Mathematisches Forschungsinstitut Oberwolfach

Report No. 12/2021

DOI: 10.4171/OWR/2021/12

Homotopic and Geometric Galois Theory

Organized by
Benjamin Collas, Kyoto
Pierre Dèbes, Villeneuve d'Ascq
Hiroaki Nakamura, Osaka
Jakob Stix, Frankfurt

7 March – 13 March 2021

Abstract. In his "Letter to Faltings", Grothendieck lays the foundation of what will become part of his multi-faceted legacy to arithmetic geometry. This includes the following three branches discussed in the workshop: the arithmetic of Galois covers, the theory of motives and the theory of anabelian Galois representations. Their geometrical paradigms endow similar but complementary arithmetic insights for the study of the absolute Galois group $\mathrm{G}_{\mathbb{Q}}$ of the field of rational numbers that initially crystallized into a functorially group-theoretic unifying approach. Recent years have seen some new enrichments based on modern geometrical constructions – e.g. simplicial homotopy, Tannaka perversity, automorphic forms – that endow some higher considerations and outline new geometric principles. This workshop brought together an international panel of young and senior experts of arithmetic geometry who sketched the future desire paths of homotopic and geometric Galois theory.

Mathematics Subject Classification (2010): 12F12, 14G32, 14H30, 14H45 (Primary); 14F05, 55Pxx, 14F22, 11F70, 14F42 (Secondary).

Introduction by the Organizers

Understanding the absolute Galois group $\mathrm{G}_{\mathbb{Q}}$ by geometric means is a broad program, which, since Grothendieck, has been developed along three parallel branches: *(a) the Arithmetic of Galois Covers*, *(b) the Motivic Galois Representations*, and *(c) Anabelian Geometry.* The workshop *Homotopic and Geometric Galois Theory* dealt with recent progress around these branches, which in fact showed reuniting trends *towards a new geometry of Galois symmetries of spaces.* Essential concepts crystallize the existence of cross-bridging principles, which are pushing the seminal programs of the three branches beyond their original frontiers. The specifics of higher dimensions and stacks symmetries act as one joint guiding beacon, the search for unified minimal and functorial anabelian constructions as a second one, confrontation with key seminal objects and results as a third one.

Overview. A previous 2018 Oberwolfach mini-workshop – *Arithmetic Geometry and Symmetries around Galois and Fundamental Groups* – had reported on the most striking developments and connections of the three branches:

(a) the success for supersolvable groups of the Colliot-Thélène approach to the Noether program (Harpaz-Wittenberg), a realizing-lifting-parametrizing program pushing further the Hilbert specialization method (Dèbes, Fried, et al.), Tannakian considerations within $\mathbb{Q}_\ell$-perverse sheaves (Dettweiler et al.), the use of patching methods for local-global issues (Harbater et al.);
(b) the motivic constructions of given Tannaka groups using automorphic and perverse techniques (Yun, Patrikis, Katz), the use of p-adic or ultraproduct techniques (Cadoret, Ambrosi) to study ℓ-adic motives, the characterization of geometric representations in deformation rings (Litt), the proof of a Deligne conjectured fixed-point counting formula (Yu);
(c) the successful introduction of methods from étale homotopy theory (Schmidt-Stix) and from motivic homotopy theory for moduli stacks of curves (Collas), the import of operads (Fresse-Horel), a computable echo of the Galois techniques in the Ihara/Oda-Matsumoto problem (Pop) and of anabelian group-theoretic reconstructions (Hoshi, Mochizuki).

Building on this first round of investigations, the 2021 workshop provided more mature encounters that resulted *in a unifying view of these topics.* With the goal of exploiting new arithmetic-geometric symmetries – in *higher dimension*, in *higher categories* – as a common guide, the set of contributions revealed the hidden desire paths of homotopic and geometric Galois theory: there is *a return from Grothendieck's classical group-theoretic legacy to a new "geometrification" of Arithmetic Geometry.* For example, the workshop showed

– the *application of classical approaches* – e.g. formal patching, the "realizing-lifting-parametrizing" program for covers, a section conjecture in localisation – *beyond their original geometric frontier*;

– constructions in *anabelian geometries with an essential abelian nature* – e.g. abelian-by-central extensions, anabelian-motivic use of étale types;

– the *intermingling of analytic and étale Tannaka symmetries* – e.g. the use of automorphic forms in étale local systems;

– the *(re)construction of new arithmetic-geometry contexts* – e.g. the recent developments of anabelian geometry towards understanding $\widehat{GT}$ and $G_{\mathbb{Q}}$.

The presentations. The workshop developed in three *movements*[1] that, in order to set the tone, we formulate as follows: the first movement in *the arithmetic of*

[1]The original branches are now so intermingled that the word "movement" seems appropriate. We also allude to the remark of an eminent researcher in the field who spoke of the *MFO symphony* in describing the magical atmosphere of in-person workshops at MFO.

(mostly) finite covers, the second movement of *motivic aspects of Galois representations*, and the third movement with *Galois theory of arithmetic fundamental groups* including in particular aspects of *anabelian geometry.*

The talk schedule started with Karemaker's presentation on the towers of iterated Belyĭ maps and their Galois groups in terms of arboreal representations. Bary-Soroker addressed the topic of the distribution of Galois groups of *random polynomials* starting from the original contribution of van der Waerden to the latest results and some new heuristics.

A few talks focused on complementary aspects of the *realizing-lifting-parametrizing program for Galois covers*, which all originated in the Hilbert's Irreducibility Theorem (HIT). Legrand explained to what extent, for a given finite Galois cover f of $\mathbb{P}^1_{\mathbb{Q}}$ with group G, "almost all" Galois extensions of $\mathbb{Q}$ with group G do not occur as specializations of f (in connection to the *abc-conjecture* and *Malle's conjecture*). Dèbes discussed a version "over the ring" of HIT that relates to a polynomial analog of the Schinzel hypothesis. König explained how, together with Neftin, he could handle the decomposable case of the Hilbert-Siegel problem on the exceptional specialization set. Neftin discussed new arithmetic dimensions for finite groups, which measure the existence of Galois parametrizing field extensions of small transcendence degree, and which he compared with the essential dimension. Fehm reported on *the minimal ramification problem* for a finite group G, which asks for the minimal number of ramified primes in a G-Galois extension. He mostly considered the special situation the base field is $\mathbb{F}_q(t)$ and G is S_n or A_n.

Fried explained how he could refine the original *Modular Tower program* by introducing ℓ-Frattini lattice quotients. This allows, starting from modular curves, to capture the full relation between the regular inverse Galois problem and precisely generalizing Serre's Open Image Theorem.

A. Hoshi gave a survey of recent developments in the *rationality problem for fields of invariants*, e.g. Noether's problem, rationality problem for algebraic tori, rationality problem for quasi-monomial actions; he notably showed negative results by using such birational invariants as flabby class and unramified Brauer group, but also some coming from 2 and 3 dimensional group cohomology. Harbater showed how *patching methods*, originally designed for inverse Galois theory, can also be used for direct Galois theory; a main example he developed was about the local-global principle: if a G-torsor is locally trivial, must it be trivial?

Several talks dealt with *motivic aspects of Galois representations*, which are at once of algebraic and analytic in nature – see the (algebraic cycles) Tate and (automorphic forms) Langlands conjectures respectively. The realization of exceptional Lie groups (Yun, Patrikis et al.) and a back-and-forth from Galois to Tannaka (Collas, Dettweiler et al., see MFO18 report), sketches some bridges, but interconnections run *structurally deeper.* A coherent net of conjectures provides indeed a multi-faceted insight of the motivic properties of ℓ-adic representations: in terms of deformation of local systems (via Simpson's rigidity-integrality of motivic nature, Patrikis et al.), of the isotypicity of cusp forms for a Lefschetz-like trace formula (via global Langlands, Yu), or of family of Picard groups (via Tate-conjecture for K3 surfaces, Tang et al.). We refer to Cadoret's work (joint with Tamagawa) on the theory of local systems with ultra-product and (over)convergent coefficients that illustrates further the interplay of these Tannaka, Frobenius weight, Langlands/companions theories. Collas displayed a blackboard from étale topological type to Morel-Voevodsky motivic homotopy type for schemes and stacks, emphasizing how the Quillen formalism connects functorially the anabelian and cohomological contexts in terms of Grothendieck's conjectures.

New *anabelian geometry with minimalistic or close-to-abelian* insights were explained in several talks. Lüdkte reported on minimalistic anabelian geometry for localised p-adic curves, a result in between the birational case and the case of p-adic algebraic curves. Topaz explained (joint work with Pop) how a two-step version for complements of line arrangements on the plane allows to complete Pop's pro-ℓ abelian-by-central variant of the Ihara/Oda-Matsumoto problem leading to a new "linear Grothendieck-Teichmüller group" and thus a new $G_{\mathbb{Q}}$-characterization. Pop presented work (joint with Topaz) on a minimalistic Saïdi-Tamagawa's m-step Neukirch-Uchida theorem.

In a reverse direction, Horel discussed a non-trivial action of $\widehat{\mathrm{GT}}$ on the configuration category of $\mathbb{R}^d$ $(d \geq 2)$ and reported an application to computing the higher homotopy groups of the space of knots in $\mathbb{R}^d$ localized at a prime via the Goodwillie-Weiss manifold calculus.

A series of talks presented more variants of the latest results in anabelian geometry of curves and configuration spaces: Y. Hoshi reported a new class of geometric objects, the quasi-tripods, that provides relative and absolute anabelian results in higher dimensions. Sawada discussed how the graded Lie algebra structure associated to a fundamental group recovers the geometric type of configuration spaces of a hyperbolic curve. Minamide reported a result determining the outer automorphism group of a profinite braid group in terms of the profinite Grothendieck-Teichmüller group $\widehat{\mathrm{GT}}$.

Balakrishnan reported on recent progress on the quadratic Coleman-Chabauty-Kim p-adic integration method for Diophantine problems and for new applications to the determination of rational points on modular curves. The question of single valued constructions in terms of canonical path in the archimedean and p-adic and tropical settings of iterated integration was presented by Litt – see also Litt's MFO18 report. Pries presented formulas that describe the Galois actions on mod p central series of the fundamental group of a Fermat curve in view of Anderson's work. She illustrated their consequences with computational applications and open questions. Considering the Anderson-Ihara-Wojtkowiak ℓ-adic Galois associator, where Coleman-type iterated integral theory is unavailable, Nakamura discussed functional equations between ℓ-adic Galois multiple polylogarithmic functions on the absolute Galois group.

Poster session for Oberwolfach Leibniz Fellows. In addition to the oral communications above, *a poster session* via the Slack workspace was organized for the OWLG fellows to introduce their field of research: (1) Philip uses ℓ-adic monodromy techniques to study the *semi-stability degree of abelian varieties* over number fields; (2) SHIRAISHI develops the ℓ-adic *Galois polylogarithms for a reciprocity law* of the triple ℓth power residue symbols; and (3) YUJI deals with the *categorical reconstruction of a scheme S* being given its abstract category of S-schemes Sch_S.

