where the upper horizontal arrow and the vertical arrows are injective.

Write $G_k := \mathrm{Gal}(\overline{k}/k)$. The following theorem is fundamental for $\rho^{\Sigma}_{g,r}$ and $\rho^{\Sigma\text{-geo}}_{g,r}$.

Theorem 1 (Ihara, Oda, Nakamura, Takao, Ueno, Matsumoto, Hoshi–Mochizuki)**.** *Suppose that Σ is equal to either $\mathcal{P}$ or $\{l\}$. Then the kernel of the natural homomorphism $G_k \twoheadrightarrow \mathrm{im}(\rho^{\Sigma}_{g,r})/\mathrm{im}(\rho^{\Sigma\text{-geo}}_{g,r})$ is equal to the kernel of ρ^{Σ}_T.*

In the above, one has identified $G_k \simeq \pi_1(\mathcal{M}_{g,r})/\Gamma_{g,r}$. We refer to [Tak12, Theorem 0.5, (2)], [NodNon, Corollary 6.4] for proof and original statements.

Remark 2. It is well-known that the kernel of $\rho^{\mathcal{P}}_T$ is equal to the kernel of the natural homomorphism $G_k \to G_{\mathbb{Q}}$ (cf. [Bel79, Corollary to Theorem 4]). Also, the field corresponding to the kernel of $\rho^{\{l\}}_T$ is generated by the higher circular l-units, i.e., the elements of $\overline{k}$ obtained from the set $\{0, 1, \infty\}$ by iterated processes of taking l-power and cross ratios (cf. [AI88, Theorem B]).

In the rest of this report, we assume that $k = \overline{k}$, hence also, $\pi_1(\mathcal{M}_{g,r}) = \Gamma_{g,r}$ and $\rho^{\Sigma}_{g,r} = \rho^{\Sigma\text{-geo}}_{g,r}$.

2. The congruence subgroup problem of the mapping class group

The following problem is known as the congruence subgroup problem of the mapping class group.

Problem 1. Is the universal pro-$\mathcal{P}$ outer monodromy representation $\rho^{\mathcal{P}}_{g,r}$ injective?

For the congruence subgroup problem of the mapping class group, the following affirmative results are known.

Theorem 2 (Asada, Boggi)**.** *Suppose that $g \leq 2$. Then $\rho^{\mathcal{P}}_{g,r}$ is injective.*

We refer to [Asa01, Theorem] for genus 0, 1 and [Bog20, Theorem 1.4, (ii)] for $g = 2$ for proofs and original statements. See also to [DDH89] for $g = 0$.

Let us introduce a pro-l version of the congruence subgroup problem of the mapping class group.

Definition 2. We shall write $\Gamma_{g,r}[l]$ for the kernel of the natural action $\Gamma_{g,r} \to \mathrm{Aut}((\Pi_g^{\{l\}})^{\mathrm{ab}} \otimes_{\mathbf{Z}_l} (\mathbf{Z}/l))$ determined by $\rho_{g,r}^{\{l\}}$, and $\Gamma_{g,r}\{l\}$ for the maximal pro-$\{l\}$ quotient of $\Gamma_{g,r}[l]$. Note that the restriction $\rho_{g,r}^{\{l\}}|_{\Gamma_{g,r}[l]} \colon \Gamma_{g,r}[l] \to \mathrm{Out}(\Pi_{g,r}^{\{l\}})$ of $\rho_{g,r}^{\{l\}}$ to $\Gamma_{g,r}[l]$ factors through $\Gamma_{g,r}[l] \twoheadrightarrow \Gamma_{g,r}\{l\}$. We shall write

$$\rho_{g,r}^{l\text{-csp}} \colon \Gamma_{g,r}\{l\} \longrightarrow \mathrm{Out}(\Pi_{g,r}^{\{l\}})$$

for the resulting homomorphism.

The following problem may be regarded as a pro-l version of the congruence subgroup problem of the mapping class group.

Problem 2. Is $\rho_{g,r}^{l\text{-csp}}$ injective?

For the pro-l congruence subgroup problem of the mapping class group, the following affirmative results are known.

Theorem 3 (Asada, Hoshi–Iijima, Boggi)**.** *Suppose that one of the following two conditions is satisfied:* (a) $g = 0$ *or* (b) $g \leq 2$ *and* $l = 2$*. Then* $\rho_{g,r}^{l\text{-csp}}$ *is injective.*

We refer to the remark at the end of [Asa01, §1], [Bog20, Theorem 1.4, (ii)] for proof and original statements.

On the other hand, for the pro-l congruence subgroup problem of the mapping class group, the following negative result is also known.

Theorem 4 (Hoshi–Iijima)**.** *Suppose that* $g = 1$*, and that* $l > 7$*. Then* $\rho_{g,r}^{l\text{-csp}}$ *is not injective.*

We refer to [HI19, Theorem A, (ii)] for proof and original statement.

3. A geometric version of the Grothendieck conjecture for the moduli stack of hyperbolic curves

We introduce a subgroup of $\mathrm{Out}(\Pi_{g,r}^{\Sigma})$ for the study of the universal pro-Σ outer monodromy representation.

Definition 3. We shall write $\mathrm{Out}^{\mathrm{C}}(\Pi_{g,r}^{\Sigma})$ for *the group of C-admissible outer automorphisms of* $\Pi_{g,r}^{\Sigma}$, i.e., outer automorphisms which induce self-bijections of the set of conjugacy classes of cuspidal inertia subgroups of $\Pi_{g,r}^{\Sigma}$.

Note that $\rho_{g,r}^{\Sigma} \colon \Gamma_{g,r} \longrightarrow \mathrm{Out}(\Pi_{g,r}^{\Sigma})$ factors through $\mathrm{Out}^{\mathrm{C}}(\Pi_{g,r}^{\Sigma}) \hookrightarrow \mathrm{Out}(\Pi_{g,r}^{\Sigma})$.

Let H be an open subgroup of $\Gamma_{g,r}$. We consider the group $\mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r})$ of automorphisms of the universal curve $\mathcal{C}_{g,r}$ over $\mathcal{M}_{g,r}$, and the group $\mathrm{Aut}_{\Gamma_{g,r}}(\pi_1(\mathcal{C}_{g,r}))$

of automorphisms of $\pi_1(\mathcal{C}_{g,r})$ over $\Gamma_{g,r}$ and the natural surjection $\pi_1(\mathcal{C}_{g,r}) \twoheadrightarrow \Gamma_{g,r}$. We then obtain a composition of natural homorphisms

$$\begin{aligned}(2)\quad \mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r}) &\longrightarrow \mathrm{Aut}_{\Gamma_{g,r}}(\pi_1(\mathcal{C}_{g,r}))/\mathrm{Inn}(\Pi_{g,r}) \\ &\longrightarrow Z_{\mathrm{Out}(\Pi^{\Sigma}_{g,r})}(\mathrm{im}(\rho^{\Sigma}_{g,r})) \subseteq Z_{\mathrm{Out}(\Pi^{\Sigma}_{g,r})}(\rho^{\Sigma}_{g,r}(H))\end{aligned}$$

where $Z_{(\cdot)}(\cdot)$ denotes the centralizer.

The following theorem is known as *a geometric version of the Grothendieck conjecture* for the moduli stack of hyperbolic curves which may be regarded as an analogue of the Grothendieck conjecture for a single hyperbolic curve.

Theorem 5 (Hoshi–Mochizuki)**.** *Let H be an open subgroup of $\Gamma_{g,r}$, and suppose that $2g-2+r>1$. Then the composite of natural homomorphisms of Eq.* (2) *determines an isomorphism*

$$\mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r}) \xrightarrow{\sim} Z_{\mathrm{Out^C}(\Pi^{\Sigma}_{g,r})}(\rho^{\Sigma}_{g,r}(H)).$$

In the case above, note that $\mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r})$ is isomorphic to

$$\begin{cases}\mathbf{Z}/2\times\mathbf{Z}/2 & \text{if } (g,r)=(0,4);\\ \mathbf{Z}/2 & \text{if } (g,r)\in\{(1,1),(1,2),(2,0)\};\\ \{1\} & \text{if } (g,r)\notin\{(0,4),(1,1),(1,2),(2,0)\}.\end{cases}$$

For proof and original statement, we refer to [CbTpI, Theorem D, (i)].

The author proved the following theorem which is a generalization of Theorem 5.

Theorem 6 (Iijima)**.** *Let H be an open subgroup of $\Gamma_{g,r}$, and suppose that $2g-2+r>1$. Then the composite of natural homomorphisms of Eq.* (2) *determines an isomorphism*

$$\mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r}) \xrightarrow{\sim} Z_{\mathrm{Out}(\Pi^{\Sigma}_{g,r})}(\rho^{\Sigma}_{g,r}(H)).$$

We refer to [Iij23, Theorem A] for a proof and original statement.

Remark 3. By combining Theorem 3 with the commutative diagram of groups of Remark 1, we may obtain an isomorphism

$$\mathrm{Aut}_{\mathcal{M}_{g,r}}(\mathcal{C}_{g,r}) \xrightarrow{\sim} Z_{\mathrm{Out}(\Pi^{\mathrm{disc}}_{g,r})}(\mathrm{MCG}_{g,r})$$

even if $r>0$, cf. [Iij23, Corollary 4.2].

References

[AI88] G. Anderson and Y. Ihara. Pro-l branched coverings of $\mathbf{P}^1$ and higher circular l-units. *Ann. of Math. (2)*, 128(2):271–293, 1988.

[Asa01] M. Asada. The faithfulness of the monodromy representations associated with certain families of algebraic curves. *J. Pure Appl. Algebra*, 159(2-3):123–147, 2001.

[Bel79] G. V. Belyĭ. Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(2):267–276, 479, 1979.

[Bog20] M. Boggi. Congruence topologies on the mapping class group. *J. Algebra*, 546:518–552, 2020.

[DDH89] S. Diaz, R. Donagi, and D. Harbater. Every curve is a Hurwitz space. *Duke Math. J.*, 59:737–746, 1989.

[HI19] Y. Hoshi and Y. Iijima. A pro-l version of the congruence subgroup problem for mapping class groups of genus one. *J. Algebra*, 520:1–31, 2019.
[NodNon] Y. Hoshi and S. Mochizuki. On the combinatorial anabelian geometry of nodally nondegenerate outer representations. *Hiroshima Math. J.*, 41(3):275–342, 2011.
[CbTpI] Y. Hoshi and S. Mochizuki. Topics surrounding the combinatorial anabelian geometry of hyperbolic curves I: inertia groups and profinite Dehn twists. In *Galois-Teichmüller theory and arithmetic geometry*, volume 63 of *Adv. Stud. Pure Math.*, pages 659–811. Math. Soc. Japan, Tokyo, 2012.
[Iij23] Y. Iijima. On the centralizer of the image of the universal outer monodromy representation of the moduli stack of pointed hyperbolic curves. to appear in *Manuscripta Math.*
[Iva06] N. Ivanov. Fifteen problems about the mapping class groups in Problems on mapping class groups and related topics, In *Proc. Sympos. Pure Math.*, vol, 74, pages 71–80. Amer. Math. Soc, 2006.
[Tak12] N. Takao. Braid monodromies on proper curves and pro-ℓ Galois representations. *J. Inst. Math. Jussieu*, 11(1):161–181, 2012.

Covers of $\mathbb{P}^1$ and their moduli: where arithmetic, geometry and combinatorics meet

Béranger Seguin

During the last fifty years, the theory of finite branched covers of the projective line has played a major role in inverse Galois theory. The main reason behind this success is that this theory makes it possible to use topological and geometric arguments to study Galois theory over function fields (with consequences over number fields because of Hilbert's irreducibility theorem). Moreover, the topological objects involved admit combinatorial descriptions — this has allowed computational approaches to shed new light on various aspects of inverse Galois theory.

In this report, we present two contributions: the first one is the description of combinatorial objects generalizing *dessins d'enfants* to covers of the line with arbitrary numbers of branch points, the second one is a patching result over number fields for components of Hurwitz spaces, i.e. irreducible families of covers.

For the whole report, we fix a finite group G and an integer n.

1. Covers of the line

We fix a set $\underline{t} = \{t_1, \dots, t_n\}$ of n distinct points of the complex projective line $\mathbb{P}^1(\mathbb{C})$ (which we call a *configuration*) and a basepoint $t_0 \in \mathbb{P}^1(\mathbb{C}) \setminus \underline{t}$. We start by recalling some terminology to avoid any ambiguity.

1.1. *G***-covers.** In this report, a *cover* (branched at $\underline{t}$) always refers to a finite covering map $p : Y \to \mathbb{P}^1(\mathbb{C}) \setminus \underline{t}$. A *marked* cover comes with a point in the fiber $p^{-1}(t_0)$. A *G-cover* comes with a group morphism $G \to \mathrm{Aut}(p)$ inducing a simply transitive action of G on $p^{-1}(t_0)$. We do **not** require connectedness. *Connected* G-covers are Galois covers with automorphism group isomorphic to G.

The *monodromy morphism* of a marked G-cover is a group morphism $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \underline{t}, t_0) \to G$, which is surjective if and only if the cover is connected. Its image is the *monodromy group* of the cover. Each group morphism $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \underline{t},\, t_0) \to G$ is the monodromy morphism of a marked G-cover, unique up to isomorphism.

Since the fundamental group of $\mathbb{P}^1 \setminus \underline{t}$ is generated by loops $\gamma_1, \ldots, \gamma_n$ subject to the sole relation $\gamma_1 \cdots \gamma_n = 1$, isomorphism classes of marked G-covers branched at $\underline{t}$ correspond to n-tuples $(g_1, \ldots, g_n)$ of elements of G (the *monodromy elements*) satisfying $g_1 \cdots g_n = 1$. Connectedness corresponds to the condition that the monodromy elements generate G.

1.2. **Generalized dessins.** In the case $n = 3$, a combinatorial model of covers of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ has been introduced in [Gro97] under the name *dessins d'enfants*. The case $n = 3$ is special in two ways:

(1) Since $\mathrm{PSL}_2(\mathbb{C})$ acts 3-transitively on points, all choices of $\underline{t}$ are equivalent.
(2) This case is universal for the study of algebraic curves: by Belyĭ's theorem, every curve defined over $\bar{\mathbb{Q}}$ covers $\mathbb{P}^1(\mathbb{C})$ with at most 3 branch points.

However, if one is interested not in algebraic curves, but in covers (*morphisms* between curves) with arbitrary numbers of branch points, which many applications in inverse Galois theory involve, then this description is not enough. For example, there are no connected G-covers when $n = 3$ and G is not 2-generated.

In ongoing work[1], we define and study a notion of "generalized dessins". These objects may be described as $(n-1)$-partite "rainbow-colored" hypermaps (instead of being edges, the "hyperedges" are $(n-1)$-gones with one vertex of each color, and there are $n-1$ colors) embedded on surfaces. One hope is that, starting with this description, a program to describe the Galois action on covers combinatorially is developed, in the spirit of Grothendieck-Teichmüller theory which has basically (although this is a vast simplification) come out of the case $n = 3$.

Here is an example:

gendess.pdf

Fig 1. A generalized dessin corresponding to the case $n = 4$, where we have labeled the hyperedges (grey triangles)

Write down the cycles corresponding to the appearance order of the hyperedges during a counterclockwise rotation around each white vertex. The product of these cycles defines a permutation $\sigma_\circ = (152)(364)$ of the hyperedges. Doing the same for crossed and black vertices yields $\sigma_\otimes = (14)$ and $\sigma_\bullet = (16)(24)(35)$. Finally, let $\sigma_\infty = (\sigma_\circ\, \sigma_\otimes\, \sigma_\bullet)^{-1} = (13)(45)$, whose four cycles correspond to the four connected components of the complement of the dessin (i.e. the white areas) – depending on which component the $\bullet\!\!-\!\!\circ$ boundary of a given hyperedge touches. The permutations $\sigma_\circ, \sigma_\otimes, \sigma_\bullet, \sigma_\infty$ are the monodromy elements of a cover: this dessin corresponds to a non-Galois connected cover of degree 6 of the projective line branched at four

[1]At the moment, this work has only been made public as a series of blog posts, accessible at the following URL: `https://lebarde.alwaysdata.net/blog/2023/dessins-1/`.

points. Its monodromy group is the subgroup of $\mathfrak{S}_6$ generated by $\sigma_\circ$, $\sigma_\otimes$, and $\sigma_\bullet$, which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_4$. This cover has genus 0 (it is embedded in this page!).

triangle.pdf

Fig 2. A triangle, drawn on $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, t_2, t_3, \infty\}$, whose preimage under a covering map gives the corresponding dessin.

2. Patching components of Hurwitz spaces over number fields

In this section, we present Hurwitz spaces, their components, and the gluing of components, and we give number-theoretical applications of these objects. The original results in this section are all in [Seg22, Seg23b, Seg23a]. We fix a number field K.

2.1. **Hurwitz spaces.** Riemann's existence theorem implies that covers form a category equivalent to that of *algebraic covers*, i.e. generically étale finite morphisms from a smooth curve to $\mathbb{P}^1_{\mathbb{C}}$. Since smooth curves are determined by their function fields, connected G-covers correspond to Galois extensions of $\mathbb{C}(T)$ with Galois group G. If a G-cover is moreover defined over K, it corresponds to a *regular* extension $F|K(T)$, where regular means that $F \cap \bar{K} = K$.

There is a $\mathbf{Z}[1/|G|]$-scheme $\mathrm{Hur}^*_{G,n}$, the *Hurwitz space*, whose $\mathbb{C}$-points correspond to marked G-covers branched at n distinct points. Moreover, K-points of this scheme correspond to regular Galois G-extension of $K(T)$ having an unramified prime of degree 1. To put it shortly, this turns instances of the inverse Galois problem into Diophantine problems: do Hurwitz spaces have rational points?

2.2. **Fields of definitions of concatenated components.** From now on, we call *component* a geometrically connected component of the Hurwitz space $\mathrm{Hur}^*_{G,n}$. Since a K-point must lie in a component defined over K, fields of definition of components are of special interest for inverse Galois theory: they tell us where to look for. There is a topological *gluing* operation on components, induced in terms of tuples by the concatenation:

$$(g_1, \dots, g_n), (g'_1, \dots, g'_{n'}) \mapsto (g_1, \dots, g_n, g'_1, \dots, g'_{n'}).$$

We denote by xy the component obtained by gluing two components x and y. The focus of [Seg23b] is the following question:

Problem 1. Are components obtained by gluing components defined over K themselves defined over K?

Previous work on this question includes [Cau12], where Cau obtains some positive results generalizing those of [DE06]. The following result is [Seg23b, Theorem 5.4]:

Theorem 1. *Let x, y be components defined over K with respective monodromy groups H_1, H_2 ($\subseteq G$). Let $H = \langle H_1, H_2\rangle$. Then there is an element $\gamma \in H$ such that $H = \langle H_1, H_2^\gamma\rangle$ and such that xy^γ is defined over K.*

The proof of the theorem is in three steps:

Step 1 – construct infinitely many linearly disjoint extensions of K over which x and y have points. Take arbitrary geometric points in the components x and y lying above a K-rational configuration, and denote by K_1 the smallest Galois extension of K over which they are rational. By Hilbert's irreducibility theorem, there is a K-rational configuration above which the fibers of x and y are both irreducible over K_1. Choose arbitrary geometric points in the fibers of x and y above $\underline{t}$. Let K_2 be the smallest Galois extension of K over which these points are both rational. By irreducibility of the fibers, K_2 and K_1 are linearly disjoint over K. Iterate this process to define an infinite sequence $K_1, K_2, \ldots$ of pairwise linearly disjoint extensions of K such that for all $i \geq 1$, the components x, y both have K_i-points, denoted respectively f_i and g_i.

Step 2 – patching. See f_i and g_i as covers over the complete valued field $K_i(\!(X)\!)$. Use the algebraic variant of Harbater's theory of patching (cf. [HV96]) to patch them into a cover defined over $K_i(\!(X)\!)$ with monodromy group H. By a result of Cau [Cau12, Prop. 3.9], the patched cover is in a component c_i of the form $x^{\gamma_i'}y^{\gamma_i}$.

Step 3 – pigeonhole. Since there are finitely many components of the form $x^{\gamma'}y^{\gamma}$, there are distinct i, i' such that $c_i = c_{i'}$. The component $c_i = c_{i'}$ is defined over $\bar{K} \cap K_i(\!(X)\!) \cap K_{i'}(\!(X)\!) = K$. Finally, conjugate c_i by $(\gamma_i')^{-1}$ to ensure $\gamma' = 1$. □

This theorem may be used to construct components defined over $\mathbb{Q}$ with relatively few branch points compared to those constructed in [Cau12]:

Corollary 1 ([Seg23a, Proposition 8.4.8])**.** *If G is generated by elements $g_1, \ldots, g_n$ among which $m(i)$ elements are of order i, there is a component defined over $\mathbb{Q}$ of the Hurwitz space of connected G-covers whose number of branch points is $2m(2) + \sum_{i\geq 3} m(i)\varphi(i)$, where φ denotes Euler's totient function.*

For example, if the group G is generated by two elements with orders in $\{2, 3, 4, 6\}$, then there are components defined over $\mathbb{Q}$ of connected G-covers with four branch points (of Harbater-Mumford type). This applies to the Mathieu group M_{23} and to the group $\mathrm{PSL}_2(16) \rtimes \mathbb{Z}/2\mathbb{Z}$.

2.3. **The use of gluing for enumerative problems, and extensions of $\mathbb{F}_q(T)$.** Besides allowing to construct components with small fields of definition, the gluing operation also helps in estimating the asymptotical homology of Hurwitz spaces, which is key to the study of Malle's conjecture over function fields over finite fields. We refer to [ETW23] or to Westerland's talk in the present volume for additional details.

The gluing operation on components of Hurwitz spaces induces a ring structure on the set of formal sums of components (the "ring of components"). In [Seg22], we studied this ring closely in order to compute both the exponent (the "splitting number") and the leading coefficient of the asymptotical number of components as the number of branch points increases. This estimate has been applied in the updated version of [ETW23] to the question of the distribution of G-extensions of $\mathbb{F}_q(T)$.

References

[Cau12] O. Cau, *Delta-composantes des espaces de modules de revêtements*, Journal de Théorie des Nombres de Bordeaux **24.3** (2012), 557–582.

[ETW23] J. S. Ellenberg, T. Tran, and C. Westerland, *Fox-Neuwirth- Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields*, arXiv:1701.04541v2 [math.NT] (2023).

[DE06] P. Dèbes and M. Emsalem. *Harbater-Mumford Components and Towers of Moduli Spaces*, Journal of the Institute of Mathematics of Jussieu **5** (2006), 351–371.

[Gro97] A. Grothendieck, *Esquisse d'un programme* (1984). Published in *Geometric Galois Actions Vol. 1*, editors: P. Lochak, L. Schneps (1997), pp. 5-48 (English translation: pp. 243-283).

[HV96] D. Haran and H. Völklein, *Galois groups over complete valued fields*, Israel Journal of Mathematics **93** (1996), 9–27.

[Seg22] B. Seguin. *The Geometry of Rings of Components of Hurwitz Spaces*, arXiv:2210.12793 [math.NT] (2022)

[Seg23a] B. Seguin, *Géométrie et arithmétique des composantes des espaces de Hurwitz*, PhD thesis, Université de Lille (2023).

[Seg23b] B. Seguin, *Fields of Definition of Components of Hurwitz Spaces*, arXiv:2303.05903 [math.NT] (2023)

Twisted Heilbronn Virtual Characters

Go Yamashita

This report deals with some analyticity of Artin L-functions. We discuss a twisted version of Heilbronn characters, used for establishing zero-poles and analycity properties of Artin L-functions via group-theoretic machinery. We establish generalisations of (untwisted) theorems of Heilbronn, Stark, and Foote-Murty on holomorphicity and report generalisations of (untwisted) theorems of Hu-Kaneko-Martin-Schildkraut and Browkin on the zeros and poles of Artin L-functions. The proofs are similar as the ones in the untwisted versions except that we use a theorem in the finite group theory as a new ingredient in the theory of Heilbronn virtual characters, cf. [Yam23].

The original motivation of this study to provide complementary information to forthcoming developments of inter-universal Teichmüller theory, especially applications to L-functions and their distribution of zero-poles. However, at the time of writing, this study has no logical relation to them.

1. Analyticity results for Artin L-functions

Let F be a number field, and fix an algebraic closure $\overline{F}$ of F. Set $G_F := \mathrm{Gal}(\overline{F}/F)$ and consider K a finite Galois extension of F in $\overline{F}$. Set $G_K := \mathrm{Gal}(\overline{F}/K)$. We recall that to an Artin representation (= a continuous action on a finite dimensional $\mathbb{C}$-vector space) α of the Galois group G_K, one attaches an Artin L-function $L_K(s, \alpha)$

defined as an Euler product. Recall that an A-group is a group whose Sylow subgroups are all abelian (see also Definition 1 below):

Theorem 1 (Theorem 1.4 of [Yam23]). *Let F, K, and the Galois groups G_F and G_K as above. Let α be an Artin representation of G_F. We further assume that $\mathrm{Im}(\alpha|_{G_K})$ is an A-group. Then, for any irreducible Artin representation ρ of $\mathrm{Gal}(K/F)$, we have the following:*

(1) A generalisation of Heilbronn-Stark's theorem. *If $s = s_0 \neq 1$ is not a zero of $L_K(s, \alpha|_{G_K})$, then $L_F(s, \rho \otimes \alpha)$ is holomorphic at $s = s_0$ and does not vanish at $s = s_0$.*

(2) A generalisation of Stark's theorem. *If $L_K(s, \alpha|_{G_K})$ has a simple zero at $s = s_0 \neq 1$, then $L_F(s, \rho \otimes \alpha)$ is holomorphic at $s = s_0$, and the order of zero at $s = s_0$ is at most 1.*

(3) A generalisation of Foote-Murty, Aramata-Brauer's theorem. *Both of $L_K(s, \alpha|_{G_K})L_F(s, \rho \otimes \alpha)$ and $L_K(s, \alpha|_{G_K})L_F(s, \rho \otimes \alpha)^{-1}$ are holomorphic at $s \neq 1$.*

Here, note that $\rho \otimes \alpha$ is the tensor product representation of G_F when we regard ρ as the Artin representation of G_F via the natural quotient $G_F \twoheadrightarrow \mathrm{Gal}(K/F)$. For classical case (i.e., the case where α is the trivial representation), we refer to Heilbronn-Stark's theorem cf. [FGM15, p.471, l.12], Stark's theorem [Sta74, Theorem 3], and Foote-Murty, Aramata-Brauer's theorem [FM89, Corollary 4].

One also has the following two related results on zero and poles of Artin L-functions.

Theorem 2 (A generalisation of Hu-Kaneko-Martin-Schildkraut's theorem, Theorem 1.6 of [Yam23]). *Let K be any non-abelian finite Galois extension of F. Let χ be an Artin representation of G_K such that $\mathrm{Im}(\chi)$ is an A-group, and χ is extendable to G_F. Then, $L_K(s, \chi)$ has infinitely many zeros of order > 1 in the critical strip $0 < \mathrm{Re}(s) < 1$.*

We refer to [HKMS22, Theorem 1.1] for the classical case (i.e., the case where χ is the trivial representation).

Theorem 3 (A generalisation of Browkin's theorem, Theorem 1.7 of [Yam23]). *For any number field F and any natural number n, there exists a finite Galois extension K of F such that, for any Artin representation χ of G_K whose image is an A-group and which is extendable to G_F, $L_K(s, \chi)$ has infinitely many zeros of order $\geq n$ in the critical strip $0 < \mathrm{Re}(s) < 1$.*

We refer to [Bro13, Th. 5.1] for the classical case (i.e., the case where χ is the trivial representation).

2. Finite Group Properties

We recall some basic definitions in the theory of finite groups that will be applied to the case where G is a finite subquotient of the Galois group G_F.

Definition 1. Let G be a finite group.

(1) G is called **supersolvable**, if there exist subgroups $H_0 \subset H_1 \subset \cdots \subset H_n \subset G$ such that $H_0 = \{1\}$, $H_n = G$, all H_i's are normal subgroups of G, and all H_{i+1}/H_i's are cyclic.
(2) G is called an ***A*-group**, if all Sylow subgroups are abelian (Following P. Hall cf. [Ito52]).
(3) G is called **monomial**, or ***M*-group**, if any irreducible representation of G is the induced representation of a one-dimensional representation of a subgroup of G.

It is well-known that any supersolvable group is monomial. Ito's theorem says that any A-group is monomial [Ito52]. Taketa's theorem says that any monomial group is solvable [Tak30].

Remark 1. We have the following implications for finite groups:

$$\begin{tikzcd}
\text{nilpotent} \arrow[r, Rightarrow] & \text{supersolvable} \arrow[r, Rightarrow] & \text{monomial} \arrow[r, Rightarrow, "\text{Taketa}"] & \text{solvable} \\
\text{abelian} \arrow[u, Rightarrow] \arrow[urr, phantom, "\ulcorner", very near start] \arrow[rr, Rightarrow] & & A\text{-group,} \arrow[u, Rightarrow, "\text{Ito}"'] &
\end{tikzcd}$$

where the left bottom is a cartesian, i.e., a nilpotent group is an A-group if and only if it is abelian. Note that all implications are strict and that there is no implication between supersolvable groups and A-groups.

The following is a key ingredient for the generalisation to the twisted version of the theory of Heilbronn virtual characters.

Theorem 4. *Let G be a finite group, and H a normal subgroup of G. If we assume that H is an A-group, and that G/H is supersolvable, then G is monomial.*

This result is indeed Huppert's theorem [Hup53] combined with Ito's theorem [Ito52] and Taketa's theorem [Tak30].

3. Twisted Heilbronn Virtual Characters

Let $K \subset L\,(\subset \overline{F})$ be finite Galois extensions of F in $\overline{F}$. We write $G := \mathrm{Gal}(K/F)$, and $\widetilde{G} := \mathrm{Gal}(L/F)$. Fix $1 \neq s_0 \in \mathbb{C}$. Put

$$n_{\widetilde{G}}(\alpha) := \mathrm{ord}_{s=s_0} L_F(s, \alpha)$$

for any Artin representation α of $\widetilde{G}$, where $L_F(s,\alpha)$ is the Artin L-function attached to α. For any subgroup $H \subset G$, let $\widetilde{H} \subset \widetilde{G}$ denote the pullback of H via the canonical quotient $\widetilde{G} \twoheadrightarrow G$ (Hence, $\widetilde{\{1\}} = \mathrm{Gal}(L/K)$).

Definition 2. For an Artin representation α of $\widetilde{G}$, we define

$$\theta_G^\alpha := \sum_{\rho \in \mathrm{Irr}(G)} n_{\widetilde{G}}(\rho^{\widetilde{G}} \otimes \alpha) \mathrm{Tr}(\rho)$$

that we call **Heilbronn virtual character twisted by $\boldsymbol{\alpha}$**.

Here, we write $\rho^{\widetilde{G}}$ for the representation of $\widetilde{G}$ obtained by the composition of the canonical quotient $\widetilde{G} \twoheadrightarrow G$ and ρ. Note that while θ_G^α is a virtual character of G, $\rho^{\widetilde{G}} \otimes \alpha$ is however not a representation of G in general, but a representation of $\widetilde{G}$. Note also that, when $\alpha = \mathbf{1}$ and $\widetilde{G} = G$, then $\theta_G^{\mathbf{1}}$ is the usual (untwisted) Heilbronn virtual character θ_G so far, cf. [FGM15].

We further write

$$r_\alpha := n_{\widetilde{\{1\}}}(\alpha|_{\widetilde{\{1\}}}) = n_{\widetilde{\{1\}}}(\alpha|_{\ker(\widetilde{G} \twoheadrightarrow G)}) = \mathrm{ord}_{s=s_0} L_K(s, \alpha|_{G_K}).$$

By *the decomposition of the regular representation of* G and the *projection formula*, we can show a **Takagi-type equality**

$$\sum_{\rho \in \mathrm{Irr}(G)} (\dim \rho)\, n_{\widetilde{G}}(\rho^{\widetilde{G}} \otimes \alpha) = r_\alpha \tag{Tak}$$

In the untwisted case, this equality comes from the (Artin-)Takagi's decomposition $\zeta_K(s) = \prod_{\rho \in \mathrm{Irr}(G)} L_F(s, \rho)^{\dim \rho}$.

The following lemma, which comes from *the compatibility of induced representations with Artin L-functions* and the *projection formula* in the twisted case, is a key in the theory of Heilbronn virtual characters:

Lemma 1 (Lemma 3.2, (3), (5) of [Yam23])**.** *For any Artin representation α of $\widetilde{G}$ and any subgroup $H \subset G$, we have*

$$\mathrm{Res}^G_H(\theta^\alpha_G) = \theta_H^{\mathrm{Res}^{\widetilde{G}}_{\widetilde{H}} \alpha}.$$

In particular, we have $\theta^\alpha_G(1) = \theta^\alpha_G|_{\{1\}}(1) = \theta^{\mathbf{1}}_{\{1\}}(1) = r_\alpha$.

Remark 2. We can also show that for any subgroup $H \subset G$ and any Artin representation β of $\widetilde{H}$, one has

$$\mathrm{Ind}^G_H(\theta^\beta_H) = \theta_G^{\mathrm{Ind}^{\widetilde{G}}_{\widetilde{H}} \beta}$$

cf. [Yam23, Lemma 3.2, (4)]. Unlike the usual (untwisted) Heilbronn virtual characters, the twisted Heilbronn virtual characters are **stable** under taking the induced representations. This is a characteristic advantageous property of the **twisted** Heilbronn virtual characters, and further research and applications of using this stability property is awaited, because this property is not used in the current study yet.

By combining Theorem 4 and Lemma 1, we have the following corollary:

Corollary 1 (Corollary 3.3, (1), (2), (4) of [Yam23])**.** *Let α be an Artin representation α of G_F, and K a finite Galois extension of F. We write $L := K(\overline{F})^{\ker(\alpha)}$ $(\subset \overline{F})$, and put $\widetilde{G} = \mathrm{Gal}(L/F)$ and $G = \mathrm{Gal}(K/F)$. We assume that*

$$\mathrm{Im}(\alpha|_{\widetilde{\{1\}}})\, (\cong \mathrm{Gal}(L/K) = \ker(\widetilde{G} \twoheadrightarrow G)) \text{ is an } A\text{-group}.$$

Then, for any supersolvable subgroup $H \subset G$, $\theta^\alpha_G|_H$ is a (genuine) character of degree r_α. In particular, for any $g \in G$, we have $|\theta^\alpha_G(g)| = |\theta^\alpha_G|_{\langle g \rangle}(g)| \leq r_\alpha$, *where* $\langle g\rangle\,(\subset G)$ *denotes the subgroup of* G *generated by* g*. Hence, we obtain a* **Heilbronn-type inequality**

$$\sum_{\rho\in\mathrm{Irr}(G)} n_{\widetilde{G}}(\rho^{\widetilde{G}}\otimes\alpha)^2 = \langle\theta_G^\alpha,\theta_G^\alpha\rangle_G \le r_\alpha^2. \tag{Heil}$$

We can easily deduce Theorem 1 from the above two formulae (Tak) and (Heil) that we recall below:

$$\sum_{\rho\in\mathrm{Irr}(G)} (\dim\rho)\, n_{\widetilde{G}}(\rho^{\widetilde{G}}\otimes\alpha) = r_\alpha \quad \text{and} \quad \sum_{\rho\in\mathrm{Irr}(G)} n_{\widetilde{G}}(\rho^{\widetilde{G}}\otimes\alpha)^2 \le r_\alpha^2.$$

Note that the assumption in the Theorem 1 implies that $\ker(\widetilde{G}\twoheadrightarrow G)$ is monomial by Ito's theorem [Ito52], hence, $r_\alpha \ge 0$.

References

[Ara33] H. Aramata, "*Über die Teilbarkeit der Dedekindschen Zetafunktionen*", Proc. Imp. Acad. Tokyo, **9** (1933), no. 2, 31–34.

[Bro13] J. Browkin, "*Multiple zeros of Dedekind zeta functions*", Funct. Approx. Comment. Math. **49** (2013), no. 2, 383–390.

[FGM15] R. Foote, H. Ginsberg, V. K. Murty, "*Heilbronn characters*", Bull. Amer. Math. Soc. (N.S.) **52** (2015), no. 3, 465–496.