A workshops that never sleeps. Over the week, the online workshop gathered 37 participants distributed over 3 main time-zones (US: 9, EU: 18, JP: 10). The program consisted of 26 forty-minutes presentations each one followed by a twenty-minute extension time for informal discussion with the audience. Most of the talks were given live on `Zoom`, at least one was pre-recorded, and due to some technical problem, one was even a one-blackboard presentation.

The recordings of the talks were paired with a dedicated `HGGT-MFO21 slack workspace` for *asynchronous* comments and questions, and with 2 three-hours daily "gather sessions" on `gather.town` for *live encounters* of all the participants.

Thanks to the commitment of the participants (with an average of 21 ± 3 participants per talk, full 20-minute discussions for all talks, and $\sim 1\ 500$ slack messages (25% private) over 5 days), it resulted in some lively stimulating exchanges, some fierce discussions, and *a HGGT workshop that never sleeps.*

This workshop confirmed the momentum initiated in the previous MFO18 mini-workshop and in the Tatihou meeting on *Field Arithmetic and Arithmetic Geometry* ("Rencontres arithmétiques de Caen 2019"). Following the strong support and feedback of the participants, agreement has been made to meet again within the next two years for reporting on the new research lines that appeared during this workshop.

Acknowledgement: 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-1641185, "US Junior Oberwolfach Fellows". This workshop was partially supported by JSPS KAKENHI Grant Number JP20H00115. The organizer BC is grateful to Anna Cadoret for sharing with him, in 2019, her enlightening views on the second movement.

Homotopic and Geometric Galois Theory

Table of Contents

Valentijn Karemaker (joint with Irene Bouw, Özlem Ejder)
Arboreal Galois representations 9

François Legrand (joint with Joachim König)
Density results for specialization sets of Galois covers 12

Michael D. Fried
The Modular Tower version of the Fried-Serre Lift invariant 15

Daniel Litt
Hodge, p-adic, and tropical iterated integrals 18

Pierre Dèbes (joint with Arnaud Bodin, Joachim König, Salah Najib)
On the Hilbert property over rings and the Schinzel hypothesis 20

Akinari Hoshi
Rationality problem for fields of invariants 23

Stefan Patrikis (joint with Christian Klevdal)
G-rigid local systems are integral 26

Arno Fehm (joint with Lior Bary-Soroker, Alexei Entin)
The minimal ramification problem for function fields 29

Martin Lüdtke
The p-adic section conjecture for localisations of curves 32

Joachim König (joint with Danny Neftin)
On the exceptional set in Hilbert's Irreducibility Theorem 35

Hiroaki Nakamura
Some aspects of arithmetic functions in Grothendieck-Teichmüller theory 38

Danny Neftin (joint with Pierre Débes, Francois Legrand, Joachim König)
The parametric dimension 40

Hongjie Yu
Irreducible automorphic representations with prescribed local behaviours 42

Yunqing Tang (joint with Ananth Shankar, Arul Shankar, Salim Tayou)
Reductions of K3 surfaces over number fields 44

Adam Topaz (joint with Florian Pop)
A linear variant of GT 47

Benjamin Collas
Simplicial and homotopical aspects of arithmetic geometry 50

Koichiro Sawada
Reconstruction of invariants of configuration spaces of a hyperbolic curves from associated Lie algebras 53

Arata Minamide (joint with Hiroaki Nakamura)
The outer automorphism groups of the profinite braid groups 55

Jennifer S. Balakrishnan
Iterated p-adic integration and rational points on curves 57

Anna Cadoret
Tannakian Cebotarev density theorems 58

David Harbater (joint with Jean-Louis Colliot-Thélène, Julia Hartmann, Daniel Krashen, R. Parimala, V. Suresh)
Galois theory, patching, and local-global principles 63

Lior Bary-Soroker
Probabilistic Galois theory 66

Geoffroy Horel
The Grothendieck-Teichmüller group in topology 67

Yuichiro Hoshi
The absolute anabelian geometry of quasi-tripods 69

Rachel Pries (joint with Rachel Davis, Vesna Stojanoska, Kirsten Wickelgren)
Galois action on the étale fundamental group of the Fermat curve 72

Florian Pop (joint with Adam Topaz)
Towards minimalistic Neukirch and Uchida theorems 75

Abstracts

Arboreal Galois representations

Valentijn Karemaker
(joint work with Irene Bouw, Özlem Ejder)

1. Motivation: dynamical sequences

A *dynamical sequence* in a field K is a sequence $\{a_i\}_{i\geq 1}$ with $a_i \in K$ such that $a_i = f(a_{i-1})$ for some map $f : K \to K$. Prime divisors of entries of such sequences were studied from the 1970's, starting with linear recurrences, and were first studied using Galois theory by Odoni in [Odo85] in the 1980's.

For any set S of prime numbers, let $\delta(S)$ denote its natural density if it exists. Also denote the nth iterate of the map f by f^n. For dynamical sequences in $\mathbb{Q}$, the Chebotarev density theorem yields the observation

$$\delta(\{p \text{ prime s.t. } a_i \equiv a \pmod p \text{ for some } i \geq 1\}) \leq$$
$$\delta(\{p \text{ prime s.t. } a_i \not\equiv a \pmod p,\ i \leq n-1, \text{ and } f^n(x) - a \text{ has a root modulo } p\})$$

for any $a \in \mathbb{Q}$. This shows the usefulness of Galois theory in studying the density of prime divisors of dynamical sequences. We do this for a particular class of maps.

2. Dynamical Belyi maps

A *Belyi map* is a finite cover $f : X \to \mathbb{P}^1$ of smooth projective curves over $\mathbb{C}$ that is branched exactly over $x_1 = 0$, $x_2 = 1$, and $x_3 = \infty$. By Belyi's theorem, the curve X is defined over $\overline{\mathbb{Q}}$ if and only if there exists a Belyi map $f : X \to \mathbb{P}^1$. We consider a special kind of Belyi maps:

Definition 1. A *dynamical Belyi map* f satisfies the following conditions:

(1) We have $X = \mathbb{P}^1$, that is, the Belyi map has genus zero.
(2) The map is *single cycle*, i.e., there is a unique ramification point over each of the three branch points.
(3) The map is *normalized*, i.e., its ramification points are $0, 1, \infty$, and moreover $f(0) = 0$, $f(1) = 1$, and $f(\infty) = \infty$.

A dynamical Belyi map f has a *(combinatorial) type*, which is the tuple $(d; e_1, e_2, e_3)$, where $d = \deg(f)$ and e_i is the ramification index of the unique ramification point above x_i. Without loss of generality we may assume that $e_1 \leq e_2 \leq e_3$. The Riemann–Hurwitz formula implies that the type of a single-cycle genus-0 Belyi map of type $(d; e_1, e_2, e_3)$ satisfies $2d + 1 = e_1 + e_2 + e_3$.

Example 2. The dynamical Belyi map $f(x) = -2x^3 + 3x^2$ has type $(3; 2, 2, 3)$.

A classical result, whose proof can be found in [ABEGKM18, Proposition 1], states that a dynamical Belyi map f is completely determined by its type and is defined over $\mathbb{Q}$.

The goal of this project was to determine and relate the following Galois groups:

Definition 3.

(1) Write $F_0 := \mathbb{Q}(t)$ for the function field of $\mathbb{P}^1_{\mathbb{Q}}$ and F_n/F_0 for the extension of function fields corresponding to $f^n : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$. We choose a normal closure M_n/F_0 of F_n/F_0 such that M_n contains M_{n-1} for any $n \geq 1$ and define $G_{n,\mathbb{Q}} = \mathrm{Gal}(M_n/F_0)$ for arbitrary $n \geq 1$.

(2) The extension $\left(F_n \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}\right)/\overline{\mathbb{Q}}(t)$ corresponds to $f^n : \mathbb{P}^1_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ considered as map over the algebraic closure $\overline{\mathbb{Q}}$. Then $\left(M_n \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}\right)/\overline{\mathbb{Q}}(t)$ is a normal closure of $\left(F_n \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}\right)/\overline{\mathbb{Q}}(t)$. For arbitrary $n \geq 1$ we define $G_{n,\overline{\mathbb{Q}}} = \mathrm{Gal}(\left(M_n \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}\right)/\overline{\mathbb{Q}}(t))$. In particular, $G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,\mathbb{Q}}$.

(3) Let $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$ such that the numerator $f(n, a)$ of $f^n - a$ is irreducible for all $n \geq 1$ and define $K_{n,a}$ as the extension of $K_{0,a} := \mathbb{Q}$ obtained by adjoining a root of $f(n, a)$. For arbitrary $n \geq 1$, we denote by $G_{n,a}$ the Galois group of the normal closure of $K_{n,a}/K_{0,a}$.

To study the groups just defined, we embed them into automorphism groups of trees.

3. Arboreal representations

For any $d \geq 2$ and $n \geq 1$, let T_n be the regular d-ary rooted tree of level n. There is an injective group homomorphism $\iota_n : \mathrm{Aut}(T_n) \hookrightarrow S_{d^n}$. We also view $\mathrm{Aut}(T_n)$ as a subgroup of the n-fold iterated wreath product of S_d by itself:

$$\mathrm{Aut}(T_n) \simeq \mathrm{Aut}(T_{n-1}) \wr \mathrm{Aut}(T_1) \text{ for } n \geq 2. \tag{1}$$

Our conventions imply that $G_{n,\mathbb{Q}}$, and hence $G_{n,\overline{\mathbb{Q}}}$, naturally has the structure of a wreath product. Identifying the sheets of f^n above a chosen base point in $\mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$ with the leaves of the tree T_n, and taking limits, yields inclusions

$$\begin{aligned} G_{n,\mathbb{Q}} &\hookrightarrow \mathrm{Aut}(T_n), \\ G_{\infty,\mathbb{Q}} &\hookrightarrow \mathrm{Aut}(T_\infty). \end{aligned} \tag{2}$$

The maps in Equation (2) are called *arboreal representations*. We use these to obtain our main results; proofs and explanations can be found in [BEK20].

4. Results

Definition 4. We define the *wreath-product sign* $\mathrm{sgn}_2 \colon \mathrm{Aut}(T_2) \to \{\pm 1\}$ by setting

$$\mathrm{sgn}_2(((\sigma_1, \ldots, \sigma_d), \tau)) = \mathrm{sgn}(\tau) \prod_{i=1}^{d} \mathrm{sgn}(\sigma_i). \tag{3}$$

Here sgn is the usual sign on $\mathrm{Aut}(T_1) \simeq S_d$. For $n > 2$ we define

$$\mathrm{sgn}_2 := \mathrm{sgn}_2 \circ \pi_2 : \mathrm{Aut}(T_n) \to \{\pm 1\}. \tag{4}$$

Theorem 1. *Let f be a normalized Belyi map of type $\underline{C} = (d; e_1, e_2, e_3) \notin \{(4; 3, 3, 3), (6; 4, 4, 5)\}$.*

(1) *Assume that* $G_{1,\overline{\mathbb{Q}}} \simeq S_d$. *Then for* $n \geq 1$ *we inductively have*

$$G_{n,\overline{\mathbb{Q}}} \simeq (G_{n-1,\overline{\mathbb{Q}}} \wr G_{1,\overline{\mathbb{Q}}}) \cap \ker(\mathrm{sgn}_2).$$

(2) *Assume that* $G_{1,\overline{\mathbb{Q}}} \simeq A_d$, *i.e., that all* e_j *are odd. Then* $G_{n,\overline{\mathbb{Q}}}$ *is the* n*-fold iterated wreath product of* A_d *with itself.*

Theorem 2. *Let* f *be a dynamical Belyi map for which one of the following holds:*

(1) *We have* $G_{1,\mathbb{Q}} \simeq G_{1,\overline{\mathbb{Q}}} \simeq A_d$;
(2) *We have* $G_{1,\overline{\mathbb{Q}}} \simeq S_d$ *and* $d = \deg(f)$ *is odd, and either* f *is polynomial or has type* $(d; d-k, 2k+1, d-k)$.

Then $G_{n,\mathbb{Q}} \simeq G_{n,\overline{\mathbb{Q}}}$ *for all* $n \geq 2$, *that is, descent holds for all* $n \geq 1$.

Theorem 3. *Let* f *be a dynamical Belyi map of type* $(d; e_1, e_2, e_3)$. *Choose* $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$ *and distinct primes* p, q_1, q_2, q_3 *such that* f *has good monomial reduction at* p *and good separable reduction at* q_1, q_2, q_3, *and we have*

$$\nu_p(a) = 1, \qquad \nu_{q_1}(a) > 0, \qquad \nu_{q_2}(1-a) > 0, \qquad \nu_{q_3}(a) < 0.$$

Then $G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,a}$ *for all* $n \geq 2$.

Corollary. *If the conditions of both Theorems 2 and 3 are satisfied, then for all* $n \geq 1$ *we have*

$$G_{n,a} \simeq G_{n,\overline{\mathbb{Q}}} \simeq G_{n,\mathbb{Q}}.$$

We can apply the above results to the motivating problem of prime divisors in dynamical sequences:

Theorem 4. *Let* f *be a dynamical Belyi map with splitting field* K. *Choose* $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$ *and distinct primes* p, q_1, q_2, q_3 *such that* $G_{n,a} \simeq G_{n,\overline{\mathbb{Q}}} \simeq G_{n,\mathbb{Q}}$ *for all* $n \geq 1$. *Consider the dynamical sequence* $\{a_i\}_{i \geq 0}$ *with* $a_1 = a$ *and* $a_n = f(a_{n-1})$.

(1) *The density* $\delta(\{p \text{ prime s.t. } a_i \equiv a \pmod{p} \text{ for some } i \geq 1\})$ *is zero.*
(2) *If* $G_{n,b_j,K} \simeq G_{n,K} \simeq G_{n,\mathbb{Q}}$ *for any* $n \geq 1$ *and any nonzero preimage* b_j *of zero under* f, *then the density*

$$\delta(\{p \text{ prime s.t. } p \text{ divides at least one nonzero term of } \{a_i\}_{i \geq 0}\})$$

is also zero.

References

[ABEGKM18] J. Anderson, I. Bouw, O. Ejder, N. Girgin, V. Karemaker, and M. Manes, *Dynamical Belyi maps*, Women in Numbers Europe II, Association for Women in Mathematics Series, vol. 11, Springer, 2018, 57–82.

[BEK20] I. Bouw, O. Ejder, and V. Karemaker, *Dynamical Belyi maps and arboreal Galois groups*, manuscripta math. (2020).

[LO08] F. Liu and B. Osserman, *The irreducibility of certain pure-cycle Hurwitz spaces*, Amer. J. Math. **130** (2008), no. 6, 1687–1708.

[Odo85] R.W.K. Odoni, *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \cdots w_n$, J. London Math. Soc. (2) **32** (1985), no. 1, 1–11.

Density results for specialization sets of Galois covers

François Legrand
(joint work with Joachim König)

The inverse Galois problem, a question going back to Hilbert and Noether, asks whether every finite group is the Galois group of a Galois (field) extension of $\mathbb{Q}$. The geometric approach to realize a finite group G consists in producing a Galois extension E of the rational function field $\mathbb{Q}(T)$ with Galois group G that is $\mathbb{Q}$-regular (i.e., $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$). For such $E/\mathbb{Q}(T)$, *Hilbert's irreducibility theorem* provides infinitely many $t_0 \in \mathbb{P}^1(\mathbb{Q})$ such that the *specialization* $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at t_0 has Galois group G. Several finite groups, including non-abelian simple ones, have been realized by this method. See, e.g., the book [MM18] for more details.

Let $\mathcal{S}(G)$ be the set of all Galois extensions of $\mathbb{Q}$ with given Galois group G. Given a $\mathbb{Q}$-regular Galois extension $E/\mathbb{Q}(T)$ of group G, let $\mathrm{Sp}(E)$ be the set of all specializations of $E/\mathbb{Q}(T)$ at points $t_0 \in \mathbb{P}^1(\mathbb{Q})$. The first aim of the talk, which is based on a joint work with J. König [KL19], was to provide evidence for this conclusion: $\mathrm{Sp}(E)$ *is small within* $\mathcal{S}(G)$ [1]. To make this more precise, we stated:

Definition 1. Let $E/\mathbb{Q}(T)$ be a $\mathbb{Q}$-regular Galois extension of group G.
(1) For $x \geq 1$, let $\mathcal{S}(G,x)$ denote the (finite) subset of $\mathcal{S}(G)$ defined by the extra condition that the absolute discriminant is bounded by x.
(2) We say that the set $\mathrm{Sp}(E)$ has *density* $d \in [0,1]$ if

$$\frac{|\mathrm{Sp}(E) \cap \mathcal{S}(G,x)|}{|\mathcal{S}(G,x)|} \longrightarrow d \text{ as } x \longrightarrow \infty.$$

Question 1. *Let $E/\mathbb{Q}(T)$ be a $\mathbb{Q}$-regular Galois extension of group G. Assume the genus g of the function field E fulfills $g \geq 2$. Does $\mathrm{Sp}(E)$ have density $d = 0$?*

After giving motivations for the condition $g \geq 2$, we presented the next theorem:

Theorem 1 (König–L.)**.** *Let $E/\mathbb{Q}(T)$ be a $\mathbb{Q}$-regular Galois extension of group G with $r \geq 5$ branch points (hence, $g \geq 2$). Under the abc-conjecture*[2]*, there is some $e > 0$ such that, for every $\epsilon > 0$ and every sufficiently large x, we have*

$$|\mathrm{Sp}(E) \cap \mathcal{S}(G,x)| \leq x^{e+\epsilon}.$$

To show that $\mathrm{Sp}(E)$ has density $d = 0$ (under the abc-conjecture and the assumption that r is sufficiently large), it then suffices to show that $|\mathcal{S}(G,x)|$ is asymptotically “bigger" than x^e. We then recalled the lower bound of the Malle conjecture (see [Mal02] for more details), which is a classical landmark in this context:

[1] Although $\mathrm{Sp}(E) \cap \mathcal{S}(G)$ is always infinite by Hilbert's irreducibility theorem (if $|G| \geq 2$).

[2] Recall that the abc-conjecture asserts that, for every $\epsilon > 0$, there exists a positive constant $K(\epsilon)$ such that, for all coprime integers a, b, and c fulfilling $a+b = c$, one has $c \leq K(\epsilon)\cdot \mathrm{rad}(abc)^{1+\epsilon}$, where the radical $\mathrm{rad}(n)$ of $n \geq 1$ is the product of the distinct prime factors of n.

The Malle conjecture (lower bound). *Let G be a non-trivial finite group and p the least prime divisor of $|G|$. There exists a positive constant $c(G)$ such that*

$$c(G) \cdot x^{\alpha(G)} \leq |\mathcal{S}(G, x)|$$

for every sufficiently large integer x, where $\alpha(G) = p/((p-1)|G|)$.

Note that, if the bound above holds for a given finite group G (for sufficiently large x), then G occurs as a Galois group over $\mathbb{Q}$.

Combining Theorem 1 and the lower bound of the Malle conjecture then led us to the following answer to Question 1:

Theorem 2 (König–L.)**.** *Let $E/\mathbb{Q}(T)$ be a $\mathbb{Q}$-regular Galois extension of group G with $r \geq 7$ branch points. Under the abc-conjecture and the lower bound of the Malle conjecture (for the group G), the set* $\mathrm{Sp}(E)$ *has density $d = 0$.*

We concluded this part by examples of finite groups G for which $d = 0$ holds true for *every* $\mathbb{Q}$-regular Galois extension $E/\mathbb{Q}(T)$ of group G, under the abc-conjecture, in connection with the previous unconditional examples of finite groups G with no *parametric* extension $E/\mathbb{Q}(T)$ from [KL18] and [KLN19].

In the second part of the talk, we had some more local considerations. Given a $\mathbb{Q}$-regular Galois extension $E/\mathbb{Q}(T)$ of group G, let $\mathrm{Sp}(E)^{\mathrm{loc}}$ be the set of all Galois extensions $F/\mathbb{Q}$ of group G such that $F\mathbb{Q}_p/\mathbb{Q}_p$ is a specialization of $E\mathbb{Q}_p(T)/\mathbb{Q}_p(T)$ for all prime numbers p and $F\mathbb{R}/\mathbb{R}$ is a specialization of $E\mathbb{R}/\mathbb{R}(T)$.

Question 2. *Let $E/\mathbb{Q}(T)$ be a $\mathbb{Q}$-regular Galois extension of group G. Does*

$$\frac{|\mathrm{Sp}(E) \cap \mathcal{S}(G, x)|}{|\mathrm{Sp}(E)^{\mathrm{loc}} \cap \mathcal{S}(G, x)|}$$

tend to 0 as x tends to ∞, under the assumption $g \geq 2$?

As in Question 1, a positive answer means that "many" elements of $\mathcal{S}(G)$ are not in $\mathrm{Sp}(E)$ but the latter cannot be detected by considering local aspects only, thus implying a failure of a local-global principle for specializations.

Theorem 3 (König–L.)**.** *Let $E/\mathbb{Q}(T)$ be a $\mathbb{Q}$-regular Galois extension with abelian Galois group G.*

(1) *For some constant $C(E) > 0$ and every sufficiently large x, we have*

$$|\mathrm{Sp}(E)^{\mathrm{loc}} \cap \mathcal{S}(G, x)| \geq C(E) \cdot x^{\alpha(G)} \cdot \log^{-1}(x).$$

(2) *Assume $r \geq 7$. Then, under the abc-conjecture, the ratio*

$$\frac{|\mathrm{Sp}(E) \cap \mathcal{S}(G, x)|}{|\mathrm{Sp}(E)^{\mathrm{loc}} \cap \mathcal{S}(G, x)|}$$

tends to 0 as x tends to ∞.