[FM89] R. Foote, V. K. Murty, "*Zeros and poles of Artin L-series*", Math. Proc. Cambridge Philos. Soc. **105** (1989), no. 1, 5–11.

[Hup53] B. Huppert, "*Monomiale Darstellung endlicher Gruppen*", Nagoya Math. J., **6** (1953), 93–94.

[HKMS22] D. Hu, I. Kaneko, S. Martin, C. Schildkraut, "*Order of zeros of Dedekind zeta functions*", Proc. Amer. Math. Soc. **150** (2022), no. 12, 5111–5120.

[Ito52] N. Ito, "*Note on A-groups*", Nagoya Math. J. **4** (1952), 79–81.

[Sta74] H. M. Stark, "*Some effective cases of the Brauer-Siegel theorem*", Invent. Math. **23** (1974), 135–152.

[Tak30] K. Taketa, "*Über die Gruppen, deren Darstellungen sich sämtlich auf monomiale Gestalt transformieren lassen*", Proc. Imp. Acad. Tokyo, **6** (1930), no. 2, 31–33.

[Yam23] G. Yamashita, *Twisted Heilbronn Virtual Characters*, Hokkaido Math. J. (accepted 2024), 2023, 9 pages.

Large monodromy groups of polynomial compositions

Danny Neftin

(joint work with Joachim König and Shai Rosenberg)

1. Background

The study of monodromy groups $\mathrm{Mon}(f) := \mathrm{Gal}(f(x)-t,\mathbb{Q}(t))$ of polynomial maps $\mathbb{P}^1_{\mathbb{Q}}\to\mathbb{P}^1_{\mathbb{Q}}$, $x\mapsto f(x)$ for $f\in\mathbb{Q}[x]$, lies at the heart of many problems in number theory, dynamics, complex analysis, and other subjects.

One of the original motivating questions in arithmetic dynamics is the following: Given $a\in\mathbf{Z}$ and a sequence $(a_n)_{n=0}^\infty$, such as an orbit $a_{n+1}=f(a_n)$ of $f\in\mathbf{Z}[x]$, what is the (natural) density $\delta_c(f,a,a_0)=\delta_{\text{congruence}}(f,a,a_0)$ of primes p such that

$a_n \equiv a \bmod p$ for some $n \in \mathbb{N}$? For example, when $a = -1$, $a_0 = 2$, and $a_{n+1} = a_n^2$ is an orbit of $f(x) = x^2$, the quantity $\delta_c(x^2, -1, 2)$ is the density of primes p which divide some Fermat number $a_n + 1 = 2^{2^n} + 1$. In this case $\delta_c(x^2, -1, 2) = 0$. Although $\delta_c(f, a, a_0)$ is often expected to be small, finding δ_c for an arbitrary polynomial $f \in \mathbb{Z}[x]$ for a positive proportion of $a \in \mathbb{Z}$ and $a_0 \in \mathbb{Z}$, is a widely open problem [Jon08].

On the other hand, the (natural) densities $\delta_{ns}(f, a) = \delta_{\text{non-stable}}(f, a)$ of primes p such that the fiber of $f^{\circ n}$ over $a \in \mathbb{Q}$ is reducible mod p for some $n \in \mathbb{N}$, are "usually" expected to be 1. Here, the fiber of $f^{\circ n}$ over a is said to be reducible mod p if $f^{\circ n}(x) - a$ is reducible mod p.

Consequences regarding the above densities and many other problems follow from "largeness" properties of $\mathrm{Mon}(f^{\circ n})$: Namely, these are encoded in the action of the image $\mathrm{Im}\,\rho^{(n)}_{a,f} := \mathrm{Gal}(f^{\circ n}(x) - a, \mathbb{Q})$ of an arboreal representation on the tree $T^{(n)}_{a,f} = \bigcup_{i=0}^{n} (f^{\circ n})^{-1}(a)$ of preimages of a, and as a varies, in the action of $\mathrm{Mon}(f^{\circ n}) = \mathrm{Gal}(f^{\circ n}(x) - t, \mathbb{Q}(t))$ on $T^{(n)} = T^{(n)}_{t,f}$. When the image is the full group $\mathrm{Aut}(T^{(n)})$, or under mild conditions even merely if its index in $\mathrm{Aut}(T^{(n)})$ is bounded independently of n, it is known that $\delta_c(f, a, a_0) = 0$, and $\delta_{ns}(f, a) = 1$. Note that $\mathrm{Aut}(T^{(n)})$ is well known to be the n-fold iterated wreath product $[S_d]^n = S_d \wr \cdots \wr S_d$, where $S_d \wr S_d = S_d^d \rtimes S_d$ is the (standard imprimitive) wreath product and $d := \deg f$.

Much of the difficulty in the above problems lies in determining when $\mathrm{Im}\,\rho^{(n)}_{a,f}$ and $\mathrm{Mon}(f^{\circ n})$ are "large" in a sense compatible with the problem. The groups $\mathrm{Mon}(f)$, $f \in \mathbb{Q}[x]$ were classified for indecomposable f by Feit and Müller, but up until recently little was known on the possibilities for $\mathrm{Mon}(f)$ for decomposable $f \in \mathbb{Q}[x]$. Most of the work towards determining $\mathrm{Mon}(f^{\circ n})$ is devoted to quadratic polynomials. One exception is the recent work of Bouw-Ejder–Karemaker [BEK21] who show that $\mathrm{Mon}(f^{\circ n})$ are "large" for so called normalized Belyi maps f, that is, maps with three ramification points that map to themselves. For such maps, $\Gamma := \mathrm{Mon}(f)$ is alternating or symmetric and $\mathrm{Mon}(f^{\circ n})$ is either the full group $[\Gamma]^n$ or a large subgroup $E_n \supseteq [A_d]^n$.

2. Results and applications

2.1. **Monodromy.** It turns out that in various aspects it is easier to show that $\mathrm{Mon}(f)$ is "large" for compositions $f = f_1 \circ \cdots \circ f_r$ of indecomposable polynomials which are not x^d or a Chebyshev polynomial T_d up to composition with linear polynomials. In this paper, we prove a strong largeness property of $\mathrm{Mon}(f)$ for such polynomials f. When $\mathrm{Mon}(f_i)$ is alternating or symmetric, it takes the form:

Theorem 1. *Suppose $f = f_1 \circ \cdots \circ f_r$ for $f_i \in \mathbb{Q}[x]$ of degree $d_i \geq 5$ with $\mathrm{Mon}(f_i) \in \{A_{d_i}, S_{d_i}\}$, $i = 1, \ldots, r$. Then $\mathrm{Mon}(f)$ contains $A_{d_r} \wr \cdots \wr A_{d_1}$.*

To word the analogous property when the groups $\Gamma_i := \mathrm{Mon}(f_i)$, $i = 1, \ldots, r$ are not necessarily alternating or symmetric, recall the following. Given a sequence of polynomials $f_n \in \mathbb{Q}[x]$, $n \in \mathbb{N}$, one has natural epimorphisms $\pi_n : \mathrm{Mon}(f_1 \circ \cdots \circ$

$f_n) \to \mathrm{Mon}(f_1 \circ \dots f_{n-1})$, with kernel embedding into $\Gamma_n^{\deg(f_1\circ\cdots\circ f_{n-1})}$. Say that $\ker(\pi_n)$ is *large*, if it contains the full direct product of socles $\mathrm{soc}(\Gamma_n)^{\deg(f_1\circ\cdots\circ f_{n-1})}$, where the *socle* $\mathrm{soc}(\Gamma)$ of a group Γ is the subgroup generated by the minimal normal subgroups of Γ.

Assume now $f_i \in \mathbb{Q}[x]$, $i = 1, \dots, r$ are indecomposable of degree ≥ 5 and are not linearly related to x^d or T_d over $\mathbb{C}$, that is, there are no linear $\mu_1, \mu_2 \in \mathbb{C}[x]$ such that $f_i = \mu_1 \circ x^d \circ \mu_2$ or $\mu_1 \circ T_d \circ \mu_2$, for $d = \deg f_i$. Our generalization of Theorem 1 states that under these conditions (and with the above notation), $\ker(\pi_n)$ is large for all $n \in \mathbb{N}$. This amount to saying that for all $n \in \mathbb{N}$, $\mathrm{Mon}(f_1 \circ \cdots \circ f_n)$ contains the multiset of (Jordan-Hölder) composition factors of $[\mathrm{soc}(\Gamma_i)]_{i=1}^r = \mathrm{soc}(\Gamma_r) \wr \cdots \wr \mathrm{soc}(\Gamma_1)$.

2.2. **Application to arboreal representations.** For iterates of an indecomposable polynomial $f \in \mathbb{Q}[x]$ of degree $d \geq 5$ with nonsolvable monodromy group Γ, it follows by Hilbert's irreducibility theorem that $\mathrm{Im}\,\rho_{a,f}^{(n)}$ contains the composition factors of $[\mathrm{soc}(\Gamma)]^n$ for a Hilbert subset of $a \in \mathbb{Q}$, that is, for any $a \in \mathbb{Q}$ in the complement of a union of finitely many value sets of morphisms $g_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}$, yielding immediately:

Corollary 1. *Let $n \geq 2$ be an integer and $f \in \mathbb{Q}[x]$ be indecomposable of degree $d \geq 5$ that is not linearly related to x^d or T_d over $\mathbb{C}$. Set $\Gamma := \mathrm{Mon}(f)$. Then $\mathrm{Im}\,\rho_{a,f}^{(n)}$ contains the composition factors of $[\mathrm{soc}(\Gamma)]^n$ for all a in a Hilbert subset of $\mathbb{Q}$.*

For more details and further applications in this direction we refer to König's report [Kön23] in this volume. Furthermore, see [DK22] for the incompatibility of the problem with Hilbert's irreducibility theorem.

2.3. **Largeness and prime density.** These largeness properties for $\mathrm{Mon}(f^{\circ n})$ and $\mathrm{Im}\,\rho_{f,a}^{(n)}$ are compatible with bounding the above prime densities. For "nonspecial" f and most $a \in \mathbf{Z}$, the density $\delta_c(f, a, a_0)$ of primes for which a meets an orbit of f mod p is arbitrary small, and the density $\delta_{ns}(f, a, N)$ of primes p over which the fiber of $f^{\circ N}$ (and hence of $f^{\circ n}$ for $n \leq N$) over a is reducible mod p is arbitrary large:

Corollary 2. *Suppose $\varepsilon > 0$, $N \in \mathbb{N}$, and $f \in \mathbf{Z}[x]$ is indecomposable of degree $d \geq 5$ which is not linearly related to x^d or T_d over $\mathbb{C}$. Then there exists*

(1) a Hilbert subset $A_\varepsilon^N \subset \mathbb{Q}$ such that $\delta_{ns}(f, a, N) > 1 - \varepsilon$ for all $a \in A_\varepsilon^N$; and
(2) a Hilbert subset $A_\varepsilon \subset \mathbb{Q}$ such that $\delta_c(f, a, a_0) < \varepsilon$ for all $a \in A_\varepsilon$, $a_0 \in \mathbf{Z}$.

Further applications to explicit versions of Hilberts irreducibility appear in [KN20] and the relevant counterexamples are given in [DF99].

3. Methods

3.1. **Obstructions to largeness.** The main theorem is of group theoretic nature and applies much more generally to decompositions $f = f_1 \circ f_2$ for finite surjective morphisms f_1 and f_2 of varieties over arbitrary fields of characteristic 0, whenever

$\Gamma := \mathrm{Mon}(f_2)$ is nonsolvable with a unique minimal normal subgroup. For such decompositions, there are several obstructions that may occur and prevent $\mathrm{Mon}(f)$ from being large, that is, prevent it from containing $\mathrm{soc}(\Gamma)^{\deg f_1}$. The theorem asserts that unless certain obstructions occur, $\mathrm{Mon}(f)$ is indeed large. For simplicity in what follows, we assume f_1, f_2 are indecomposable.

The first obstruction is a Ritt type of decomposition for f. Namely, if $f = f_1 \circ f_2 = g_1 \circ g_2$ are sufficiently different decompositions of f, i.e. $f_1 \circ f_2$ is not an invariant decomposition, then they yield distinct minimal normal subgroups of $\mathrm{Mon}(f)$ which necessarily centralize each other, contradicting that one of them is the large subgroup $\mathrm{soc}(\Gamma)^{\deg f_1}$. The second and third obstructions are related to trivial extensions of monodromy groups. Namely, it could happen that $f_1 \circ f_2$ is a subcover of the Galois closure of f_1 in which case $\mathrm{Mon}(f_1 \circ f_2) = \mathrm{Mon}(f_1)$; and it could happen that $\mathrm{Mon}(f_1)$ preserves the Galois closure of f_2 in which case $\mathrm{Mon}(f_1 \circ f_2)$ coincides with a subgroup of $\mathrm{Aut}(\mathrm{Mon}(f_2))$. It is easy to see that in both cases $\mathrm{soc}(\Gamma)^{\deg f_1}$ cannot be contained in $\mathrm{Mon}(f)$.

The last obstruction, conjugation compatibility, is more intricate and relates to the conjugation action of $\mathrm{Mon}(f)$ on a minimal normal subgroup of the kernel of the projection $\mathrm{Mon}(f) \to \mathrm{Mon}(f_1)$. Let $U := \mathrm{Mon}(f_2)$ and assume $\mathrm{soc}(U) \cong L^I$ for a nonabelian simple L. Then $\mathrm{Mon}(f) \cap \mathrm{soc}(U)^m = \mathrm{Mon}(f) \cap L^{[m]\times I} \cong L^P$ for a partition P of $[m] \times I$. Let $\pi : P \to \{\text{Subsets of } [m]\}$ be the projection. We say $f = f_1 \circ f_2$ is *conjugation-compatible* if π induces a partition of $[m]$. Note that this is automatic if $\#I = 1$.

3.2. **Sufficiency of obstructions.** When all obstructions vanish we get:

Theorem 2. *Let $f = f_1 \circ f_2$ be a conjugation-compatible decomposition. Set $U := \mathrm{Mon}(f_2)$. Assume $\mathrm{soc}(U)$ is a power of a nonabelian simple group. For all decompositions $f_1 = g_1 \circ g_2$, $\deg g_2 > 1$, assume $g_2 \circ f_2$ is proper, invariant, with monodromy not embedding in $\mathrm{Aut}(\mathrm{soc}(U))$. Then $\mathrm{Mon}(f) \supseteq \mathrm{soc}(U)^m$.*

It is rather easy to deduce from theorems of Ritt and Burnside that the above obstructions vanish for polynomial compositions $f_1 \circ \cdots \circ f_r$ when $\mathrm{Mon}(f_i)$ are nonsolvable, and even under more relaxed conditions. Namely, Ritt's theorem implies that decompositions of such polynomials are unique up to composition with linear polynomials, and Burnside's theorem implies that the above groups Γ are almost simple, so that the conjugation compatibility condition holds trivially. The polynomial case seems like the opposite scenario of the above phenomena occurs, and we expect that the above phenomena will not occur for much wider classes of rational functions and morphisms.

References

[BEK21] I. I. Bouw, Ö. Ejder, V. Karemaker, *Dynamical Belyi maps and arboreal Galois groups*, Manuscripta Math. **165** (2021), 1–34.

[DF99] P. Dèbes, M. D. Fried, *Integral specialization of families of rational functions*, Pacific J. Math. **190** (1999), 45–85.

[DK22] P. Dittmann, B. Kadets, Odoni's conjecture on arboreal Galois representations is false, Proc. Amer. Math. Soc. 150 (2022), 3335–3343.

[Jon08] R. Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. Lond. Math. Soc. **78** (2008), 523–544.
[Kön23] J. König, *On the largeness of arboreal Galois representations*, MFO-RIMS Tandem workshop "Arithmetic homotopy Galois theory", OWR report (2023).
[KN20] J. König, D. Neftin, *Reducible fibers of polynomial maps.* To appear in IMRN. Preprint at arXiv:2001.03630 [math.NT], 2020

On pro-p outer Galois representations associated to once-punctured CM elliptic curves

Shun Ishii

Let p be an odd prime. We present recent progress on the outer action of Galois groups on the maximal pro-p quotients of the geometric étale fundamental groups of CM elliptic curves minus their origins (*once-punctured CM elliptic curves*).

In the case of the projective line minus three points, Anderson and Ihara asked if the field Ω^* corresponding to the kernel of the associated pro-p outer Galois representation is equal to the maximal pro-p extension of the p-th cyclotomic field $\mathbb{Q}(\mu_p)$ unramified outside p. Later, Sharifi proved that for p regular their question is affirmative under the Deligne-Ihara conjecture (now Hain-Matsumoto's and Brown's theorem) on the structure of a graded Lie algebra over $\mathbb{Q}_p$ associated to a certain filtration on $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

In this report, we enounce a conjecture analogue to Deligne-Ihara and establish an analogue of Sharifi's result for once-punctured CM elliptic curves over imaginary quadratic fields when p is ordinary.

1. The projective line minus three points

In this section, we review previous results on $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$. We denote the maximal pro-p quotient $\pi_1(\mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0, 1, \infty\})^{(p)}$ of the geometric étale fundamental group of $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ by $\Pi_{0,3}$. The étale homotopy exact sequence determines *the pro-p outer Galois representation*

$$\rho_{0,3} \colon G_{\mathbb{Q}} \to \mathrm{Out}(\Pi_{0,3}).$$

Then one can observe that

(1) The field Ω^* is a pro-p extension over $\mathbb{Q}(\mu_p)$, and
(2) the extension $\Omega^*/\mathbb{Q}$ is unramified outside p.

Anderson and Ihara [AI88] studied the pro-p outer Galois representation associated to hyperbolic curves of genus zero and proved that Ω^* is generated by all higher circular p-units. In that paper, they posed the following question:

> *Is Ω^* equal to the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p?*

which has motivated further work of Rasmussen and Tamagawa [RT08], and also of Matsumoto, Nakamura, Takao and other on the related Oda's problem, see Philip's report in this volume.

1.1. **The Deligne-Ihara conjecture.** To consider this question, let us firstly observe that the Galois group $G_{\mathbb{Q}}$ comes equipped with a descending central filtration $\{F^m G_{\mathbb{Q}}\}_{m\geq 1}$ induced by the descending central series $\{\Pi_{0,3}(m)\}_{m\geq 1}$ of $\Pi_{0,3}$:

$$F^m G_{\mathbb{Q}} := \ker \left[G_{\mathbb{Q}} \xrightarrow{\rho_{0,3}} \mathrm{Out}(\Pi_{0,3}) \to \mathrm{Out}(\Pi_{0,3}/\Pi_{0,3}(m+1)) \right].$$

It is known that

(1) $\mathrm{gr}^m G_{\mathbb{Q}} := F^m G_{\mathbb{Q}}/F^{m+1}G_{\mathbb{Q}}$ is isomorphic to a finite direct sum of the m-th Tate twist $\mathbb{Z}_p(m)$, and
(2) For each odd $m \geq 3$, *the m-th Soulé character* $\kappa_m \colon G_{\mathbb{Q}(\mu_{p^\infty})} \to \mathbb{Z}_p(m)$ restricted to $F^m G_{\mathbb{Q}}$ is nontrivial and factors through $F^m G_{\mathbb{Q}} \twoheadrightarrow \mathrm{gr}^m G_{\mathbb{Q}}$.

Here, the m-th Soulé character $\kappa_m \colon G_{\mathbb{Q}(\mu_{p^\infty})} \to \mathbb{Z}_p(m)$ is a certain nontrivial Kummer character which is described in terms of cyclotomic p-units. For its fundamental properties, we refer to Ichimura-Sakaguchi [IS87].

The direct sum $\mathfrak{g} := \oplus_{m\geq 1}\mathrm{gr}^m G_{\mathbb{Q}}$ is a graded Lie algebra over $\mathbb{Z}_p$ whose brackets are induced by commutators on $G_{\mathbb{Q}}$. For each odd $m \geq 3$, let $\sigma_m \in \mathrm{gr}^m G_{\mathbb{Q}}$ be an arbitrary element such that $\kappa_m(\sigma_m)$ generates $\kappa_m(F^m G_{\mathbb{Q}})$. Such a generator $\kappa_m(\sigma_m)$ is usually called an *m-th Soulé element*.

The following was established by Hain-Matsumoto [HM03] and Brown [Bro12].

Conjecture (Deligne-Ihara). *Soulé elements $\{\sigma_m\}_{m\geq 3, odd}$ freely generate $\mathfrak{g} \otimes \mathbb{Q}_p$ as a graded Lie algebra over $\mathbb{Q}_p$.*

In this result, Hain and Matsumoto establish the generating part and, as a consequence of properties of motivic periods of mixed Tate motives over $\mathrm{Spec}(\mathbb{Z})$, Brown establishes the freeness part.

1.2. **Anderson-Ihara's question, a blueprint proof.** Sharifi obtained the following affirmative result for Anderson-Ihara's question.

Theorem 1 (Theorem 1.1 in [Sha02]). *Let p be an odd irregular prime. Then the equality $\Omega^* = \Omega$ holds.*

We explain the strategy of Theorem 1 since the proof of our main result follows this strategy. First, we choose an appropriate lift $\tilde{\sigma}_m \in F^m G_{\mathbb{Q}}$ of an m-th Soulé element to $F^m G_{\mathbb{Q}}$ for $m = 3, 5, \ldots, p$. If we take a lift $\gamma \in \mathrm{Gal}(\Omega/\mathbb{Q}(\mu_p))$ of a generator of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p))$, one can show that $\gamma, \tilde{\sigma}_3, \ldots, \tilde{\sigma}_p$ form a free basis of the Galois group $\mathrm{Gal}(\Omega/\mathbb{Q}(\mu_p))$ since p is odd and regular.

Moreover, one can inductively construct a lift $\tilde{\sigma}_m \in F^m G_{\mathbb{Q}}$ of an m-th Soulé element for every odd $m > p$ from $\gamma, \tilde{\sigma}_3, \ldots, \tilde{\sigma}_p$ with the property that $\{\tilde{\sigma}_m\}_{m\geq 3,\text{odd}}$ forms a free basis of $\mathrm{Gal}(\Omega/\mathbb{Q}(\mu_{p^\infty}))$, cf. [Sha02, §2 and §3].

Then the filtration $\{F^m\mathrm{Gal}(\Omega/\mathbb{Q}(\mu_{p^\infty}))\}_{m\geq 1}$ induced by $\{F^m G_{\mathbb{Q}}\}_{m\geq 1}$ coincides with the fastest descending central filtration with the property that $\tilde{\sigma}_m$ is contained in the m-th component of the filtration for every odd $m \geq 3$ (here we use the Deligne-Ihara conjecture). Since the intersection of such the fastest filtration is trivial, we have $\cap_{m\geq 1} F^m \mathrm{Gal}(\Omega/\mathbb{Q}(\mu_{p^\infty}) = \mathrm{Gal}(\Omega/\Omega^*) = \{1\}$ as desired.

Remark 1.

(1) As a byproduct, one can show that Soulé elements freely generate $\mathfrak{g}$ if p is odd and regular.
(2) Conversely, Sharifi [Sha02, Theorem 1.3] observed that the Soulé elements *do not* generate $\mathfrak{g}$ if p is irregular and Greenberg's generalized conjecture holds for $\mathbb{Q}(\mu_p)$.

2. The case of once-punctured CM elliptic curves

Let k be an imaginary quadratic field and (E, O) an elliptic curve over k, with origin $O \in E[k]$, and which has complex multiplication by the ring of integers of k. Moreover, assume that $p \geq 5$ and E has good ordinary reduction at primes above p. Then p splits into two primes in k as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and we have two characters $\chi_1, \chi_2 \colon G_k \to \mathbb{Z}_p^\times$ corresponding to the $\mathfrak{p}$-adic and $\bar{\mathfrak{p}}$-adic Tate module $T_{\mathfrak{p}}(E)$ and $T_{\bar{\mathfrak{p}}}(E)$ of E, respectively.

In this section, we denote the pro-p geometric étale fundamental group of $E \setminus O$ by $\Pi_{1,1}$. We have the associated outer representation

$$\rho_{1,1} \colon G_k \to \mathrm{Out}(\Pi_{1,1}).$$

As in the previous section, G_k comes with a descending central filtration $\{F^m G_k\}_{m\geq 1}$ on G_k associated to the descending central series $\{\Pi_{1,1}(m)\}_{m\geq 1}$ of $\Pi_{1,1}$. We denote the m-th associated graded quotients by $\mathrm{gr}^m G_k$.

2.1. Fixed field, Kummer characters, and a conjecture.

Regarding the fixed field of the outer Galois pro-p representation $\rho_{1,1}$, the following holds.

Lemma 1 (Lem. 2.11 and Lem. 2.12 in [Ish23b])**.** *With the notations above:*

(1) The field $\bar{\mathbb{Q}}^{\ker(\rho_{1,1})}$ is a pro-p extension over $k(E[p])$, and
(2) $\bar{\mathbb{Q}}^{\ker(\rho_{1,1})}$ is a compositum *of $k(E[p])$ and of the field Ω_k^* which is a pro-p extension of* the mod-p ray class field *$k(p)$ of k unramified outside p.*

The second claim is different from the one in the previous section. This follows since the image of the outer action of $\mathrm{Aut}(E \setminus O)$ on $\Pi_{1,1}$ is contained in $\rho_{1,1}(G_{k(p)})$.

In [Nak95], Nakamura proved that certain Kummer characters associated to special values of the fundamental theta functions can be regarded as analogues of Soulé characters, and observed that certain linear combinations of them are nontrivial. In our situation, they are elliptic Soulé characters:

$$\kappa_{m_1,m_2} \colon G_{k(E[p^\infty])} \to \mathbb{Z}_p(m_1, m_2) := \mathbb{Z}_p(\chi_1^{m_1}\chi_2^{m_2})$$

where $(m_1, m_2) \in \mathbb{Z}^2_{\geq 1} \setminus \{(1,1)\}$ satisfies $m_1 \equiv m_2 \bmod |O_k^\times|$. By using Iwasawa main conjecture for imaginary quadratic fields proved by Rubin [Rub91], we establish that:

Theorem 2 (Theorem 1.4 (1) in [Ish23a])**.** *The elliptic Soulé character κ_{m_1,m_2} is nontrivial if $H^2_{\acute{e}t}(\mathrm{Spec}(O_k[\frac{1}{p}]), \mathbb{Z}_p(m_1, m_2))$ is finite.*

The finiteness of the second cohomology group is a special case of a conjecture of Jannsen [Jan89, Conjecture 1]. We remark that $H^2_{\acute{e}t}(\mathrm{Spec}(\mathbb{Z}[\frac{1}{p}]), \mathbb{Z}_p(m))$ for $m \geq 2$ was already proved to be finite by Soulé and is crucially used to establish the nontriviality of the usual Soulé character κ_m, cf. [IS87].

Moreover, we also observed the surjectivity of κ_{m_1,m_2} is deeply related to the p-part of the class number of $k(p)$, see Theorem 1.4 in [Ish23a].

The following properties lead to our analogue of Deligne-Ihara Conjecture.

(1) $\mathrm{gr}^m G_k \otimes \mathbb{Q}_p$ is isomorphic to a finite direct sum of $\mathbb{Q}_p(m_1, m_2)$ where $(m_1, m_2) \in \mathbb{Z}^2_{\geq 1} \setminus \{(1,1)\}$ satisfies $m_1 + m_2 = m$, and
(2) If κ_{m_1,m_2} is nontrivial, then $\kappa_{m_1,m_2}\,|_{F^{m_1+m_2}G_k}$ is also nontrivial and factors through $F^{m_1+m_2}G_k \twoheadrightarrow \mathrm{gr}^{m_1+m_2}G_k$.

Conjecture 1 (Conjecture 2.10 in [Ish23b]). *For each $(m_1, m_2) \in \mathbb{Z}^2_{\geq 1} \setminus \{(1,1)\}$ such that $m_1 \equiv m_2 \bmod |O_k^\times|$, fix an element $\sigma_{(m_1,m_2)}$ in the $\chi_1^{m_1}\chi_2^{m_2}$-isotypic component of $\mathrm{gr}^{m_1+m_2}G_k$ such that $\kappa_{m_1,m_2}(\sigma_{m_1,m_2})$ generates $\kappa_{m_1,m_2}(F^{m_1+m_2}G_k)$. Then $\{\sigma_{m_1,m_2}\}_{(m_1,m_2)}$ freely generates $\bigoplus_{m\geq 1} F^m G_k \otimes \mathbb{Q}_p$ as a graded Lie algebra.*

It seems that Hain-Matsumoto's technique is also applicable to prove that $\{\sigma_{m_1,m_2}\}_{(m_1,m_2)}$ generates the Lie algebra, assuming that κ_{m_1,m_2}s are nontrivial. The speaker hopes to relate the freeness portion of Conjecture 1 with certain properties of elliptic multiple zeta values at CM points.

2.2. **Characterization of the kernel.** In the same way that Sharifi's Theorem 1 relates Anderson-Ihara's question and Deligne-Ihara conjecture, we relate Conjecture 1 to the fixed field of outer Galois representations $\rho_{1,1}$ of Lemma 1.

Theorem 3 (Theorem 2.14 in [Ish23b]). *Assume that*

(1) the class number of $k(p)$ is not divisible by p,
(2) there are exactly two primes of the mod-p^∞ ray class field $k(p^\infty)$ of k above p, and
(3) Conjecture 1 holds.

Then Ω_k^* is equal to the maximal pro-p extension Ω_k of $k(p)$ unramified outside p. In paricular, the equality $\bar{\mathbb{Q}}^{\ker(\rho_{1,1})} = k(E[p]) \cdot \Omega_k$ holds.

Basically, we follow the strategy of Theorem 1. However, there are several differences from the previous situation. For example:

- the Galois group $\mathrm{Gal}(\Omega_k/k(p))$ is not free. Therefore, we have to take the existence of a nontrivial relation into consideration when choosing lifts of Soulé elements. Here we use the first two assumptions.
- the construction of such a lift requires to introduce a two-variable version of the filtration $\{F^m G_k\}_{m\geq 1}$ coming from a certain two-variable descending central filtration $\{\Pi_{1,1}(m_1, m_2)\}$ on $\Pi_{1,1}$. This is because each graded quotient $\mathrm{gr}^m G_k \otimes \mathbb{Q}_p$ may contain several kinds of twists by powers of χ_1 and χ_2.

In [Ish23a] and [Ish23b], we further construct a particular basis $\{x_1, x_2\}$ of $\Pi_{1,1}$ such that the image of x_1, resp. x_2, in $\Pi^{\mathrm{ab}}_{1,1} \cong T_p(E)$ generates $T_{\mathfrak{p}}(E)$, resp. $T_{\bar{\mathfrak{p}}}(E)$. Using this basis, the filtered part $\Pi_{1,1}(m_1, m_2)$ is defined as follows: first, let $\Pi_{1,1}(1,0)$ (resp. $\Pi_{1,1}(0,1)$) be the normal closure of x_1 (resp. x_2). In general, $\Pi_{1,1}(m_1, m_2)$ is inductively defined as the normal closure of the subgroup generated by all $[\Pi_{1,1}(\boldsymbol{m}'), \Pi_{1,1}(\boldsymbol{m}'')]$s where $\boldsymbol{m}', \boldsymbol{m}'' \in \mathbb{Z}^2_{\geq 0} \setminus \{(0,0)\}$ satisfy $\boldsymbol{m}' + \boldsymbol{m}'' = (m_1, m_2)$. By introducing this two-variable filtration, we can construct lifts of Soulé elements in the same way.

As in the previous section, an integral version of Conjecture 1 can be related to Greenberg's generalized conjecture for $k(p)$ (manuscript in preparation).

Acknowledgement. The speaker is supported by JSPS KAKENHI Grand number 23KJ1882.

References

[AI88] G. Anderson and Y. Ihara, *Pro-l branched coverings of* $\mathbf{P}^1$ *and higher circular l-units*, Ann. of Math. (2) **128** (1988), no. 2, 271–293.

[Bro12] F. Brown, *Mixed Tate motives over* $\mathbb{Z}$, Ann. of Math. (2) **175** (2012), no. 2, 949–976.

[HM03] R. Hain and M. Matsumoto, *Weighted completion of Galois groups and Galois actions on the fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$, Compositio Math. **139** (2003), no. 2, 119–167.

[IS87] H. Ichimura and K. Sakaguchi, *The nonvanishing of a certain Kummer character* χ_m *(after C. Soulé), and some related topics*, Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math., vol. 12, North-Holland, Amsterdam, 1987, pp. 53–64.

[Ish23a] S. Ishii, *On Kummer characters arising from Galois actions on the pro-p fundamental groups of once-punctured CM elliptic curves*, in preparation, ∼30 pages.

[Ish23b] S. Ishii, *On the kernels of the pro-p outer Galois representations associated to once-punctured CM elliptic curves*, in preparation, ∼40 pages.

[Jan89] Uwe Jannsen, *On the l-adic cohomology of varieties over number fields and its Galois cohomology*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 315–360.

[Nak95] H. Nakamura, *On exterior Galois representations associated with open elliptic curves*, J. Math. Sci. Univ. Tokyo **2** (1995), no. 1, 197–231.

[RT08] Christopher Rasmussen and Akio Tamagawa, *A finiteness conjecture on abelian varieties with constrained prime power torsion*, Math. Res. Lett. **15** (2008), no. 6, 1223–1231.

[Rub91] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math., vol. 103, No. 1, 1991, p 25–68.

[Sha02] R. T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 275–284.

Formality and strong Massey vanishing for real projective groups

Gereon Quick
(joint work with Ambrus Pál)

1. Formality and Massey vanishing

A differential graded algebra $C^\bullet$ is called formal if there is a zig-zag of quasi-isomorphisms of differential graded algebras between $C^\bullet$ and its cohomology algebra with trivial differential. Formality is a rather strong property and implies, for example, the vanishing of all Massey products. Hence one may view Massey products as invariants which detect whether a differential graded algebra may contain more information than its cohomology. While there are many examples of non-vanishing Massey products in arithmetic, Hopkins and Wickelgren showed in [HW15] that all triple Massey products of degree one classes in the mod 2-Galois cohomology of global fields of characteristic different from 2 vanish, i.e., contain zero, whenever they are defined. Mináč and Tân then showed the vanishing of mod 2-triple Massey products of degree one classes for all fields. Moreover, they formulated the Massey vanishing conjecture stating that, for all fields k, all $n \geq 3$ and all primes p, the n-fold Massey product of degree one classes in mod p-Galois cohomology should vanish whenever it is defined (see [MT16]). The work of Hopkins–Wickelgren and Mináč–Tân has inspired a lot of activity in recent years. We now list the main cases we are aware of for which the Massey vanishing conjecture is now known to be true, in addition to our own work which we will describe below:

- By the work of Matzri [Mat14], Efrat–Matzri [EM17] and Mináč–Tân [MT16] for all fields, all primes p and $n = 3$.
- By the work of Harpaz–Wittenberg [HW23] for all number fields, all primes p and all $n \geq 3$.
- By the work of Pál–Szabó [PS18] for all fields with virtual cohomological dimension at most one and all pseudo p-adically closed fields, all primes and all $n \geq 3$.
- By the work of Guillot–Mináč–Topaz–Wittenberg [GMT18] for number fields and by Merkurjev–Scavia [MS16] for all fields, $p = 2$ and $n = 4$.
- Quadrelli shows that Efrat's Elementary Type Conjecture for pro-p-groups implies the Massey vanishing conjecture and proves the Massey vanishing conjecture in several further cases (see [Quad22, Corollary 1.4] for a list).

We note that Ekedahl showed in [Eke86] that there are non-vanishing triple Massey products of classes in $H^1_{\mathrm{et}}(X, \mathbb{F}_p)$ for X an absolutely irreducible smooth projective variety of dimension two over $\mathbb{C}$. Bleher–Chinburg–Gillibert show in [BCG23] that triple Massey products of classes in $H^1_{\mathrm{et}}(X, \mathbb{F}_p)$ for X an absolutely irreducible smooth projective curve over a field of characteristic different from p may not vanish.

Based on their computations of Massey products in Galois cohomology, Hopkins–Wickelgren asked in [HW15] whether the mod 2-Galois cohomology algebra of fields actually is formal. Positselski showed in [Pos17] that the answer to this question is negative in general, as there are local fields which are not formal. Harpaz–Wittenberg show in [GMT18, Example A.15] that certain fourfold Massey products are not defined, even though the neighbouring cup products vanish, and thereby show that $\mathbb{Q}(\sqrt{2}, \sqrt{17})$ is not formal. Further examples of non-formal fields have recently been discussed by Merkurjev–Scavia in [MS22].