The last part was devoted to the diophantine aspects of our results. We recalled that, given a $\mathbb{Q}$-regular Galois cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ of group G and a morphism

$\varphi : \mathrm{G}_{\mathbb{Q}} \to G$, there is a $\mathbb{Q}$-regular cover $\widetilde{f}^{\varphi} : \widetilde{X}^{\varphi} \to \mathbb{P}^1_{\mathbb{Q}}$ with $\widetilde{X}^{\varphi} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$, and such that
$(*)$ for every $t_0 \in \mathbb{P}^1(\mathbb{Q})$, not a branch point of f, there is $x_0 \in \widetilde{X}^{\varphi}(\mathbb{Q})$ with $\widetilde{f}^{\varphi}(x_0) = t_0$ if and only if the specialization morphism of f at t_0 equals φ.

Due to the condition in $(*)$ that t_0 is not a branch point, we introduced this terminology: a $\mathbb{Q}$-rational point x on $\widetilde{X}^{\varphi}$ is *non-trivial* if $\widetilde{f}^{\varphi}(x)$ is not a branch point of f. Note that, if f has no $\mathbb{Q}$-rational branch point, then every $\mathbb{Q}$-rational point on $\widetilde{X}^{\varphi}$ is necessarily non-trivial.

We then presented the following diophantine reformulation of Theorem 1, whose case $G = \mathbb{Z}/2\mathbb{Z}$ is a well-known result of Granville [Gra07]:

Theorem 4 (König–L.). *Let $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a $\mathbb{Q}$-regular Galois cover of group G with $r \geq 5$ branch points. Assume the abc-conjecture. Then, for every $\epsilon > 0$ and every sufficiently large x, the number $h(x)$ of epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ such that $\overline{\mathbb{Q}}^{\ker(\varphi)}/\mathbb{Q} \in \mathcal{S}(G, x)$ and $\widetilde{X}^{\varphi}$ has a non-trivial $\mathbb{Q}$-rational point fulfills*

$$h(x) \leq x^{e+\epsilon}.$$

Finally, using that an epimorphism $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ is a specialization morphism "everywhere locally" but "not globally" of a $\mathbb{Q}$-regular Galois cover $f \colon X \to \mathbb{P}^1_{\mathbb{Q}}$ of group G if and only if $\widetilde{X}^{\varphi}$ has non-trivial real points and non-trivial $\mathbb{Q}_p$-rational points for every prime number p, but only trivial $\mathbb{Q}$-rational points, we gave the following application of Theorem 3 to the construction of "many" curves over $\mathbb{Q}$ failing the Hasse principle (under the abc-conjecture). Note that the case $G = \mathbb{Z}/2\mathbb{Z}$ of the next result was obtained recently by Clark and Watson [CW18].

Theorem 5 (König–L.). *Let $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a $\mathbb{Q}$-regular Galois cover with abelian Galois group G and $r \geq 7$ branch points. Assume the abc-conjecture holds and f has no $\mathbb{Q}$-rational branch point with ramification index 2. Then, for some constant $C(f) > 0$ and every sufficiently large x, the number $h(x)$ of epimorphisms $\varphi \colon \mathrm{G}_{\mathbb{Q}} \to G$ such that $\overline{\mathbb{Q}}^{\ker(\varphi)}/\mathbb{Q} \in \mathcal{S}(G, x)$ and $\widetilde{X}^{\varphi}$ does not fulfill the Hasse principle is at least*

$$C(f) \cdot x^{\alpha(G)} \cdot \log^{-1}(x).$$

References

[CW18] P. Clark and L. Watson, *ABC and the Hasse principle for quadratic twists of hyperelliptic curves*, C. R. Math. Acad. Sci. Paris **356** (2018), 911–915.

[Gra07] A. Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*, Int. Math. Res. Not. IMRN **2007** (2007), Art. ID 027, 24 pp.

[KL18] J. König and F. Legrand, *Non-parametric sets of regular realizations over number fields*, J. Algebra **497** (2018), 302–336.

[KL19] J. König and F. Legrand, *Density results for specialization sets of Galois covers*, To appear in Journal of the Institute of Mathematics of Jussieu, 2019.

[KLN19] J. König and F. Legrand and D. Neftin, *On the local behavior of specializations of function field extensions*, Int. Math. Res. Not. IMRN **2019** (2019), 2951–2980.

[Mal02] G. Malle, *On the distribution of Galois groups*, J. Number Theory **92** (2002), 315–329.

[MM18] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer, Berlin, 2018. Second edition. xvii+532 pp.

The Modular Tower version of the Fried-Serre Lift invariant

Michael D. Fried

[Fr20] refined the original **MT** program by introducing *ℓ-Frattini lattice quotients*. This allows, starting from modular curves, to capture the full relation between the *regular inverse Galois problem* (**RIGP**) and precisely generalizing Serre's *Open Image Theorem* (**OIT**). §1 reminds how we define canonical towers of Hurwitz spaces. Usually assuring their levels have *fine moduli* and *moduli definition* $\mathbb{Q}$.

The rubric parameters are $(G, \ell, \mathbf{C}, M')$: ℓ a prime; G an ℓ-perfect finite group; $r \geq 4$ of its ℓ' conjugacy classes, $\mathbf{C}$; together with a $\mathbb{Z}/\ell[G]$ quotient, M', of a characteristic module ${}_\ell M_G \stackrel{\text{def}}{=} M_{\max}$. Reducing tower levels by $\mathrm{PSL}_2(\mathbb{C})$ gives natural covers of

$$\textit{Unordered (distinct) points of } \mathbb{P}^1_z\textit{: } \mathbb{P}^n \setminus D_n / \mathrm{PGL}_2(\mathbb{C}) = J_r.$$

Two sets of arithmetic problems with precise conjectures – Regular Inverse Galois (**RIGP**) and Open Image Theorem (**OIT**) – meet on such a tower with its corresponding ℓ-adic representation. We point to four Oberwolfach talk themes.

- §1 Properties of $\mathbb{H}_{G,\mathbf{C},\ell,L_{M'}} = \{\mathcal{H}_{\ell,k} \stackrel{\text{def}}{=} \mathcal{H}({}^k_\ell G = {}_\ell\tilde{G}/\ell^k L_{M'}, \mathbf{C})^{\text{rd}}\}_{k=0}^{\infty}$, the *canonical (reduced) tower* with $L_{M'}$ the attached ℓ-adic lattice.
- §2 **RIGP** and **OIT** viewed as properties of $G_{\mathbb{Q}}$ orbits on **MT**s: projective sequences of absolutely irreducible components on $\mathbb{H}_{G,\mathbf{C},\ell,L_{M'}}$.
- §3 Description of the complete set of **MT**s on one of the two examples in [Fr21b], using the **MT** version of the Fried-Serre *lift invariant* as in [Fr21a].
- §4 A **MT** version of Hilbert's Irreducibility Theorem (**HIT**) as generalizing Falting's Theorem.

Using the ℓ-Frattini lattice quotients of [Fr20] expands to give **MT**s recognizable to many – beyond those connected to *hyperelliptic Jacobians* where G is dihedral, D_ℓ, $\ell \neq 2$, and $\mathbf{C} = \mathbf{C}_{2^{2s}}$ is $2s = r$ repetitions of the involution class.

Serre's case is $s = 2$; as in the first 3rd of the 1st **MT** *paper (1995).*

Something to keep an eye on: The *Schur-lattice* captures a **MT** version of the *lift invariant*. This talk used it to track the growth of Hurwitz space components – up levels of our example canonical Hurwitz space tower. Especially the way that we understand them through two basic *Nielsen class* types:

Harbater-Mumford (**HM**) and *Double Identity* (**DI**).

1. Basic objects

A profinite cover $\psi : H \to G$ is *Frattini* if restriction $\psi_{H^*}, H^* \leq H$, is a cover, $\implies H^* = H$. The key gadget: The Universal *Abelianized* ℓ-Frattini cover of G:

$$L_{G,\ell} \stackrel{\text{def}}{=} (\mathbb{Z}_\ell)^{\ell m_G} \to {}_\ell\tilde{G}_{\text{ab}} \xrightarrow{{}_\ell\tilde{\psi}_{\text{ab}}} G \text{ (short-exact)}.$$

From this we get a characteristic $\mathbb{Z}/\ell[G]$ ℓ-Frattini module

$$\ker({}_\ell\tilde{\psi}_{\rm ab})/\ell\ker({}_\ell\tilde{\psi}_{\rm ab})) \stackrel{\rm def}{=} {}_\ell M_G = M_{\max}; L_{G,\ell} = L_{\max}, \text{for the maximal } L_{M'}.$$

For ℓ' classes $\mathbf{C}$, when the kernel of cover $H \to G$ is an ℓ-group, then

$\mathbf{C}$ lifts uniquely to classes of H; refer to $\boldsymbol{g}^* \in \mathbf{C} \cap H$.

In this talk $r = 4$. Definition of inner Nielsen classes (with diagonal action of G):

$$\mathrm{Ni}(G,\mathbf{C}) = \{(g_1, g_2, g_3, g_4) = \boldsymbol{g} \in \mathbf{C} \mid g_1g_2g_3g_4 = 1, \langle \boldsymbol{g}\rangle = G\}/G.$$

Hurwitz monodromy, H_4, action on $\mathrm{Ni}(G,\mathbf{C})$: generated by

$$\begin{aligned} q_2 :&\quad \boldsymbol{g} \mapsto (g_1, g_2g_3g_2^{-1}, g_2, g_4);\\ \mathbf{sh} :&\quad \boldsymbol{g} \mapsto (g_2, g_3, g_4, g_1) \text{ (with } q_1 = \mathbf{sh}q_2\mathbf{sh}^{-1}, q_3 = \mathbf{sh}^{-1}q_2\mathbf{sh}). \end{aligned}$$

With $\mathcal{Q}'' = \langle q_1q_3^{-1}, \mathbf{sh}^2\rangle$, reduced Nielsen Classes are $\mathrm{Ni}(G,\mathbf{C})/\mathcal{Q}'' \stackrel{\rm def}{=} \mathrm{Ni}(G,\mathbf{C})^{\rm rd}$.

2. ℓ-Frattini Lattice Quotients

Given M', form ${}^k_\ell G_{M'}$ inductively: ${}^1_\ell\psi_{M'} : {}^1_\ell G/M'' \stackrel{\rm def}{=} {}^1_\ell G_{M'} \to G$. Then, ℓ-Frattini cover ${}^2_\ell\psi_{M_{\max}}$ factors through ${}^1_\ell\psi_{M'}$. Form $\ell M'' = {}^2M''$, and then

$${}^2_\ell\psi_{M'} : {}^2_\ell G/{}^2M'' \stackrel{\rm def}{=} {}^2_\ell G_{M'} \to G.\text{; etc. to inductively form } {}_\ell\tilde{G}_{M'} \to G.$$

A **MT** is a projective sequence, $\{\mathcal{H}'_k\}_{k=0}^\infty$, of components on $\mathbb{H}_{G,\mathbf{C},\ell,L_{M'}}$.

Theorem. *It's not obvious, but $\mathcal{H}'_k \mapsto J_4 = \mathbb{P}^1_j \setminus \{\infty\}$ is an upper half-plane quotient that completes to (normal) $\overline{\mathcal{H}}'_k \to \mathbb{P}^1_j$, ramified over 0 (order 3), 1 (order 2), ∞.*

Other Structure: If G is ℓ-perfect and centerless, then:

- **Theorem.** *So is ${}^k_\ell G_{M'}$, if $\mathbf{1}_G$ is not a submodule of M'.*
- **Theorem.** *$M_{\max}$ is indecomposable, and $H^2_{\mathbb{Z}/\ell}(G, M_{\max})$ has dim.* 1.
- **Theorem.** *If $H^2_{\mathbb{Z}/\ell}(G, M')$ has dim. 1 then, so does $H^2_{\mathbb{Z}_\ell}({}_\ell\tilde{G}_{M'}, L_{M'})$.*

That is, the ℓ-Frattini lattice quotient is unique.

Special case $M' = \mathbf{1}_G = \mathrm{SM}_{G,\ell}$, the ℓ part of the Schur multiplier of G has dimension 1: $L_{M'} = \mathbb{Z}_\ell$; trivial G action.

3. Restricted Lift Invariant (suffices here)

Consider ℓ-perfect G, $\psi_H : H \to G$ a *central* ℓ-Frattini cover, $\boldsymbol{g} \in \mathrm{Ni}(G,\mathbf{C})$ and unique $\tilde{\boldsymbol{g}} \in \mathbf{C} \cap H$ over it. *The restricted lift invariant*:

$$s_{H/G}(O) \stackrel{\rm def}{=} \textstyle\prod_{i=1}^r \tilde{g}_i \in \ker(\psi_n).$$

Theorem. *The lift invariant gives these Hurwitz space component results.*

a) A precise count if multiplicity of each $\mathrm{C} \in \mathbf{C}$ *is high.*

b) On a canonical Hurwitz space tower, with $\mathbf{C}$ *fixed, whether there is a nonempty* **MT** *over a given level 0 component.*

Example ℓ-Frattini lattice quotient: With $V_{\ell,k} = (\mathbb{Z}/\ell^{k+1})^2$, $\alpha = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$, then $\alpha_0 = \left(\begin{smallmatrix} \alpha & 0 \\ \mathbf{0} & 1 \end{smallmatrix}\right)$ acts on $V_{\ell,k}$ generating $\mathbb{Z}/3$. Level k Nielsen classes for this canonical Hurwitz space tower is $\mathrm{Ni}_{\ell,k} \stackrel{\text{def}}{=} \mathrm{Ni}(G_{\ell,k} \stackrel{\text{def}}{=} V_{\ell,k} \times^s \mathbb{Z}/3, \mathbf{C}_{+3^2-3^2})$, $\ell \neq 3$.

Theorem. *For $\ell \neq 2, 3$, the Univ. ℓ-central Frattini cover of $G_{\ell,k}$ is*

$$\left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z}/\ell^{k+1} \right\} \times^s \mathbb{Z}/3 \stackrel{\text{def}}{=} R_{\ell,k}.$$

Two example Nielsen class elements at each level k.

Harbater-Mumford (**HM**): $\boldsymbol{g}_{\mathbf{HM},\boldsymbol{v}} = (\alpha_0, \alpha_0^{-1}, {}_{\boldsymbol{v}}\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1})$

Double-Identity (**DI**): $\boldsymbol{g}_{\mathbf{DI},\boldsymbol{v}} = (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, \alpha_0, {}_{\boldsymbol{w}}\alpha_0^{-1})$.

Theorem. *For $\ell \equiv \mp 1 \mod 3$, as $\boldsymbol{v}$ varies with $\langle \alpha_0, \boldsymbol{v} \rangle = G_{\ell,k}$:*

- *$s(\boldsymbol{g}_{\mathbf{DI},\boldsymbol{v}})$ varies over $(\mathbb{Z}/\ell^{k+1})^*$, with 1 component for each value.*
- *Lift inv. of $\boldsymbol{g}_{\mathbf{HM},\boldsymbol{v}}$ is 0; level k has $\frac{\ell \pm 1}{6} \cdot \ell^k$* **HM** *comps.*
- *$\mathcal{H}(R_{\ell,k}, \mathbf{C}_{+3^2-3^2})^{\mathrm{rd}}$ doesn't have fine moduli, but [3, §4]*
  $\mathcal{H}(G_{\ell,2\cdot k+1}, \mathbf{C}_{+3^2-3^2})^{\mathrm{rd}}$ covers $\mathcal{H}(R_{\ell,k}, \mathbf{C}_{+3^2-3^2})^{\mathrm{rd}}$ and it does.

4. **RIGP**, **OIT**, Faltings and **HIT** together

A sequence of (group) covers $H_{k+1} \to H_k$, $k \geq 0$ is eventually Frattini, if $\exists\, k_0$ with $H_k \to H_{k_0}$ a Frattini cover , $k \geq k_0$. With ℓ group kernels, we say ℓ-Frattini.

For a given **MT**$= \{\mathcal{H}'_k\}_{k=0}^{\infty}$: $\mathcal{G}_{\mathbf{MT}}$ its geometric monodromy:

$$\leftarrow_k \text{ geometric monodromy of } \mathcal{H}'_k \to J_r, k \geq 0.$$

Main OIT Conj. *The following are* eventually ℓ-Frattini*:*

$\mathcal{G}_{\mathbf{MT}}$, and the intersection of arithmetic monodromy, $\mathcal{A}_{\mathbf{MT},J'}$, of fibers over $J' \in J_r(K)$ with $\mathcal{G}_{\mathbf{MT}}$.

Serre used: $\{\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1})\}_{k=0}^{\infty}$ is eventually ℓ-Frattini + Tate's ℓ-adic elliptic curve $\implies$ for $j' \in \mathbb{P}^1_j(\bar{\mathbb{Q}})$ non-integral, then arithmetic fiber over j' is $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

Without non-integral j-invariant, required Falting's Theorem – many years later – for completion. If not a CM fiber, then

arithmetic group of fiber is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

Assume $\mathcal{G}_{\mathbf{MT}}$ is eventually ℓ-Frattini. Find lattice of eventually ℓ-Frattini types of $\mathcal{G}_{\mathbf{MT}}$ up to *commensurably open*: ℓ-Frattini analogs of CM and GL_2 type.

Generalize Faltings to identify, for $\boldsymbol{p} \in \mathcal{H}'_0(K)$ *over* $J' \in J_r$,
$(*)$ $\mathcal{A}_{\mathbf{MT},J'} \cap \mathcal{G}_{\mathbf{MT}}$ *as one of these.*

Gives HIT consequences: Generic fibers of $(*)$ are $\mathcal{G}_{\mathbf{MT}}$. The other fibers, in considering $(G, \mathbf{C})$ **RIGP** realizations, call for refined conjectures – as in [Fr20, Conj. 5.26] of Cadoret-Dèbes – by comparing with the CM and GL_2 cases of Serre.

References

[Fr20] M.D. Fried, *Moduli relations between l-adic representations and the regular inverse Galois problem*, **GJM**, Volume **5**, Issue 1 (2020), 38–75. This has references galore.

[Fr21a] ———, *ℓ-Frattini Lattices and the Modular Tower Lift Invariant*, preprint, the subject of this talk, except for the display of the **MT** based on $(\mathbb{Z}/\ell)^2 \times^s \mathbb{Z}/3$ and $\mathbf{C} = \mathbf{C}_{\pm 3^2}$.

[Fr21b] ———, *Hurwitz Space Components: The shift-incidence matrix*, preprint, the paper containing two series of **MT**s; the one here and the other for a series of A_n s.

Hodge, *p*-adic, and tropical iterated integrals

Daniel Litt

The goal of this talk was to discuss three types of single-valued iterated integral — one in the archimedean setting, one in the p-adic setting, and one in the tropical setting — and the relationships between them.

1. The archimedean setting

Let X be a smooth complex variety. Given a path γ between two points $a, b \in X$, and a collection of C^∞ 1-forms $\{\omega_1, \cdots, \omega_n\}$ on X, one may define the iterated integral

$$\int_\gamma \omega_1 \cdots \omega_n := \int_{0 \le t_1 \le \cdots \le t_n \le 1} \gamma^*\omega_1 \wedge \cdots \wedge \gamma^*\omega_n.$$

In general this integral depends quite a bit on γ.

Let $A^1(X)$ be the space of complex-valued C^∞ 1-forms on X, and let

$$\Omega(X) := \bigoplus_{n \ge 1} A^1(X)^{\otimes n}.$$

Iterated integration gives a functional

$$\int_\gamma \Omega(X) \to \mathbb{C},$$

defined as in the previous paragraph and extended linearly. We say an element $\omega \in \Omega(X)$ is *homotopy-invariant* if, for all paths γ, $\int_\gamma \omega$ depends only on the based homotopy class of ω. Let $B^0(X) \subset \Omega(X)$ denote the space of homotopy-invariant forms. If X is a compact Riemann surface, examples of homotopy-invariant forms include, for example, the subspace of $\Omega(X)$ spanned by (tensors of) holomorphic 1-forms.

Our main result (joint with Aleksander Shmakov) in the archimedean setting is a construction of a *single-valued* iterated integral for homotopy invariant forms; that is, for each $a, b \in X$ we construct a map

$$\fint_a^b : B^0(X) \to \mathbb{C}$$

such that

– For $\omega \in B^0(X)$ analytic, $\fint_a^b \omega$ varies real-analytically in a and b.
– $\fint$ is functorial, i.e. if $f : X \to Y$ is a map of algebraic varieties,

$$\fint_a^b f^*\omega = \fint_{f(a)}^{f(b)} \omega.$$

–

$$\fint_a^b \omega_1 \otimes \cdots \otimes \omega_n = \sum_i \fint_a^c \omega_1 \otimes \cdots \otimes \omega_i \fint_c^b \omega_{i+1} \otimes \cdots \otimes \omega_n.$$

– The integrals in question are in general non-zero, and agree with existing constructions of Deligne and Brown [Bro14] when those constructions apply.
– Various other good properties.

The construction uses the mixed Hodge structure on the pro-unipotent fundamental group of a complex algebraic variety.

2. The p-adic setting

The main results in the p-adic setting are joint with Eric Katz, and are a p-adic analogue of the results described above. Let K be a p-adic field with ring of integers $\mathscr{O}_K$ and residue field k. Let $X/\mathscr{O}_K$ be a proper, strictly semi-stable curve with smooth generic fiber. If X has good reduction, Coleman defines a single-valued theory of iterated integration; in the bad reduction setting, Berkovich [Ber07] describes a theory of iterated integration which is no longer single-valued, but rather has monodromy given by the fundamental group of the dual graph of X_k.

Vologodsky [Vol03] has observed that there should be a single-valued variant of Berkovich integration, as a consequence of the weight-monodromy conjecture for the pro-unipotent fundamental group of a curve. The goal of our work is to make this single-valued variant of Berkovich integration explicit. Our main result is too involved to include in this abstract, but can loosely be formulated as:

Theorem 1 (Katz, L–). *The single-valued Vologodsky integral is an explicit linear combination of Berkovich integrals, whose coefficients may be computed purely combinatorially, in terms of a* tropical *iterated integral defined in previous work of Cheng and Katz* [CK21].