In [PQ22], however, we show that there is a large class of fields for which formality holds. In particular, this implies the Massey vanishing conjecture for all primes p and all $n \geq 3$ and all nonzero cohomological degrees for these fields. We will now briefly describe the main results of [PQ22].

2. Formality of real projective groups

Let G be a profinite group. An *embedding problem for G* is a solid diagram

$$\begin{tikzcd} & G \arrow[dl, dotted, "\widetilde{\phi}"'] \arrow[d, "\phi"] \\ B \arrow[r, "\alpha"] & A, \end{tikzcd}$$

where A, B are finite groups, the solid arrows are continuous homomorphisms and α is surjective. A solution of this embedding problem is a continuous homomorphism $\widetilde{\phi} \colon G \to B$ which makes the diagram commutative. The embedding problem above is called *real* if for every involution $t \in G$ with $\phi(t) \neq 1$ there is an involution $b \in B$ with $\alpha(b) = \phi(t)$. Following Haran and Jarden [HJ85], a profinite group G is called *real projective* if G has an open subgroup without 2-torsion, and if every real embedding problem for G has a solution. In [PQ22] we prove the following result:

Theorem 1 ([PQ22])**.** *Let G be a real projective profinite group and p be a prime number, and let $C^\bullet(G, \mathbb{F}_p)$ denote the differential graded $\mathbb{F}_p$-algebra of continuous cochains of G with values in $\mathbb{F}_p$. Then $C^\bullet(G, \mathbb{F}_p)$ is formal.*

To prove the theorem we use the work of Scheiderer on the cohomology of real projective groups and calculate the graded Hochschild cohomology groups of a sum of certain quadratic algebras. Then we apply a criterion for formality due to Kadeishvili which states that the formality of a dg-algebra $C^\bullet$ is implied by the vanishing of the Hochschild cohomology groups $\mathrm{HH}^{n,2-n}(H^\bullet(C^\bullet), H^\bullet(C^\bullet))$ for all $n \geq 3$.

3. Implications for absolute Galois groups of fields

Now we describe the implications of Theorem 1 for fields. By the work of Haran and Jarden, the class of real projective groups is associated to the following class of fields. Recall that a field k has *virtual* cohomological dimension ≤ 1 if there is a finite separable extension K/k with $\mathrm{cd}(K) \leq 1$. Since the only torsion elements in the absolute Galois group of k are the involutions coming from the orderings of k, it is equivalent to require $\mathrm{cd}(K) \leq 1$ for any fixed finite separable extension K of k without orderings, for example for $K = k(\mathbf{i})$ where $\mathbf{i} = \sqrt{-1}$. In particular, if k itself cannot be ordered (which is equivalent to -1 being a sum of squares in k), this condition is equivalent to $\mathrm{cd}(k) \leq 1$. Since by classical Artin–Schreier theory every involution in the absolute Galois group of a field is self-centralising, Haran's work [Ahr93, Theorem A on page 219] implies that the absolute Galois group of a field k is real projective if and only if k satisfies $\mathrm{cd}(k(\mathbf{i})) \leq 1$.

Example 1. Examples of fields k which can be ordered with $\mathrm{cd}(k(\mathbf{i})) \leq 1$ include real closed fields, function fields in one variable over any real closed ground field, the field of Laurent series in one variable over any real closed ground field, and the field $\mathbb{Q}^{ab} \cap \mathbb{R}$ which is the subfield of $\mathbb{R}$ generated by the numbers $\cos(\frac{2\pi}{n})$ where $n \in \mathbb{N}$.

Furthermore, Haran and Jarden show in [HJ85] that the following important class of fields has real projective absolute Galois groups. For a field k, let $\mathrm{Spr}(k)$ denote the real spectrum of k, i.e., the set of all orderings of k. For an ordering $<\in \mathrm{Spr}(k)$, let $k_<$ denote the real closure of the ordered field $(k, <)$. A field k is called *pseudo real closed* if every absolutely irreducible variety defined over k which has a $k_<$-rational simple point for every $<\in \mathrm{Spr}(k)$ has a k-rational point. In particular, a pseudo real closed field with no orderings is pseudo algebraically closed, i.e., every absolutely irreducible variety defined over the field has a rational point. Moreover, if k is pseudo real closed, then $k(\mathbf{i})$ is pseudo algebraically closed, as $k_<(\mathbf{i})$ is algebraically closed for every $<\in \mathrm{Spr}(k)$ by Artin–Schreier theory. Hence k has virtual cohomological dimension ≤ 1, and in particular the absolute Galois group $\Gamma(k)$ is real projective by Haran's work. In [HJ85, Theorem on page 450] Haran–Jarden show that the absolute Galois group $\Gamma(k)$ of a pseudo real closed field k is real projective, and conversely, if G is a real projective group, then there is a pseudo real closed field k such that $\Gamma(k) \cong G$. Therefore, the Hopkins–Wickelgren formality conjecture for the class of fields of virtual cohomological dimension ≤ 1 is the same as for the class of pseudo real closed fields, and it is a purely group-theoretical problem for the class of real projective profinite groups. As a consequence of Theorem 1 we then obtain the following result, which provides the first example of a class of fields with infinite cohomological dimension for which formality holds.

Theorem 2 ([PQ22]). *Let k be a field with virtual cohomological dimension ≤ 1 and let $\Gamma(k)$ denote its absolute Galois group. Then, for all primes p, $C^\bullet(\Gamma(k), \mathbb{F}_p)$ is formal and satisfies strong Massey vanishing, i.e., whenever the Massey product of any number of elements of any nonzero cohomological degrees is defined then it contains zero.*

4. Koszulity conjecture

Another consequence of our methods is a positive case of a conjecture by Positselski and Voevodsky on the Koszulity of Galois cohomology [Pos14, §0.1, page 128]. One way to formulate the conjecture is that, for every field k containing a primitive pth root of unity and absolute Galois group $\Gamma(k)$, the algebra $H^\bullet(\Gamma(k), \mathbb{F}_p)$ is Koszul (see also [MPQT21]). One of the significances of the conjecture is that Positselski and Vishik show in [PV95] that Koszulity of the Galois cohomology would be a key ingredient in a potential alternative way to prove the Milnor–Bloch–Kato conjecture, i.e., the Norm Residue Theorem. In [PQ22] we prove the following result:

Theorem 3 ([PQ22])**.** *Let k be a field with virtual cohomological dimension ≤ 1 and p be a prime number. Then the cohomology algebra $H^\bullet(\Gamma(k), \mathbb{F}_p)$ is Koszul.*

Recently, other positive cases of the Koszulity conjecture of Positselski and Voevodsky were proven in [MPQT21, Theorem D].

References

[BCG23] F. M. Bleher, T. Chinburg and J. Gillibert, *Massey products and elliptic curves*, Proc. Lond. Math. Soc. (3) **127** (2023), no.1, 134–164.

[EM17] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math. Soc. **19** (2017), no. 12, 3629–3640.

[Eke86] T. Ekedahl, *Two examples of smooth projective varieties with nonzero Massey products*, Algebra, algebraic topology and their interactions (Stockholm, 1983), Lecture Notes in Math., vol. 1183, Springer-Verlag, Berlin, 1986, pp. 128–132.

[GMT18] P. Guillot, J. Mináč and A. Topaz, *Four-fold Massey products in Galois cohomology*, Compos. Math. **154** (2018), no. 9, 1921–1959, with an appendix by O. Wittenberg.

[Ahr93] D. Haran, *On the cohomological dimension of Artin-Schreier structures*, J. Algebra **156** (1993), 219–236.

[HJ85] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field*, Ann. Sc. Norm. Sup. Pisa **12** (1985), 449–489.

[HW23] Y. Harpaz and O. Wittenberg, *The Massey vanishing conjecture for number fields*, Duke Math. J. **172** (2023), no. 1, 1–41.

[HW15] M. Hopkins and K. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra **219** (2015), 1304–1319.

[Mat14] E. Matzri, *Triple Massey products and Galois cohomology*, preprint, arXiv:1411.4146 [math.RA](2014).

[MS22] A. Merkurjev and F. Scavia, *Degenerate fourfold Massey products over arbitrary fields*, preprint, arXiv:2208.13011 [math.NT] (2022).

[MS16] A. Merkurjev and F. Scavia, *The Massey Vanishing Conjecture for fourfold Massey products modulo 2*, preprint, arXiv:2301.09290 [math.NT] (2023).

[MT16] J. Mináč and N. D. Tân, *Triple Massey products vanish over all fields*, J. Lond. Math. Soc. (2) **94** (2016), no. 3, 909–932.

[MT17] J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*, J. Eur. Math. Soc. **19** (2017), 255–284.

[MPQT21] J. Mináč, F. W. Pasini, C. Quadrelli and N. D. Tân, *Koszul algebras and quadratic duals in Galois cohomology*, Adv. Math. **380** (2021), Paper No. 107569, 49 pp.

[PQ22] A. Pál and G. Quick, *Real projective groups are formal*, preprint, arXiv:2206.14645 [math.NT] (2022).

[PS18] A. Pál and E. Szabó, *The strong Massey vanishing conjecture for fields with virtual cohomological dimension at most* 1, arXiv:1811.06192 [math.AG], to appear in Israel J. Math.

[PV95] L. Positselski and A. Vishik, *Koszul duality and Galois cohomology*, Mathematical Research Letters **2** (1995), 771–781.

[Pos14] L. Positselski, *Galois cohomology of a number field is Koszul*, J. Number Theory **145** (2014), 126–152.

[Pos17] L. Positselski, *Koszulity of cohomology* $= K(\pi, 1)$*-ness + quasi-formality*, J. Algebra **483** (2017), 188–229.

[Quad22] C. Quadrelli, *Massey products in Galois cohomology and the Elementary Type Conjecture*, arXiv:2203.16232v6 [math.NT] (2022), to appear in J. Number Theory.

Finiteness theorems in Galois cohomology over function fields

David Harari

Let G be an algebraic group over a field K. Let $\overline{K}$ be a separable closure of K, with Galois group $\Gamma_K := \mathrm{Gal}(\overline{K}/K)$. The Galois cohomology set

$$H^i(K, G) := H^i(\Gamma_K, G(\overline{K}))$$

is defined for $i = 0, 1$. If G is commutative, it is defined for all non negative i and is an abelian group. The set $H^1(K, G)$ is especially interesting, as it classifies G-torsors (that is: principal homogeneous spaces of G) over K. It is therefore natural to ask about the finiteness of $H^1(K, G)$.

The first important results are due to Borel and Serre, in a 1964 paper ([BS64]):

Theorem 1 (Borel-Serre)**.** *If K is a p-adic field and G is linear, then the set $H^1(K, G)$ is finite.*

For G finite, this follows from the fact that a p-adic field is *of type (F)* (for every $d > 0$, it has only finitely many extensions of degree d up to isomorphism). The proof then proceeds by devissage: the case of tori easily reduces to finite commutative groups; for a semi-simple group L, one can either use that $H^1(K, L) = 0$ for L simply connected (Kneser), or show that the map $H^1(K, N) \to H^1(K, L)$ is onto, where N is the normalizer of a maximal K-torus of L (which follows from conjugacy of maximal tori over $\overline{K}$).

The case of a number field k (with ring of integers $\mathcal{O}_k$) is more complicated. Obviously $H^1(k, G)$ is not finite in general (this already fails for $G = \mathbf{Z}/2$). One is led to introduce the *Tate-Shafarevich set* (analogue of the classical Tate-Shafarevich group of an abelian variety)

$$Ш^1(G) := \ker[H^1(k, G) \to \prod_{v \in \Omega} H^1(k_v, G)],$$

where Ω is the set of all places of k and k_v is the completion of k at v. In their 1964 article, Borel and Serre give a global version of the previous theorem:

Theorem 2 (Borel-Serre)**.** *If G is linear, then $Ш^1(G)$ is finite.*

In general $Ш^1$ does not behave well by devissage, but étale cohomology does. If $\mathcal{G}$ is a smooth model of G over some non empty Zariski open subset U of $\mathrm{Spec}\,\mathcal{O}_k$, it is actually sufficient to prove that the image of the étale cohomology set $H^1(U, \mathcal{G})$ into $H^1(K, G)$ is finite. The commutative case reduces to Dirichlet's theorem on units plus the finiteness of the ideal class group. The case when G is semi-simple was done by Borel via harmonic analysis on adeles. It can also be settled by application of Kneser-Harder-Chernousov theorem, which asserts the nullity of $Ш^1(G)$ if G is semi-simple and simply connected (only a case by case proof is known; the case of type E_8 was done by Chernousov at the end of the eighties).

Here are a few other cases over local fields and global fields :

- For an abelian variety A of positive dimension over a p-adic field K, the group $H^1(K, A)$ is always infinite (it is dual to the profinite group $A^t(K)$, where A^t is the dual abelian variety of A, by a classical theorem of Tate). The finiteness of $Ш^1(A)$ over a number field is a conjecture, known in a few cases.
- In positive characteristic, one has to work with the flat cohomology set instead of the étale one (they coincide if the group G is smooth). Over a local field K of characteristic p like $\mathbf{F}_p((t))$, the set $H^1(K, G)$ might be infinite if there is no smoothness assumption (ex. $G = \mu_p$). However, the analogue of the Borel-Serre theorem still holds (Conrad, [Con12]) over a global field of characteristic p like $\mathbf{F}_p(t)$.

From now on we consider the case of the function field K of a curve C defined over a field k of characteristic zero. Let X be a projective and smooth compactification of C. For any algebraic K-group G, we define

$$Ш^1_C(G) := \ker[H^1(K, G) \to \prod_{c \in C^{(1)}} H^1(K_c, G)],$$

where $C^{(1)}$ is the set of closed points of C and K_c the completion of K for the discrete valuation associated to C. Set $Ш^1(G) = Ш^1_X(G)$.

Theorem 3 (Saidi-Tamagawa [ST20]). *Assume that k is finitely generated over $\mathbf{Q}$ and that $G = A$ is an abelian variety. Then the N-torsion part of $Ш^1_C(A)$ is finite for every positive N, and $Ш^1_C(A)$ itself is finite if A is isotrivial (that is: $A_{\overline{K}} = A \times_K \overline{K}$ is defined over $\bar{k}$).*

Saidi-Tamagawa's result is motivated by the anabelian section conjecture (to reduce it from finitely generated fields to number fields). It seems reasonable to conjecture that $Ш^1_C(A)$ is always finite (they make similar conjectures in their paper).

Theorem 4 (Harari-Szamuely [HS22]). *Let G_k be a commutative algebraic group over a number field k, set $G = G_k \times_k K$. Then $Ш^1_C(G)$ is finite (and this extends to finitely generated fields k if $C(k) \neq \emptyset$).*

Using Saidi-Tamagawa's theorem, the crucial case is when G_k is an algebraic torus. Whence the following conjecture :

Conjecture 1. *Assume that k is a number field. For every K-torus (or even group of multiplicative type) T, the group $Ш^1_C(T)$ is finite.*

In [HS22], examples with $Ш^1_C(T) \neq 0$ are given, even for $C = X$ (with isotrivial or non-isotrivial tori). Also, observe that the local groups $H^1(K_c, T)$ are in general infinite. The conjecture is known for a stably rational K-torus T (loc. cit.). The similar question for a non commutative linear group G is completely open.

Finally, a specialization argument and Hilbert's irreducibility Theorem show that if M is a finite type Γ_K-module and k is finitely generated over $\mathbf{Q}$, then

$Ш^1_C(M) = 0$. For M finite, A. and I. Rapinchuk recently showed that for a finite Γ_K-group G (and k arbitrary), the map

$$H^1(K, G) \to \prod_{c \in C^{(1)}} H^1(K_c, G)$$

is proper.

Suppose now that k is a p-adic field, hence K is the function field of a p-adic curve. Here the local groups $H^1(K_c, G)$ are finite because K_c, which is a finite extension of $k((t))$, is of type (F). Thus the finiteness of $Ш^1_C(G)$ is equivalent to the finiteness of $Ш^1(G) = Ш^1_X(G)$.

Theorem 5 (Harari-Szamuely [HS16])**.** *If G is commutative and linear, then $Ш^1(G)$ is finite.*

Again, examples with $Ш^1(T) \neq 0$ do exist with T a K-torus. The proof of the theorem uses duality theorems à la Poitou-Tate. It has been extended by A. and I. Rapinchuk to X of arbitrary dimension (using points of codimension 1 instead of closed points to define $Ш^1$) and any k of type (F).

It is reasonable to conjecture that the previous theorem still holds for a non commutative linear group (but this has been shown by Izquierdo to fail in general for an abelian variety [Izq17]). This can be reduced to G semi-simple and simply connected. A few cases are known by work of Yisheng Tian. The answer is also positive for all quasi-split groups (except of E_8 type) if the curve X has good reduction, see [HS16].

References

[BS64] A. Borel, J-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comment. Math. Helv. **39** (1964), 111–164.

[Con12] B. Conrad, *Finiteness theorems for algebraic groups over function fields*, Compos. Math. **148** (2012), no 2, 555–639.

[HS16] D. Harari, T. Szamuely, *Local-global questions for tori over p-adic function fields*, J. Algebraic Geom. **23**, no 3 (2016), 571–605.

[HS22] D. Harari, T. Szamuely, *On Tate–Shafarevich groups of one-dimensional families of commutative group schemes over number fields*, Math. Z. **302** (2022), 935–948.

[Izq17] D. Izquierdo, *Variétés abéliennes sur les corps de fonctions de courbes sur des corps locaux*, Doc. Math.. **22** (2017), 297–361.

[ST20] M. Saidi, A. Tamagawa, *On the arithmetic of abelian varieties*, J. reine angew. Math. **762** (2020), 1–33.

On the toric locus of ℓ-adic local systems arising from geometry

Anna Cadoret
(joint work with Jakob Stix)

For an algebraic group G, let G° denote its neutral component. Let k be a number field. Let X be a smooth, separated, geometrically connected variety over k and let $|X|$ denote the set of closed points of X. For an infinite $\infty : k \hookrightarrow \mathbb{C}$ (resp. finite $v : k \hookrightarrow k_v$) places, let $X \rightsquigarrow X_\infty \rightsquigarrow X_\infty^{\mathrm{an}}$ (resp. $X \rightsquigarrow X_v \rightsquigarrow X_v^{\mathrm{an}}$) denote the base-change and analytification functors. Fix a prime ℓ and a $\mathbb{Q}_\ell$-local system $\mathcal{V}_\ell$ on X *viz* a continuous representation of the étale fundamental group $\pi_1(X, \bar{x})$ on $V_\ell := \mathcal{V}_{\ell,\bar{x}}$. Write $\overline{G}_\ell$, $G_\ell \subset \mathrm{GL}_{V_\ell}$ for the Zariski-closure of the images of $\pi_1(X_{\bar{k}})$ and $\pi_1(X)$ acting on V_ℓ and, for $x \in X$, write $G_{\ell,x} \subset \mathrm{GL}_{V_\ell}$ for "the"[1] Zariski-closure of the image of $\pi_1(x)$ acting on V_ℓ *via* $\pi_1(x) \to \pi_1(X)$. The degeneracy locus of $\mathcal{V}_\ell$ is the set

$$|X|_{\mathcal{V}_\ell} := \{x \in |X| \mid G_{\ell,x}^\circ \subsetneq G_\ell^\circ\}$$

For a smooth projective morphism $f : Y \to X$, the $\mathbb{Q}_\ell$-local systems of the form $\mathcal{V}_\ell = R^i f_* \mathbb{Q}_\ell(j)$ control certain arithmetico-geometric invariants of the Y_x, $x \in |X|$ (*e.g.* ℓ-primary torsion of the Picard variety or of the Brauer group, rank of the Néron-Severi group, of motivated cycles, rank of the the Picard variety *etc.*) and understanding $|X|_{\mathcal{V}_\ell}$ amounts to understanding how those invariants degenerate in the family Y_x, $x \in |X|$ - see [Cad23, §3] for details.

The leading conjecture about $|X|_{\mathcal{V}_\ell}$ is the following. For every integer $d \geq 1$ let $|X|^{\leq d}$ denote the set of all $x \in |X|$ such that $[k(x) : k] \leq d$. Then

Conjecture 1. *Assume $\overline{G}_\ell$ has finite abelianization. Then $|X|_{\mathcal{V}_\ell} \cap |X|^{\leq d}$ is not Zariski-dense in X.*

For X a curve, Conjecture 1 is proved in [CT13]. In contrast, if X has dimension ≥ 2, it is widely open. Actually, the strategy of [CT13] provides a heuristic for Conj. 1 when $d = 1$ - see [Cad23, §4]; this heuristic relies on the diophantine Lang conjecture (that on a number field k the set of k-rational point of a variety of general type is not Zariski-dense), which seems currently out of reach, even for surfaces.

Assume $\mathcal{V}_\ell = R^i f_* \mathbb{Q}_\ell(j)$ for some smooth projective morphism $f : Y \to X$. In this case $\overline{G}_\ell$ is known to be semisimple - hence, in particular, to have finite abelianization; assume furthermore it is not finite. In this work, we investigate a weaker form of Conj. 1, replacing $|X|_{\mathcal{V}_\ell}$ by the toric locus $|X|_{\mathcal{V}_\ell}^{\mathrm{tor}} := \{x \in |X| \mid G_{\ell,x}^\circ \text{ is a torus}\}$, which, informally, corresponds to the most degenerate members of the family of motivated motive $\mathfrak{h}^i(Y_x)(j)$.

Conjecture 2. *With the above assumptions, $|X|_{\mathcal{V}_\ell}^{\mathrm{tor}} \cap |X|^{\leq d}$ is not Zariski-dense in X.*

[1] Actually only well defined up to conjugacy.

Conjecture 2 follows from Conjecture 1 but it is also a consequence of the Mumford-Tate conjecture and the generalized André-Oort conjecture (an unlikely intersection type conjecture); this implication is deep as it involves the average Colmez conjecture. Actually, the Mumford-Tate conjecture predicts that the points $x \in X_\infty(\mathbb{C})$ lifting those of $|X|^{\mathrm{tor}}_{\mathcal{V}_\ell}$ are exactly the CM points of the polarizable $\mathbb{Q}$-VHS $\mathcal{V}_\infty := R^i f^{\mathrm{an}}_\infty \mathbb{Q}(j)$ and that $|X|^{\mathrm{tor}}_{\mathcal{V}_\ell}$ should play a similar part in controlling the geometry of the exceptional locus $|X|_{\mathcal{V}_\ell}$ as the CM points do in controlling the geometry of the Hodge locus.Unfortunately, in general, we do not know how $|X|^{\mathrm{tor}}_{\mathcal{V}_\ell}$ compares with the CM locus; actually, we do not even know if $|X|^{\mathrm{tor}}_{\mathcal{V}_\ell}$ is independent of ℓ.

The only things which are known are that

(1) the solvable locus $|X|^{\mathrm{solv}}_{\mathcal{V}_\ell} := \{x \in |X| \mid G^\circ_{\ell,x} \text{ is solvable}\} \subset |X|_{\mathcal{V}_\ell}$, is independent of ℓ; this follows from class field theory [Se68] (and is true more generally for any $\mathbb{Q}_\ell$-local system which is almost pointwise geometric in the sense of Fontaine-Mazur).
(2) For every prime ℓ, $|X|^{\mathrm{tor}}_{\mathcal{V}_\ell}$ contains the set $|X|^{\mathrm{tor}}_{\mathcal{V}_{\mathrm{mot}}}$ of all $x \in |X|$ such that the connected component of the motivated Galois group (in the sense of André) of the motivated motive $\mathfrak{h}^i(Y_x)(j)$ is a torus.

Our main result is the following. We keep the assumptions in Conjecture 2. Consider the level condition: (Lev$_\ell$) The image of $\pi_1(X_{\bar{k}})$ acting on V_ℓ is a pro-ℓ group.

Theorem 1. *Assume (Lev$_\ell$) holds for at least two primes $\ell_1 \neq \ell_2$. Then there exists a set $\mathcal{L}$ of primes of positive Dirichlet density such that for every $\ell \in \mathcal{L}$ the set $|X|^{\mathrm{tor}-}_{\mathcal{V}_\ell} \cap X(k)$ is not Zariski-dense in X. Furthermore, if the complex period map describing $\mathcal{V}_\infty$ is finite-to-one, then $|X|^{\mathrm{tor}-}_{\mathcal{V}_\ell} \cap X(k)$ is finite.*

Here, $|X|^{\mathrm{tor}-}_{\mathcal{V}_\ell}$ denotes the subset of all $x \in |X|^{\mathrm{tor}}_{\mathcal{V}_\ell}$ such that $x \in |X|^{\mathrm{tor}}_{\mathcal{V}_{\ell_x}}$ for another $\ell_x \neq \ell$. In particular, $|X|^{\mathrm{tor}}_{\mathcal{V}_{\mathrm{mot}}} \cap X(k)$ is not Zariski-dense in X.

Remark 1. We hope our strategy to prove Theorem 1 can be extended to prove Conjecture 2 in general (namely for arbitrary $d \geq 1$ and without level conditions) but still with the restriction that ℓ belongs to a subset $\mathcal{L}$ of primes of positive Dirichlet density. For the time being, treating all primes ℓ seems to require a truely new idea.

1. Brief sketch of proof

Step 1: "toric points are integral". Fix a non-empty open subscheme $U \subset \mathrm{spec}(\mathcal{O}_k)$ and $\mathcal{Y} \xrightarrow{f} \mathcal{X} \hookrightarrow \mathcal{X}^{\mathrm{cpt}} \to U$ with $\mathcal{X}^{\mathrm{cpt}} \to U$ smooth, projective, $\mathcal{X} \hookrightarrow \mathcal{X}^{\mathrm{cpt}}$ an open immersion such that $\mathcal{Z} := \mathcal{X}^{\mathrm{cpt}} \setminus \mathcal{X} \to U$ is a relative normal crossing divisor and $f : \mathcal{Y} \to \mathcal{X}$ a smooth projective morphism with generic fiber $f : Y \to X$. Let $\mathcal{Z}^+ \subset \mathcal{Z}$ denote the union of those irreducible components around which the monodromy of $\mathcal{V}_\infty$ is trivial and set $\mathcal{X}^+ := \mathcal{X} \cup \mathcal{Z}^+$. It is not difficult to check that

$\mathcal{V}_\ell$ extends to a $\mathbb{Q}_\ell$-local system on the generic fiber X^+ of $\mathcal{X}^+$. By the nilpotent orbit theorem, $\mathcal{V}_\infty$ also extends to a polarizable $\mathbb{Z}$-VHS on $X_\infty^{+\mathrm{an}}$.

The key lemma is the following. Fix $v \in U$, $v|p$ let $\mathcal{O}_v$, k_v denote respectively the completions of $\mathcal{O}_k$, k at v.

Lemma 1 (Good reduction criterion)**.** *Let $\ell \neq p$ be a prime such that the image of $\pi_1(X_{k_v})$ acting on V_ℓ is of prime-to-p order. Then for every $x \in X^+(k_v)$, $x \in \mathcal{X}^+(\mathcal{O}_v)$ iff $x^*\mathcal{V}_\ell$ is unramified at v.*

The proof of Lemma 1 is similar to [PST21, §4]; it relies on the interpretation of Kummer theory in terms of intersection data and the nilpotent orbit theorem. That Lemma 1 applies to toric points follows from the theory of complex multiplication [Se68], Serre-Tate criterion [SeT68], and the level assumption in Theorem 1. It is to apply Lemma 1 that we have to replace $|X|^{\mathrm{tor}}_{\mathcal{V}_\ell}$ with $|X|^{\mathrm{tor}-}_{\mathcal{V}_\ell}$.

Step 2: "Integral toric points are not Zariski-dense". This step follows the strategy of [LawV20] using the enhanced version of the local v-adic period map constructed in [BS22] (building on recent development in variational p-adic Hodge theory - [LiZ17], [Shi20], [DLanLiZ23]).

Write $\mathcal{V}_{\mathrm{dR}} := \mathbb{R}^i f_*\Omega_{Y|X}$ for the relative de Rham cohomology; this is a filtered vector bundle with flat connexion. The strategy of [LawV20] relies on the motivic properties of the collection $\mathcal{V}_p$, $\mathcal{V}_{\mathrm{dR}}$, $\mathcal{V}_\infty$ - in particular that $\mathcal{V}_p$ be pointwise pure with characteristic polynomial of Frobenius in $\mathbb{Q}[T]$ and with bounded denominators, that $(\mathcal{V}_\infty, \mathcal{V}^{\mathrm{an}}_{\mathrm{dR},\infty})$ is a polarizable $\mathbb{Z}$-VHS on X^{an}_∞, that $(\mathcal{V}_p, \mathcal{V}^{\mathrm{an}}_{\mathrm{dR},v})$ is a de Rham pair on X^{an}_v*etc.* In step 1, we have extended $\mathcal{V}_p$ from X to X^+ but there is no reason why $f : Y \to X$ should extend to a smooth projective morphism over X^+ (and it does not in general) so, to run the [LawV20] strategy, we have to check that $\mathcal{V}_p$, $\mathcal{V}_{\mathrm{dR}}$, $\mathcal{V}_\infty$ extend from X to X^+ with all the expected properties; this involves the nilpotent orbit theorem (as already mentioned in step 1), the companion conjecture [Laf02, Thm. VII.6] and the rigidity of the de Rham property [LiZ17, Thm. 3.9 (iv)].

Once this is done, fix $v \in U_p$. Let $\underline{r}$ be the type of the filtration on $\mathcal{V}_{\mathrm{dR}}$ and let $\check{\mathbf{D}}(\underline{r})$ denote the Grassmaniann over k classifying filtration of type $\underline{r}$ on $\mathcal{V}_{\mathrm{dR},x} \simeq k^{\oplus r}$. The crux of the argument is that for every $x_0 \in \Sigma := |X^+|^{\mathrm{tor}}_{\mathcal{V}_p} \cap X(k)$ there exists an admissible open neighbourhood U_v of x_0 in $X_v^{+\mathrm{an}}$ and a v-adic analytic period map $\Phi_v : U_v \to \check{\mathbf{D}}(\underline{r})^{\mathrm{an}}_v$ such that the fibers of $\Phi_v : U_v \to \check{\mathbf{D}}(\underline{r})^{\mathrm{an}}_v$ above points in $\Phi_v(X(k) \cap U_v)$ are not-Zariski dense in X (see [LawV20, §9.2]), and which, for every $x \in U_v$, fits into a commutative diagram:

(∗)

$$\begin{tikzcd}
U_v \arrow[r, "\Phi_{\mathrm{et}}"] \arrow[d, dotted] \arrow[dr, "\Phi_{\mathrm{pH}}"] \arrow[dd, bend right=60, "\Phi_v"'] & \mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\pi_1(k_v)) \arrow[r, "\pi_0"] \arrow[d, hook, "D_{\mathrm{cris}}"] & \pi_0(\mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\pi_1(k_v))) \arrow[d, hook, "D_{\mathrm{cris}}"] \\
\mathrm{FM}_{k_v}(M_{0,x}, \underline{r}) \arrow[r, hook] \arrow[d] & \mathrm{FM}_{k_v}(\phi) \arrow[r, "\pi_0"] & \pi_0(\mathrm{FM}_{k_v}(\phi)), \\
\check{\mathbf{D}}(\underline{r})^{\mathrm{an}}_v \arrow[urr, "\alpha_x"'] & &
\end{tikzcd}$$

where $\Phi_{\mathrm{et}} : U_v \to \mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\pi_1(k_v))$ is the map that sends $x \in U_v$ to $x^*\mathcal{V}_v$, which is automatically crystalline - [Shi20], $D_{\mathrm{cris}} : \mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\pi_1(k_v)) \to \mathrm{FM}_{k_v}(\phi)$ is Fontaine's crystalline period functor $V_p \to (V_p \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})^{\pi_1(k_v)}$ (with value in the category $\mathrm{FM}_{k_v}(\phi)$ of filtered ϕ-modules); $\mathrm{FM}_{k_v}(M_{\mathrm{cris},x}, \underline{r})$ denotes the set of filtered ϕ-modules with fixed underlying ϕ-module $(M_{0,x}, \phi_x)$ and filtration of fixed type $\underline{r}$ and $\pi_0(-)$ denotes the set of isomorphism classes (of p-adic $\pi_1(k_v)$-representations and filtered ϕ-modules respectively). From step 1, $\Sigma \subset \mathcal{X}^+(\mathcal{O}_v)$ hence, as $\mathcal{X}^+(\mathcal{O}_v)$ is compact, one can cover Σ by finitely many U_v as above. This reduces the proof of Theorem 1 to showing that (1) $\pi_0 \circ \Phi_{\mathrm{et}}(\Sigma \cap U_v)$ is finite and (2) for every $x \in \Sigma \cap U_v$, the set $\alpha_x^{-1}(\alpha_x \circ \Phi_v(x))$ is finite[2].

Assertion (1) follows from a classical lemma of Faltings [FW84, V.5]. The proof of Assertion (2) is more demanding; the rough idea is as follows. Let $G_{\mathrm{cris},v}$ denote the Galois group of $\Phi_{pH}(x) = (M_{0,x}, \phi_x, F_x^\bullet)$ in $\mathrm{FM}_{k_v}(\phi)$ extended from $\mathbb{Q}_p$ to k_v so that, tautologically its centralizer $Z(G_{\mathrm{cris},v})$ stabilizes $F_x^\bullet$ and is contained in the centralizer $Z(\varphi_x)$ of the linearized crystalline Frobenius φ_x. Assertion (2) amounts to showing that $Z(\varphi_x)$ stabilizes $F_x^\bullet$ so that to conclude, it is enough to show $Z(\varphi_x) = Z(G_{\mathrm{cris},v})$. By the fully faithfullness of $D_{\mathrm{cris}} : \mathrm{Rep}^{\mathrm{cris}}_{\mathbb{Q}_p}(\pi_1(k_v)) \to \mathrm{FM}_{k_v}(\phi)$, and the fact that $x \in |X|^{\mathrm{tor}}_{\mathcal{V}_p}$, we already know that $G_{\mathrm{cris},v}$ is a torus so that it is actually enough to show that φ_x has maximal rank in $G_{\mathrm{cris},v}$. This is to ensure the later hold for *every* (*a priori* infinitely many!) $x \in \Sigma$ that we have to restrict to a subset $\mathcal{L}$ of primes of positive Dirichlet density. On top of several ingredients already mentioned, the proof uses Frobenius tori, [KM74] and, as one can guess, the Cebotarev density theorem.

References

[BS22] A. Betts and J. Stix *Galois sections and p-adic period mappings*, Preprint arXiv:2204.13674 [math.NT] (2022).

[Cad23] A. Cadoret, *Degeneration locus of $\mathbb{Q}_p$ local systems: conjectures*, Expositiones Math. vol. **41**, Iss. 3 - Special issue in the memory of Bas Edixhoven, p. 675–708, 2023

[2] By construction, the fibers of $\alpha_x : \check{\mathbf{D}}(\underline{r})^{\mathrm{an}}_v \to \pi_0(\mathrm{FM}_{k_v}(\phi))$ are homogeneous spaces under the centralizer $Z(\phi_x)$ of the crystalline Frobenius so, another way to phrase (2) is to say that points in $\alpha_x \circ \phi_v(\Sigma \cap U_v)$ have finite $Z(\phi_x)$-orbits.