References

[Ber07] V. Berkovich, *Integration of one-forms on p-adic analytic spaces*, Annals of Mathematics Studies, vol. 162, Princeton University Press, Princeton, NJ, 2007.
[Bro14] F. Brown, *Single-valued motivic periods and multiple zeta values,* Forum Math. Sigma 2 (2014), Paper No. e25, 37 pp.

[CK21] R. Cheng, E. Katz, *Combinatorial Iterated Integrals and the Harmonic Volume of Graphs,* Adv. in Appl. Math. 128 (2021), 102190.
[Vol03] V. Vologodsky, *Hodge structure on the fundamental group and its application to p-adic integration*, Mosc. Math. J. 3 (2003), no. 1, 205–247, 260.

On the Hilbert property over rings and the Schinzel hypothesis

Pierre Dèbes
(joint work with Arnaud Bodin, Joachim König, Salah Najib)

Hilbert's Irreducibility Theorem (HIT) is a fundamental statement in Arithmetic Geometry which basically started Inverse Galois Theory. HIT is about fields and polynomials. Denote the variables, which are of two types by $\underline{t} = (t_1, \dots, t_k)$ and $\underline{y} = (y_1, \dots, y_n)$ $(k, n \geq 1)$: the t_i are those to be specialized, unlike the y_i. The issue is whether, starting from polynomials that are irreducible and of positive degree in $\underline{y}$, the variables t_i can be specialized to some values in the ground field (containing the coefficients of the polynomials) in such a way that irreducibility is preserved. The field is called *Hilbertian* when that is the case.

A large family of Hilbertian fields, which we work with here, is that of *fields with a product formula*; see [FJ08, §15.3]. The basic example is the field $\mathbb{Q}$. The product formula is: $\prod_p |a|_p \cdot |a| = 1$ for every nonzero $a \in \mathbb{Q}$, where p ranges over all prime numbers, $|\cdot|_p$ is the p-adic absolute value and $|\cdot|$ is the standard absolute value. Rational function fields $k(x_1, \dots, x_r)$ in $r \geq 1$ variables over a field k, and finite extensions of fields with the product formula are other examples. We also assume that our ground field Q is *imperfect if of characteristic* $p > 0$ (otherwise, the polynomial $y^p - t$ is always reducible when t is specialized in Q).

Weissauer proved in 1982 that such fields Q are indeed Hilbertian [FJ08, Theorem 15.3.3], the special case $Q = \mathbb{Q}$ being the original HIT, proved in 1892.

1. The Hilbert-Schinzel specialization property

Assume now that a subring $Z \subset Q$ with fraction field Q is given. Our main goal is to extend the Hilbert specialization property to a property *over the ring* Z. That is: assuming the initial polynomials have coefficients in Z and are irreducible over Z, find specializations of the variables $\underline{t}$ in Z such that the resulting polynomials are irreducible over Z? Classically, it suffices to guarantee that these specialized polynomials are irreducible over Q and that they are *primitive w.r.t. the ring* Z (i.e., the coefficients have no common divisors in Z other than units); and this is in fact necessary if Z is a Unique Factorization Domain (UFD).

This is not true in general. For example, $(t^2 - t)y + (t^2 - t + 2) \in \mathbb{Z}[t, y]$ is always divisible by $a = 2$, hence reducible in $\mathbb{Z}[y]$ when t is specialized in $\mathbb{Z}$. Similarly, $(t^q - t + u)y + (t^q - t) \in \mathbb{F}_q[u][t, y]$ is always divisible by $a = u$, hence reducible in $\mathbb{F}_q[u][y]$ when t is specialized in $\mathbb{F}_q[u]$.

Definition 1. A non-unit $a \in Z$, $a \neq 0$, is *a fixed divisor of some polynomial* $P(\underline{t}, \underline{y}) \in Z[\underline{t}, \underline{y}]$ *with respect to* $\underline{t}$ if $P(\underline{m}, \underline{y}) \equiv 0 \pmod a$ for every $\underline{m} \in Z^k$.

For example, in the preceding examples, $2 \in \mathbb{Z}$ and $u \in \mathbb{F}_q[u]$ are fixed divisors.

Definition 2. An integral domain Z is a near UFD if every non-zero element has finitely many prime divisors, and every non-unit has at least one.

Interestingly enough, an integral domain is a UFD if and only if it is a near UFD and it is Noetherian. Also, in a near UFD, every irreducible is a prime.

Over a near UFD, existence of fixed divisors is the only obstruction to our goal.

Theorem 1. [BDKN21] (Hilbert-Schinzel specialization property over Z). *Assume that Z is a near UFD and $Q = \mathrm{Frac(Z)}$ is a field with a product formula, of characteristic 0 or imperfect. Let $P_1(\underline{t}, \underline{y}), \ldots, P_s(\underline{t}, \underline{y}) \in Z[\underline{t}, \underline{y}]$ be $s \geq 1$ polynomials, irreducible in $Q[\underline{t}, \underline{y}]$, primitive w.r.t. Z, of positive degree in $\underline{y}$ and such that the product $P_1 \cdots P_s$ has no fixed divisors w.r.t. the variables $\underline{t}$. Then for every $\underline{m}$ in some Zariski-dense subset $H \subset Z^k$, the polynomials $P_1(\underline{m}, \underline{y}), \ldots, P_s(\underline{m}, \underline{y})$ are irreducible in $Q[\underline{y}]$ and primitive w.r.t. Z (hence irreducible in $Z[\underline{y}]$).*

Furthermore, the same holds with $k = 1$ (a single variable t_i) if Z is a Dedekind domain (instead of a near UFD).

Addendum. (a) The assumption on the fixed divisors is called *the Schinzel condition*. It automatically holds (and so may be omitted) if every principal prime ideal $pZ \subset Z$ is of infinite norm $|Z/pZ|$. That is the case for every polynomial ring $Z = R[\underline{u}]$ in variables $\underline{u} = (u_1, \ldots, u_r)$ $(r \geq 1)$ over an integral domain R, unless $Z = \mathbb{F}_q[u]$. The Schinzel condition does not always hold either for $Z = \mathbb{Z}$.

(b) In general, over a near UFD or a Dedekind domain, the product $P_1 \cdots P_s$ can only have finitely fixed prime divisors w.r.t. $\underline{t}$ (modulo units of Z). Denoting the product of them by φ, we obtain this *more intrinsic version of Theorem 1*:

(*) *Under the same assumptions* except that the Schinzel condition is not assumed, *there exists a nonzero element $\varphi \in Z$ with this property. For every $\underline{m}$ in some Zariski-dense subset $H \subset Z[1/\varphi]^k$, the polynomials $P_1(\underline{m}, \underline{y}), \ldots, P_s(\underline{m}, \underline{y})$ are irreducible in $Q[\underline{y}]$ and primitive w.r.t. $Z[1/\varphi]$ (hence irreducible in $Z[1/\varphi][\underline{y}]$).*

2. The Schinzel hypothesis for polynomial rings

The next result shows another way to get rid of the Schinzel condition. For simplicity, we state the result for $k = 1$ only (i.e., a single variable t_i).

Theorem 2. [BDN19] (Schinzel hypothesis for polynomial rings). *Let Z, Q and $P_1(t, \underline{y}), \ldots, P_s(t, \underline{y})$ be as in Theorem 1,* except that the Schinzel condition is not assumed. *Then there exist polynomials $m(\underline{y}) \in Z[\underline{y}]$ of arbitrarily large partial degrees such that the polynomials $P_1(m(\underline{y}), \underline{y}), \ldots, P_s(m(\underline{y}), \underline{y})$ are irreducible in $Q[\underline{y}]$ and primitive w.r.t. Z (hence irreducible in $Z[\underline{y}]$).*

In characteristic 0, the polynomials $m(\underline{y})$ can even be requested to be of any *prescribed* arbitrarily large partial degrees.

Theorem 2 is a polynomial version of the following celebrated statement: our polynomial ring $Z[\underline{y}]$ replaces the ring $\mathbb{Z}$ of integers.

Schinzel Hypothesis. *Let $P_1(t), \dots, P_s(t)$ be $s \geq 1$ polynomials, irreducible in $\mathbb{Z}[t]$ and such that the product $P_1 \cdots P_s$ has no fixed divisor in $\mathbb{Z}$ w.r.t. t. Then there are infinitely many $m \in \mathbb{Z}$ such that $P_1(m), \dots, P_s(m)$ are prime numbers.*

Recall that, unlike Theorem 2, the Schinzel Hypothesis is a wide open conjecture; for example, the mere special case $P_1(t) = t$ and $P_2(t) = t+2$ would yield the Twin Prime conjecture.

Remark 3. (a) Our polynomial Schinzel hypothesis clearly fails if $Z = \overline{Q}$ is an algebraically closed field and $n = 1$ (i.e. a single variable y_i). It also fails for $Z = \mathbb{F}_2$ and $P_1 = \{t^8 + y^3\}$: from an example of Swan [Sw62, pp.1102-1103], $m(y)^8 + y^3$ is reducible in $\mathbb{F}_2[y]$ for every $m(y) \in \mathbb{F}_2[y]$. These cases are not covered by our results; the fields $\overline{Q}$ and $\mathbb{F}_2$ are not Hilbertian.
(b) The situation $Z = \mathbb{F}_q$ of finite fields has however been much investigated, leading to the conclusion that the polynomial Schinzel hypothesis holds if q is big enough. An analog of a quantitative form of the Schinzel hypothesis, known as the Bateman-Horn conjecture, could even be recently proved, by Entin. We refer to [BW05] and [En16] for these developments, which involve different methods.

3. The coprime Schinzel hypothesis

There is another connection between our results and the Schinzel hypothesis. The primitivity part of the original problem reduces to the following question, which is interesting for its own sake. Given some polynomials $Q(\underline{t}) \in Z[\underline{t}]$ assumed to be coprime in $Z[\underline{t}]$ and to satisfy some Schinzel condition, can one find tuples $\underline{m} \in Z^k$ such that the values $Q(\underline{m})$ are coprime in Z? Roughly speaking, *do coprime polynomials assume coprime values*?

The following statement is our answer. Note that the field Q is arbitrary here.

Theorem 3. [BDKN21] (Coprime Schinzel hypothesis*). Assume Z is a near UFD. Let $Q_1(\underline{t}), \dots, Q_\ell(\underline{t}) \in Z[\underline{t}]$ be $\ell \geq 2$ polynomials, coprime in $Q[\underline{t}]$ and satisfying this Schinzel condition: no non-unit of Z divides all values $Q_1(\underline{z}), \dots, Q_\ell(\underline{z})$ where $\underline{z}$ ranges over Z^k. Then $Q_1(\underline{m}), \dots, Q_\ell(\underline{m})$ are coprime in Z for some $\underline{m} \in Z^k$.*

Furthermore, the set of good $\underline{m}$ is Zariski-dense in Z^k if Z is infinite.

Remark 4. The coprime Schinzel hypothesis also holds for the ring $\mathcal{Z}$ of all entire functions, and for every Dedekind domain if $k = 1$ (one variable t_i). But it fails for $\mathbb{Z}[\sqrt{5}]$. The rings $\mathcal{Z}$ and $\mathbb{Z}[\sqrt{5}]$ are neither near UFD nor Dedekind domains.

The coprime Schinzel hypothesis was known in the case $Z = \mathbb{Z}$ and $Z = \mathbb{F}_q[u]$ from works of Schinzel [Sc02] and Poonen [Po03] (the second one offering further a quantitative form for these two rings). For Principal Ideal Domains (PID), the following stronger and maybe more intrinsic property can be proved.

Theorem 4 ([BDN20], [BD21])**.** *Assume Z is a PID. Let $Q_1(\underline{t}), \dots, Q_\ell(\underline{t}) \in Z[\underline{t}]$ be $\ell \geq 2$ polynomials, coprime in $Q[\underline{t}]$. For every $\underline{m} \in Z^k$, denote by $d_{\underline{m}}$ the* gcd *of $Q_1(\underline{m}), \dots, Q_\ell(\underline{m})$, with the convention that the* gcd *of $0, \dots, 0$ is 0. Then the subset $\mathcal{D} \subset Z$ of all $d_{\underline{m}}$ where $\underline{m}$ ranges over Z^k is stable under* gcd.

It follows from Z being Noetherian that the gcd of all elements of $\mathcal{D}$ is a nonzero element $d \in Z$ and that it is the gcd of finitely many $d_{\underline{m}}$. If the Schinzel condition from Theorem 3 holds, then $d = 1$. It follows then from the gcd stability property of $\mathcal{D}$ that $d = 1 \in \mathcal{D}$, i.e., the conclusion of the coprime Schinzel hypothesis holds, thus showing indeed that for a PID, Theorem 4 is stronger than Theorem 3.

References

[BW05] A. Bender and O. Wittenberg, *A potential analogue of Schinzel's hypothesis for polynomials with coefficients in* $\mathbb{F}_q[t]$, Int. Math. Res. Not. **36** (2005), 2237–2248.

[BDN19] A. Bodin, P. Dèbes and S. Najib, *The Schinzel Hypothesis for polynomials*, Trans. Amer. Math. Soc. **373** (2020), 8339–8364.

[BDN20] ———, *Prime and coprime values of polynomials*, Enseign. Math. **66** (2020), 173–186.

[BDKN21] A. Bodin, P. Dèbes, J. König and S. Najib, *The Hilbert-Schinzel specialization property*, arXiv:2009.07254 [math.NT] (2021).

[BD21] A. Bodin and P. Dèbes, *Coprime values of multivariable polynomials*, manuscript.

[En16] A. Entin, *On the Bateman-Horn conjecture for polynomials over large finite fields*, Compos. Math. **152** (2016), 2525–2544

[FJ08] M.D. Fried and M. Jarden, *Field arithmetic*, (3rd edition) Springer-Verlag, Berlin (2008).

[Po03] B. Poonen, *Squarefree values of multivariable polynomials*, Monatsh. Math.**12** (1962), 1099–1106.

[Sc02] A. Schinzel, *A property of polynomials with an application to Siegel's lemma*, Monatsh. Math.**12** (1962), 1099–1106.

[Sw62] R.G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **137** (2002), 239–251.

Rationality problem for fields of invariants

Akinari Hoshi

1. Introduction

Let k be a field, K be a finite field extension of k and $K(x_1, \ldots, x_n)$ be the rational function field over K with n variables $x_1, \ldots, x_n$. Let G be a finite subgroup of $\mathrm{Aut}_k(K(x_1, \ldots, x_n))$. The action of G on $K(x_1, \ldots, x_n)$ is called *quasi-monomial* if it satisfies the following three conditions:
(i) $\sigma(K) \subset K$ for any $\sigma \in G$;
(ii) $K^G = k$, where K^G is the fixed field under the action of G;
(iii) for any $\sigma \in G$ and any $1 \le j \le n$,

$$\sigma(x_j) = c_j(\sigma) \prod_{i=1}^{n} x_i^{a_{ij}}$$

where $c_j(\sigma) \in K^\times$ and $[a_{ij}]_{1 \le i,j \le n} \in GL_n(\mathbb{Z})$.

Question 1. *Let K/k be a finite extension of fields and G be a finite group acting on $K(x_1, \ldots, x_n)$ by quasi-monomial k-automorphisms. Under what situation is the fixed field $K(x_1, \ldots, x_n)^G$ k-rational?*

This question includes Noether's problem over k and the rationality problem for algebraic tori as in Sections 2, 3 and 4.

2. Noether's problem over $\mathbb{Q}$

When G acts on $K(x_1, \ldots, x_n)$ by permutation of the variables $x_1, \ldots, x_n$ and trivially on K, i.e. $k = K$, the rationality problem for $K(x_1, \ldots, x_n)^G$ over k is called *Noether's problem*. Define $k(G) = k(x_g : g \in G)^G$ where G acts on $k(x_g : g \in G)$ by $h(x_g) = x_{hg}$ for any $g, h \in G$.

When G is abelian, after works of Masuda, Swan, Endo and Miyata, Voskresenskii, Lenstra [Len74] gave a necessary and sufficient condition to Noether's problem.

Let C_p be a cyclic group of order p. By using PARI/GP, Hoshi [Hos15] confirmed that for primes $p < 20000$, $\mathbb{Q}(C_p)$ is not $\mathbb{Q}$-rational except for 17 rational cases with $p \leq 43$ and $p = 61, 67, 71$ and undetermined 46 cases. Eventually, Plans determined the complete set of primes p for which $\mathbb{Q}(C_p)$ is $\mathbb{Q}$-rational:

Theorem 1 (Plans [Pla17, Theorem 1.1])**.** *Let p be a prime number. Then $\mathbb{Q}(C_p)$ is $\mathbb{Q}$-rational if and only if $p \leq 43$, $p = 61, 67$ or 71.*

When G is non-abelian, only a few results are known, see Garibaldi, Merkurjev and Serre [GMS03].

3. Noether's problem over $\mathbb{C}$

Let G be a finite group, $Z(G)$ be the center of G and $[G, G]$ be the commutator subgroup of G. Two finite groups G_1 and G_2 are called *isoclinic* if there exist group isomorphisms $\theta\colon G_1/Z(G_1) \to G_2/Z(G_2)$ and $\phi\colon [G_1, G_1] \to [G_2, G_2]$ such that $\phi([g, h]) = [g', h']$ for any $g, h \in G_1$ with $g' \in \theta(gZ(G_1))$, $h' \in \theta(hZ(G_1))$:

$$\begin{tikzcd} G_1/Z_1 \times G_1/Z_1 \arrow[r, "(\theta,\theta)"] \arrow[d, "{[\cdot,\cdot]}"'] \arrow[dr, phantom, "\circlearrowleft"] & G_2/Z_2 \times G_2/Z_2 \arrow[d, "{[\cdot,\cdot]}"] \\ {[G_1, G_1]} \arrow[r, "\phi"] & {[G_2, G_2]}. \end{tikzcd}$$

Denote by $G_n(p)$ the set of all the non-isomorphic p-groups of order p^n. In $G_n(p)$, consider an equivalence relation: two groups G_1 and G_2 are equivalent if and only if they are isoclinic. Each equivalence class of $G_n(p)$ is called an *isoclinism family*.

Colliot-Thélène and Ojanguren [CTO89] defined the unramified cohomology groups $H^i_{\mathrm{nr}}(K/\mathbb{C}, \mathbb{Q}/\mathbb{Z})$ of a function field K over $\mathbb{C}$ of degree $i \geq 2$.

Theorem 2 (Hoshi, Kang and Kunyavskii [HKK13, Theorem 1.12])**.** *Let p be any odd prime number and G be a group of order p^5. Then $H^2_{\mathrm{nr}}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \neq 0$ if and only if G belongs to the isoclinism family Φ_{10}. In particular, if G belongs to Φ_{10}, then $\mathbb{C}(G)$ is not retract $\mathbb{C}$-rational.*

The following theorem of Bogomolov and Böhning answers [HKK13, Question 1.11].

Theorem 3 (Bogomolov and Böhning [BB13, Theorem 6])**.** *If G_1 and G_2 are isoclinic finite groups, then $\mathbb{C}(G_1)$ and $\mathbb{C}(G_2)$ are stably $\mathbb{C}$-isomorphic. In particular, $H^i_{\mathrm{nr}}(\mathbb{C}(G_1)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^i_{\mathrm{nr}}(\mathbb{C}(G_2)/\mathbb{C}, \mathbb{Q}/\mathbb{Z})$.*

We obtain the following theorems using GAP:

Theorem 4 (Hoshi, Kang and Yamasaki [HKY20, Theorem 1.14]). *Let G be a group of order 3^5. Then $H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \neq 0$ if and only if G belongs to the isoclinism family Φ_7. Moreover, if $H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \neq 0$, then $H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$.*

$\lvert G\rvert = 3^5$	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7	Φ_8	Φ_9	Φ_{10}
$H^2_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z})$	0	0	0	0	0	0	0	0	0	$\mathbb{Z}/3\mathbb{Z}$
$H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z})$	0	0	0	0	0	0	$\mathbb{Z}/3\mathbb{Z}$	0	0	0

Theorem 5 (Hoshi, Kang and Yamasaki [HKY20, Theorem 1.15]). *Let G be a group of order p^5 where $p = 5$ or $p = 7$. Then $H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \neq 0$ if and only if G belongs to the isoclinism family Φ_6, Φ_7 or Φ_{10}. Moreover, if $H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \neq 0$, then $H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$.*

$\lvert G\rvert = p^5$ $(p = 5, 7)$	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7	Φ_8	Φ_9	Φ_{10}
$H^2_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z})$	0	0	0	0	0	0	0	0	0	$\mathbb{Z}/p\mathbb{Z}$
$H^3_{\rm nr}(\mathbb{C}(G)/\mathbb{C}, \mathbb{Q}/\mathbb{Z})$	0	0	0	0	0	$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}$	0	0	$\mathbb{Z}/p\mathbb{Z}$

As a consequence of Theorem 4, we get an answer to Noether's problem over $\mathbb{C}$ (rationality problem for $\mathbb{C}(G)$) for groups G of order 243:

Theorem 6 (Hoshi, Kang and Yamasaki [HKY20, Theorem 1.16]). *Let G be a group of order 3^5. Then $\mathbb{C}(G)$ is $\mathbb{C}$-rational if and only if $\mathbb{C}(G)$ is retract $\mathbb{C}$-rational if and only if G belongs to the isoclinism family Φ_i where $1 \leq i \leq 6$ or $8 \leq i \leq 9$.*

4. Rationality problem for algebraic tori

When G acts on $K(x_1, \ldots, x_n)$ by purely quasi-monomial k-automorphisms, i.e. $c_j(\sigma) = 1$ for any $\sigma \in G$ and any $1 \leq j \leq n$ in the definition, and G is isomorphic to $\mathrm{Gal}(K/k)$, the fixed field $K(x_1, \ldots, x_n)^G$ is a function field of some algebraic k-torus which splits over K (see Voskresenskii [Vos98, Chapter 2]).