[CT13] A. Cadoret and A. Tamagawa , *A uniform open image theorem for l-adic representations II* Duke Math. Journal **162**, p. 2301–2344, 2013.
[DLanLiZ23] H. Diao, K.W. Lan, R. Liu and X. Zh,. *Logarithmic Riemann–Hilbert correspondences for rigid varieties*, Journal of the American Math. Soc. **36**, p. 483–562, 2023.
[FW84] G. Faltings, G. Wüstholz (eds.), *Rational Points*, Aspects of Mathematics, E6, Friedr. Vieweg & Sohn, 1984.
[KM74] N. M. Katz and W. Messing, *Some consequences of the Riemann hypothesis for varieties over finite fields*, Invent. Math. **23**, p. 73–77, 1974.
[Laf02] L. Lafforgue, *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. Math. **147**, p.1–241, 2002.
[LawV20] B. Lawrence and A. Venkatesh, *Diophantine problems and p-adic period mappings*, Invent. Math. **221**, p. 893–999, 2020.
[LiZ17] R. Liu and X. Zhu, *Rigidity and a Rieman–Hilbert correspondence for p-adic local systems*, Invent. Math. **207**, p. 291–343, 2017.
[PST21] J. Pila, A. Shankar and J. Tsimerman, *Canonical heights on Shimura varieties and the André-Oort conjectures*, Preprint arXiv:2109.08788 [math.NT] (2021)
[Se68] J.-P. Serre, *Abelian ℓ-adic representations and Elliptic curves*, W.A. Benjamin, 1968.
[SeT68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Math. **88**, p. 492-517, 1968.
[Shi20] K. Shimizu, *A p-adic monodromy theorem for de Rham local systems*, Compositio Math. **158**, p. 2157–2205, 2022.

p-adic Hodge Theory and obstructions to rational points

L. Alexander Betts
(joint work with Theresa Kumpitsch, Martin Lüdtke, and Jakob Stix)

Let K be a number field and Y/K a smooth projective curve of genus ≥ 2. One common approach to studying the K-rational points on Y is to try to define an *obstruction locus*: a subset

$$Y(\mathbb{A}_K)^{(?)} \subseteq Y(\mathbb{A}_K)$$

of the adelic points of Y containing the K-rational points. The idea here is that by understanding or computing the locus $Y(\mathbb{A}_K)^{(?)}$, we can obtain some control on the K-rational points of Y, and thereby prove results about them.

The most famous examples of these kinds of obstruction loci are those cut out by the Brauer–Manin or finite descent obstructions [Sko01, Sto07]. However, other well-known techniques also fall within this general paradigm. The Chabauty–Kim method for a curve over $K = \mathbb{Q}$ attempts to compute $Y(\mathbb{Q})$ via the *Chabauty–Kim locus* [Kim09]

$$Y(\mathbb{Q}_p)^{\mathrm{CK}} \subseteq Y(\mathbb{Q}_p)\,,$$

a subset of the p-adic points of Y containing the rational points, which is often computable in practice. (Here, due to current limitations of the method, the prime p needs to be of good reduction for Y.) Similarly, the recent re-proof of the Mordell Conjecture by Lawrence and Venkatesh [LV20] can be construed as studying a certain *Lawrence–Venkatesh locus*

$$Y(K_v)^{\mathrm{LV}} \subseteq Y(K_v)$$

for v a finite place of K, containing the rational points. The overall structure of their argument shows that, for suitably chosen places v, the obstruction locus $Y(K_v)^{\mathrm{LV}}$ is finite, and hence so too is $Y(K)$.

1. Rational points and Selmer sections

In the context of this workshop, the relevance of this perspective is that these kinds of obstructions do not just constrain rational points, but also *Selmer*[1] *sections*: sections s of the fundamental exact sequence for Y/K which come from a K_v-point $y_v \in Y(K_v)$ at every place v of K. For v a finite place, we call the point y_v the *localisation* $\mathrm{loc}_v(s)$ of s. One can show, for every Selmer section s, that:

- the associated adelic point $(y_v)_v \in Y(\mathbb{A}_K)$ lies in the finite descent locus (this is a result of Harari–Stix [HS12]);
- the associated K_v-point $y_v \in Y(K_v)$ lies in the Lawrence–Venkatesh locus $Y(K_v)^{\mathrm{LV}}$ for all finite places v of K;
- when $K = \mathbb{Q}$, the associated $\mathbb{Q}_p$-point $y_p \in Y(\mathbb{Q}_p)$ lies in the Chabauty–Kim locus for all primes p of good reduction.

Thus, these obstructions do not just allow us to study rational points, they allow us to study Selmer sections in quite an explicit manner. Following this idea with the Lawrence–Venkatesh and Chabauty–Kim methods yields the following two results:

Theorem 1 (B.–Stix, [BS22])**.** *For all number fields K and all smooth projective curves Y/K of genus ≥ 2, the image of the localisation map*

$$\mathrm{loc}_v \colon \{\textit{Selmer sections}\} \to Y(K_v)$$

is finite for all self-conjugate[2] *places v.*

Theorem 2 (B.–Kumpitsch–Lüdtke, [BKL23])**.** *For $Y = \mathbb{P}^1_{\mathbb{Z}[1/2]} \smallsetminus \{0, 1, \infty\}$ the thrice-punctured line over $\mathbb{Z}[1/2]$, the set of $\mathbb{Z}[1/2]$-Selmer*[3] *sections on Y has exactly three elements, namely the sections attached to the three $\mathbb{Z}[1/2]$-integral points -1, 2 and $1/2$ on Y.*

2. Local systems: obstructions with additional structures

The subject of my talk in this workshop is a rather technical dive into the kinds of theoretical tools one uses to study the Chabauty–Kim and Lawrence–Venkatesh loci. For this, we recall in outline how these obstructions are defined.

[1] or *locally geometric* in S. Mochizuki's talk

[2] This is a technical condition required to make the argument work. Over $K = \mathbb{Q}$, all finite places are self-conjugate, so in this case there is no restriction.

[3] i.e. coming from a $\mathbb{Q}_2$-point of Y at 2 and coming from a $\mathbb{Z}_\ell$-point of Y at all odd primes ℓ

2.1. **Obstructions from local systems.** Let $\mathbb{E}$ be a $\mathbb{Q}_p$-local system on Y in the étale topology. For any K-rational point $y \in Y(K)$, the fibre $\mathbb{E}_y$ of $\mathbb{E}$ at (the geometric point corresponding to) y is a continuous representation of the absolute Galois group G_K of K. So one can associate to $\mathbb{E}$ an obstruction locus

$$Y(K_v)_{\mathbb{E}} \subseteq Y(K_v)\,,$$

namely the set of all v-adic points y_v for which the fibre $\mathbb{E}_{y_v}$ is the restriction of a G_K-representation satisfying appropriate local properties. (In all our cases, we will want to choose the place v to divide p.) This locus clearly contains the set of K-rational points.

2.2. **Extra structures on local systems.** If $\mathbb{E}$ comes with extra structures, then one can give a variant of this definition where one requires that $\mathbb{E}_{y_v}$ is the restriction of a G_K-representation with the corresponding structures. For example, in the Lawrence–Venkatesh method, the local system one considers is the first relative étale cohomology of a smooth proper family $X \to Y$, where $X \to Y$ is the composite of a finite étale covering $Y' \to Y$ and a polarised abelian scheme $X \to Y'$.

In this case, $\mathbb{E}$ comes endowed with the structure of a symplectic module over the 0th relative étale cohomology, and the Lawrence–Venkatesh locus is defined to be the set of local points $y_v \in Y(K_v)$ for which $\mathbb{E}_{y_v}$ is the restriction of a symplectic module object in the category of G_K-representations, again satisfying some local conditions.

In the Chabauty–Kim method, $\mathbb{E}$ is taken to be the universal pro-unipotent $\mathbb{Q}_p$-local system, and this comes with an extra structure in the form of an action of the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $Y_{\bar{\mathbb{Q}}}$.

3. Fontaine's theory of potentially semistable representations

In order to study an obstruction locus $Y(K_v)_{\mathbb{E}}$ of this kind, we need to understand for which points $y_v \in Y(K_v)$ the local representation $\mathbb{E}_{y_v}$ lies in some fixed collection of isomorphism classes. In other words, we want to understand how the local representation $\mathbb{E}_{y_v}$ varies as we vary the point $y_v \in Y(K_v)$.

To make sense of this question, we use Fontaine's theory [Fon94b]. To any de Rham representation V of the local Galois group G_v, we can associate a filtered (φ, N, G_v)-module $\mathsf{D}_{\mathrm{pH}}(V)$, i.e. a vector space D over the maximal unramified extension $\mathbb{Q}_p^{\mathrm{nr}}$ of $\mathbb{Q}_p$, endowed with a semilinear Frobenius automorphism φ, a monodromy endomorphism N, a semilinear action of G_v, and a K_v-linear filtration on $D_{K_v} = (\bar{K}_v \otimes_{\mathbb{Q}_p^{\mathrm{nr}}} D)^{G_v}$, satisfying certain compatibility properties. Using work of Shimizu [Shi22], one can show that if the local system $\mathbb{E}$ is de Rham (in the sense of Scholze's relative p-adic Hodge theory [Sch13, Sch16]), then the isomorphism class of $\mathsf{D}_{\mathrm{pH}}(\mathbb{E}_{y_v})$ as a (non-filtered!) (φ, N, G_v)-module is locally constant on $Y(K_v)$ for the v-adic topology.

3.1. **Period map and filtration.** Thus, if we restrict to y_v lying in a suitably small v-adic disc in $Y(K_v)$, then $\mathsf{D}_{\mathrm{pH}}(\mathbb{E}_{y_v})$ is independent of y_v provided we ignore filtrations, and it only remains to understand how the filtration varies on this constant (φ, N, G_v)-module. This is controlled by the theory of period maps. If $\mathcal{E}$ denotes the filtered vector bundle with integrable connection on Y_{K_v} associated to $\mathbb{E}$ by Scholze's theory, then for y_v in a sufficiently small disc, we may identify the fibres $\mathcal{E}_{y_v}$ via parallel transport. Shimizu's theory tells us that $\mathsf{D}_{\mathrm{pH}}(\mathbb{E}_{y_v})_{K_v}$ may be identified with the fibre $\mathcal{E}_{y_v}$ in a manner compatible with filtrations. Thus, understanding how the filtration on $\mathsf{D}_{\mathrm{pH}}(\mathbb{E}_{y_v})$ varies with y_v becomes the same as understanding how the filtration on $\mathcal{E}_{y_v}$ varies with y_v.

This latter problem is well-studied. Explicitly, for a fixed basepoint $y_0 \in Y(K_v)$, the set of filtrations on the fibre $\mathcal{E}_{y_0}$ is a certain flag variety $\mathcal{G}_{y_0}$, and the map sending a point y_v nearby y_0 to the filtration on $\mathcal{E}_{y_0} = \mathcal{E}_{y_v}$ identified via parallel transport, is known as the *period map* Φ_{y_0}. The period map is K_v-analytic.

3.2. **Finiteness results via period maps.** In practice, what this means is the following. For any of our v-adic obstructions (e.g. Lawrence–Venkatesh, Chabauty–Kim), we are interested in studying the set of local points y_v for which $\mathbb{E}_{y_v}$ lies in a certain set of isomorphism classes. Restricting to a small neighbourhood of a point $y_0 \in Y(K_v)$, this becomes equivalent to the problem of determining when $\Phi_{y_0}(y_v)$ lies in a particular subset $\mathcal{G}_{y_0}(K_v)^{\mathrm{glob}} \subseteq \mathcal{G}_{y_0}(K_v)$. In the cases of interest, we take care to ensure that the following key condition is satisfied:

> The Zariski-closure of $\mathcal{G}_{y_0}(K_v)^{\mathrm{glob}}$ inside $\mathcal{G}_{y_0}$ does not contain the image of the period map Φ_{y_0}.

(This condition holds in the Chabauty–Kim setting when a certain dimension inequality holds, and holds in the Lawrence–Venkatesh setting when the abelian-by-finite family is chosen suitably. In both cases, this is a delicate argument, using that one knows what the vector bundle $\mathcal{E}$ is in both cases.) The significance of this condition is that it ensures that

$$Y(K_v)_{\mathbb{E}} \cap (\text{small disc about } y_0) = \Phi_{y_0}^{-1}(\mathcal{G}_{y_0}(K_v))$$

is contained in the vanishing locus of a *non-zero* rigid-analytic function on a small neighbourhood of y_0, so is finite. This is what ultimately allows one to prove finiteness results for the v-adic obstruction loci $Y(K_v)_{\mathbb{E}}$.

References

[BKL23] L.A. Betts, T. Kumpitsch and M. Lüdtke. Chabauty–Kim and the Section Conjecture for locally geometric sections. arXiv:2305.09462 [math.NT], 2023.

[BS22] L.A. Betts and J. Stix. Galois sections and p-adic period mappings. arXiv:2204.13674 [math.NT], 2022.

[Fon94b] J.-M. Fontaine. Représentations p-adiques semi-stables. *Astérisque*, 223:113–184, 1994. With an appendix by P. Colmez.

[HS12] D. Harari and J. Stix. *Descent obstruction and fundamental exact sequence*, volume 2 of *Contributions in Mathematical and Computational Sciences*, chapter 7, pages 147–166. Springer-Verlag, 2012.

[Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.

[LV20] B. Lawrence and A. Venkatesh. Diophantine problems and p-adic period mappings. *Invent. Math.*, 221(3):893–999, 2020.

[Sch13] P. Scholze. p-adic Hodge theory for rigid-analytic varieties. *Forum of Mathematics, Pi*, 1:e1, 2013.
[Sch16] P. Scholze. p-adic Hodge theory for rigid-analytic varieties – corrigendum. *Forum of Mathematics, Pi*, 4:e6, 2016.
[Shi22] K. Shimizu. A p-adic monodromy theorem for de Rham local systems. *Compositio mathematica*, 158(2):2157–2205, 2022.
[Sko01] A. Skorobogatov Torsors and rational points. Cambridge Tracts in Mathematics 144. Cambridge University Press, 2001.
[Sto07] M. Stoll. Finite descent obstructions and rational points on curves. *Algebra & Number Theory*, 1(4):349–391, 2007.

Inter-universal Teichmüller Theory as an Anabelian Gateway to Diophantine Geometry and Analytic Number Theory

Shinichi Mochizuki
(joint work with Yuichiro Hoshi, Arata Minamide, Shota Tsujimura, and Go Yamashita)

1. Overview via a famous quote of Poincaré

One question that is frequently asked concerning inter-universal Teichmüller theory (IUT) is the following:

> Why/how does IUT allow one to apply **anabelian geometry** to prove **diophantine** results?

In this report, we address this question by giving an *overview of various aspects of IUT*, many of which may be regarded as *striking examples* of the famous quote of *Poincaré* to the effect that

> "**mathematics is the art of giving the same name to different things**"

— which was apparently *originally motivated* by various observations on the part of Poincaré concerning certain remarkable similarities between *transformation group symmetries* of modular functions such as *theta functions*, on the one hand, and *symmetry groups* of the *hyperbolic geometry* of the *upper half-plane*, on the other — all of which are *closely related to IUT* (cf. [EssLgc], §1.5; the discussion surrounding (InfH) in [EssLgc], §3.3; [EssLgc], Example 3.3.2). Here, we note that there are (at least) *three ways* in which this quote of *Poincaré* is related to *IUT*:

(1) the *original motivation* of Poincaré (mentioned above),
(2) the key IUT notions of *coricity/multiradiality* (cf. §2.1, §2.2, §3.2 below), and
(3) *new applications* of the *Galois-orbit version of IUT* (cf. §4 below).

One important theme in this context consists of the observation that one may acquire a rough *survey-level* understanding of IUT using only a knowledge of such elementary topics as

(a) the notions of *rings/fields/groups/monoids* (cf. §2 below; [EssLgc], Example 2.4.8) and

(b) the elementary geometry of the *projective line/Riemann sphere/analytic continuation* (cf. §3 below; [EssLgc], Example 2.4.7).

A more detailed exposition of IUT may be found in the *survey texts* [Alien], [EssLgc], as well as, of course, in the original papers [IUTch], which are exposed in the *videos/slides* available at [ExHr21a, ExHr21b].

2. The N-th power map and Galois groups as abstract groups

Let R be an *integral domain* (such as $\mathbb{Z} \subseteq \mathbb{Q}$) equipped with the action of a *group* G, $(\mathbb{Z} \ni)$ $N \geq 2$. For simplicity, we assume that $N = 1 + \cdots + 1 \neq 0 \in R$, and that R has *no nontrivial N-th roots of unity.* Write $R^{\rhd} \subseteq R$ for the *multiplicative monoid* $R \setminus \{0\}$.

Then let us observe that the *N-th power map* on $R^{\rhd}$ determines an *isomorphism of multiplicative monoids* equipped with actions by G, i.e.,

$$G \curvearrowright \; R^{\rhd} \; \stackrel{\sim}{\to} \; (R^{\rhd})^N \; (\subseteq R^{\rhd}) \; \curvearrowleft \; G,$$

that does *not arise* from a *ring homomorphism*, i.e., is clearly *not compatible* with *addition* (cf. our assumption on N!).

2.1. Distinct ring structures. Next, let ${}^{\dagger}R$, ${}^{\ddagger}R$ be *two distinct copies* of the integral domain R, equipped with respective actions by *two distinct copies* ${}^{\dagger}G$, ${}^{\ddagger}G$ of the group G. We shall use similar notation for objects with labels "†", "‡" to the previously introduced notation. Then one may use the *isomorphism of multiplicative monoids* arising from the *N-th power map* discussed above to *glue* together

$${}^{\dagger}G \curvearrowright {}^{\dagger}R \supseteq ({}^{\dagger}R^{\rhd})^N \quad \stackrel{\sim}{\leftarrow} \quad {}^{\ddagger}R^{\rhd} \subseteq {}^{\ddagger}R \curvearrowleft {}^{\ddagger}G$$

the *ring* ${}^{\dagger}R$ to the *ring* ${}^{\ddagger}R$ along the *multiplicative monoid* $({}^{\dagger}R^{\rhd})^N \stackrel{\sim}{\leftarrow} {}^{\ddagger}R^{\rhd}$.

This gluing is *compatible* with the respective actions of ${}^{\dagger}G$, ${}^{\ddagger}G$ relative to the isomorphism ${}^{\dagger}G \stackrel{\sim}{\to} {}^{\ddagger}G$ given by forgetting the labels "†", "‡", but, since the N-th power map is **not compatible** with **addition** (!), this isomorphism ${}^{\dagger}G \stackrel{\sim}{\to} {}^{\ddagger}G$ may be regarded either as an isomorphism of (*"coric"*, i.e., *invariant* with respect to the N-th power map) **abstract groups** (cf. the notion of *"inter-universality"*, as discussed in [EssLgc], §3.2, §3.8) or as an isomorphism of groups equipped with actions on certain *multiplicative monoids*, but **not** as an isomorphism of (**"Galois"** — cf. the *classical inner automorphism indeterminacies* of SGA1) groups equipped with actions on *rings/fields.*

2.2. The multiradial algorithm. The problem of *describing (certain portions of the) ring structure* of ${}^{\dagger}R$ in terms of the *ring structure* of ${}^{\ddagger}R$ — in a fashion that is *compatible* with the *gluing* and via a *single* algorithm that may be applied to the *common* (cf. *"logical AND $\wedge$"!) glued data* to reconstruct *simultaneously* (certain portions of) the ring structures of *both* ${}^{\dagger}R$ and ${}^{\ddagger}R$, up to suitable relatively mild *indeterminacies* (cf. the theory of *crystals*!) — seems (at first glance/in general) to be *hopelessly intractable*[1] (cf. the case where $R = \mathbb{Z}$)!

This is precisely what is *achieved in IUT* (cf. the quote of *Poincaré*!) by means of the **multiradial algorithm** for the **Θ-pilot** via

- **anabelian geometry** (cf. the *abstract groups* ${}^{\dagger}G$, ${}^{\ddagger}G$!),
- the ***p*-adic/complex logarithm** and **theta functions**, and
- **Kummer theory** (to relate **Frobenius-/étale-like** versions of objects).

Thus, in summary,

> the *multiplicative monoid* and *abstract group* structures (but *not* the ring structures!) are *common* (cf. *"logical AND $\wedge$"!*) to †, ‡.

On the other hand, once one *deletes* the *labels* "†", "‡" to secure a "common R", one obtains a *meaningless* situation, where the common glued data may be related via "†" *OR "$\vee$"* via "‡" to the common R, but *not simultaneously* to both.

When $R = \mathbb{Z}$ (or, more generally, the *ring of integers* "$\mathcal{O}_F$" of a number field F — cf. the multiplicative *norm map* $\mathrm{N}_{F/\mathbb{Q}} : F \to \mathbb{Q}$), one may consider the **"height"** $\log(|x|) \in \mathbb{R}$ for $0 \neq x \in \mathbb{Z}$. Then the *N-th power map* corresponds, after passing to *heights*, to *multiplication by N*; the *multiradial algorithm* corresponds to saying that the height is *unaffected (up to a mild error term!)* by *multiplication by N*, i.e., that the *height is bounded.*

3. Conceptual analogies with the projective line/Riemann sphere

Let k be a *field* (which, in fact, could be taken to be an arbitrary ring), R a *k-algebra.* Denote the *units* of a ring by a superscript "$\times$". Write $\mathbb{A}^1$ for the *affine line* $\operatorname{Spec}(k[T])$ over k, $\mathbb{G}_{\mathrm{m}}$ for the open subscheme $\operatorname{Spec}(k[T, T^{-1}])$ of $\mathbb{A}^1$ obtained by removing the origin.

Recall that the standard coordinate T on $\mathbb{A}^1$ and $\mathbb{G}_{\mathrm{m}}$ determines

$$\textit{natural bijections } \mathbb{A}^1(R) \xrightarrow{\sim} R, \ \mathbb{G}_{\mathrm{m}}(R) \xrightarrow{\sim} R^{\times}$$

that are compatible with the well-known natural structures on $\mathbb{A}^1$ and $\mathbb{G}_{\mathrm{m}}$, respectively, of *ring scheme/(multiplicative) group scheme* over k.

3.1. Gluing together distinctly labeled ring schemes. Next, write ${}^{\dagger}\mathbb{A}^1$, ${}^{\ddagger}\mathbb{A}^1$ for the *k-ring schemes* given by *copies* of $\mathbb{A}^1$ equipped with *labels* "†", "‡". Observe that there exists a *unique isomorphism* of *k-ring schemes* ${}^{\dagger}\mathbb{A}^1 \xrightarrow{\sim} {}^{\ddagger}\mathbb{A}^1$; moreover, there exists a *unique isomorphism* of *k-group schemes* $(-)^{-1} : {}^{\dagger}\mathbb{G}_{\mathrm{m}} \xrightarrow{\sim} {}^{\ddagger}\mathbb{G}_{\mathrm{m}}$ that maps ${}^{\dagger}T \mapsto {}^{\ddagger}T^{-1}$. Note that $(-)^{-1}$ does *not extend* to an isomorphism ${}^{\dagger}\mathbb{A}^1 \xrightarrow{\sim} {}^{\ddagger}\mathbb{A}^1$ and is clearly *not compatible* with the *k-ring scheme structures* of ${}^{\dagger}\mathbb{A}^1$ ($\supseteq {}^{\dagger}\mathbb{G}_{\mathrm{m}}$), ${}^{\ddagger}\mathbb{A}^1$ ($\supseteq {}^{\ddagger}\mathbb{G}_{\mathrm{m}}$).

The *standard construction* of the *projective line* $\mathbb{P}^1$ may be understood as the result of *gluing* ${}^{\dagger}\mathbb{A}^1$ to ${}^{\ddagger}\mathbb{A}^1$ along the isomorphism

[1] One well-known example may be seen in the situation where, when $N = p$, one works *modulo p* (cf. the point of view of *indeterminacies*, the analogy with *crystals*!), so that there is a *common ring structure* that is *compatible* with the *p-th power map.*

$$^\dagger\mathbb{A}^1 \ \supseteq \ ^\dagger\mathbb{G}_\mathrm{m} \stackrel{(-)^{-1}}{\longrightarrow} \ ^\ddagger\mathbb{G}_\mathrm{m} \ \subseteq \ ^\ddagger\mathbb{A}^1$$

— i.e., at the level of *R-rational points* $^\dagger R \ \supseteq \ ^\dagger R^\times \stackrel{(-)^{-1}}{\longrightarrow} \ ^\ddagger R^\times \ \subseteq \ ^\ddagger R$ — where $^\Box R = {}^\Box\mathbb{A}^1(R)$, $^\Box R^\times = {}^\Box\mathbb{G}_\mathrm{m}(R)$, for $\Box \in \{\dagger, \ddagger\}$ (cf. the *gluing* situation discussed in §2, where "$(-)^{-1}$" corresponds to "$(-)^N$"!). In particular, *relative to this gluing*, we observe that there exists a *single rational function* on the copy of "$\mathbb{G}_\mathrm{m}$" that appears in the gluing that is *simultaneously* equal to the rational function $^\dagger T$ on $^\dagger\mathbb{A}^1$ *AND* [cf. "$\wedge$"!] to the rational function $^\ddagger T^{-1}$ on $^\ddagger\mathbb{A}^1$. Thus, in summary,

> the standard construction of $\mathbb{P}^1$ may be regarded as consisting of a *gluing* of two *ring schemes* along an *isomorphism* of *multiplicative group schemes* that is *not compatible* with the *ring scheme* structures on either side of the gluing.

Here, we observe that if, in the gluing under discussion, one *arbitrarily deletes* the *distinct labels* "†", "‡" (e.g., on the grounds that both ring schemes represent "THE" structure sheaf "$\mathcal{O}_X$" of a k-scheme X!), then the resulting *"gluing without labels"* amounts to a gluing of a *single copy* of $\mathbb{A}^1$ to itself that maps the standard coordinate T on $\mathbb{A}^1$ (regarded, say, as a rational function on $\mathbb{A}^1$) to T^{-1}. That is to say, such a *deletion of labels* (even when restricted to the (abstractly isomorphic) multiplicative monoids $^\dagger T^\mathbb{Z}$, $^\ddagger T^\mathbb{Z}$!) immediately results in a *contradiction* (i.e., since $T \neq T^{-1}$!), unless one passes to some sort of *quotient* of $\mathbb{A}^1$, e.g., by introducing some sort of *indeterminacy*, which amounts to the consideration of some sort of *collection of possibilities* [cf. "$\vee$"!].

3.2. **Analogy with the geodesic flow on the Riemann sphere.** When $k = \mathbb{C}$ (i.e., the *complex number field*), one may think of $\mathbb{P}^1$ as the *Riemann sphere* $\mathbb{S}^2$ equipped with the *Fubini-Study metric* and of the gluing under discussion as the gluing, along the *equator* $\mathbb{E}$, of the *northern hemisphere* $\mathbb{H}^+$ to the *southern hemisphere* $\mathbb{H}^-$.

Then the above discussion of standard coordinates "$^\dagger T$", "$^\ddagger T$" translates into the following (at first glance, *self-contradictory*!) phenomenon: an *oriented flow* along the *equator* — which may be thought of physically as a sort of *east-to-west wind current* — appears *simultaneously* to be flowing in the *clockwise* direction, from the point of view of $\mathbb{H}^+ \subseteq \mathbb{S}^2$, *AND* in the *counterclockwise* direction, from the point of view of $\mathbb{H}^- \subseteq \mathbb{S}^2$. Indeed, if one *arbitrarily deletes the labels* "+", "−" and *identifies* $\mathbb{H}^-$ with $\mathbb{H}^+$, then one literally obtains a *contradiction.*

On the other hand, one may relate $\mathbb{H}^-$ to $\mathbb{H}^+$ (*not* by such an arbitrary deletion of labels (!), but rather) by applying the well-known **metric/geodesic geometry/isometric symmetries** of $\mathbb{S}^2$ — i.e., by considering the *geodesic flow* along *great circles/lines of longitude* — to **represent**, up to a *relatively mild distortion*, the entirety of $\mathbb{S}^2$, i.e., including $\mathbb{H}^- \subseteq \mathbb{S}^2$, as a sort of **deformation/displacement** of $\mathbb{H}^+$ (cf. the point of view of *cartography*!).

It is precisely this metric/geodesic/symmetry-based approach that corresponds to the *anabelian geometry*-based *multiradial algorithm for the* Θ*-pilot* in IUT (cf.

the analogy discussed in [Alien], §3.1, (iv), (v), as well as in [EssLgc], §3.5, §3.10, between *multiradiality* and *connections/parallel transport/crystals*!).

3.3. **Foundational aspects: universes, diagrams, and data types.** In this context, it is important to remember that, just like SGA, IUT is *formulated entirely in the framework* of **"ZFCG"** (i.e., ZFC, plus Grothendieck's axiom on the existence of universes), especially when considering various *set-theoretic/foundational* aspects of *"gluing"* operations in IUT (cf. [EssLgc], §1.5, §3.8, §3.9, as well as [EssLgc], §3.10, especially the discussion of *"log-shift adjustment"* in (Stp 7)), such as the following:

- gluings are performed at the abstract level of *diagrams* (cf. graphs of groups/anabelioids) and are *not* equipped with any *embedding* into some *familiar ambient space* (like a sphere);
- the *output of reconstruction algorithms* is only well-defined at the level of *objects up to isomorphism* (up to *suitable indeterminacies*), i.e., "types/ packages of data" (such as groups, rings, monoids, diagrams, etc.) called *"species"* — one consequence of which is the central importance of *closed loops* in order to obtain *set-theoretic comparisons* that are *not possible at intermediate steps.*

Here, we note the importance of working with

- *"types/packages of data"* (cf., e.g., the *diagrams* referred to above), as opposed to certain particular underlying sets of interest (cf. the classical functoriality of *resolutions* up to *homotopy* in cohomology, as well as of *algebraic closures* of fields up to *conjugacy indeterminacies* — which become unnecessary, e.g., if one considers *norms*), as well as
- the importance of working with **"closed loops"** (cf. *norms* in Galois theory; the classical theory of *analytic continuation/Riemann surfaces* — which is reminiscent of the classical *Riemann-Weierstrass* dispute! (cf. [EssLgc], §1.5); the *geodesic completeness/closed geodesics/isometric symmetries* of the sphere).

4. New enhanced versions of IUT and related work in progress

Recent joint work in progress focuses on the *Section Conjecture ("SC")* in anabelian geometry and allows one (cf. [GSCsp]), using *"resolution of nonsingularities (RNS)"* (cf. [RNSPM]), together with a result of Stoll,

> to reduce the geometricity of an arbitrary Galois section of a hyperbolic curve over a number field to **local geometricity** at each nonarchimedean prime, together with *3 global conditions*, which correspond, respectively, to **3 new enhanced versions of IUT** that are currently under development.

Moreover, this theory of [GSCsp], when combined with other joint work in progress (cf. [AnPf]), has led to substantial progress on the *p-adic SC* that is closely related to the use of *Raynaud-Tamagawa "new-ordinariness"* in the theory of *RNS* (cf. [RNSPM]), and which is noteworthy in that it functions as a sort of *local p-adic* *analogue of IUT*, via the following analogy: "Norm$(-) = (-)$" $\longleftrightarrow$ "$N \cdot (-) \approx (-)$" (cf. §2.2).

4.1. **Applications of the Galois-orbit version of IUT.** One such new enhanced version of IUT is the *Galois-orbit version of IUT (GalOrbIUT)*, which implies the following:

- *"intersection-finiteness"*, one of the 3 global conditions mentioned above in the discussion of the *SC*,
- the *nonexistence of Siegel zeroes* of Dirichlet *L*-functions associated to imaginary quadratic number fields (i.e., by applying the work of Colmez/ Granville-Stark/Táfula), and
- a *numerically stronger* version of the *abc/Szpiro* inequalities.

That is to say, we obtain three *a priori different* applications to *anabelian geometry* (the "local-global" SC), *analytic number theory* (nonexistence of Siegel zeroes), and *diophantine geometry* (abc/Szpiro inequalities) — a *striking example* of *Poincaré's quote*, i.e., all three are essentially the **same mathematical phenomenon** of **bounding heights**, i.e., **bounding "local denominators"**.

Indeed, one key aspect of the *local-global SC* application is

> to exhibit IUT as "*anabelian geometry* applied to obtain more *anabelian geometry*"

(hence is less psychologically/intuitively surprising than the other two applications). Other noteworthy aspects include the following:

- it is *technically the most difficult/essential* of the three, i.e., to the extent that the *other two* applications may be thought of, to a substantial extent, as being *"inessential by-products"*;
- it is similar in spirit to the *historical point of view* (cf., e.g., of Grothendieck's famous "letter to Faltings") that suggests (*without any proof!*) that the SC might imply results in diophantine geometry (such as the Mordell Conjecture).

4.2. **Anabelian conceptualization of the abc inequality.** Finally, in this context, it is interesting to recall (cf. [Alien], §3.11, (iii)) that the essential content of *anabelian geometry* may be understood as a sort of **"conceptual translation"** of the *abc inequality*:

> indeed, just as **anabelian geometry** centers around reconstructing *addition* from *multiplication*, the **abc inequality** may be thought of as a bound on the *height (or "additive size")* of a number by the *conductor (or "multiplicative size")* of the number,

i.e., both of these situations exhibit **addition** as being "**dominated** by" **multiplication**. This "conceptual"/"numerical" correspondence is reminiscent of the well-known correspondence between the *conceptual* nature of the *Weil Conjectures* and the corresponding *numerical inequalities* for the number of rational points of a variety over a finite field.

References

[ExHr21a] *Invitation to Inter-universal Teichmüller theory*, in "Expanding Horizons of Inter-universal Teichmüller Theory" conference, RIMS Kyoto, online, 2021, notes and videos at https://www.kurims.kyoto-u.ac.jp/~motizuki/ExpHorizIUT21/WS3/ExpHorizIUT21-InvitationIUT-notes.html

[ExHr21b] *Inter-universal Teichmller Theory (IUT) Summit 2021*, in "Expanding Horizons of Inter-universal Teichmüller Theory" conference, RIMS Kyoto, online, 2021, notes and videos at https://www.kurims.kyoto-u.ac.jp/~motizuki/ExpHorizIUT21/WS4/ExpHorizIUT21-IUTSummit-notes.html

[IUTch] S. Mochizuki, *Inter-universal Teichmüller Theory I: Construction of Hodge Theaters*, Publ. Res. Inst. Math. Sci. **57** (2021), 3–207; *II: Hodge-Arakelov-theoretic Evaluation*, Publ. Res. Inst. Math. Sci. **57** (2021), 209–401; *III: Canonical Splittings of the Log-theta-lattice*, Publ. Res. Inst. Math. Sci. **57** (2021), 403–626; *IV: Log-volume Computations and Set-theoretic Foundations*, Publ. Res. Inst. Math. Sci. **57** (2021), 627–723.

[Alien] S. Mochizuki, *The Mathematics of Mutually Alien Copies: from Gaussian Integrals to Inter-universal Teichmüller Theory*, Inter-universal Teichmüller Theory Summit 2016, RIMS Kōkyūroku Bessatsu **B84**, Res. Inst. Math. Sci. (RIMS), Kyoto (2021), 23–192; available at https://www.kurims.kyoto-u.ac.jp/~motizuki/Alien%20Copies,%20Gaussians,%20and%20Inter-universal%20Teichmuller%20Theory.pdf

[EssLgc] S. Mochizuki, *On the essential logical structure of inter-universal Teichmüller theory in terms of logical AND "$\wedge$"/logical OR "$\vee$" relations: Report on the occasion of the publication of the four main papers on inter-universal Teichmüller theory*, RIMS Preprint **1968** (November 2022); updated version available at: https://www.kurims.kyoto-u.ac.jp/~motizuki/Essential%20Logical%20Structure%20of%20Inter-universal%20Teichmuller%20Theory.pdf

[RNSPM] S. Mochizuki, S. Tsujimura, *Resolution of Nonsingularities, Point-theoreticity, and Metric-admissibility for p-adic Hyperbolic Curves*, RIMS Preprint **1974** (June 2023).

[GSCsp] Y. Hoshi, S. Mochizuki, *Arithmetic cuspidalization of Galois sections of hyperbolic curves*, manuscript in preparation.

[AnPf] Y. Hoshi, S. Mochizuki, S. Tsujimura, G. Yamashita, *Anabelian geometry over complete discrete valuation rings with perfect residue fields*, manuscript in preparation.

Arithmetic statistics for function fields via homological stability

Craig Westerland

(joint work with Jordan Ellenberg, Akshay Venkatesh; TriThang Tran; Jonas Bergström, Adrian Diaconu, Dan Petersen)

This was an overview talk on algebro-topological methods for approaching questions in arithmetic statistics over function fields. I discussed work with coauthors (listed above) in the papers [EVW16, ETW23, BDPW23], as well as work of Ronno Das [Das21] and Weiyan Chen [Che17].

While many famous problems in number theory are about the existence of certain arithmetic objects, arithmetic statistics addresses questions of the probability or frequency of their occurrence. For instance, a positive solution to the inverse Galois problem for a finite group G and a field K would furnish a field extension L/K whose Galois group $\mathrm{Gal}(L/K)$ is isomorphic to G. In contrast, when K is a global field, Malle has conjectured an asymptotic formula for the *number* of such extensions, as a function of the discriminant $\Delta_{L/K}$ of the extension.

More precisely, we let G be a transitive subgroup of S_m, and let $\overline{K}$ be a separable closure of K. Define a function which counts degree n extensions of K inside of $\overline{K}$ with Galois group G:

$$N_{G,K}(X) := \#\{L \leq \overline{K} \mid \deg(L/K) = m,\ \mathrm{Gal}(L/K) \cong G,\ |\Delta_{L/K}| \leq X\}. \tag{1}$$

Here the isomorphism $\mathrm{Gal}(L/K) \cong G$ is required to be one of groups acting on the set of m embeddings of L into $\overline{K}$. In [Mal04], Malle conjectures an asymptotic for this quantity:

$$N_{G,K}(X) \sim cX^a \log(X)^{b-1},$$

where the constants a and b are given in terms of the group theory of $G \leq S_m$ and the action of $\mathrm{Gal}(\overline{K}/K)$ on $G = \mathrm{Hom}(\widehat{\mathbb{Z}}, G)$ through the cyclotomic character. When G is abelian, this conjecture is a theorem of Wright's [Wri89] proven using methods of the class field theory.

In the number field setting, Malle's conjecture is supported by a weight of computational evidence, but has been proven in very few non-abelian cases; see, e.g., [DH71, Bha05, Bha10, Wan21]. In joint work with Ellenberg and Tran, we proved an upper bound when K is taken to be the function field $\mathbb{F}_q(t)$:

Theorem 1. *For each integer m and each transitive $G \leq S_m$, there are constants $C(G), Q(G)$, and $e(G)$ such that, for all $q > Q(G)$ coprime to $\#G$ and all $X > 0$,*

$$N_{G,\mathbb{F}_q(t)}(X) \leq C(G)X^{a(G)} \log(X)^{e(G)}$$

Here the exponent $e(G)$ is always at least as large as Malle's $b - 1$.

The main distinction between the number field and function field settings is geometric. By definition, function fields are tied to the geometry of curves, and their extensions correspond to ramified covering maps between curves. Specifically, extensions $L/k(t)$ correspond to curves $\Sigma = \mathrm{Spec}(\mathcal{O}_L)$ defined over k, and maps $\Sigma \to \mathbb{A}^1_k = \mathrm{Spec}\, k[t]$. When $K = \mathbb{F}_q[t]$, the set being counted in Eq. (1) can be reinterpreted as the set of isomorphism classes of such branched covers. This, in turn, may be identified as the set of $\mathbb{F}_q$-points of a moduli space of branched covers.

Explicitly, we make the following definition: for $n \in \mathbb{Z}_{\geq 0}$, the *Hurwitz moduli space* $\mathrm{Hur}_{G,n}$ is a scheme whose k points (with $\mathrm{char}(k)$ coprime to $\#G$) parameterize $\{(\pi, \tau)\}/\cong$, where

- Σ is a smooth projective curve, and $\pi : \Sigma \to \mathbb{P}^1_k$ is a branched cover:
- Away from a reduced divisor $D \subseteq \mathbb{P}^1_k$, π is a G-Galois cover.
- $\deg(D \cap \mathbb{A}^1) = n$.
- π is tamely ramified at D.
- $\tau : \pi^{-1}(v) \cong G$ is a trivialization of the fibre over a tangential point $v : \mathrm{Spec}(k((t))) \to \mathbb{A}^1_k$ at ∞.

Write $\mathrm{CHur}_{G,n}$ for the subscheme where Σ is geometrically connected. G acts on these schemes by changing τ. By replacing a G-Galois cover Σ with the degree m cover $\Sigma \times_G [m]$, we may show

$$N_{G,\mathbb{F}_q(t)}(X) = \sum_{|\Delta| \leq X} \#[\mathrm{CHur}_{G,n}/G](\mathbb{F}_q).$$

where the sum is over those components of $[\mathrm{CHur}_{G,n}/G]$ whose associated extensions have discriminant less than X. This discriminant may be computed as a product over the branch locus of π of q^{m-d}, where d is the number of cycles in the ramification above the branch point; thus to obtain $|\Delta| = X$, n ranges between $\log_q(X)/(m-D)$ and $\log_q(X)$, where D is the largest possible number of cycles allowed by elements of $G \leq S_m$. In this language, the constant $a(G)$ in Theorem 1 is easy to explain: $a(G)^{-1} = m - D$.

To prove Theorem 1, then, we must bound the quantity $\#[\mathrm{CHur}_{G,n}/G](\mathbb{F}_q)$ as a function of n; it suffices to do so for the larger scheme $\mathrm{Hur}_{G,n}$. To do this, we employ the Grothendieck-Lefschetz trace formula. In our setting, this is the statement that

$$\#\,\mathrm{Hur}_{G,n}(\mathbb{F}_q) = q^n \sum_{i=0}^{2n} (-1)^i \operatorname{tr}(\mathrm{Frob}_q \circlearrowright H^i_{et}(\mathrm{Hur}_{G,n}|_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell))$$

The trace on H^0_{et} is the number of $\mathbb{F}_q$-rational components. Deligne shows that the eigenvalues on H^i_{et} are bounded above by $q^{-i/2}$, so

$$\#\,\mathrm{Hur}_{G,n}(\mathbb{F}_q) - q^n \#\pi_0(\mathrm{Hur}_{G,n}|_{\mathbb{F}_q}) \leq \sum_{i=1}^{2n} q^{n-i/2} \operatorname{rk}_{\mathbb{Q}_\ell}(H^i_{et}(\mathrm{Hur}_{G,n}|_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell))$$

Further, comparison theorems identify

$$\operatorname{rk}_{\mathbb{Q}_\ell}(H^i_{et}(\mathrm{Hur}_{G,n}|_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)) = \operatorname{rk}_{\mathbb{Q}}(H^i_{sing}(\mathrm{Hur}_{G,n}(\mathbb{C}), \mathbb{Q})) =: r(i,n).$$

Thus, our task is to show that $r(i,n)$ does not grow too quickly: at worst exponentially in i polynomially in n (of growth rate at worst that of $\#\pi_0(\mathrm{Hur}_{G,n}|_{\mathbb{F}_q})$).

Notice that at this point, the problem has been reduced to a computation purely within the realm of algebraic topology. In particular, the function $\mathrm{Hur}_{G,n}(\mathbb{C}) \to \mathrm{Conf}_n(\mathbb{C})$ which carries a branched covering to its branch locus is a covering space. Further, the configuration space $\mathrm{Conf}_n(\mathbb{C}) = K(B_n, 1)$ is an Eilenberg-MacLane space for the n^{th} *braid group* B_n. Thus the computation of $H^i_{sing}(\mathrm{Hur}_{G,n}(\mathbb{C}), \mathbb{Q})$ may be rephrased as a group cohomology computation for B_n with coefficients in the *Hurwitz representation*.

In [EVW16], Ellenberg, Venkatesh, and I gave the desired cohomological bound when G is drawn from a certain class of generalized dihedral groups; our application was to a function field version of Cohen-Lenstra's conjecture on the distribution of class groups of imaginary quadratic fields. In [ETW23] with Ellenberg and Tran, we extended these results (using new topological methods) to the general setting. In the first case, our methods built on classical homological stability for braid groups. In the second, we used the Fuks/Fox-Neuwirth cellular stratification of configuration space to give an interpretation of the computation in terms of the cohomology of objects arising in the theory of quantum groups. Unfortunately, our cohomological calculations are insufficient to provide the lower bound in Malle's conjecture.

This method may be summarized as follows:

(1) Translate the statistical question over $\mathbb{F}_q(t)$ into a question about (asymptotically) estimating $\#M_n(\mathbb{F}_q)$, where M_n is a moduli stack parameterizing the objects of interest of "complexity" n.
(2) Compute $\#M_n(\mathbb{F}_q)$ in terms of Lefschetz numbers in étale cohomology.
(3) The contribution from $H_0(M_n)$ is usually the main term in the asymptotic.
(4) To establish this, one must show that $\operatorname{rk} H_{>0}(M_n)$ isn't too large.
(5) Conclude that the contribution from $H_{>0}(M_n)$ is of lower order via Deligne's bounds on the eigenvalues of Frobenius.

There are by now a number of other examples where this method has been employed to establish arithmetic statistical results over function fields:

- In [EL23], Ellenberg and Landesman study the distribution of Selmer groups of elliptic curves over $\mathbb{F}_q(t)$ as they vary in quadratic twist families. They establish that the Bhargava-Kane-Lenstra-Poonen-Rains heuristics (see [BKL$^+$15]) hold for these families. Their homological method is very closely based on that of [EVW16].
- In [Das21], Das shows that (except at a finite number of characteristics) the average number of points on a smooth cubic surface $S \subset \mathbb{P}^3_{\mathbb{F}_q}$ is precisely $q^2 + q + 1 = \#\mathbb{P}^2(\mathbb{F}_q)$. He does so by analyzing the cohomology of the moduli space $\mathcal{M}$ of such surfaces, as well as the cohomology of the universal surface $\mathcal{U}$ over $\mathcal{M}$. Then
$$\text{average number of points on } S = \frac{\#\mathcal{U}(\mathbb{F}_q)}{\#\mathcal{M}(\mathbb{F}_q)}.$$
But Das shows that the map $\mathcal{U} \to \mathcal{M} \times \mathbb{P}^3$ induces an isomorphism
$$H^*(\mathcal{U}(\mathbb{C}), \mathbb{Q}) \cong H^*(\mathcal{M}(\mathbb{C}), \mathbb{Q}) \otimes H^*(\mathbb{P}^2(\mathbb{C}), \mathbb{Q}),$$
from which the result follows.
- In [Che17], Chen studies the related question about the average number of points on a superelliptic curve. For a monic squarefree polynomial $f(x)$ of degree n and integer e, there is an (affine) *superelliptic curve* X_f defined by
$$X_f := \{(x, y) \mid y^e = f(x)\}.$$
Chen shows that if n or e is odd, the average number of $\mathbb{F}_q$-points on X_f is precisely q. To do so, we think of Conf_n as the space of monic squarefree polynomials of degree n (by sending f to its roots). Then there is a universal superelliptic curve $\pi : E_{n,e} \to \operatorname{Conf}_n$; as before,
$$\text{average number of points on } X_f = \frac{\#E_{n,e}(\mathbb{F}_q)}{\#\operatorname{Conf}_n(\mathbb{F}_q)}.$$
Chen computes $H^*(E_{n,e}(\mathbb{C}), \mathbb{Q})$ in terms of the cohomology of the Burau representation, specialized at e^{th} roots of unity. He shows that π^* is an isomorphism, which gives the result.
- On a related subject, in [BDPW23], Bergström, Diaconu, Petersen, and I study the moments of quadratic Dirichlet L-functions over $\mathbb{F}_q(t)$. The central value of such an L-function is closely related to the central value of

the zeta function of the associated hyperelliptic curve. As the the curves range over the hyperelliptic ensemble, the associated moments can be computed in terms of the trace of Frobenius on the cohomology of $\mathrm{Conf}_n(\mathbb{C})$ (in its guise as a hyperelliptic moduli space) with coefficients in certain Schur functors applied to the Burau representation. We compute the stable cohomology, but are currently lacking a strong enough homological stability result to yield the desired asymptotics as conjectured in papers of Andrade, Conrey, Farmer, Keating, Rubinstein, and Snaith [AK14, CFK+05].

References

[AK14] J. C. Andrade and J. P. Keating, *Conjectures for the integral moments and ratios of L-functions over function fields*, J. Number Theory **142** (2014), 102–148.

[BDPW23] J. Bergström, A. Diaconu, D. Petersen, and C. Westerland, *Hyperelliptic curves, the scanning map, and moments of families of quadratic L-functions*, 2023.

[Bha05] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.

[Bha10] ———, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), no. 3, 1559–1591.

[BKL+15] M. Bhargava, D. M. Kane, H. W. Lenstra, Jr., B. Poonen, and E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Camb. J. Math. **3** (2015), no. 3, 275–321.

[CFK+05] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, *Integral moments of L-functions*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 33–104.

[Che17] W. Chen, *Homology of braid groups, the Burau representation, and points on superelliptic curves over finite fields*, Israel J. Math. **220** (2017), no. 2, 739–762.

[Das21] R. Das, *Cohomology of the universal smooth cubic surface*, Q. J. Math. **72** (2021), no. 3, 795–815.

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[EL23] J. S. Ellenberg and A. Landesman, *Homological stability for generalized Hurwitz spaces and Selmer groups in quadratic twist families over function fields*, 2023.

[ETW23] J. S. Ellenberg, T. Tran, and C. Westerland, *Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields*, 2023.

[EVW16] J. S. Ellenberg, A. Venkatesh, and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, Ann. of Math. (2) **183** (2016), no. 3, 729–786.

[Mal04] G. Malle, *On the distribution of Galois groups. II*, Experiment. Math. **13** (2004), no. 2, 129–135.

[Wan21] J. Wang, *Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$*, Compos. Math. **157** (2021), no. 1, 83–121. MR 4219215

[Wri89] D. J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), no. 1, 17–50.

Massey products for curves

Frauke M. Bleher

(joint work with Ted Chinburg, Jean Gillibert)

1. Motivation

The application of Massey products to understand the Galois groups of extensions of number fields is a longstanding research topic. We consider triple and higher Massey products on $\mathrm{H}^1(X, \mathbb{Z}/\ell)$ when ℓ is an odd prime number and X is a smooth projective variety over a field F in which ℓ is invertible. When $d = \dim(X) = 0$, Mináč and Tân showed in [MT16] that triple Massey products always vanish for arbitrary F. This followed earlier work by Hopkins and Wickelgren [HW15], Matzri [Mat14], Efrat and Matzri [EM17], and others. When $d = 0$ and F is a number field, Harpaz and Wittenberg showed in [HW23] that all t-fold Massey products vanish for $t \geq 3$. Ekedahl gave an example in [Ekd86] showing that triple Massey products need not vanish when $d = 2$ and $F = \mathbb{C}$.

It is thus a natural question to ask what happens when $d = 1$. Our main results show that in fact triple Massey products need not vanish when X is an elliptic curve.

2. Massey products and embedding problems

Suppose now that X is a smooth projective geometrically irreducible curve over an arbitrary field F, let $\bar{F}$ be the separable closure of F, and let $\bar{X} = X \otimes_F \bar{F}$. It follows from [Ach15, §2.1.2] that if $\bar{X}$ is not isomorphic to $\mathbb{P}^1_{\bar{F}}$ then there is a natural isomorphism

$$\mathrm{H}^i(X, \mathbb{Z}/\ell) \cong \mathrm{H}^i(\pi_1(X), \mathbb{Z}/\ell)$$

for all $i \geq 1$.

For $t \geq 3$, let $\chi_1, \dots, \chi_t \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$. The t-fold Massey product $\langle \chi_1, \dots, \chi_t \rangle$ is a subset of $\mathrm{H}^2(X, \mathbb{Z}/\ell)$ which could be empty. For example, if $t = 3$ then $\langle \chi_1, \chi_2, \chi_3 \rangle \neq \emptyset$ if and only if the cup products $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$. We say $\langle \chi_1, \chi_2, \chi_3 \rangle$ does not vanish if $\langle \chi_1, \chi_2, \chi_3 \rangle \neq \emptyset$ and $\langle \chi_1, \chi_2, \chi_3 \rangle$ does not contain the zero element of $\mathrm{H}^2(X, \mathbb{Z}/\ell)$.

We get the following connection to embedding problems (see [Dwy75]) where $U_4(\mathbb{Z}/\ell)$ denotes the group of 4×4 upper triangular unipotent matrices with entries in $\mathbb{Z}/\ell$:

Suppose $\langle \chi_1, \chi_2, \chi_3 \rangle \neq \emptyset$. Then $\langle \chi_1, \chi_2, \chi_3 \rangle$ vanishes if and only if the finite weak embedding problem determined by

- $\underline{\chi} : \pi_1(X) \to (\mathbb{Z}/\ell) \times (\mathbb{Z}/\ell) \times (\mathbb{Z}/\ell)$, given by $\sigma \mapsto (\chi_1(\sigma), \chi_2(\sigma), \chi_3(\sigma))$, and
- $\pi : U_4(\mathbb{Z}/\ell) \to (\mathbb{Z}/\ell) \times (\mathbb{Z}/\ell) \times (\mathbb{Z}/\ell)$, given by $\begin{pmatrix} 1 & a & d & f \\ 0 & 1 & b & e \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \mapsto (a, b, c)$,

has a weak solution, i.e. there exists a continuous group homomorphism $\rho : \pi_1(X) \to U_4(\mathbb{Z}/\ell)$ such that $\pi \circ \rho = \underline{\chi}$.

3. Overview of results

We have the following results:

3.1. When $F = \bar{F}$ then all t-fold Massey products vanish for $t \geq 3$.

3.2. When $F \neq \bar{F}$ then this does not have to be true, and we have examples of non-vanishing triple Massey products when X is an elliptic curve and F is a number field or a finite field.

3.3. More specifically, when $X = E$ is an elliptic curve, we classify precisely when triple Massey products do not vanish in the following two cases:

(a) the ℓ-torsion $\bar{E}[\ell]$ is defined over F, or
(b) F is a finite field.

4. More details

In the case 3.3 (a), i.e. when $\bar{E}[\ell]$ is defined over F, we show that the only case in which a non-empty triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ does not vanish is when $\ell = 3$ and each of χ_1, χ_2, χ_3 generates the same one-dimensional subspace of $\mathrm{H}^1(E, \mathbb{Z}/\ell)$. We prove the following result, where $G_F^{(3)}$ denotes the pro-3 completion of the absolute Galois group of F:

Theorem 1. *If $\bar{E}[3]$ is defined over F and $\mathrm{char}(F) \neq 3$, then there exists a character $\chi \in \mathrm{H}^1(E, \mathbb{Z}/3)$ such that $\langle \chi, \chi, \chi \rangle$ does not contain zero if and only if either*

(i) the action of $G_F^{(3)}$ on $\bar{E}[9]$ is not given by multiplication by scalars in $(\mathbb{Z}/9)^\times$, or
(ii) the action of $G_F^{(3)}$ on $\bar{E}[9]$ is given by multiplication by scalars in $(\mathbb{Z}/9)^\times$ and there exists a primitive ninth root of unity $\zeta_9 \in \bar{F}$ such that $\zeta_9 \notin F$ and $F(\zeta_9)$ is not the only cubic extension of F inside $\bar{F}$.

For example, if E is the elliptic curve over $F = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ with model $y^2 = x^3 - 1$, then $\bar{E}[3]$ is defined over F and F does not contain a primitive ninth root of unity. Hence there exists a character $\chi \in \mathrm{H}^1(E, \mathbb{Z}/3)$ with non-vanishing triple Massey product.

Another family of examples is constructed as follows:

Example 1. Let t be an indeterminate, and let E_t be the generic Legendre elliptic curve over $\mathbb{Q}(t)$ defined by the equation

$$y^2 = x(x-1)(x-t).$$

For an odd integer n, let $k := \mathbb{Q}(\zeta_n, t)$, and let $k(\bar{E}_t[n])$ be the field obtained from k by adjoining the coordinates of the n-torsion points of $\bar{E}_t$. By Igusa [Igu59, Theorem 3], the Galois representation

$$\mathrm{Gal}(k(\bar{E}_t[n])/k) \to \mathrm{GL}_2(\mathbb{Z}/n)$$

has image equal to $\mathrm{SL}_2(\mathbb{Z}/n)$. Considering $n = 9$ and $n = 3$, we get an exact sequence

$$1 \to \mathrm{Gal}(k(\bar{E}_t[9])/k(\bar{E}_t[3])) \to \mathrm{SL}_2(\mathbb{Z}/9) \to \mathrm{SL}_2(\mathbb{Z}/3) \to 1.$$

According to Hilbert's irreducibility theorem, these Galois groups remain the same for infinitely many rational specializations t_0 of the parameter t. Therefore, one obtains infinitely many (non-isomorphic) elliptic curves E_{t_0} over $F_{t_0} := \mathbb{Q}(\zeta_9, \bar{E}_{t_0}[3])$ that satisfy condition (i) of the previous theorem. In particular, there exists a character $\chi \in \mathrm{H}^1(E_{t_0}, \mathbb{Z}/3)$ with non-vanishing triple Massey product.

In the case 3.3 (b), i.e. when F is a finite field, we also consider the case when $\bar{E}[\ell]$ is not defined over F, so $\ell > 3$ is possible. We obtain the following result:

Theorem 2. *Suppose $\ell > 3$. There exist a prime number $p \neq \ell$, an elliptic curve E defined over $\mathbb{F}_p$, and non-trivial characters $\chi_1, \chi_2, \chi_3 \in \mathrm{H}^1(E, \mathbb{Z}/\ell)$ such that $\langle \chi_1, \chi_2, \chi_3 \rangle$ is not empty and does not contain zero.*

These results have recently been published in [BCG23].

5. Outlook

We are currently working on the following problems and questions:

5.1. Study vanishing and non-vanishing of triple Massey products for curves X of genus $g(X) \geq 2$, especially when $\ell > 3$. In particular, is it more likely for triple Massey products to not vanish for higher genus?

5.2. Study vanishing and non-vanishing of t-fold Massey products for curves X when $t \geq 4$. In particular, is it more likely for higher Massey products to vanish?

5.3. Relate Massey products on integral models $\mathcal{X}$ of curves X over a number field F to Massey products in the fibres. In particular, what can we say about the classes in $\mathrm{H}^2(\mathcal{X}, \mathbb{Z}/\ell)$ that are trivial on all fibres?

References

[Ach15] P. Achinger, *$K(\pi, 1)$-Spaces in Algebraic Geometry*, Thesis (Ph.D.) – University of California, Berkeley, 2015.

[BCG23] F. M. Bleher, T. Chinburg and J. Gillibert, *Massey products and elliptic curves*, Proc. Lond. Math. Soc. (3) **127** (2023), 134–164.

[EM17] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math. Soc. **19** (2017), no. 12, 3629–3640.

[Dwy75] W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), no. 2, 177–190.

[Ekd86] T. Ekedahl, *Two examples of smooth projective varieties with non-zero Massey products*, in: Algebra, algebraic topology and their interactions (Stockholm, 1983), 128–132, Lecture Notes in Math., 1183, Springer, Berlin, 1986.

[HW23] Y. Harpaz and O. Wittenberg, *The Massey vanishing conjecture for number fields*, Duke Math. J. **172** (2023), no. 1, 1–41.

[HW15] M. Hopkins and K. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra **219** (2015), 1304–1319.

[Igu59] J.-I. Igusa, *Fibre Systems of Jacobian Varieties: (III. Fibre Systems of Elliptic Curves)*, Amer. J. Math. **81** (1959), 453–476.

[Mat14] E. Matzri, *Triple Massey products in Galois cohomology*, arXiv:1411.4146 [math.RA], preprint 2014.

[MT16] J. Mináč and N. D. Tân, *Triple Massey products vanish over all fields*, J. Lond. Math. Soc. (2) **94** (2016), no. 3, 909–932.

Oda's problem for cyclic special loci

Séverin Philip
(joint work with B. Collas)

We report on recent progress on the arithmetic of ℓ-outer monodromy representations of moduli stacks of curves in relation with a question of Oda on the associated monodromy fixed fields and with the stack structure of moduli space of curves, see [CP23].

1. The classical Oda's problem

Let $\mathcal{M}_{g,m}$ be the moduli space of curves of genus g with m marked points satisfying the hyperbolicity condition $2g-2+m \geq 1$. Oda showed in [Oda97] that there is an exact sequence of étale fundamental groups induced by the point forgetting map

$$1 \longrightarrow \pi_1(C_{\overline{\mathbf{Q}}}) \longrightarrow \pi_1(\mathcal{M}_{g,m+1}) \longrightarrow \pi_1(\mathcal{M}_{g,m}) \longrightarrow 1$$

where $C/\mathbf{Q}$ is a hyperbolic curve represented on $\mathcal{M}_{g,m}$. From this exact sequence and by pro-ℓ completion we obtain a universal ℓ-monodromy outer action $\Phi^{\ell}_{g,m}\colon \pi_1(\mathcal{M}_{g,m}) \to \operatorname{Out}\pi_1^{\ell}(C_{\overline{\mathbf{Q}}})$ for any fixed prime ℓ. The universality is to be understood by the fact that for any such curve $C/\mathbf{Q}$ the usual ℓ-monodromy outer action $\varphi^{\ell}_C\colon G_{\mathbf{Q}} \to \operatorname{Out}\pi_1^{\ell}(C_{\overline{\mathbf{Q}}})$[1] induced by the homotopy exact sequence of C factors through $\Phi^{\ell}_{g,m}$ in the following commutative triangle

$$\begin{tikzcd} G_{\mathbf{Q}} \arrow[r, "\varphi^{\ell}_C"] \arrow[d, "s_C"'] & \operatorname{Out}\pi_1^{\ell}(C_{\overline{\mathbf{Q}}}) \\ \pi_1(\mathcal{M}_{g,m}) \arrow[ur, "\Phi^{\ell}_{g,m}"'] & \end{tikzcd}$$

where s_C is the section of the canonical projection $p\colon \pi_1(\mathcal{M}_{g,m}) \to G_{\mathbf{Q}}$ induced by the rational point representing C.

From these outer actions we define ℓ-monodromy fixed fields $\mathbf{Q}^{\ell}_{g,m} := \overline{\mathbf{Q}}^{p(\operatorname{Ker}\Phi^{\ell}_{g,m})}$ and $\mathbf{Q}^{\ell}_C := \overline{\mathbf{Q}}^{\operatorname{Ker}\varphi^{\ell}_C}$. Note that by the universality of $\Phi^{\ell}_{g,m}$ we have the inclusion $\mathbf{Q}^{\ell}_{g,m} \subset \mathbf{Q}^{\ell}_C$ and also that by specifying to $(g,m) = (0,3)$ we have $\Phi^{\ell}_{g,m} = \varphi^{\ell}_{\mathbf{P}^1_{\mathbf{Q}}\setminus\{0,1,\infty\}}$.

Oda's problem is then concerned by the independence in (g,m) of the ℓ-monodromy fixed fields $\mathbf{Q}^{\ell}_{g,m}$. The complete proof of independence has been obtained through different techniques such as computations with Lie algebras [Ma96], consideration of divisorial stratifications of the moduli spaces [IN97] and combinatorial anabelian geometry [HM11], we refer to [Tak14] for a survey.

[1] Contrary to the profinite case where injectivity follows from Belyi's theorem, the kernel of the pro-ℓ outer action is non-trivial.

Theorem 1 (Hoshi, Ihara, Matsumoto, Mochizuki, Nakamura, Oda, Takao, Ueno). *For all (g, m) of hyperbolic type we have*

$$\mathbf{Q}^{\ell}_{g,m} = \mathbf{Q}^{\ell}_{0,3}.$$

2. A cyclic special loci version of Oda's problem

For G a finite group let $\mathcal{M}_{g,[m]}[G]$ be the moduli space of triples

$$(C/S, D, \iota\colon G \hookrightarrow \operatorname{Aut}_S C)$$

with C a curve of genus g and D a divisor on C of degree m. The G-special loci is defined as the image $\mathcal{M}_{g,[m]}(G)$ of $\mathcal{M}_{g,[m]}[G]$ in $\mathcal{M}_{g,[m]}$ by the map induced by forgetting the G-action. From the work of Collas-Maugeais in [CM15] the irreducible components of the G-special loci for cyclic G are geometrically irreducible and classified by a combinatorial data noted $\underline{kr}$, we denote them by $\mathcal{M}_{g,[m]}(G)_{\underline{kr}}$.

Similarly to the classical situation there is a universal ℓ-monodromy outer action $\Phi^{\ell}_{g,m}(G)_{\underline{kr}}$ and thus ℓ-monodromy fixed fields $\mathbf{Q}^{\ell}_{g,m}(G)_{\underline{kr}}$. Oda's problem for the cyclic special loci is then the question of the independence of these fields, at fixed cyclic G, in the data (g, m) and $\underline{kr}$. For simple cyclic groups this question can be resolved.

Theorem 2 (Theorem 5.3 of [CP23]). *For $G = \mathbf{Z}/\ell\mathbf{Z}$, (g, m) of hyperbolic type and associated abstract Hurwitz data $\underline{kr}$ such that $\mathcal{M}_{g,[m]}(G)_{\underline{kr}}$ is non-empty, we have*

$$\mathbf{Q}^{\ell}_{g,m}(G)_{\underline{kr}} = \mathbf{Q}^{\ell}_{0,3}.$$

3. The maximal degeneration method with Matsumoto-Seyama curves

The proof is made by an adaptation of the method of maximal degeneration by Ihara and Nakamura in [IN97]. We produce a curve X_η represented on the moduli stack $\mathcal{M}_{g,[m]}(G)_{\underline{kr}}$ such that $\varphi^{\ell}_{X_\eta} = \mathbf{Q}^{\ell}_{0,3}$ as the generic curve of a degenerating family X with special fiber X_s on the boundary of the compactification of $\mathcal{M}_{g,[m]}(G)_{\underline{kr}}$. The construction of X is made explicit by first constructing the singular curve X_s as a G-stable diagram, i.e. a specific gluing of curves represented by the following figure.

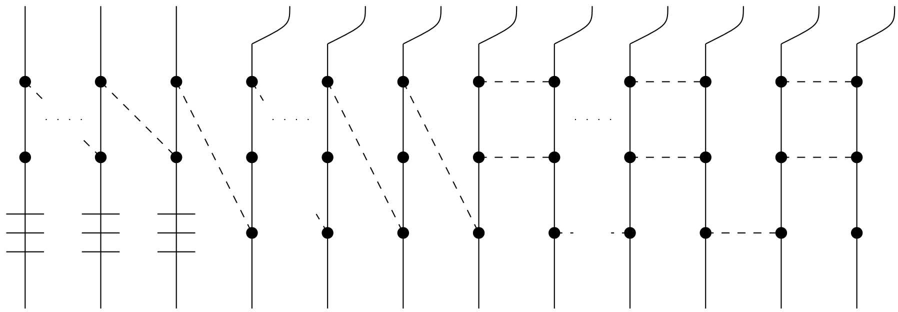

FIG 1. $\mathbf{Z}/\ell\mathbf{Z}$-stable diagram

The curves depictured are one of the C_r curves given by

- The smooth G-curve birational to $y^r(y-1) = x^\ell$, with 3 ramified points represented by black dots for $1 \leq r \leq \ell - 2$.
- The projective line $\mathbf{P}^1$ with its G-action having 2 ramified points as black dots 0 and ∞ and ℓ unramified points given by μ_ℓ and represented by dashes for $r = 0$.

The curves C_r are called Matsumoto-Seyama curves and have the specific property that $\mathbf{Q}^\ell_{C_r} = \mathbf{Q}^\ell_{0,3}$.

A one-dimensional deformation family X is then explicitly given through formal geometry and affine patches. In order to relate the Galois action of the generic curve X_η to the one of the irreducible components of the special fiber (i.e. Matsumoto-Seyama curves by construction) we use Grothendieck-Murre theory. At each double point μ of X_s we construct a fiber functor $\vec{\mu}$ for the category $\mathrm{Rev}^D(X)$ of étale covers of X tamely ramified at the divisor D made of X_s and the marked points. The construction of such fiber functors comes with a choice of Galois action on the étale fundamental group. In our situation the following facts follow from Grothendieck-Murre theory:

(*i*) There are Galois equivariant isomorphisms

$$\pi_1^{\mathcal{D}}(\mathfrak{X}) \simeq \pi_1^D(X) \simeq \pi_1(X_{\overline{\eta}} \setminus \{P_1, \ldots, P_m\})$$

where $\mathfrak{X}$ is the formal scheme underlying X with its corresponding divisor $\mathcal{D}$ and $P_1, \ldots, P_m$ are the marked points of the geometric generic fiber $X_{\overline{\eta}}$. Remark that the Galois action on $\pi_1(X_{\overline{\eta}} \setminus \{P_1, \ldots, P_m\})$ given by the fiber functors $\vec{\mu}$ is a choice of a lift of the usual outer Galois action.

(*ii*) The groupoid $\Pi_1^{\mathcal{D}}((X), \vec{\mu}, \vec{\mu'})$ is generated by the images of all the maps coming from the irreducible components.

By pullbacks to the irreducible components of X_s the formal double-points μ give rise to tangential basepoints that fit in a commutative square

$$\begin{tikzcd}
\mathrm{Spf}\,\mathbf{Q}[[T_1,T_2]]/(T_1T_2) \arrow[d] & \mathrm{Spec}\,\mathbf{Q}((X)) \arrow[l] \arrow[d, "t_\mu"] \\
\mathfrak{X} & C_r \arrow[l]
\end{tikzcd}$$

The construction of the family X is made explicit specifically in order to control the Galois action obtained on $\pi_1(C_{r\overline{\mathbf{Q}}})$ from the tangential basepoints t_μ. This is done so in a way such that t_μ is a lift of one of Deligne's tangential basepoint on $\mathbf{P}^1 \setminus \{0,1,\infty\}$. This assures that the fixed field of the resulting Galois action is again $\mathbf{Q}^\ell_{0,3}$ and thus by the fact (ii) we are done.

In relation to the Anderson-Ihara question of identifying the field $\mathbf{Q}^\ell_C$, we refer to Ishii's report in this volume for $\ell \geq 5$ and C an elliptic curve with complex multiplication.

Acknowledgement. This work is supported by JSPS KAKENHI Grant number 22F22015.

References

[CM15] B. Collas and S. Maugeais, “Composantes irréductibles de lieux spéciaux d'espaces de modules de courbes, action galoisienne en genre quelconque,” *Ann. Inst. Fourier*, vol. 65, no. 1, pp. 245–276, 2015.

[CP23] B. Collas and S. Philip, *On Oda's problem and special loci*, arXiv:2311.15515 [math.AG], 36 pages (2023).

[HM11] Y. Hoshi and S. Mochizuki, ”On the combinatorial anabelian geometry of nodally non-degenerate outer representations,” *Hiroshima Math. J.* 41 (2011), pp. 275–342.

[IN97] Y. Ihara and H. Nakamura, “On deformation of maximally degenerate stable marked curves and Oda's problem,” *J. Reine Angew. Math.*, vol. 487, pp. 125–151, 1997.

[Ma96] M. Matsumoto, ”Galois representations on pronite braid groups on curves,” *J. reine angew. Math.* 474 (1996), pp. 169-219.

[Oda97] T. Oda, “Etale homotopy type of the moduli spaces of algebraic curves,” *Geometric Galois actions*, London Math. Soc. Lecture Note Ser., 242, Cambridge University Press, Cambridge, pp. 85–95, 1997.

[Tak14] N. Takao, “Some remarks on field towers arising from pro-nilpotent universal monodromy representations,” *RIMS Kôkyûroku Bessatsu*, vol. B51, pp. 55–70, 2014.

Towards Grothendieck's anabelian dream for curves over algebraically closed fields of characteristic p

Yu Yang

1. Anabelian geometry: towards positive characteristic

1.1. Grothendieck's anabelian philosophy. In 1980s, in his famous letter to Faltings, Grothendieck suggested the theory of "anabelian geometry". This theory aims to reconstruct algebraic varieties from their algebraic fundamental groups. In particular, for the case of 1-dimensional schemes, *Grothendieck's anabelian philosophy* is as follows:

> *The set of dominate morphisms of hyperbolic curves can be completely determined by the set of open continuous homomorphisms of their algebraic fundamental groups (e.g. étale, tame, etc.).*

Since Grothendieck introduced the theory of anabelian geometry, this philosophy offers a framework for theoretical progression and serves as a guiding principle for the development of this field (in particular, for studying anabelian geometry of curves over arithmetic field of characteristic 0).

The various formulations based on the above anabelian philosophy are called Grothendieck's anabelian conjectures. It's worth highlighting that the most significant instances of Grothendieck's anabelian conjectures over arithmetic fields, such as number fields, p-adic fields, and finite fields, have been proved by H. Nakamura, S. Mochizuki and A. Tamagawa[1]. Note that the Galois actions play the crucial role in their proofs of Grothendieck's anabelian conjectures for curves over arithmetic fields.

1.2. Fundamental groups in positive characteristic. In 1996, Tamagawa made a surprising discovery, suggesting the possible existence of anabelian phenomena for curves over *algebraically closed fields of characteristic* $p > 0$ (note that no anabelian phenomena exist for curves over algebraically closed fields of characteristic 0). Subsequently, from 1996 to 2001, these anabelian phenomena were deeply investigated by F. Pop, M. Saïdi, M. Raynaud, and A. Tamagawa. All of their researches focus on the so-called "*the weak Isom-version conjecture*" which was formulated by Tamagawa [Tam02] based on the anabelian philosophy mentioned in § 1.1. Roughly speaking, this conjecture says that the isomorphism classes of hyperbolic curves over algebraically closed fields of characteristic p can be reconstructed group-theoretically from their geometric fundamental groups (i.e. *without using Galois actions*).

While the weak Isom-version conjecture remains a wild open problem at present, Tamagawa has nonetheless achieved an important result known as the "*finiteness theorem*" [Tam04]:

> Over $\overline{\mathbb{F}}_p$, only finitely many isomorphism classes of hyperbolic curves have the same tame fundamental groups.

This result is one of the highest achievements in the theory of anabelian geometry.

[1] We refer to "H. Nakamura, A. Tamagawa, S. Mochizuki, *The Grothendieck conjecture on the fundamental groups of algebraic curves*, Sugaku Expo. **14**, No. 1 (2001), 31–53; translation from Sūgaku 50, No. 2, 113-129 (1998)" for a panorama of techniques, principles and results.

2. Moduli spaces of fundamental groups

Let $X_i^\bullet \stackrel{\text{def}}{=} (X_i, D_{X_i})$, $i \in \{1,2\}$, be a pointed stable curve of type (g,n) over an algebraically closed field k_i of characteristic $p > 0$. Here, X_i denotes the underlying semi-stable curve of $X_i^\bullet$ of genus g, and D_{X_i} denotes the set of marked points of cardinality n.

2.1. **Mysterious phenomena and the fundamental question.** By choosing suitable base point $x_i \in X_i \setminus D_{X_i}$, we have the so-called *admissible fundamental group* (or *geometric log étale fundamental group*) $\pi_1^{\mathrm{adm}}(X_i^\bullet, x_i)$ of $X_i^\bullet$ (see [Ya18] for more details about admissible fundamental groups). The admissible fundamental groups are natural generalizations of the tame fundamental groups of *smooth* pointed stable curves to the case of arbitrary (possibly *singular*) pointed stable curves. In particular, $\pi_1^{\mathrm{adm}}(X_i^\bullet, x_i) = \pi_1^{\mathrm{tame}}(X_i^\bullet, x_i)$ if $X_i^\bullet$ is smooth over k_i.

Moreover, the structure of the maximal pro-prime-to-p quotient of $\pi_1^{\mathrm{adm}}(X_i^\bullet, x_i)$ is well-known if $p > 0$ (resp. the structure of $\pi_1^{\mathrm{adm}}(X_i^\bullet, x_i)$ is well-known if $p = 0$), and it is isomorphic to the pro-prime-to-p completion (resp. the profinite completion) of the topological fundamental group of a Riemann surface of type (g,n). Since we only focus on the isomorphism class of $\pi_1^{\mathrm{adm}}(X_i^\bullet, x_i)$, for simplicity, we omit the base point x_i and use the notation $\Pi_{X_i^\bullet}$ to denote $\pi_1^{\mathrm{adm}}(X_i^\bullet, x_i)$.

In 1990s, Tamagawa noted that the following phenomenon exists in positive characteristic:

$$\mathrm{Hom}^{\mathrm{dom}}(X_1^\bullet, X_2^\bullet) = \emptyset \text{ but } \mathrm{Hom}^{\mathrm{op}}(\Pi_{X_1^\bullet}, \Pi_{X_2^\bullet}) \neq \emptyset.$$

Here, $\mathrm{Hom}^{\mathrm{dom}}(X_1^\bullet, X_2^\bullet)$ denotes the set of dominate morphisms of curves, and $\mathrm{Hom}^{\mathrm{op}}(\Pi_{X_1^\bullet}, \Pi_{X_2^\bullet})$ denotes the set of open continuous homomorphisms of profinite groups. The above phenomenon means that *anabelian philosophy suggested originally by Grothendieck mentioned in § 1.1 does not hold for curves over algebraically closed fields of characteristic p.*

Now, the author considered the following the fundamental question:

Does there exist *anabelian explanation* for $\mathrm{Hom}^{\mathrm{op}}(\Pi_{X_1^\bullet}, \Pi_{X_2^\bullet})$?

The theory of "*moduli spaces of fundamental groups*" and its main conjecture "*the homeomorphism conjecture*" established by the author provide a reasonable answer to this fundamental question.

2.2. **Anabelian philosophy via moduli spaces of fundamental groups.** In [HYZ23], the author discovered a new kind of anabelian phenomenon that shows that *the sets of open continuous homomorphisms of admissible fundamental groups contains deformation information of curves.* This new anabelian phenomenon can be precisely captured by using the so-called "moduli spaces of fundamental groups" and "the homeomorphism conjecture".

Roughly speaking, in [Ya20a], the author introduced

$$\overline{\Pi}_{g,n}, \textit{the moduli space of admissible fundamental groups of type } (g,n),$$

a topological space whose underlying set is the set of the isomorphism classes of admissible fundamental groups of curves of type (g,n) over algebraically closed fields of characteristic p, and whose topology can be completely determined by the set of finite quotients of admissible fundamental groups.

Let $\overline{M}_{g,n}$ be the coarse moduli spaces of the moduli stack over $\overline{\mathbb{F}}_p$ classifying pointed stable curves of type (g,n). By introducing the so-called "Frobenius equivalence $\sim_{fe}$" on $\overline{M}_{g,n}$ [Ya21], the author proved the existence of a continuous map

$$\pi^{\mathrm{adm}}_{g,n} : \overline{\mathfrak{M}}_{g,n} \overset{\mathrm{def}}{=} \overline{M}_{g,n}/\sim_{fe} \twoheadrightarrow \overline{\Pi}_{g,n},\ [q] \mapsto [\Pi_q],$$

where $[q]$ denotes the equivalence class of $q \in \overline{M}_{g,n}$, Π_q denotes the admissible fundamental group of a curve corresponding to a geometric point over q, and $[\Pi_q]$ denotes the isomorphic class of Π_q. The main conjecture of the theory of moduli spaces of fundamental groups is the following:

Homeomorphism conjecture: *The continuous map $\pi^{\mathrm{adm}}_{g,n} : \overline{\mathfrak{M}}_{g,n} \twoheadrightarrow \overline{\Pi}_{g,n}$ is a homeomorphism.*

Note that the weak Isom-version conjecture only says that $\pi^{\mathrm{adm}}_{g,n}$ is a bijection as *sets*. This conjecture generalizes all the known conjectures concerning tame anabelian geometry of curves over algebraically closed fields of characteristic p. Furthermore, it supplies a viewpoint to consider anabelian geometry of curves over algebraically closed fields of characteristic p based on the following *new anabelian philosophy*:

> *The* anabelian properties *concerning pointed stable curves over algebraically closed fields of characteristic p are equivalent to the* topological properties *of moduli spaces of admissible fundamental groups.*

The above philosophy tells us *what are the anabelian phenomena that we can reasonably expect* for pointed stable curves over algebraically closed fields of characteristic p. This means that the homeomorphism conjecture is a *dictionary* between the geometry of pointed stable curves (or moduli spaces of curves) and the anabelian properties of pointed stable curves. It has raised a host of new questions and new conjectures concerning anabelian phenomena in positive characteristic which cannot be seen if we only consider the weak Isom-version conjecture.

The author believes that the theory of moduli spaces of fundamental groups and the homeomorphism conjecture offer an approach towards Grothendieck's anabelian dream for curves over algebraically closed fields of characteristic $p > 0$.

2.3. **Fundamental groups in positive characteristic as local moduli.** By using the new anabelian philosophy mentioned above, the author obtained the following insight:

> *The admissible fundamental groups of pointed stable curves over algebraically closed fields of characteristic p can be regarded as an analogue of local moduli spaces of the curves.*

Roughly speaking, this means that for $q' \in \overline{M}_{g,n}$ an arbitrary point and $X^{\bullet}_{q'}$ the curve corresponding to a geometric point over q':

(1) We can group-theoretically detect, "up to Frobenius", whether or not $X^{\bullet}_{q'}$ is a deformation of $X^{\bullet}_{q}$ from $\mathrm{Hom}^{\mathrm{op}}(\Pi_{q'}, \Pi_q)$ – i.e. "up to Frobenius", q is a specialization (in the sense of moduli space) of q' if and only if $\mathrm{Hom}^{\mathrm{op}}(\Pi_{q'}, \Pi_q) \neq \emptyset$.
(2) The deformations of $X^{\bullet}_{q}$ can be reconstructed group-theoretically from $\mathrm{Hom}^{\mathrm{op}}(-, \Pi_q)$ – with certain addition conditions.

3. A series of evidences for the anabelian insight

The following results obtained by the author provide strong evidence for the above insight:

(1) The homeomorphism conjecture holds for 1-dimensional moduli spaces, see [Ya20a, Ya21a].
(2) (With Y. Hoshi) A new proof of Mochizuki's famous result on (Isom-version) Grothendieck's anabelian conjecture for curves over sub-p-adic fields [Moc99], see [HY22]. Note that our proof does not rely on Faltings' p-adic Hodge theory.

Furthermore, in [Ya21b], the author posed an ultimate generalization of the so-called "combinatorial Grothendieck conjecture in positive characteristic" [Tam03, Ya18] which we call "*the group-theoretical specialization conjecture*". Roughly speaking, this conjecture means that *open continuous homomorphisms of admissible fundamental groups can completely determine the topological and group-theoretical degeneration of curves.* We have the following result:

(3) In [Ya23], the author proved that the group-theoretical specialization conjecture holds. As an application, one obtains that the combinatorial stratification (i.e. the stratification by using dual semi-graphs) of moduli spaces of curves can be completely reconstructed group-theoretically (as topological spaces!) from admissible fundamental groups.

References

[Moc99] S. Mochizuki, *The local pro-p anabelian geometry of curves*, Invent. Math. **138** (1999), 319–423".

[Tam02] A. Tamagawa, *Fundamental groups and geometry of curves in positive characteristic.* Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 297–333, Proc. Sympos. Pure Math., **70**, Amer. Math. Soc., Providence, RI, 2002.

[Tam03] A. Tamagawa, *On the tame fundamental groups of curves over algebraically closed fields of characteristic* > 0. Galois groups and fundamental groups, 47–105, Math. Sci. Res. Inst. Publ., **41**, Cambridge Univ. Press, Cambridge, 2003.

[Tam04] A. Tamagawa, *Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups*, J. Algebr. Geom. **13**, No. 4 (2004), 675–724.

[Ya18] Y. Yang, *On the admissible fundamental groups of curves over algebraically closed fields of characteristic* $p > 0$, Publ. Res. Inst. Math. Sci. **54** (2018), 649–678.

[Ya21] Y. Yang, *On the existence of specialization isomorphisms of admissible fundamental groups in positive characteristic*, Math. Res. Lett. **28** (2021), 1941–1959.

[HYZ23] Z. Hu, Y. Yang, R. Zong, *Topological structures of moduli spaces of curves and anabelian geometry in positive characteristic*, arXiv:2301.04864 [math.AG] (2023), or see `http://www.kurims.kyoto-u.ac.jp/~yuyang/` for the latest version.

[Ya20a] Y. Yang, *Moduli spaces of fundamental groups of curves in positive characteristic I*, arXiv:2010.01806 [math.AG] (2020), or see http://www.kurims.kyoto-u.ac.jp/~yuyang/ for the latest version.
[Ya21a] Y. Yang, *Moduli spaces of fundamental groups of curves in positive characteristic II*, in preparation.
[Ya21b] Y. Yang, *Topological and group-theoretical specializations of fundamental groups of curves in positive characteristic.* See http://www.kurims.kyoto-u.ac.jp/~yuyang/
[HY22] Y. Hoshi, Y. Yang, *On the arithmetic fundamental groups of curves over local fields.* See http://www.kurims.kyoto-u.ac.jp/~yuyang/
[Ya23] Y. Yang, *On the group-theoretical specialization conjecture*, in preparation.

The étale homotopy obstruction and its applications

David Corwin

1. Introduction

1.1. **The Hasse Principle.** Let K be a number field, $\mathbb{A}_K$ the adèle ring of K, and X a variety over K. Clearly, if $X(\mathbb{A}_K) = \emptyset$, then $X(K) = \emptyset$. The Hasse-Minkowski Theorem states that the converse holds if X is a quadric hypersurface. Lind, Reichardt, Selmer, and many others subsequently found examples of X for which the converse is false; such an example is known as a *counterexample to the Hasse principle* or *local-global Principle.*

1.2. **Obstructions to the Hasse Principle.** Yuri Manin initiated the notion of an *obstruction to the Hasse principle*: a subset of $X(\mathbb{A}_K)$, functorial in X, that always contains $X(K)$. Manin's obstruction [Man71] is known as the Brauer-Manin obstruction and denoted $X(\mathbb{A}_K)^{\mathrm{Br}}$. Others include the finite abelian descent obstruction $X(\mathbb{A}_K)^{\mathrm{f-ab}}$, the finite descent obstruction $X(\mathbb{A}_K)^{\mathrm{fin}}$, the descent obstruction $X(\mathbb{A}_K)^{\mathrm{descent}}$, and the étale-Brauer obstruction $X(\mathbb{A}_K)^{\mathrm{\acute{e}t,Br}}$ of Skorobogatov [Sk99].

Harpaz and Schlank defined the *étale homotopy* $X(\mathbb{A}_K)^h$ and *étale homology* $X(\mathbb{A}_K)^{\mathbb{Z}h}$ obstructions using a more general and less ad hoc procedure than the previous obstructions. However, they found (at least for number fields) that $X(\mathbb{A}_K)^{\mathbb{Z}h} = X(\mathbb{A}_K)^{\mathrm{Br}}$, and $X(\mathbb{A}_K)^h = X(\mathbb{A}_K)^{\mathrm{\acute{e}t,Br}}$, which follow from cohomological duality for number fields. Nonetheless, these obstructions have provided insight into these already-known obstructions and suggested new avenues of attack for related problems, such as existence of rational 0-cycles and rational points over higher-dimensional function fields K.

2. Etale Homotopy Obstructions

A series of obstructions is defined in [HS13]:

$$X(\mathbb{A}_K)^h \subseteq \cdots \subseteq X(\mathbb{A}_K)^{h,2} \subseteq X(\mathbb{A}_K)^{h,1} \subseteq X(\mathbb{A}_K)$$

and

$$X(\mathbb{A}_K)^{\mathbb{Z}h} \subseteq \cdots \subseteq X(\mathbb{A}_K)^{\mathbb{Z}h,2} \subseteq X(\mathbb{A}_K)^{\mathbb{Z}h,1} \subseteq X(\mathbb{A}_K)$$

such that $X(\mathbb{A}_K)^{h,n} \subseteq X(\mathbb{A}_K)^{\mathbb{Z}h,n}$ for all n, $X(\mathbb{A}_K)^{\mathbb{Z}h} = \bigcap_n X(\mathbb{A}_K)^{\mathbb{Z}h,n}$, and $X(\mathbb{A}_K)^h = \bigcap_n X(\mathbb{A}_K)^{h,n}$.

2.1. **Homotopy Fixed Points.** They are defined by first defining a sequence of sets and maps

$$\begin{tikzcd} X(K) \arrow[r] & X(hK) \arrow[r] \arrow[d] & \cdots \arrow[r] & X(h_3K) \arrow[r] \arrow[d] & X(h_2K) \arrow[r] \arrow[d] & X(h_1K) \arrow[r] \arrow[d] & X(h_0K) \arrow[d] \\ & X(\mathbb{Z}hK) \arrow[r] & \cdots \arrow[r] & X(\mathbb{Z}h_3K) \arrow[r] & X(\mathbb{Z}h_2K) \arrow[r] & X(\mathbb{Z}h_1K) \arrow[r] & X(\mathbb{Z}h_0K), \end{tikzcd}$$

for any variety X over a field K of characteristic 0, all of which are functorial in both X and K. Here, $X(h_0K)$ is $\pi_0(\overline{X})^{G_K}$, the set of G_K-fixed geometric connected components, while for X geometrically connected, $X(h_1K)$ is the set of fundamental group sections familiar from anabelian geometry. To go further, there are exact sequences

$$H^n(G_K; \pi_n^{\mathrm{et}}(\overline{X})) \to X(h_nK) \to X(h_{n-1}K) \tag{1}$$

$$H^n(G_K; H_n^{\mathrm{et}}(\overline{X})) \to X(\mathbb{Z}h_nK) \to X(\mathbb{Z}h_{n-1}K), \tag{2}$$

the former of pointed sets and the latter of abelian groups. In particular, $X(hK) = X(h_nK)$ and $X(\mathbb{Z}hK) = X(\mathbb{Z}h_nK)$ for n at least the cohomological dimension of K.

More precisely, $X(hK)$ is defined by applying a homotopy fixed-point construction ^{hG_K} to the étale homotopy type $\hat{\mathrm{Et}}\, X_{\overline{K}}$ and taking π_0. There is a (non-abelian) *descent spectral sequence*

$$E_2^{s,t}(X, b) = H^s(K; \pi_t^{\mathrm{et}}(\overline{X}, b)) \implies \pi_{t-s}((\hat{\mathrm{Et}}\, X_{\overline{K}})^{hG_K}, b)$$

relative to a homotopy basepoint b (c.f. [CS20] §8.1), along with a related (abelian) spectral sequence $H^s(K; H_t^{\mathrm{et}}(\overline{X})) \implies \pi_{t-s}((\mathbb{Z}\,\hat{\mathrm{Et}}\, X_{\overline{K}})^{hG_K})$, where $X(\mathbb{Z}hK) = \pi_0(\mathbb{Z}\,\hat{\mathrm{Et}}\, X^{hG_K})$. The latter in fact has a more classical description in terms of hypercohomology: we have $X(\mathbb{Z}hK) = \mathbb{H}^0(G_K; \widetilde{H}_\bullet^{\mathrm{et}}(\overline{X}))$, where $\widetilde{H}_\bullet^{\mathrm{et}}(\overline{X})$ is viewed as an object of the derived category of continuous profinite G_K-modules. We refer to [CS20] § 8 for technical details, which uses the theory of [Qui08, Qui11].

2.2. **Obstructions.** For α of the form h, h_n, $\mathbb{Z}h$, $\mathbb{Z}h_n$, we set $X(\mathbb{A}_K)^\alpha$ to be the subset of $X(\mathbb{A}_K)$ whose image in the lower right object is in the image of loc in the diagram

$$\begin{tikzcd} X(K) \arrow[r] \arrow[d] & X(\mathbb{A}_K) \arrow[d] \\ X(\alpha K) \arrow[r, "\mathrm{loc}"] & \prod_v X(\alpha K_v). \end{tikzcd}$$

Note that $X(\mathbb{A}_K)^\alpha$ is functorial in X for morphisms of K-schemes.

2.3. **Comparison with Classical Obstructions.** The main theorem of [HS13] is:

Theorem 1 ([HS13] Theorem 9.136)**.** *For a smooth geometrically connected variety X over a number field K,*

$$\begin{aligned} X(\mathbb{A}_K)^h = X(\mathbb{A}_K)^{\text{ét,Br}} &= X(\mathbb{A}_K)^{\text{descent}} \\ X(\mathbb{A}_K)^{\mathbb{Z}h} = X(\mathbb{A}_K)^{\text{Br}} &= X(\mathbb{A}_K)^{\text{c}-\text{descent}} \\ X(\mathbb{A}_K)^{h,1} &= X(\mathbb{A}_K)^{\text{f}-\text{cov}} \\ X(\mathbb{A}_K)^{\mathbb{Z}h,1} &= X(\mathbb{A}_K)^{\text{f}-\text{ab}}. \end{aligned}$$

3. Consequences for Classical Obstructions

While the previous theorem is disappointing in the sense that it implies the étale homotopy obstruction gives nothing new, the reinterpretation in terms of étale homotopy sometimes elucidates the properties of and connections between the obstructions.

Thus the following results can be proven otherwise but are simpler to prove using the étale homotopy obstruction formalism.

3.1. **Basic Comparisons.** The fact that $X(\mathbb{A}_K)^{\mathbb{Z}h,2} \subseteq X(\mathbb{A}_K)^{\mathbb{Z}h,1}$ gives us:

Theorem 2. *For a variety X over K, $X(\mathbb{A}_K)^{\text{Br}} \subseteq X(\mathbb{A}_K)^{\text{f}-\text{ab}}$.*

The exact sequence (2) tells us:

Theorem 3 ([HS13] Theorem 9.152)**.** *If $H_2^{\text{et}}(X_{\overline{K}}) = 0$, then*

$$X(\mathbb{A}_K)^{\text{Br}} = X(\mathbb{A}_K)^{\mathbb{Z}h,2} = X(\mathbb{A}_K)^{\mathbb{Z}h,1} = X(\mathbb{A}_K)^{\text{f}-\text{ab}}$$

The exact sequence (1) similarly tells us:

Theorem 4 ([HS13] Theorem 9.148)**.** *If $\pi_2^{\text{et}}(X_{\overline{K}}) = 0$ (e.g., X a nonrational curve), then*

$$X(\mathbb{A}_K)^{\text{ét,Br}} = X(\mathbb{A}_K)^{h,2} = X(\mathbb{A}_K)^{h,1} = X(\mathbb{A}_K)^{\text{fin}}.$$

3.2. **Products.** The homotopy fixed point construction ^{hG_K} is a kind of higher-categorical limit and therefore commutes with products. Since π_0 also commutes with products, we have, for varieties X and Y over K, that $(X \times Y)(hK) = X(hK) \times Y(hK)$. This then implies:

Theorem 5 ([HS13] Theorem 9.147)**.** *For varieties X and Y over K, we have*

$$(X \times Y)(\mathbb{A}_K)^{\text{ét,Br}} = X(\mathbb{A}_K)^{\text{ét,Br}} \times Y(\mathbb{A}_K)^{\text{ét,Br}}$$

It is not obvious how to prove this otherwise, since the Brauer group of a product is not the product of the Brauer groups.

3.3. **Fibrations.** The theorems above are fairly simple consequences of the homotopy formalism. We now mention a result about the étale-Brauer obstruction that fundamentally uses étale homotopy but is less immediate. We denote by $X(\mathbb{A}_K^f)^{\text{ét,Br}}$ the projection of $X(\mathbb{A}_K)^{\text{ét,Br}}$ along $X(\mathbb{A}_K) \to X(\mathbb{A}_K^f)$.

Theorem 6 ([CS20] Theorem 1.2)**.** *Let $f\colon X \to S$ be a geometric fibration (), and suppose that $S(K) = S(\mathbb{A}_K^f)^{\text{ét,Br}}$ and that for all $a \in S(K)$, we have $X_a(K) = X_a(\mathbb{A}_K^f)^{\text{ét,Br}}$.*

Suppose furthermore that conditions (2)-(5) of [CS20] *Theorem 9.7 holds - for example, if S is an elliptic curve with finite Tate-Shafarevich group or a hyperbolic curve satisfying the Section Conjecture, and K is totally imaginary or $S(\mathbb{R})$ is simply-connected. Then*

$$X(K) = X(\mathbb{A}_K^f)^{\text{ét,Br}}.$$

4. Stable Homotopy Obstructions to Zero-Cycles

4.1. **More on the Etale Homology Obstruction.** Given a topological space Y, there is an associated $H\mathbb{Z}$-module spectrum (equivalently, a complex of abelian groups up to quasi-isomorphism:

$$\mathbb{Z}Y := \Sigma^\infty Y \wedge H\mathbb{Z}$$

such that $\pi_i(\mathbb{Z}Y) = H_i(Y;\mathbb{Z})$.

In fact $X(\mathbb{Z}hK)$ is most naturally defined by applying this construction to the étale homotopy type of $\overline{X}$ and then applying the same construction that defines $X(hK)$; i.e.,

$$X(\mathbb{Z}hK) = \mathbb{H}^0(G_K; \widetilde{H}_*^{\text{et}}(X_{\overline{K}})) = \pi_0((\mathbb{Z}\,\hat{\text{Et}}(X_{\overline{K}}))^{hG_K})$$

The category of $H\mathbb{Z}$-module spectra is additive, which makes $X(\mathbb{Z}hK)$ into an abelian group (a fact that can also be seen by the description $X(\mathbb{Z}hK) = \mathbb{H}^0(G_K; H_\bullet^{\text{et}}(\overline{X})))$. This means that $X(\mathbb{Z}hK)$ receives a map not just from $X(K)$ but from linear combinations $\mathbb{Z}X(K)$. More importantly, by a Galois descent argument, it receives a map from the group $\text{CH}_0(X)$ of zero-cycles and thus can be used to define an obstruction to the existence of zero-cycles of degree 1 (or any degree d). This obstruction the produces a set $\text{CH}_0(X_{\mathbb{A}_K})^{\text{Br}}_{\deg=1}$ of adelic zero-cycles orthogonal to $\operatorname{Br} X$.

In fact, it was realized before the advent of the étale homotopy obstructions that the Brauer-Manin obstruction obstructs 0-cycles. By a similar argument as for rational points, the étale homology obstruction to zero-cycles is the same as the Brauer-Manin obstruction. The stronger étale-Brauer obstruction, on the other hand, is not additive and thus applies only to rational points.

4.2. **From Homology to Stable Homotopy.** If we look back at the formula $\mathbb{Z}Y = \Sigma^\infty Y \wedge H\mathbb{Z}$, something is staring at us: $\Sigma^\infty Y$ is a spectrum, which is already additive! In other words, we don't have to smash with $H\mathbb{Z}$ to get an additive object. In other words, we can define an intermediate

$$X(hK) \to X(\Sigma hK) := \pi_0((\Sigma^\infty\,\hat{\text{Et}}(X_{\overline{K}}))^{hG_K}) \to X(\mathbb{Z}hK)$$

One might ask what more this gives us beyond the Brauer-Manin obstruction. In fact, one may show that the additional obstruction is 2-torsion, and for a surprising reason: because $\pi_4(S^3) = \pi_1^{\mathrm{st}}(\mathbb{S}) \cong \mathbb{Z}/2\mathbb{Z}$!

5. Non-Local-Global Etale Homotopy Obstructions

The local-global obstruction is mediated by $X(hK)$, which serves as a kind of container for rational points and is filtered by $H^i(G_K; \pi_i^{\mathrm{et}}(X_{\overline{K}}))$.

On the other hand, if we think of the question of finding a rational point on a smooth variety X/K as finding a section of the fibration and apply ideas from classical obstruction theory to the étale homology type, one finds there are obstruction classes in $H^{i+1}(G_K; \pi_i^{\mathrm{et}}(X_{\overline{K}}))$. For example:

$$\begin{tikzcd} X \arrow[d] \\ \operatorname{Spec} K \end{tikzcd}$$

The class in $H^2(G_K; \pi_1^{\mathrm{et}}(X_{\overline{K}}))$ is the class of the extension

$$0 \to \pi_1^{\mathrm{et}}(X_{\overline{K}}) \to \pi_1^{\mathrm{et}}(X) \to G_K \to 0.$$

We mention two applications of these ideas:

5.1. Obstructions for Arithmetic Spheres.

The paper [ACS19] considers étale homotopy obstruction classes for varieties of the form $a_0x_0^2 + a_1x_1^2 + \cdots + a_mx_m^2 = 1$, known as *arithmetic spheres*. One may think of such a variety as a sphere bundle over $\operatorname{Spec} K$, and sphere bundles have associated Stiefel-Whitney classes. It turns out that there is an étale version of these Steifel-Whitney classes, and the main result of loc.cit. is that they are related to classical Hasse-Witt classes.

5.2. Applications to Galois embedding problems.

Carlson and Schlank apply étale homotopy obstruction classes to inverse Galois problems. For example, they prove the following:

Theorem 7 ([CS17] Corollary 3.2)**.** *Let p_1, p_2, p_3 be three primes such that $p_1p_2p_3 \cong 3 \pmod 4$ and $\left(\frac{p_i}{p_j}\right) = -1$. Then $\operatorname{Aut}(\mathrm{PSL}_2(\mathbb{F}_{q^2}))$ cannot be realized as the Galois group of an unramified extension of $\mathbb{Q}(\sqrt{-p_1p_2p_3})$, but $(\mathbb{Z}/2\mathbb{Z})^2$ can.*

6. Obstructions over Higher Dimensional Fields

6.1. Number Fields Revisited.

The proof of the equality $X(\mathbb{A}_K)^{\mathbb{Z}h} = X(\mathbb{A}_K)^{\mathrm{Br}}$ for K a number field uses cohomological (Poitou-Tate) duality. The proof that $X(\mathbb{A}_K)^h = X(\mathbb{A}_K)^{\text{ét},\mathrm{Br}}$ then uses this fact along with the fact that number fields have cohomological dimension 2[1] The cohomological dimension implies that only π_1 and π_2 play a role, and the former may be accessed by finite étale covers while the latter is the second homology of the universal cover and thus may be accessed via H^2 of finite étale covers.

[1] Modulo issues at real places, which go away when considering local-to-global problems.

6.2. **Higher Dimensional Global Fields.** There are many fields K for which there is a notion of completions K_v and adele ring $\mathbb{A}_K$ but for which K has cohomological dimension > 2. A natural example comes from considering a curve C over a field k and taking $K = k(C)$; then K has cohomological dimension one higher than that of k. In particular, if we take $k/\mathbb{Q}_p$ finite, then there is a Poitou-Tate duality where we take the places of K to be the closed points of C. This can even be used to show that $X(\mathbb{A}_K)^{\mathbb{Z}h}$ is the same as an analogue of the Brauer-Manin obstruction using $H^3(X;\mathbb{Q}/\mathbb{Z}(2))$ in place of $\operatorname{Br} X = H^2(X;\mathbb{Q}/\mathbb{Z}(1))$.

6.3. **Obstruction from π_3.** But what's more is that over such a field, it is conceivable to get a nontrivial obstruction coming from the (geometric étale) π_3 of X. The simplest test-case is a (geometrically) simply-connected variety with trivial H_3. This happens if X is a smooth projective geometrically rational surface or a homogeneous space under a simple simply connected algebraic group with stabilizer a sufficiently large torus. In this case, the triviality of π_1 implies $H_2^{\text{et}}(\overline{X};\mathbb{Z}) = \pi_2^{\text{et}}(\overline{X})$, and along with the triviality of H_3, this means

$$X(\mathbb{A}_K)^{\mathbb{Z}h} = X(\mathbb{A}_K)^{\mathbb{Z}h,2} = X(\mathbb{A}_K)^{h,2}.$$

A natural question is to find examples where $X(\mathbb{A}_K)^h \subsetneq X(\mathbb{A}_K)^{h,2}$. There is already some progress as part of a larger work-in-progress by Carlson-C.-Schlank.

References

[ACS19] E. Arad and S. Carmeli and T. Schlank, *Étale Homotopy Obstructions of Arithmetic Spheres*, arXiv:1902.03404 [math.AG] (2019).

[CS17] M. Carlson and T. Schlank, *The unramified inverse Galois problem and cohomology rings of totally imaginary number fields*, arXiv:1612.01766 [math.NT] (2017).

[CS20] D. Corwin and T. Schlank, *Brauer and etale homotopy obstructions to rational points on open covers*, arXiv:2006.11699 [math.NT] (2020).

[HS13] Y. Harpaz and T. Schlank, *Homotopy obstructions to rational points*, In Torsors, étale homotopy and applications to rational points, of London Math. Soc. Lecture Note Ser. **Volume 405** (2013), pages 280–413.

[Man71] Y. I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, In Actes du Congrès International des Mathématiciens (Nice, 1970) **Tome 1** (1971), pages 401–411.

[Qui08] G. Quick, *Profinite homotopy theory*, Doc. Math. **13** (2008), 585–612.

[Qui11] ———, *Continuous group actions on profinite spaces*, J. Pure Appl. Algebra **215(5)** (2011), 1024–1039.

[Sk99] A. Skorobogatov, *Beyond the Manin obstruction*, Invent. Math. **135(2)** (1999), 399–424.

On the largeness or arboreal Galois representations

Joachim König

(joint work with Danny Neftin, Shai Rosenberg)

Let $f \in K[X]$ be a degree-d polynomial over a number field K, and $f^{\circ n} := f \circ \cdots \circ f$ its n-th iterate. The study of arithmetic properties of $f^{\circ n}$ as $n \to \infty$ has been one of the main objectives of the rapidly growing field of arithmetic dynamics. In particular, the structure of the Galois group $G_{a,\infty} := \varprojlim \operatorname{Gal}(f^{\circ n}(X) - a/K)$, where $a \in K$, is of relevance to a great variety of problems, but still mysterious in general.

It is clear that this group is bounded in size by $G_{t,\infty} := \varprojlim \mathrm{Gal}(f^{\circ n}(X) - t/K(t))$ (where t is a transcendental over K), which in terms is a subgroup of $Aut(T_{d,\infty}) = [S_d]^\infty := \varprojlim_n \underbrace{S_d \wr \cdots \wr S_d}_{n \text{ times}}$, the automorphism group of an infinite rooted d-ary tree. For this reason, the epimorphism $\rho_{f,a} : G_K \to G_{a,\infty}$ is called an arboreal Galois representation. These representations have obtained a great deal of attention recently, see e.g. [BJ07] or [Jon13].

Among the key questions commonly asked about this representation are the following:

1) Under what conditions is $G_{t,\infty}$ "large" (in one of various possible senses) inside $Aut(T_{d,\infty})$?
2) Under what conditions is $G_{a,\infty}$ "large" inside $G_{t,\infty}$?

Particular instances of "largeness" include "finite index" conditions, but also the notions of stability (resp., eventual stability) of iterates. Here (f, a) is called stable (resp., eventually stable), if all $f^{\circ n}(X) - a$ are irreducible (resp., have a bounded number of irreducible factors). In particular, stability translates to transitivity of $G_{a,\infty}$ on each layer of the arboreal representation.

There are by now quite concrete conjectures regarding the above notions (see, e.g., [Jon13]); however, the gap between conjectural and proven results is very large.

1. New existene results for large arboreal representations

In joint work with Danny Neftin and Shai Rosenberg [KNR], we pursue the following notion of "large" arboreal representation: Given an indecomposable polynomial f and a value $a \in K$, one has, for every $n \in \mathbb{N}$, a projection $\pi_n : \mathrm{Gal}(f^{\circ n}(X) - a/K) \to \mathrm{Gal}(f^{\circ n-1}(X) - a/K)$, with kernel $\ker(\pi_n) \leq \Gamma^{\deg(f)^{n-1}}$, where Γ denotes the monodromy group of f.

Definition 1. With the above notions, call the associated arboreal representation $\rho_{f,a}$ "large" if, for every $n \in \mathbb{N}$, the kernel $\ker(\pi_n)$ contains all of $\mathrm{soc}(\Gamma)^{\deg(f)^{n-1}}$, where $\mathrm{soc}(\Gamma)$ denotes the socle of Γ.

This turns out to be a very useful condition for many arithmetic applications. To give an example, if the monodromy group of f is the symmetric group S_d ($d \geq 5$), as is the case for a generic degree-d polynomial, then this notion of largeness translates to saying that $\mathrm{Gal}(f^{\circ n}(X) - a/K)$ contains all the alternating composition factors of the n-fold iterated wreath product of symmetric groups S_d, for all $n \in \mathbb{N}$.

Regarding the above question on largeness of $G_{a,\infty}$, we have the following result, whose proof builds on recent results by the same authors on largeness of $G_{t,\infty}$, see the abstract by D. Neftin in this volume:

Theorem 1 (K.-Neftin-Rosenberg, 2023)**.** *Let F be a number field and $f \in F[X]$ an indecomposable polynomial with nonsolvable almost simple monodromy group $S \leq \Gamma \leq Aut(S)$, where S denotes the (simple) socle of Γ. Assume furthermore that*

i) every critical value of f is also a critical point, and
ii) the inertia groups of the map $x \mapsto f(x)$ invariably generate a group containing S.

Then there exist infinitely many $a \in F$ such that the associated arboreal repesentation $\rho_{f,a}$ is large (in the sense defined above). In particular (f, a) is stable for all these a.

Note that the assumption on f having almost simple monodromy group is not at all a strong extra assumption; in fact the only polynomials failing it are those of degree 4 and those linearly related (over $\mathbb{C}$) to monomials, Chebyshev polynomials. The above theorem subsumes previously considered cases such as the case of "normalized Belyi maps" considered in [BEK21]. Still, Condition i) is somewhat restrictive, since it implies in particular that f is a PCF map. Future work will aim at relaxing this condition as much as possible. Note also that the stability conclusion, i.e., the conclusion of irreducibility of $f^{\circ n}(X) - a$ for all $n \in \mathbb{N}$ simultaneously may be seen as a strengthening (for this concrete scenario) of Hilbert's irreducibility theorem, which would give infinitely many a rendering $f^{\circ n}(X) - a$ irreducible for a *fixed* n. For the related problem of determining the set of exceptional values (in the sense of Hilbert's irreducibility theorem) for a *fixed* n, very general results were previously obtained in [KN01].

2. Applications to questions on mod-p behavior

A large arboreal representation also has concrete implications on the mod-p behavior of $f^{\circ n}(x) - a$, cf. [Jon07]. This is relevant, e.g., for the following problems which have received considerable attention in special cases, without a full answer being in sight.

1) ("mod-p stability"): Given $f \in K[X]$ and $a \in K$, what is the density of the set of stable (resp., almost stable) primes of (f, a), i.e., the primes p of K such that all polynomials $f^{\circ n}(X) - a$, $n \in \mathbb{N}$, are irreducible (resp., have a bounded number of irreducible factors)?
2) ("prime divisors in dynamical sequences"): Given $f \in K[X]$ and $a_0 \in K$, what is the density of the set of primes dividing at least one non-zero term $f^{\circ n}(a_0)$, $n \in \mathbb{N}$?

Both of these problem translate naturally (via Chebotarev's density theorem) to statements about elements of certain cycle types in the associated dynamical Galois groups.

For both problems, it is expected that "usually" the respective sets of primes are of density 0, see e.g., [MOS85] or [Jon08] for results on the first, resp. the second problem in the special case of quadratic polynomials. It should be noted that for both problems, explicit examples yielding positive density sets of primes are also known.

It turns out that the notion of largeness discussed above is useful for deducing density-0 results for problems such as the above. In particular, we have the following two results, see [KNR]:

Theorem 2. *Assume $f \in K[X]$ to be indecomposable and $a \in K$ to be such that the arboreal representation $\rho_{f,a}$ is large.*

(1) Then for any fixed integer N, the density of the set of primes modulo which the number of irreducible factors of $f^{\circ n}(X) - a$ is universally bounded by N is 0. In particular, the set of stable primes of (f, a) is of density 0.
(2) If f is of degree ≥ 5 and not linearly related to a monomial or Chebyshev polynomial, then for any a_0 not lying in the backward orbit of a under f, the set of primes p such that $f^{\circ n}(a_0) \equiv a \bmod p$ for some $n \in \mathbb{N}$ is of density 0.

In fact, both conclusions hold under weaker "largeness" assumptions as well. Notably, a sufficient assumption for the set of stable primes of (f, a) to be of density 0 is that the number of nonsolvable composition factors of $\mathrm{Gal}(f^{\circ n})(X) - a$ is unbounded as $n \to \infty$, cf. [K]; this widely generalizes previous density-0 results such as [Fer18], and is relevant in particular because it is at least conveicable and consistent with current knowledge (cf. [BDGHT21]) that outside of some very concrete and well-understood exceptions (all of which can be verified to still yield the same density-0 conclusion), *every* arboreal representation $\rho_{f,a}$ for a polynomial f with nonsolvable monodromy group might fulfill this weakened assumption.

Building on this, a somewhat more detailed analysis, cf. [K], gives rise to the conjecture that in fact any polynomial f which achieves a positive density proportion of stable primes must be a composition of linears, monomials and Chebyshev polynomials.

Note: This report forms the second part of a two-part project, the first part of which is summarized in the report by *D. Neftin "Large monodromy groups of polynomial compositions"* in this volume.

References

[BJ07] N. Boston, R. Jones, Arboreal Galois representations. Geom. Dedicata 124 (2007), 27–35.
[BEK21] I. I. Bouw, Ö. Ejder, V. Karemaker, Dynamical Belyi maps and arboreal Galois groups. Manuscripta Math. 165 (2021), 1–34.
[BDGHT21] A. Bridy, J.R. Doyle, D. Ghioca, L.-C. Hsia, T.J Tucker, A question for iterated Galois groups in arithmetic dynamics. Can. Math. Bull. 64(2) (2021), 401–417
[Fer18] A. Ferraguti, The set of stable primes for polynomial sequences with large Galois group. Proc. Amer. Math. Soc. 146(7) (2018), 2773–2784.
[Jon08] R. Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, J. Lond. Math. Soc. 78 (2008), 523–544.
[Jon13] R. Jones, Galois representations from pre-image trees: an arboreal survey. Pub. Math. Besancon (2013), 107–136.
[Jon07] R. Jones, Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set, Compositio Math. 143 (5) (2007), 1108–1126.
[KN01] J. König, D. Neftin, Reducible fibers of polynomial maps. To appear in IMRN. Preprint at arXiv:2001.03630 [math.NT]
[KNR] J. König, D. Neftin, S. Rosenberg, Polynomial compositions with large monodromy groups and applications to arithmetic dynamics. Work in progress.
[K] J. König, Sparsity of stable primes for dynamical sequences. Work in progress.

[MOS85] L. Mérai, A. Ostafe, I.E. Shparlinski, Dynamical irreducibility of polynomials modulo primes. Math. Z. 298 (2021), 1187–1199.
[Odo85] R.W.K. Odoni, The Galois theory of iterates and composites of polynomials, Proc. London Math. Soc. (3) 51 (1985), no. 3, 385–414.

Resolution of Non-Singularities

Emmanuel Lepage

Given a hyperbolic curve X over an algebraically closed non-archimedean field of mixed characteristics, we want to understand where can appear irreducible components of the special fiber of the stable model of finite étale covers of X. This is of anabelian interest in contexts where the dual graph of the special fiber of the stable model can be reconstructed from anabelian data (it is for example the case when this datum is the étale fundamental group of a hyperbolic curve over a finite extension of $\mathbb{Q}_p$ or the tempered fundamental group): the tower of dual graphs gives a finer combinatorial approximation of the curve, that is ultimately related to the Berkovich topological space of the curve.

This problem originates as a by-product of S. Mochizuki's seminal anabelian approach [pGC] and was first formulated by A. Tamagawa in [Tam04], which establishes the first result related to resolution of non-singularities (RNS) in the case of *stable model of hyperbolic curves*, that is:

> For every hyperbolic curve X over an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and every closed point x of the stable model $\mathfrak{X}$ of X, there exists a finite étale cover $f : Y \to X$ such that its extension to the stable models $\tilde{f} : \mathfrak{Y} \to \mathfrak{X}$ has a fiber $\tilde{f}^{-1}(x)$ of dimension 1,

i.e. some irreducible component of the special fiber of $\mathfrak{Y}$ lies above x.

This report presents S. Mochizuki and S. Tsujimura's result [RNS] which extends Tamagawa's result to arbitrary semi-stable models of X (see Theorem 2 for a precise statement) and provides a final answer to this problem over finite extensions of $\mathbb{Q}_p$. Such an extension to arbitrary semi-stable models was first considered, and proven for Mumford curves, in [Lep13] using analytic techniques. The RNS has consequences in Grothendieck's section conjecture [PS17] and [RNS, Theorem F], for the Grothendieck-Teichmüller group ibid. Theorem G, and establish Grothendieck's *absolute* anabelian conjecture over $\mathbb{Q}_p$, see ibid. Theorems D-E and below.

1. Absolute anabelian reconstruction

We first explain how the RNS given by Theorem 2 implies Grothendieck's absolute anabelian conjecture, see also [Lep23, Thm 0.2]:

Theorem 1. [RNS, Thm D] *Let X/K and Y/L be hyperbolic curves over finite extensions of $\mathbb{Q}_p$. Then every isomorphism of étale fundamental groups $\phi : \pi_1(X) \to \pi_1(Y)$ is geometric, i.e. it is induced by an isomorphism $X \to Y$.*

The term *absolute* refers to the fact ϕ is not supposed a priori to be compatible with an isomorphism of base fields. More precisely, under the assumptions of Theorem 1, the morphism ϕ induces an isomorphism of absolute Galois groups $\phi^{base} : G_K \to G_L$. If ϕ^{base} is geometric, i.e. induced by an isomorphism $K \to L$, then the *relative* anabelian conjecture, proven by Mochizuki in [pGC], shows that ϕ is also geometric. Mochizuki proved that to show that ϕ^{base} is geometric, it is enough to show that ϕ preserves geometric Galois sections [AbsTopII, Thm 2.9]: a closed subgroup $D \subset \pi_1(X)$ is the decomposition group of a closed point $x \in X$ if and only if $\phi(D)$ is the decomposition group of a closed point in Y.

1.1. **A Berkovich homeomorphism.** Let $\widetilde{X}$ be a pro-universal étale cover of X: $X = \varprojlim S$ where S goes through pointed finite étale cover of X. Let $\widetilde{X}^{an} = \varprojlim_S \overline{S}^{an}$, where $\overline{S}^{an}$ denotes the Berkovich space of the compactification $\overline{S}$ of S. Let $\mathbb{G}_X$ be the dual graph of the stable reduction of $X_{\overline{\mathbb{Q}}_p}$. Then, there is a natural continuous map $f_X : \widetilde{X}^{an} \to \varprojlim_S \mathbb{G}_S$, and Theorem 2 implies that f_Z is a homeomorphism – see [Lep13, Thm 3.10], [Lep23, Prop 2.1], and [RNS, Prop 3.5].

1.2. **Decomposition groups reconstruction.** There is a functorial group-theoretic reconstruction $\mathbb{G}(\pi_1(X))$ of $\mathbb{G}_X$ from $\pi_1(X)$ considered as an abstract topological group [AbsAnAb, Thm 2.7]. By passing to the inverse limit along open subgroups of $\pi_1(X)$, one obtains a group-theoretic topological space $\widetilde{\mathbb{G}}(\pi_1(X)) := \varprojlim_H \mathbb{G}(H)$, where the projective limit is indexed by open subgroups of G, and the natural map $\widetilde{X}^{an} \to \widetilde{\mathbb{G}}(\pi_1(X))$ is an isomorphism. This map is $\pi_1(X)$-equivariant. The rigid points $\tilde{x} \in \widetilde{X}^{an}$ are characterized by the fact that their stabilizer $D_{\tilde{x}} := \{g \in \pi_1(X), g(\tilde{x}) = \tilde{x}\}$ injects in G_K and has open image, see [Lep23, Prop 4.3], and [RNS, Prop 3.9]. In particular, ϕ preserves decomposition groups of rigid points of $\widetilde{X}^{an}$.

The RNS for hyperbolic curves over p-adic fields

While the original approach of [RNS] is purely written in the language of schemes and formal schemes, our presentation borrows to the Berkovich theory of analytic spaces and valuations as in [Lep23].

We will say that a valuation on $K(X)$ extending the valuation on $\mathbb{Q}_p$ is of type 2 if its residue field is of transcendance degree 1 over $\mathbb{F}_p$ (this is equivalent to the fact that its valuation ring is the stalk $\mathcal{O}_{\mathfrak{X},z}$ at the generic point z of some irreducible component of the special fiber of some semi-stable model $\mathfrak{X}$ of X). If v is a valuation of type 2, then its residue field is isomorphic to the function field of a curve over an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, and g_v will denote the geometric genus of that curve.

Theorem 2. [RNS, Thm A] *Let X be a hyperbolic curve over an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and v a valuation 2 on $K(X)$. Then there exists a finite étale cover Y of X and an extension w of v to $K(Y)$ such that $g_w \neq 0$ (in particular, its valuation ring is the stalk $\mathcal{O}_{\mathfrak{Y},z}$ at the generic point z of some irreducible component of the special fiber of the stable model $\mathfrak{Y}$ of Y).*

1.3. **A log-differential existence criterion.** In terms of the notations of Theorem 2, it is enough to proof that the valuations v of type 2 satisfying the wanted property are dense for the Berkovich topology. The proof of Theorem 2 relies on a local criterion in terms of the Hodge-Tate map

$$HT_X : H^1(X, \mathbf{Z}_p(1)) \to H^0(X, \Omega^1_{X_{\mathbb{C}_p}}),$$

which locally for the rigid topology sends the Kummer class of $f \in \mathcal{O}^\times(U)$ to $\frac{df}{f} \in H^0(U, \Omega^1_{X_{\mathbb{C}_p}})$ (actually, the proof of [RNS] only uses this local ad hoc definition on small disks and one does not need to know that the Hodge-Tate map is globally defined).

Let $x \in X(\mathbb{C}_p)$ and let D be a closed analytic disk containing x. A valuation v on $K(X)$ is in D if $v(f) \geq \inf_{y \in D(\mathbb{C}_p)} v_{\mathbb{C}_p}(f(y))$ for all $f \in K(X)$. Let $c \in H^1(X, \mathbf{Z}_p(1))$ s.t. $HT_X(c) \neq 0$. Let $\phi_{n,c} : Y_{n,c} \overset{\mu_{p^n}}{\to} X$ be the μ_{p^n}-torsor corresponding to c.

Lemma 1 ([Lep13, Prop 2.4], [Lep23, Prop 1.3], and [RNS, Prop 1.6, Rem 1.6.2])**.** *Assume $e := mult_x HT_X(c)$ is not of the form $p^k - 1$ for any integer $k \geq 0$. Then, for n big enough, there is a valuation v_n of type 2 in D and an extension w_n of v_n to $K(Y_{n,c})$ such that $g_{w_n} \neq 0$.*

To show this lemma, up to reducing to a smaller disk, one can assume that c is the Kummer class of some $f \in \mathcal{O}^\times(D)$. Then w_n is an extension to $K(Y_{n,c})$ of the Gauss valuation v_n of the disk of convergence of a p^nth root of f, and the extension of residue fields $\widetilde{K(Y_{n,c})}_{w_n}/\widetilde{K(X)}_{v_n}$ is an explicit Artin-Schreier extension, so that one can directly calculate g_{w_n}.

1.4. **Dimensional criterion.** Let $x \in X(\overline{\mathbb{Q}}_p)$ and let K be a finite extension of $\mathbb{Q}_p$ such that X is the pullback to $\overline{\mathbb{Q}}_p$ of a hyperbolic curve X_K over K and $x \in X_K(K)$. Let t be a local parameter at x. Then the composite

$$H^1(X_{\mathbb{C}_p}, \mathbf{Z}_p(1)) \overset{HT_X}{\to} H^0(X, \Omega^1_{X_{\mathbb{C}_p}}) \overset{ev_{x,d}}{\to} \Omega^1_{X_{\mathbb{C}_p},x}/\mathfrak{m}^d_{X_{\mathbb{C}_p},x}\Omega^1_{X_{\mathbb{C}_p},x} \simeq \mathbb{C}_p[[t]]/t^d$$

is G_K-equivariant. For $d \geq 2g_X$, the evaluation map $ev_{x,d}$ is injective by Riemann-Roch theorem [RNS, Lem 2.14]. In particular, one gets an injective map of finite dimensional $\mathbb{Q}_p$-vector spaces:

$$V_X := (H^1(X, \mathbb{Q}_p(1))/Ker(HT_X))^{G_K} \to K[[t]]/t^{2g_X}.$$

If the assumption of Lemma 1 is satisfied for no $c \in H^1(X, \mathbb{Q}_p(1))$, then V_X must be small: $\dim_{\mathbb{Q}_p} V_X \leq C[K : \mathbb{Q}_p] \log(g_X)$ for some constant C independent of X and K, see [RNS, Lem 2.15].

1.5. **Dimensional estimation.**

1.5.1. *Ordinary case.* The dimension of V_X can be for example explicitly computed if X_K has split stable reduction and all the irreducible components of the special fiber of the stable model $\mathfrak{X}$ are ordinary.

Let J_K be the Jacobian of X_K. Then J has a rigid uniformisation by a semi-abelian variety J^∞, which is an extension of an abelian variety B with good reduction $\mathfrak{B}_\mathfrak{s}$ by a split torus. The Tate module T_pJ of J is an extension of its étale part by its connected part:

$$1 \to T_p^{cnn}J \to T_pJ \to T_p^{et}J \to 1$$

and the isomorphism $H^1(X, \mathbb{Q}_p(1)) \simeq \mathrm{Hom}(T_pJ, \mathbb{Q}_p(1))$ maps the subgroup $\mathrm{Ker}(\mathrm{HT}_\mathrm{X})$ to $\mathrm{Hom}(T_p^{et}J, \mathbb{Q}_p(1))$, so that $V_X \simeq \mathrm{Hom}_{G_K}(T_p^{cnn}J, \mathbb{Q}_p(1))$. Moreover, self-duality on J induces a map $\mathrm{Hom}(T_p^{cnn}J, \mathbb{Q}_p(1)) \to T_{p,\mathbb{Q}}^{et}J$ that is an isomorphism under the ordinary assumption. The action of G_K on $T_{p,\mathbb{Q}}^{et}J$ factors through an action of the absolute Galois group $G_{\widetilde{K}}$ of the residue field $\widetilde{K}$ of K and $T_{p,\mathbb{Q}}^{et}J$ is an extension of a combinatorial part $T_{p,\mathbb{Q}}^{cb}J \simeq \mathrm{Gal}(J^\infty/J) \otimes_\mathbf{Z} \mathbb{Q}_p \simeq \pi_1^{top}(\mathbb{G}_X) \otimes_\mathbf{Z} \mathbb{Q}_p$, on which G_K acts trivially, by $T_{p,\mathbb{Q}}^{et}\mathfrak{B}_\mathfrak{s}$, on which 1 is not an eigenvalue of Frobenius by Weil's conjectures. Therefore $V_X \simeq (T_{p,\mathbb{Q}}^{et}J)^{G_K} \xrightarrow{\sim} T_{p,\mathbb{Q}}^{cb}J$ is of dimension the loop number h_X of the dual graph $\mathbb{G}_X$ (i.e the minimal number of edge on $\mathbb{G}_X$ one needs to erase to get a tree).

If X' is a combinatorial finite étale cover, corresponding to a topological cover of X, then

$$g_{X'} - 1 = (g_X - 1)\deg(X'/X) \text{ and } h_{X'} - 1 = (h_X - 1)\deg(X'/X)$$

and the preimages of x in X' are also rational points. In particular, if $h_X \geq 2$, then $\dim_{\mathbb{Q}_p} V_{X'}$ asymptotically grows like $g_{X'}$ when $\deg(X'/X)$ goes to infinity, so that the inequality $\dim_{\mathbb{Q}_p} V_{X'} \leq C[K:\mathbb{Q}_p]\log(g_{X'})$ must be false when $\deg(X'/X)$ is big enough, and therefore, using Lemma 1, the curve X satisfies resolution of non-singularities.

1.5.2. *General case.* One reduces to the previous computation for ordinary abelian varieties by using the following result of Tamagawa, based on previous results of Raynaud [Ray82, Thm 4.3.1], that ensures the existence of finite étale covers with ordinary new part:

Theorem 3. [Tam97, Lem 1.9] *Let S be a proper smooth curve over $\overline{\mathbb{F}}_p$ of genus $g_S \geq 2$. Let $l \neq p$ be a prime number. Then for m big enough, there exists an étale $\mathbf{Z}/l^m\mathbf{Z}$-cover $S_2 \to S$ such that* $\mathrm{Coker}(J_{S_1} \to J_{S_2})$ *is ordinary, with S_1 the intermediate cover $S_2 \xrightarrow{l} S_1 \xrightarrow{l^{m-1}} S$.*

Up to replacing X by a finite étale cover, and K by a finite extension, one can assume that X has a split stable model $\mathfrak{X}$, that $h_X \geq 2$ and that all the irreducible components of the special fiber $\mathfrak{X}_s$ of $\mathfrak{X}$ are of genus greater than 1. One then applies Theorem 3 to the irreducible components of the smooth locus of the special fiber $\mathfrak{X}_\mathfrak{s}$ of the stable model $\mathfrak{X}$ of X, glue them (compatibly with the $\mathbf{Z}/l^m\mathbf{Z}$-actions) together into étale covers of $\mathfrak{X}_\mathfrak{s}$, that extends to covers of $\mathfrak{X}$.

One obtains on the generic fiber an étale $\mathbf{Z}/l^m\mathbf{Z}$-cover $Z \to X$, that factors into a $\mathbf{Z}/l^{m-1}\mathbf{Z}$-cover $Y \to X$ and a $\mathbf{Z}/l\mathbf{Z}$-cover $Z \to Y$ such that the good reduction part B of $A = \mathrm{Coker}(J_Y \to J_Z)$ is ordinary (i.e. A^∞ is an extension of the ordinary abelian variety B by a split torus).

The proof is then similar to the ordinary case where J_X is now replaced by A. The composite

$$V_A := \mathrm{Hom}_{G_K}(T_p^{cnn} A, \mathbb{Q}_p(1)) \to V_Y = \mathrm{Hom}(T_p^{cnn} J_Z, \mathbb{Q}_p(1))$$

is injective so that $\dim_{\mathbb{Q}_p} V_Z \geq \dim_{\mathbb{Q}_p} V_A = h_Z - h_Y$. Up to replacing K by a finite extension one can assume that the preimages of x in Z are still rational points.

Let Y' be a combinatorial finite étale cover of Y, let $Z' = Z \times_Y Y'$ and $A' = \mathrm{Coker}(J_{Y'} \to J_{Z'})$. Then $\dim_{\mathbb{Q}_p} V_{Z'} \geq h_{Z'} - h_{Y'} = \deg(Y'/Y)(h_Z - h_Y)$ and $g_{Z'} = \deg(Y/Y')g_Z$, so that the inequality $\dim_{\mathbb{Q}_p} V_{Z'} \leq C[K : \mathbb{Q}_p] \log(g_{Z'})$ must be false when $\deg(Y'/Y)$ is big enough, and therefore X, using Lemma 1, satisfies resolution of non singularities.

References

[Lep13] E. Lepage, *Resolution of nonsingularities for Mumford curves*, Publ. Res. Inst. Math. Sci. **49** (2013), no. 4, 861–891.

[Lep23] ———, *Resolution of non-singularities and the absolute anabelian conjecture*, arXiv:2306.07058 [math.AG] (2023)

[pGC] S. Mochizuki, *The local pro-p anabelian geometry of curves*, Inventiones Mathematicae **138** (1999), 319–423.

[AbsAnAb] ———, *The absolute anabelian geometry of hyperbolic curves*, Galois theory and modular forms, Kluwer Academic publishers, 2003, 77–122.

[AbsTopII] ———, *Topics in anabelian geometry II: Decomposition groups and endomorphisms*, J. Math. Sci. Univ Tokyo **20** (2013), 171–269.

[RNS] S. Mochizuki and S. Tsujimura, *Resolution of Nonsingularities, Point-theoreticity, and Metric-admissibility for p-adic Hyperbolic Curves*, RIMS preprint 1974, (2023).

[PS17] F. Pop and J. Stix, *Arithmetic in the fundamental group of a p-adic curve. On the p-adic section conjecture for curves*, Journal für die reine und angewandte Mathematik (Crelles Journal), vol. **2017**, no. 725, 2017, pp. 1–40.

[Ray82] M. Raynaud, *Sections des fibrés vectoriels sur une courbe*, Bull. Soc. Math. France **110** (1982), 103—125.

[Tam97] A.Tamagawa, *The Grothendieck conjecture for affine curves*, Compositio Math. **109** (1997), 135–194

[Tam04] ———, *Resolution of nonsingularities of families of curves*, Publ. Res. Inst. Math. Sci. **40** (2004), no. 4, 1291–1336.

Past and Present of Probabilistic Galois Theory: A Comprehensive Overview

Lior Bary-Soroker

The goal of the talk was to introduce the recent developments in probabilistic Galois theory. There are several approaches to probabilistic Galois theory, and in this talk we focused on the Galois group of random polynomials whose coefficients are independent random variables. In this setting, the most classical model is the so-called large box model (LBM) in which the degree of the polynomial is fixed and the coefficients are uniform on an interval whose length grows to infinity. Here it is known from about a century that the Galois group is the full symmetric group, and the main question is what is the next most probable group (this is the content of the so-called "van der Waerden conjecture"). Along the years there were abundance of results bounding the probability that the group is not the full symmetric group, and in a very recent groundbreaking result by Bhargava, he showed that this probability has the same order of magnitude as of the Galois group being the stabilizer of a point. In particular, he proved that the most probable group after the full symmetric group is either the alternating group of the stabilizer of a point. In the talk, we also presented lower bounds of the probability of the group being the alternating group that is much bigger than the naive heuristic, by using linear symmetries (e.g. is the degree is divisible by 4 and the polynomial plus its derivative is a square, then the discriminant is a square).

The other model that we discussed is the restricted coefficients model. In a general, but not the most general, form we choose the coefficients by a fixed distribution. For example, we choose uniformly $-1, 0, 1$ – the Littlewood polynomials or $-1, 1$ – the Radamacher polynomials) and we let the degree go to infinity. In this model, we know much less than in the LBM. For example, the content of the Odlyzko-Poonen conjecture is that the probability for the polynomial f to be irreducible goes to one (conditioned on $f(0) \neq 0$). Breuillard and Varju proved that the general Riemann hypothesis implies the Odlyzko-Poonen conjecture. The state-of-the-art unconditional result is due to the speaker, Koukoulopoulos and Kozma, who proved that for each non-degenerate distribution there exists a constant $\theta > 0$ such that the limit inferior of the probability to be irreducible is at least θ. The constant is explicit, and if the distribution is uniform on an interval of length at least 35, $\theta = 1$. We discussed the connection to the arithmetic of random polynomials over finite fields and the connections to analytic number theory. We also mentioned briefly what happens if one goes from finite fields to the p-adics, and the conjecture of Bhargava-Cremona-Fisher-Gajovic which deals with uniform random polynomials, and some of the results including Shmueli's results for non-uniform polynomials.

Locally conjugate Galois sections

Wojciech Porowski

Let X be a smooth geometrically connected curve over a number field K, write $G_K = \mathrm{Gal}(\overline{K}/K)$ for the absolute Galois group of K and consider the étale homotopy exact sequence

$$1 \to \Delta_X \to \Pi_X \to G_K \to 1, \tag{1}$$

where Π_X and Δ_X are the étale fundamental groups of X and $X_{\overline{K}}$, respectively.

The question of Grothendieck's section conjecture – "when does a section of Sequence (1) come from a K-rational point of X?" – is the object of multiple studies, see [Sti12] for a comprehensive discussion and [Ho14] for a study of the birational case. We report on an approach regarding the local-global properties of sections of the homotopy sequence obtained by the author in [Po23].

1. A local-global principle for anabelian sections

We will be interested in conjugacy classes of sections of Sequence (1). Write $V(K)$ for the set of nonarchimedean valuations of K and for every $v \in V(K)$ write $G_v \subset G_K$ for a decomposition group associated to v.

Let s and t denote two sections of Sequence (1):

(1) For $v \in V(K)$ we say that *s and t are conjugate at v* if restrictions of s and t to G_v are conjugate.
(2) For a nonempty subset $\Omega \subset V(K)$ we say that *s and t are conjugate on Ω* if they are conjugate at every $v \in \Omega$.

One may wonder whether two sections that are conjugate on a 'large' set of valuations are necessarily globally conjugate. This question served as the original motivation for the present work and we can provide an answer in the following form.

Theorem 1. *Suppose that Ω is of density one. Then, any two sections of the étale homotopy sequence* (1) *that are conjugate on Ω are conjugate.*

In other words, Theorem 1 gives a local-global principle for conjugacy classes of sections. It is an interesting problem whether one can relax the assumption on the density of Ω and require only that Ω has positive density. The section conjecture, which predicts that every section of Sequence (1) is either cuspidal or comes from a K-rational point of X, would imply that the answer to this stronger question is positive. Unfortunately, the methods we use to prove Theorem 1 are not strong enough to apply here; the problem is that in the proof we need to have the flexibility to pass to finite field extensions where we may lose control of the density of Ω.

In fact, Theorem 1 will be proved as a corollary of a more general property of the étale homotopy sequence (1), so-called finite covering property which we introduce in the next section.

2. The finite covering property

Slightly more generally, we can consider the same problem as above for any short exact sequence of profinite groups

$$1 \to \Delta \to \Pi \to G_K \to 1. \tag{2}$$

Let $s, t_1, \dots t_n$ be sections of Sequence (2) for some $n \geq 1$ and let Ω be a nonempty subset of $V(K)$. We say that sections t_i *cover* section s on Ω if for every $v \in \Omega$ there exists $1 \leq i \leq n$ such that s and t_i are conjugate at v. We say that Sequence (2) has *finite covering property* if (a) for every $\Omega \subset V(K)$ of density one and (b) for every $n \geq 1$ the following condition is satisfied:

whenever $s, t_1, \ldots, t_n$ are sections of sequence (2) such that sections t_i cover section s on Ω then there exists $1 \leq i \leq n$ such that s and t_i are conjugate.

With these definitions, we can state our main result.

Theorem 2. *The étale homotopy exact sequence* (1) *has finite covering property.*

As we have mentioned, Theorem 1 follows directly from Theorem 2 by taking $n = 1$ in the definition of the finite covering property.

The first step in establishing Theorem 2 goes through establishing its abelian version. The abelian version of finite covering property is given as follows. Let M be a topological G_K-module. For $v \in V(K)$, write loc_v for the restriction map

$$H^1(G_K, M) \to H^1(G_v, M).$$

Let $c, c_1 \ldots, c_n$ be cohomology classes in $H^1(G_K, M)$ for some $n \geq 1$ and let $\Omega \subset V(K)$ be a nonempty subset of valuations. We say that classes c_i *cover* class c on Ω if for every $v \in \Omega$ there exists $1 \leq i \leq n$ such that $loc_v(c) = loc_v(c_i)$. We say that a G_K-module M has *finite covering property* if for every $\Omega \subset V(K)$ of density one and for every $n \geq 1$ the following condition is satisfied: whenever $c, c_1, \ldots, c_n$ are cohomology classes in $H^1(G_K, M)$ such that classes c_i cover c on Ω then there exists $1 \leq i \leq n$ such that $c = c_i$. We prove the following abelianized version of Theorem 2.

Theorem 3. *Write Δ_X^{ab} for the (topological) abelianization of the geometric fundamental group of X. Then, G_K-module Δ_X^{ab} has finite covering property.*

The proof of Theorem 3 follows the strategy used by Stoll in Section 3 of [Sto07], with minor modifications. Comparing with our situation, the difference is that in [Sto07] only Tate modules of abelian varieties are considered whereas when X is affine and of positive genus we have a short exact sequence

$$1 \to \hat{\mathbb{Z}}(1)^{\oplus r} \to \Delta_X^{ab} \to T(A) \to 1,$$

where $r \geq 1$ and $T(A)$ is the Tate module of an abelian variety A over K (at least after restricting to an open subgroup of G_K). The main input to prove Theorem 3 are two theorems of Serre (see [Se86], Thm. 1 and Thm. 2) which say, roughly speaking, that the image of the Galois action in $\mathrm{Aut}(T(A))$ contains a 'large' subgroup of homotheties.

3. From abelian to étale

In this section we sketch how to extend our result from the abelian case to the case of the étale homotopy sequence (1). It is at this point that the additional flexibility in the definition of the finite covering property becomes crucial for the argument.

Write Δ_X^{sol} for the maximal pro-solvable quotient of Δ_X and $\Pi_X^{(sol)}$ for the quotient of Π_X which makes the following sequence exact

$$1 \to \Delta_X^{sol} \to \Pi_X^{(sol)} \to G_K \to 1. \tag{3}$$

For technical reasons, it is convenient to prove first the following intermediate theorem.

Theorem 4. *The pro-solvable homotopy exact sequence* (3) *has finite covering property.*

Let us indicate a general strategy of proving Theorems 4 and 2. For a section s of Sequence (2) we say that an open subgroup $U \subset \Pi$ is a *neighbourhood* of s if $s(G_K) \subset U$. If t is another section of sequence (2) then to prove that s and t are conjugate it is enough to show that for every neighbourhood U of s there exists a section t' which is conjugate to t and $t'(G_K) \subset U$. Hence we need to analyse the 'splitting' of the conjugacy class of section t in open subgroups of Π, which replaces conjugacy class of t by finitely many conjugacy classes of 'quasi-sections' $t_1, \ldots, t_n$. This is the main reason why the more general situation considered in Theorem 2 is necessary even if one is only interested in proving Theorem 1.

With this approach, Theorem 4 is deduced from appropriate m-step solvable versions for all $m \geq 1$ which are proved inductively on m; the case $m = 1$ is Theorem 3.

Finally, one deduces Theorem 2 by applying Theorem 4 to all neighbourhoods of section s and using the already mentioned strategy of splitting conjugacy classes of sections in open subgroups of Π_X.

We remark that the two essential properties of curve X and its corresponding étale homotopy sequence (1) that we use in this work are:

(1) the finite covering property of the abelianized geometric fundamental group Δ_X^{ab}, i.e., validity of Theorem 3,
(2) triviality of centralizers of sections of Sequence (1).

Note that these two properties should be true for every finite étale cover of X. To the author's knowledge, the only known nontrivial examples of varieties satisfying these requirements are hyperbolic curves and semi-abelian varieties. It is an interesting problem to find other nontrivial examples of such varieties.

References

[Se86] J.P. Serre, *Groupes linéaires modulo p et points d'ordere fini des varietés abéliennes*, Note of a cours at Collège de France (1986).

[Sto07] M. Stoll, *Finite descent obstructions and rational points on curves*, Algebra & Number Theory **1** (2007), 349–391.

[Sti12] J. Stix, *Rational points and arithmetic of fundamental groups: Evidence for the section conjecture*, Vol. 2054, (2012), Springer.

[Ho14] Y. Hoshi, *Conditional results on the birational section conjecture over small number fields*, Automorphic Forms and Galois Representations. vol. 2, (2014), 187–230, London Math. Soc. Lecture Note Ser., 415, Cambridge Univ. Press, Cambridge.

[Po23] W. Porowski, *Locally conjugate Galois sections*, preprint (2023) (in preparation).

On functional equations of ℓ-adic Galois polylogarithms

Densuke Shiraishi
(joint work with Hiroaki Nakamura)

The ℓ-adic Galois polylogarithm $Li_k^\ell(z)$ was introduced by Z. Wojtkowiak [Woj04]-[Woj05b] as the ℓ-adic étale analog of the complex polylogarithm for any prime number ℓ. In this talk, based on [NS] and [Shi23b], we discussed Landen's and Spence-Kummer's functional equations of the ℓ-adic Galois trilogarithm $Li_3^\ell(z)$.

1. ℓ-adic Galois polylogarithms

Let K be a subfield of $\mathbb{C}$ with its algebraic closure $\overline{K}$. Let G_K be the absolute Galois group of K. Take a K-rational base point z of $\mathbb{P}^1\backslash\{0,1,\infty\}$. We regard each topological path $\gamma \in \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\};\overrightarrow{01},z\right)$ form $\overrightarrow{01}$ to z as a pro-ℓ etale path $\gamma \in \pi_1^{\ell\text{-ét}}\left(\mathbb{P}^1_{\overline{K}}\backslash\{0,1,\infty\};\overrightarrow{01},z\right)$ via the comparison map. For $\sigma \in G_K$ and $\gamma \in \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\};\overrightarrow{01},z\right)$, the ℓ-adic Galois polylogarithm $Li_k^\ell(z;\gamma,\sigma)$ is defined as the signed coefficient of $e_0^{k-1}e_1$-term in the ℓ-adic Galois associator

$$\mathfrak{f}_\sigma^{z,\gamma}(e_0,e_1) \in \mathbb{Q}_\ell\langle\langle e_0,e_1\rangle\rangle,$$

i.e. the image of the pro-ℓ étale loop $\mathfrak{f}_\sigma^{z,\gamma} = \gamma\cdot\sigma(\gamma)^{-1} \in \pi_1^{\ell\text{-ét}}\left(\mathbb{P}^1_{\overline{K}}\backslash\{0,1,\infty\},\overrightarrow{01}\right)$ under an ℓ-adic Magnus embedding $\pi_1^{\ell\text{-ét}}\left(\mathbb{P}^1_{\overline{K}}\backslash\{0,1,\infty\},\overrightarrow{01}\right) \hookrightarrow \mathbb{Q}_\ell\langle\langle e_0,e_1\rangle\rangle$. We understand the symbol $Li_k^\ell(z)$ to be a map

$$Li_k^\ell(z) : \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\};\overrightarrow{01},z\right)\times G_K \to \mathbb{Q}_\ell, \quad (\gamma,\sigma)\mapsto Li_k^\ell(z;\gamma,\sigma).$$

In particular, the ℓ-adic Galois zeta value (or called the ℓ-adic Soulé element) $\boldsymbol{\zeta}_k^\ell(\sigma)$ is defined by its special value at $\overrightarrow{10}$ with the straight path from $\overrightarrow{01}$ to $\overrightarrow{10}$.

Remark 1. The typical functional equations of the ℓ-adic Galois dilogarithm $Li_2^\ell(z)$ were studied by Nakamura-Wojtkowiak [NW12, Section 6. Examples].

Remark 2. The complex KZ associator $G_0^{z,\gamma}(e_0,e_1) \in \mathbb{C}\langle\langle e_0,e_1\rangle\rangle$ is defined as a fundamental solution of the KZ equation characterized by a certain asymptotic behavior around the puncture 0. The ℓ-adic associator $\mathfrak{f}_\sigma^{z,\gamma}(e_0,e_1) \in \mathbb{Q}_\ell\langle\langle e_0,e_1\rangle\rangle$ is the ℓ-adic Galois analog of $G_0^{z,\gamma}(e_0,e_1)$. As is well known, $G_0^{z,\gamma}(e_0,e_1)$ is a generating function for iterated integrals over γ including the complex polylogarithm

$$Li_k(z) : \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\};\overrightarrow{01},z\right) \to \mathbb{C}, \quad \gamma\mapsto Li_k(z;\gamma).$$

The coefficient of e_0-term in $G_0^{z,\gamma}(e_0,e_1)$ is the complex logarithm $\log(z)$ along γ. The ℓ-adic Galois analog of $\log(z)$ is the Kummer 1-cocycle

$$\rho_{z,\gamma} : G_K \to \mathbb{Z}_\ell$$

defined by $\sigma(z^{1/\ell^k}) = z^{1/\ell^k}\cdot\zeta_{\ell^k}^{\rho_{z,\gamma}(\sigma) \bmod \ell^k}$ for the roots $\{z^{1/\ell^k}\}_{k\in\mathbb{N}}$ along γ.

2. Main results

First, we discuss the ℓ-adic Landen equation. For a standard tangential base point $*$ of $\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}$, we shall write $\delta_* \in \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}; \overrightarrow{01}, *\right)$ for the topological path through the upper half-plane. Given a K-rational (possibly, tangential base) point z of $\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}$ and a path $\gamma \in \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}; \overrightarrow{01}, z\right)$, define the paths γ', γ'' with respect to γ by

$$\gamma' := \delta_{\overrightarrow{10}} \cdot \phi_{\overrightarrow{10}}(\gamma) \in \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}; \overrightarrow{01}, 1-z\right),$$
$$\gamma'' := \delta_{\overrightarrow{0\infty}} \cdot \phi_{\overrightarrow{0\infty}}(\gamma) \in \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}; \overrightarrow{01}, \frac{z}{z-1}\right),$$

where $\phi_{\overrightarrow{10}}, \phi_{\overrightarrow{0\infty}} \in \mathrm{Aut}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}\right)$ are given by $\phi_{\overrightarrow{10}}(t) = 1-t$, $\phi_{\overrightarrow{0\infty}}(t) = \frac{t}{t-1}$. Then we get algebraic relations (chain rules) among ℓ-adic Galois associators:

$$\mathfrak{f}_\sigma^{z,\gamma}(e_0,e_1) = \mathfrak{f}_\sigma^{1-z,\gamma'}(e_1,e_0) \cdot \mathfrak{f}_\sigma^{\overrightarrow{10},\delta_{\overrightarrow{10}}}(e_0,e_1),$$
$$\mathfrak{f}_\sigma^{\frac{z}{z-1},\gamma''}(e_0,e_1) = \mathfrak{f}_\sigma^{z,\gamma}(e_0,e_\infty) \cdot \mathfrak{f}_\sigma^{\overrightarrow{0\infty},\delta_{\overrightarrow{0\infty}}}(e_0,e_1),$$

where e_∞ is the Baker-Campbell-Hausdorff sum $\mathbf{log}\left(\mathbf{exp}(-e_1)\cdot\mathbf{exp}(-e_0)\right)$.

By comparing the coefficients on both sides of these algebraic relations, we obtain the following functional equation.

Theorem 1 (The ℓ-adic Landen equation, [NS]). *For $\sigma \in G_K$, we have*

$$Li_3^\ell(z;\gamma,\sigma) + Li_3^\ell(1-z,\gamma',\sigma) + Li_3^\ell\left(\frac{z}{z-1};\gamma'',\sigma\right)$$
$$= \boldsymbol{\zeta}_3^\ell(\sigma) - \boldsymbol{\zeta}_2^\ell(\sigma)\rho_{1-z,\gamma'}(\sigma) + \frac{1}{2}\rho_{z,\gamma}(\sigma)\rho_{1-z,\gamma'}(\sigma)^2 - \frac{1}{6}\rho_{1-z,\gamma'}(\sigma)^3$$
$$- \frac{1}{2}Li_2^\ell(z;\gamma,\sigma) - \frac{1}{12}\rho_{1-z,\gamma'}(\sigma) - \frac{1}{4}\rho_{1-z,\gamma'}(\sigma)^2.$$

Remark 3. Using the former chain rule above, Nakamura derived Oi-Ueno's functional equation of ℓ-adic Galois multiple polylogarithms in [NS]. After [NS] was worked out, the author obtained a generalization of this ℓ-adic Oi-Ueno equation to higher multi-indices in [Shi23a].

We next discuss the ℓ-adic Spence-Kummer equation. The underlying geometry of this equation is the complement to the non-Fano arrangement

$$V_{\text{non-Fano}} := \mathrm{Spec}\left(\overline{K}\left[s_1, s_2, \frac{1}{s_1s_2(1-s_1)(1-s_2)(s_1-s_2)(1-s_1s_2)}\right]\right),$$

together with nine morphisms $\{f_i\}_{i=1,\ldots,9}$ from $V_{\text{non-Fano}}$ to $\mathbb{P}^1\backslash\{0,1,\infty\}$ defined as follows:

$$\begin{aligned}
&f_1(s_1,s_2) := \frac{s_1(1-s_2)^2}{s_2(1-s_1)^2}, && f_2(s_1,s_2) := s_1s_2, && f_3(s_1,s_2) := \frac{s_1}{s_2},\\
&f_4(s_1,s_2) := \frac{s_1(1-s_2)}{s_2(1-s_1)}, && f_5(s_1,s_2) := \frac{s_1(1-s_2)}{s_1-1}, && f_6(s_1,s_2) := \frac{1-s_2}{1-s_1},\\
&f_7(s_1,s_2) := \frac{1-s_2}{s_2(s_1-1)}, && f_8(s_1,s_2) := s_1, && f_9(s_1,s_2) := s_2.
\end{aligned}$$

Remark that the name of the "non-Fano" arrangement $s_1s_2(1-s_1)(1-s_2)(s_1-s_2)(1-s_1s_2)$ comes from the celebrated notion of the non-Fano matroid.

FIG 1. Key diagram

$$\begin{tikzcd}
V_{\mathrm{B}_3} \arrow[r, hook, "\substack{\text{open}\\ \text{immersion}}"] \arrow[d, two heads, "\substack{\text{finite}\\ \text{Galois}}"'] & V_{\text{non-Fano}}, \\
M_{0,5} &
\end{tikzcd}
\qquad
\begin{tikzcd}
\pi_1\left(V_{\mathrm{B}_3}\right) \arrow[r, two heads] \arrow[d, hook] & \pi_1\left(V_{\text{non-Fano}}\right) \\
\pi_1\left(M_{0,5}\right) \arrow[ur, dashed, bend right, "\substack{\text{taking}\\ \text{sub-quotient}}"'] &
\end{tikzcd}$$

We use the K-rational tangential base point

$$\vec{v} : \mathrm{Spec}\Big(K((t))\Big) \to V_{\text{non-Fano}}$$

over the $K(t)$-rational point (t^2,t). In Table 1, we identify $f_i\left(\vec{v}\right)$ with standard tangential base points of $\mathbb{P}^1\backslash\{0,1,\infty\}$ under the Galois equivalence $\approx$. Given a K-rational point $(x,y)\in V_{\text{non-Fano}}(K)$ and a path $\gamma_0\in\pi_1^{\text{top}}\left(V_{\text{non-Fano}}^{\text{an}};\vec{v},(x,y)\right)$, define the path family $\{\gamma_i\}_{i=1,\ldots,9}$ with respect to γ_0 by

$$\gamma_i := \delta_i\cdot f_i^{\text{an}}\left(\gamma_0\right)\in\pi_1^{\text{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\};\overrightarrow{01},f_i^{\text{an}}(x,y)\right)$$

where $\delta_i\in\pi_1^{\text{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\};\overrightarrow{01},f_i^{\text{an}}\left(\vec{v}\right)\right)$ are as in Table 1.

Then we get chain rules among ℓ-adic Galois associators:

$$\mathfrak{f}_\sigma^{f_i(x,y),\gamma_i}(e_0,e_1) = \left(\delta_i\cdot f_i\left(\mathfrak{f}_\sigma^{(x,y),\gamma_0}\right)\cdot\delta_i^{-1}\right)\cdot\mathfrak{f}_\sigma^{f_i(\vec{v}),\delta_i}(e_0,e_1).$$

To compute the ℓ-adic Galois associator $\mathfrak{f}_\sigma^{(x,y),\gamma_0}\in\pi_1^{\ell\text{-ét}}\left(V_{\text{non-Fano}},\vec{v}\right)$, we also consider a diagram (Figure 1) of three geometric objects: the affine variety $V_{\text{non-Fano}}$, the moduli space $M_{0,5}$, and the complement to the Coxeter B_3-arrangement

$$V_{\mathrm{B}_3} := \mathrm{Spec}\left(\overline{K}\left[s_1,s_2,\frac{1}{s_1s_2(1-s_1^2)(1-s_2^2)(s_1-s_2)(1-s_1s_2)}\right]\right).$$

Analyzing the above chain rules together with the computational method formulated by Nakamura-Wojtkowiak [NW12, Proposition 5.11], we obtain the functional equation of Theorem 2 below.

TAB 1. Fano to projective line: morphisms, tangential base points, and paths

i	$f_i(x,y)$	$f_i(\vec{v})$	$\delta_i \in \pi_1^{\mathrm{top}}\left(\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\};\overrightarrow{01}, f_i^{\mathrm{an}}(\vec{v})\right)$
1	$\frac{x(1-y)^2}{y(1-x)^2}$	$\overrightarrow{01} \approx f_1(\vec{v})$	$\delta_1 := 1$ (= trivial path)
2	xy	$\overrightarrow{01} \approx f_2(\vec{v})$	$\delta_2 := 1$
3	$\frac{x}{y}$	$\overrightarrow{01} = f_3(\vec{v})$	$\delta_3 := 1$
4	$\frac{x(1-y)}{y(1-x)}$	$\overrightarrow{01} \approx f_4(\vec{v})$	$\delta_4 := 1$
5	$\frac{x(1-y)}{x-1}$	$\overrightarrow{0\infty} \approx f_5(\vec{v})$	$\delta_5 := \delta_{\overrightarrow{0\infty}}$
6	$\frac{1-y}{1-x}$	$\overrightarrow{10} \approx f_6(\vec{v})$	$\delta_6 := \delta_{\overrightarrow{10}}$
7	$\frac{1-y}{y(x-1)}$	$\overrightarrow{\infty 0} \approx f_7(\vec{v})$	$\delta_7 := \delta_{\overrightarrow{\infty 0}}$
8	x	$\overrightarrow{01} \approx f_8(\vec{v})$	$\delta_8 := 1$
9	y	$\overrightarrow{01} = f_9(\vec{v})$	$\delta_9 := 1$

Theorem 2 (The ℓ-adic Spence-Kummer equation, [Shi23b])**.** *For any $\sigma \in G_K$, the following holds:*

$$\begin{aligned} &Li_3^\ell\left(\frac{x(1-y)^2}{y(1-x)^2};\gamma_1,\sigma\right) + Li_3^\ell(xy;\gamma_2,\sigma) + Li_3^\ell\left(\frac{x}{y};\gamma_3,\sigma\right) \\ &\quad - 2Li_3^\ell\left(\frac{x(1-y)}{y(1-x)};\gamma_4,\sigma\right) - 2Li_3^\ell\left(\frac{x(1-y)}{x-1};\gamma_5,\sigma\right) - 2Li_3^\ell\left(\frac{1-y}{1-x};\gamma_6,\sigma\right) \\ &\qquad - 2Li_3^\ell\left(\frac{1-y}{y(x-1)};\gamma_7,\sigma\right) - 2Li_3^\ell(x;\gamma_8,\sigma) - 2Li_3^\ell(y;\gamma_9,\sigma) + 2\zeta_3^\ell(\sigma) \\ &= -\rho_{y,\gamma_9}(\sigma)^2\rho_{\frac{1-y}{1-x},\gamma_6}(\sigma) + 2\zeta_2^\ell(\sigma)\rho_{y,\gamma_9}(\sigma) + \frac{1}{3}\rho_{y,\gamma_9}(\sigma)^3 - Li_2^\ell\left(\frac{x(1-y)}{x-1};\gamma_5,\sigma\right) \\ &\qquad - Li_2^\ell\left(\frac{1-y}{y(x-1)};\gamma_7,\sigma\right) + \frac{1}{2}\rho_{\frac{1-xy}{1-x},\gamma_5'}(\sigma) - \frac{1}{3}\rho_{y,\gamma_9}(\sigma). \end{aligned}$$

Remark 4. By interpreting the proof of the above ℓ-adic functional equations after replacing ℓ-adic Galois associators with complex KZ associators, we obtain an algebraic proof of the complex Landen's and Spence-Kummer's functional equations.

References

[NS] H. Nakamura, D. Shiraishi. *Landen's trilogarithm functional equation and ℓ-adic Galois multiple polylogarithms.* to appear in "Low Dimensional Topology and Number Theory" Springer Proceedings in Mathematics & Statistics.

[NW12] H. Nakamura, Z. Wojtkowiak, *Tensor and homotopy criteria for functional equations of ℓ-adic and classical iterated integrals.* Non-abelian fundamental groups and Iwasawa theory, 258–310, London Math. Soc. Lecture Note Ser., **393**, Cambridge Univ. Press, Cambridge, 2012.

[Shi23a] D. Shiraishi. *Duality-reflection formulas of multiple polylogarithms and their ℓ-adic Galois analogues.* to appear in Math. J. Okayama Univ. arXiv:2307.09403 [math.NT] (2023)

[Shi23b] D. Shiraishi. *Spence-Kummer's trilogarithm functional equation and the underlying geometry*, arXiv:2307.09414 [math.NT] (2023)
[Woj04] Z. Wojtkowiak, *On ℓ-adic iterated integrals, I – Analog of Zagier Conjecture*, Nagoya Math. J., **176** (2004), 113–158.
[Woj05a] Z. Wojtkowiak, *On ℓ-adic iterated integrals, II – Functional equations and ℓ-adic polylogarithms*, Nagoya Math. J., **177** (2005), 117–153.
[Woj05b] Z. Wojtkowiak, *On ℓ-adic iterated integrals, III – Galois actions on fundamental groups*, Nagoya Math. J., **178** (2005), 1–36.

Quasi-supersingular finite flat commutative group schemes and the Coleman conjecture on torsion points on curves

Naotake Takao

The Coleman conjecture [Col87], roughly speaking, asserts that the residue fields of torsion points on a curve with good reduction over an absolutely unramified complete discrete valuation field of mixed characteristics are unramified and, as an application, gives another proof of the Manin-Mumford conjecture (Raynaud's theorem [Ray83]) on the finiteness of torsion points on curves. Coleman proved the conjecture in the case that the residue characteristic is larger than twice the genus of the curve, or that the Jacobian has ordinary or superspecial (automatically good) reduction [Col87]. Tamagawa and Hoshi investigated the (generalized) conjecture under the situation where the curve may have stable reduction. Tamagawa achieved affirmative results in the case that the Jacobian has ordinary semistable reduction [Tam01], and Hoshi solved the (generalized) conjecture affirmatively in the case that the Jacobian has superspecial (good) reduction [Hos22].

In this report, we discuss possible strategies to solve the (generalized) conjecture in the case that the Jacobian has supersingular (good) reduction.

Let p be a prime greater than three and k a perfect field of characteristic p. Write W for the ring of Witt vectors with coefficients in k and K for the field of fractions of W. Let $\overline{K}$ be an algebraic closure of K and write I_K for the inertia subgroup of the absolute Galois group of K determined by $\overline{K}$. Let X be a proper smooth geometrically connected curve over K of genus g greater than one and write J for its Jacobian variety. Given $x_0 \in X(K)$, we have the Albanese embedding $\iota_{x_0} : X \hookrightarrow J,\ x \mapsto [x - x_0]$. Write $J(\overline{K})_{\mathrm{tors}}$ for the torsion subgroup of $J(\overline{K})$ and X_{tors} for $\iota_{x_0}(X)(\overline{K}) \cap J(\overline{K})_{\mathrm{tors}}$.

1. Quasi-supersingular finite flat commutative group schemes

Motivated by Hoshi's solution of the (generalized) Coleman conjecture in the case that J has superspecial (good) reduction (cf. [Hos22], Theorem E), we consider the following problem:

Problem 1. Is the action of I_K on X_{tors} trivial if J has supersingular (good) reduction over K?

We try to approach this problem in the same way as Hoshi's strategy in the proof of [Hos22], Theorem E. We refer to this strategy as the [Hos22]-strategy, tentatively in this report. To explain the strategy, we prepare a few terminologies. Let n be a non-negative integer and $\mathcal{G}$ a p-torsion finite flat commutative group scheme over W of rank p^{2n}. Write G for the special fiber of $\mathcal{G}$.

Definition 1.

(1) Let $\mathcal{E}$ be an elliptic curve over W. We shall say that $\mathcal{E}$ is *supersingular* if the special fiber of $\mathcal{E}$ is a supersingular elliptic curve over k.

(2) We shall say that $\mathcal{G}$ (respectively, G) is *superspecial* if the following condition is satisfied: there exist supersingular elliptic curves $\mathcal{E}_i/W$ (respectively, E_i/k) $(0 < i \leq n)$ such that

$$\mathcal{G} \simeq \oplus_{0<i\leq n}\mathcal{E}_i[p] \quad (\text{respectively, } G \simeq \oplus_{0<i\leq n}E_i[p]).$$

Here, for a commutative group scheme A/T and a positive integer m, we write $A[m]$ for the kernel of $m_A : A \to A$, where m_A stands for the multiplication by m.

(3) We shall say that $\mathcal{G}$ (respectively, G) is *quasi-supersingular* if the following condition is satisfied: there exist a sequence of p-torsion finite flat commutative group schemes over W (respectively, k)

$$\mathcal{G} = \mathcal{G}_n \supset \mathcal{G}_{n-1} \supset \cdots \supset \mathcal{G}_1 \supset \mathcal{G}_0 = 0$$

$$(\text{respectively, } G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = 0)$$

and supersingular elliptic curves $\mathcal{E}_i/W$ (respectively, E_i/k) $(0 < i \leq n)$ such that

$$\mathcal{G}_i/\mathcal{G}_{i-1} \simeq \mathcal{E}_i[p] \quad (\text{respectively, } G_i/G_{i-1} \simeq E_i[p])\ (0 < i \leq n).$$

For a quasi-supersingular $\mathcal{G}$ (respectively, G), we shall call a sequence as above a *qss sequence* of $\mathcal{G}$ (respectively, G).

(4) When the dimensions of the simple factors of the semisimplification of the action of I_K on the group of $\overline{K}$-rational points of the generic fiber $\mathcal{G}_K$ of $\mathcal{G}$ are $n_1 \geq n_2 \geq \cdots$, we shall refer to $[n_1, n_2, \ldots]$ as *the Raynaud type* of $\mathcal{G}_K$.

The outline of the proof of [Hos22], Theorem E is as follows: First, Hoshi reduces the proof to examining p-torsion points by the following remarkable theorem:

Theorem 1 ([Hos17], Theorem B)**.** *If J has good reduction over K, I_K acts on pX_{tors} trivially.*

Second, he studies the action of I_K on $J[p](\overline{K})$ by Raynaud's classification [Ray74], and proves that I_K acts on X_{tors} trivially when the Raynaud type of $J[p]$ is $[2, 2, \ldots]$. Finally, he proves that the Raynaud type of $J[p]$ is $[2, 2, \ldots]$ if J has superspecial reduction over K by proving the following theorem:

Theorem 2 ([Hos21], Theorem 4.10 (i))**.** *The following are equivalent:*

(1) $\mathcal{G}$ is superspecial. *(2) G is superspecial.*

To approach Problem 1 by the [Hos22]-strategy, it is enough to prove the supersingular version of Theorem 2. However, we get the following result:

Proposition 1. *Suppose that $n \geq 2$ and k is algebraically closed. Consider the following conditions:*

(1) $\mathcal{G}$ is quasi-supersingular. (2) G is quasi-supersingular.

Then (1) implies (2), but (2) does not imply (1) in general.

The proof of Proposition 1 is based on the theory of finite Honda systems (cf. [FL82] §9.4, [Hos21] Remark 3.5.1), which gives a classification of liftings of finite flat commutative group schemes over k. By using this theory, together with the following lemma, we obtain a necessary condition for a qss sequence of a certain type of (quasi-supersingular) p-torsion finite flat commutative group scheme over k to lift to one over W:

Lemma 1. *Suppose that k is algebraically closed. Let H be a quasi-supersingular p-torsion finite flat commutative group scheme over k of rank p^{2n} and $(H_i)_{i=0,\dots,n}$ a qss sequence of H. Write (M, F, V) and (M_i, F_i, V_i) $(0 \leq i \leq n)$ for the Dieudonné modules of H and H/H_{n-i}, respectively. Then they form a sequence of Dieudonné modules $M = M_n \supset M_{n-1} \supset \cdots \supset M_1 \supset M_0 = 0$, and there exists a basis e_i, f_i $(0 < i \leq n)$ of M (as a k-linear space) which satisfies the following conditions*

- *M_i/M_{i-1} is generated by $e_i + M_{i-1},\ f_i + M_{i-1}$ in M/M_{i-1}*
- $F(f_i) = 0$
- $F(e_i) \equiv f_i \bmod \langle\{e_j;\ 0 < j < i\}\rangle$
- $V(e_i) \equiv f_i \bmod \langle\{f_j;\ 0 < j < i\}\rangle$

for each $0 < i \leq n$. Here, $\langle S\rangle$ denotes the k-linear subspace generated by S, for a subset $S \subset M$.

Proposition 1 and its proof suggest that, for "most" X (whose Jacobian has supersingular reduction), the [Hos22]-strategy would not work as it is.

2. Other strategies

In this section, we shall discuss possible new ideas to overcome the obstacle raised by Proposition 1 and to solve Problem 1.

2.1. **Self-duality of $J[p]$.** Although J has a natural principal polarization, this fact is not reflected in Proposition 1. It would therefore be natural to examine whether conditions (1) and (2) in Proposition 1 are equivalent under the extra assumption that $\mathcal{G}$ and G are self-dual. However, we get the following result by calculations based on Lemma 1:

Proposition 2. *Suppose that $n \leq 2$. If G is quasi-supersingular, then G and $\mathcal{G}$ are automatically self-dual.*

This proposition, together with Proposition 1, implies that the [Hos22]-strategy would not work for Problem 1 when $g = 2$ even if self-duality is taken into account. We wonder whether the assertion of Proposition 2 is true for $n \geq 3$. (If it is true, we have to say that the [Hos22]-strategy would not work even if self-duality is taken into account.)

2.2. **The Raynaud type of $J[p]$.** The Coleman conjecture is a conjecture on the action I_K on X_{tors}. Thus, it is closely related to the Galois representation for the generic fiber of the Jacobian of a given curve. Hence, (taking Theorem 1 into consideration,) it is also natural to approach Problem 1 by Raynaud's description of the Galois representation associated with the generic fiber of a p-torsion finite flat commutative group scheme.

In view of the Raynaud type of $J[p]$, Tamagawa's research [Tam01] is in the case that the type is $[1, 1, \ldots]$ and Hoshi's research [Hos22] is in the case that the type is $[2, 2, \ldots]$. When $g = 2$, all the possible Raynaud types are

$$[4], \quad [3,1], \quad [2,2], \quad [2,1,1], \quad [1,1,1,1].$$

Because J is principally polarized, $J[p]$ is self-dual and the case that the Raynaud type is $[3, 1]$ does not appear. Because J has supersingular reduction, the p-rank of the special fiber of (the Néron model of) J is 0 and the case that the Raynaud type is $[2, 1, 1]$ or $[1, 1, 1, 1]$ does not appear. The case that the Raynaud type is $[2, 2]$ has already been settled by Hoshi. Thus, what remains is the case that the Raynaud type is $[4]$. We obtain the following result by proving that the image of the action of I_K on $J[p](\overline{K})$ contains $\mathbb{F}_p^\times$ using Raynaud's classification [Ray74] and self-duality of $J[p]$:

Theorem 3. *Suppose that $g = 2$. Then the answer to Problem 1 is affirmative.*

We wonder whether the answer to Problem 1 is affirmative in the case that $g \geq 3$ and the type is $[2g]$.

References

[Col87] R. F. Coleman, *Ramified torsion points on curves*, Duke Math. J. **54** (1987), no. **2**, 615–640.

[FL82] J.-M. Fontaine, G. Laffaille, *Construction de représentations p-adiques*, Ann. Sci. École. Norm. Sup. (4) **15** (1982), no. **4**, 547–608.

[Hos17] Y. Hoshi, *On ramified torsion points on a curve with stable reduction over an absolutely unramified base*, Osaka J. Math. **54** (2017), no. **4**, 767–787.

[Hos21] Y. Hoshi, *Pseudo-rigid p-torsion finite flat commutative group schemes*, J. Number Theory **229** (2021), 261–276.

[Hos22] Y. Hoshi, *Ramification of torsion points on a curve with superspecial reduction over an absolutely unramified base*, Tohoku Math. J. (2) **74** (2022), no. **4**, 521–534.

[Tam01] A. Tamagawa, *Ramification of torsion points on curves with ordinary semistable Jacobian varieties*, Duke Math. J. **106** (2001), no. **2**, 281–319.

[Ray74] M. Raynaud, *Schémas en groupe de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

[Ray83] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), no. **1**, 207–233.

Algebraic Dependence and Milnor K-theory

Adam Topaz

1. Introduction

Let F be a field. The *Milnor K-theory of F* is an object defined in term of both the multiplicative and additive structure of F,

$$\mathrm{K}_*^{\mathrm{M}}(F) := \frac{\mathrm{T}_*(F^\times)}{\langle x \otimes y \mid x + y = 1 \rangle},$$

where T_* denotes the Tensor algebra of the $\mathbb{Z}$-module $F^\times$. This object is a graded-commutative ring satisfying $\mathrm{K}_1^{\mathrm{M}}(F) = F^\times$. Thus, the multiplicative structure of F is (trivially) determined by its Milnor K-theory. The question of whether or not one can also recover the *additive structure* is a whole different matter, and turns out to be quite an interesting question. This issue was studied in the past by Bogomolov-Tschinkel [BS08] and, more recently, by Cadoret-Pirutka [CP21] who show that the answer is positive for higher-dimensional function fields over algebraically closed fields or over finite fields.

The main result I discussed in this report, which can be found in [Top23, Main Thorem], gives a positive answer in many more situations. This is its statement:

Theorem 1. *Let F be any field whose prime subfield is k_0, and assume that $F|k_0$ has transcendence degree ≥ 5. Let F^i denote the perfect closure of F. Then the isomorphism type of F^i is determined by the graded $\mathbb{Q}$-algebra $\mathrm{K}_*^{\mathrm{M}}(F) \otimes \mathbb{Q}$.*

The main feature that sets this theorem apart from previous results in this area is in the minimal assumptions on the field F. While both Bogomolov-Tschinkel [BS08] and Cadoret-Pirutka [CP21] essentially work with higher-dimensional function fields, the result above works even for (sufficiently large) *algebraically closed* fields.

As usual in anabelian geometry, the process which reconstructs the field from its Milnor K-theory in the proof of this theorem is actually *functorial* in a suitable sense. However, as soon as F is multiplicatively divisible, the quotient $F^\times/\mathrm{torsion}$ becomes a vector space over $\mathbb{Q}$, and thus multiplication by nonzero rationals in degree 1 give rise to indeterminacy in such a functorial statement. In order to control for such indeterminacy, one is essentially forced to tensor $\mathrm{K}_*^{\mathrm{M}}(F)$ with $\mathbb{Q}$ in order to obtain the uniform statement above. Once this happens, it's impossible to distinguish between F and F^i as the map $F \to F^i$ induces an isomorphism on rationalized Milnor K-theory. Because of this, the fact that one can only reconstruct F^i as opposed to F is rather expected.

Having said that, I expect that the assumption on the *transcendence degree* of F can be reduced quite significantly, as formulated in the following conjecture.

Conjecture 1. *Suppose that F is any field of Kronecker dimension ≥ 2. Then the isomorphism type of F^i is determined by the graded $\mathbb{Q}$-algebra $\mathrm{K}_*^{\mathrm{M}}(F) \otimes \mathbb{Q}$.*

2. The fundamental theorem of projective geometry, applied to function fields

Before I go into the strategy of the proof of the main theorem, let me roughly go over the arguments of Bogomolov-Tschinkel [BS08] and Cadoret-Pirutka [CP21], in the case of function fields over algebraically closed fields. In this context, one works with a function field K over a base-field $k = \bar{k}$, potentially satisfying some additional assumptions. The first step in these proofs is to use the information encoded in $\mathrm{K}^{\mathrm{M}}_*(K)$ to obtain the binary relation on elements of K given by algebraic dependence over k. To accomplish this, one can use the relationship between Milnor K-theory and ℓ-adic Galois cohomology of K, which remains sufficiently nontrivial in this context.

At this point, the context is generalized. Namely, we work with a function field $K|k$ where k is perfect, and attempt to recover K from $K^\times/k^\times$ as a multiplicative group endowed with the algebraic dependence relation described above. This is indeed possible in this level of generality, as shown in the work of Cadoret-Pirutka [CP21, Theorem 4]. Among the final key steps is the use of the *fundamental theorem of projective geometry*, applied to $K^\times/k^\times$ considered as the projectivization of K as a vector space over k. This recovers the field structure on k and the k-module structure of K, while the compatibility with the multiplicative structure of $K^\times/k^\times$ ensures that the field structure on K is recovered as well.

The proof of Theorem 1 follows the same overall approach, with a few key differences. Namely, just as in the strategy above, one first recovers information about algebraic dependence from Milnor K-theory. In our context, since we are working over very general fields whose cohomological dimension may even be 0, we can't use techniques similar to the approaches above. Nevertheless, one is indeed able to reconstruct *all information* about algebraic dependence in K over its prime subfield, starting with the (rationalized) Milnor K-theory ring of K (under mild assumptions on the transcendence degree). One then concludes by applying a remarkable theorem due to Evans-Hrushovski [EH91, EH95], extended by Gismatullin [Gis08], which shows that, again under suitable assumptions on the transcendence degree, this is sufficient to determine the field in question up-to purely inseparable extensions. This result of Evan-Hrushovski and Gismatullin could very well be considered as a (much more difficult) cousin of the fundamental theorem of projective geometry.

3. On algebraic dependence

To conclude this report, I'll give some details from the proof showing that algebraic dependence can be recovered form Milnor K-theory. To fix notation, let's take an *arbitrary* extension of fields $K|k$ with k relatively algebraically closed in K, and consider the following variant of Milnor K-theory:

$$\mathcal{K}_*(K|k) := \frac{\mathrm{K}^{\mathrm{M}}_*(K) \otimes \mathbb{Q}}{\langle k^\times \rangle}.$$

Here $\langle k^\times \rangle$ refers to the ideal generated by the image of $k^\times$ in degree 1.

Suppose that v is a K-valuation with unit group U_v, value group $\Gamma_v = K^\times/U_v$, and consider the canonical map

$$\wedge^*(\mathbb{Q} \otimes \Gamma_v) \to \frac{\mathcal{K}_*(K|k)}{\langle U_v \rangle}$$

induced by the obvious isomorphism in degree 1.

Lemma 1. *The map $\wedge^*(\mathbb{Q} \otimes \Gamma_v) \to \mathcal{K}_*(K|k)/\langle U_v \rangle$ described above is an isomorphism.*

Proof. This is a straightforward consequence of the ultrametric inequality. □

From this it is not too hard to obtain the following:

Lemma 2. *Suppose that $f_1, \dots, f_n \in K^\times$ are algebraically independent over k. Then $\{f_1, \dots, f_n\} \in \mathcal{K}_n(K|k)$ is nontrivial.*

Here the symbol $\{f_1, \dots, f_n\}$ refers to the product of the images of f_i in $\mathcal{K}_*(K|k)$, with the usual notation borrowed from Milnor K-theory.

Proof. One can find a discrete rank n k-valuation on $k(f_1, \dots, f_n)$ where the images of $f_1, \dots, f_n$ form a basis for its value group. Extend this to a valuation v of K. The image of $\{f_1, \dots, f_n\}$ in $\mathcal{K}_*(K|k)/\langle U_v \rangle$ is nontrivial by the Lemma 1, and this shows that $\{f_1, \dots, f_n\}$ must be nonzero in $\mathcal{K}_*(K|k)$. □

This at least tells us that *some* information about algebraic dependence can be recovered from $\mathcal{K}_*(K|k)$. Next, one detects valuations of K using $\mathcal{K}_*(K|k)$, by applying techniques similar to previously developed *local* results in birational anabelian geometry. One then uses the data obtained by detecting said valuations in order to upgrade the partial information about algebraic dependence discussed above, in order to recover *all possible* information about algebraic dependence in $K|k$. The precise recipes are quite involved, so I won't expand beyond this vague description; the interested reader may refer to [Top23, §3-§4].

Finally, note that in the above we worked with $\mathcal{K}_*(K|k)$, and indeed one obtains a *relative* anabelian result showing that $K^i|k^i$ is determined by this object when $K|k$ has transcendence degree ≥ 5, see [Top23, §5]. To obtain an *absolute* result as explained in Theorem 1, a bit of additional work is required to recover the kernel of the canonical map

$$\mathbb{Q} \otimes \mathrm{K}_*^{\mathrm{M}}(K) \to \mathcal{K}_*(K|k),$$

where k is the relative algebraic closure of the prime subfield of K, using only the graded $\mathbb{Q}$-algebra $\mathbb{Q} \otimes \mathrm{K}_*^{\mathrm{M}}(K)$; see [Top23, §5] for more details. This then reduces the absolute case to the relative case, which was already resolved.

References

[BS08] F. Bogomolov and Y. Tschinkel, *Milnor K_2 and field homomorphisms*, Geometry, analysis, and algebraic geometry. MA, USA, May 2008. MA: International Press, 2009, pp. 223–244.

[CP21] A. Cadoret and A. Pirutka, *Reconstructing function fields from Milnor K-theory*, Algebra Number Theory **15** (2021), no. 9, 2261-2288.

[EH91] D. Evans and E. Hrushovski, *Projective planes in algebraically closed fields*, Proc. Lond. Math. Soc. (3) 62 (1991), no. 1, 1–24.

[EH95] D. Evans and E. Hrushovski, *The automorphism group of the combinatorial geometry of an algebraically closed field*, J. Lond. Math. Soc., II. Ser. 52 (1995), no. 2, 209–225.

[Gis08] J. Gismatullin, *Combinatorial geometries of field extensions*, Bull. Lond. Math. Soc. 40 (2008), no. 5, 789–800.

[Top23] A. Topaz, *Algebraic dependence and Milnor K-theory*, arXiv:2211.14665 [math.KT] 23 p, (2023).

Reporters: Shun Ishii (Kyoto) and Béranger Seguin (Oberwolfach)