Voskresenskii [Vos67] showed that all the 2-dimensional algebraic k-tori are k-rational. Rationality problem for 3-dimensional algebraic k-tori was solved by Kunyavskii [Kun90]. Stably/retract rationality problem for algebraic k-tori of dimensions 4 and 5 was solved by Hoshi and Yamasaki [HY17]. For further developments, see [HY21], [HHY20], [HKY19], [HKY20].

References

[BB13] F.A. Bogomolov, C. Böhning, *Isoclinism and stable cohomology of wreath products*, Birational geometry, rational curves, and arithmetic, 57–76, Springer, New York, 2013.

[CTO89] J.-L. Colliot-Thélène, M. Ojanguren, *Variétés unirationnelles non rationnelles: au-delà de l'example d'Artin et Mumford*, Invent. Math. **97** (1989), 141–158.

[GMS03] S. Garibaldi, A. Merkurjev, J-P. Serre, *Cohomological invariants in Galois cohomology*, AMS Univ. Lecture Series, vol.28, Amer. Math. Soc., Providence, RI, 2003.

[HHY20] S. Hasegawa, A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori in small dimensions*, Math. Comp. **89** (2020), 923–940.

[Hos15] A. Hoshi, *On Noether's problem for cyclic groups of prime order*, Proc. Japan Acad. Ser. A **91** (2015), 39–44.

[HKY19] A. Hoshi, K. Kanai, A. Yamasaki, *Norm one tori and Hasse norm principle*, arXiv:1910.01469 [math.AG] (2019).
[HKY20] ———, *Norm one tori and Hasse norm principle, II: degree* 12 *case*, arXiv:2003.08253 [math.AG] (2020)
[HKK13] A. Hoshi, M. Kang, B.E. Kunyavskii, *Noether's problem and unramified Brauer groups*, Asian J. Math. **17** (2013), 689–714.
[HKY20] A. Hoshi, M. Kang, A. Yamasaki, *Degree three unramified cohomology groups and Noether's problem for groups of order* 243, J. Algebra **544** (2020), 262–301.
[HY17] A. Hoshi, A. Yamasaki, *Rationality problem for algebraic tori*, Mem. Amer. Math. Soc. **248** (2017), no. 1176, v+215 pp.
[HY21] ———, *Rationality problem for norm one tori*, to appear in Israel J. Math.
[Kun90] B.E. Kunyavskii, *Three-dimensional algebraic tori*, Selecta Math. Soviet. **9** (1990), 1–21.
[Len74] H.W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325.
[Pla17] B. Plans, *On Noether's rationality problem for cyclic groups over* $\mathbb{Q}$, Proc. Amer. Math. Soc. **145** (2017), 2407–2409.
[Vos67] V.E. Voskresenskii, *On two-dimensional algebraic tori II*, Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967), 711–716; translation in Math. USSR-Izv. **1** (1967), 691–696.
[Vos98] ———, *Algebraic groups and their birational invariants*, Translated from the Russian manuscript by Boris Kunyavskii, Translations of Mathematical Monographs, 179. American Mathematical Society, Providence, RI, 1998.

G-rigid local systems are integral

Stefan Patrikis
(joint work with Christian Klevdal)

1. Simpson's conjecture

Let X be a connected smooth quasi-projective variety over $\mathbb{C}$, and let $j\colon X \hookrightarrow \overline{X}$ be an open immersion into a smooth projective variety $\overline{X}$ such that the boundary $D = \overline{X} \setminus X$ is a strict normal crossings divisor. Let

$$\rho\colon \pi_1^{\mathrm{top}}(X, x) \to \mathrm{GL}_n(\mathbb{C})$$

be an irreducible representation of the topological fundamental group such that:

(1) ρ has quasi-unipotent local monodromies along D.
(2) ρ is rigid in the sense that it admits no non-trivial deformations with local monodromies isomorphic to those of ρ.

Then Simpson ([Sim92]) has made the following remarkable conjecture:

Conjecture 1 (Simpson)**.** *Such a ρ comes from geometry: there exists an open dense subvariety $U \subset X$ and a smooth projective family $f\colon Y \to U$ such that $\rho|_{\pi_1^{\mathrm{top}}(U,x)}$ is a summand of the monodromy representation associated to one of the local systems $R^n f_* \underline{\mathbb{C}}$.*

Conjecture 1 is in general wide-open; the conspicuous difficulty (cf. the Fontaine-Mazur conjecture) is that the general setup does not suggest candidates for Y. We summarize known cases:

– When $\overline{X} = \mathbb{P}^1$, Katz has proven the conjecture: see [Kat96, Theorem 8.4.1]. We remark that Katz primarily studies cohomologically rigid local systems on $X \subset \mathbb{P}^1$, those satisfying $H^1(\mathbb{P}^1(\mathbb{C}), j_*\mathrm{End}(\rho)) = 0$. Equivalently, we can replace (the locally free sheaf corresponding to) $\mathrm{End}(\rho)$ above with the subrepresentation $\mathrm{End}^0(\rho)$ on trace-zero matrices. In Katz's setting, he shows ([Kat96, Corollary 1.2.5]) that cohomological rigidity is equivalent to ρ being determined up to isomorphism, or up to one of finitely many isomorphism classes, by the conjugacy classes of its local monodromies. In particular, his work in the cohomologically rigid setting addresses Conjecture 1 as formulated above. In general, however, we have various inequivalent notions of rigidity to consider.
– For general X, Corlette-Simpson ([CS08]) have proven Conjecture 1 for ρ valued in $\mathrm{SL}_2(\mathbb{C})$. For general projective X, Simpson-Langer ([LS18]) have proven Conjecture 1 for ρ valued in $\mathrm{SL}_3(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the ring of integers in some algebraic number field.

It is this *integrality* hypothesis that will primarily concern us here. As a consequence of the motivic expectation of Conjecture 1, Simpson explicitly conjectured that any ρ as in Conjecture 1 is necessarily integral: up to conjugation, ρ factors through $\mathrm{GL}_n(\mathcal{O}_K)$ for the ring of integers $\mathcal{O}_K$ in some number field K. Esnault and Groechenig ([EG18]) have proven this for cohomologically rigid local systems:

Theorem 1 (Esnault-Groechenig)**.** *Let $X/\mathbb{C}$ be a connected smooth quasi-projective variety, and let $\rho\colon \pi_1^{\mathrm{top}}(X, x) \to \mathrm{GL}_n(\mathbb{C})$ be an irreducible representation with finite-order determinant and quasi-unipotent local monodromies that is moreover cohomologically rigid in the sense that $H^1(\overline{X}, j_{!*}\mathrm{End}^0(\rho)) = 0$. Then ρ is integral.*

We remark that the general motivic expectation would imply $\det(\rho)$ has finite order, and more generally that the Zariski closure $\overline{\mathrm{im}(\rho)}^{\mathrm{Zar}}$ of the image of ρ should be semisimple. This determinant hypothesis does not figure in the formulation of Conjecture 1 because it is automatically implied by rigidity (in the sense of the conjecture): see [LS18, Lemma 7.5].

2. The main result

Our main result generalizes the work of Esnault-Groechenig to representations valued in a connected reductive group G.

Definition 1. Let $\rho\colon \pi_1^{\mathrm{top}}(X, x) \to G(\mathbb{C})$ be a homomorphism.

– ρ is G-irreducible if it does not factor through any proper parabolic subgroup of G.
– ρ is G-cohomologically rigid if $H^1(\overline{X}, j_{!*}\rho(\mathfrak{g}^{\mathrm{der}})) = 0$, for $\rho(\mathfrak{g}^{\mathrm{der}})$ the representation $\mathrm{Ad} \circ \rho$ on the derived Lie algebra $\mathfrak{g}^{\mathrm{der}}$ of G. This condition translates to vanishing of the tangent space of a deformation functor of ρ with fixed local monodromies ([KP20, Proposition 4.7]).

Simpson's motivic expectation for rigid local systems extends to this setting of G-rigid local systems. As with Conjecture 1, there are various possibilities for what one might mean by saying such a ρ is "geometric": for simplicity we might ask that in some faithful finite-dimensional representation of G, ρ becomes geometric in the sense of Conjecture 1. We focus on the integrality question but will first mention two beautiful pieces of progress, both when $\overline{X} = \mathbb{P}^1$, on the motivic conjecture for groups other than GL_n. First, Dettweiler and Reiter ([DR14]) have proven the conjecture for many cases of G_2-rigid representations with Zariski-dense image. Second, Yun ([Yun14]) has constructed examples of G_2, E_7, and E_8-rigid representations with Zariski-dense image for which he can prove the conjecture. Crucially, both of these sets of examples involve G-cohomologically rigid local systems that do not in any faithful finite-dimensional representation of G give rise to GL_n-cohomologically rigid local systems: the theory for general G has many open problems even for $\overline{X} = \mathbb{P}^1$. (It is also not hard to construct examples of G-irreducible representations that are not irreducible in any faithful finite-dimensional representation of G). We prove ([KP20]) the following:

Theorem 2 (Klevdal-Patrikis)**.** *Let $\rho\colon \pi_1^{\mathrm{top}}(X,x) \to G(\mathbb{C})$ be a G-irreducible, G-cohomologically rigid homomorphism having quasi-unipotent local monodromies and having finite-order projection to the maximal abelian quotient of G. Then ρ is integral: there exists a number field L such that some conjugate of ρ factors through $G(\mathcal{O}_L)$. Moreover, the identity component of $\overline{\mathrm{im}(\rho)}^{\mathrm{Zar}}$ is semisimple.*

3. Overview of the proof

We follow the strategy of [EG18]. We generalize their integrality criterion to one based on the strong approximation theorem for simply-connected semisimple groups: it suffices to show that ρ factors through $G(\mathcal{O}_K[\frac{1}{\Sigma}])$ for some number field K and finite set of primes Σ of K, and that for all $\lambda' \in \Sigma$, ρ is $G(\overline{K}_{\lambda'})$-conjugate to a $G(\mathcal{O}_{\overline{K}_{\lambda'}})$-valued representation ([KP20, Proposition 3.1]). The first condition follows by showing ρ is isolated in its deformation space ([KP20, Lemma 5.3]). Having reduced to the case of G simple adjoint and fixed $h \in \mathbb{Z}$ such that the h^{th} powers of the local monodromies of ρ are unipotent, there are finitely many G-cohomologically rigid, G-irreducible $\{\rho_i\}_{i=1}^N$ with (local monodromies)^h unipotent. These all factor through some $G(\mathcal{O}_K[\frac{1}{\Sigma}])$. Fix $\lambda \notin \Sigma$. We spread X out and for a suitable prime p specialize X and all ρ_i to characteristic p, yielding representations $\rho_{i,\lambda,\bar{s}}\colon \pi_1^{\text{ét},p'}(X_{\bar{s}}, x_{\bar{s}}) \to G(\mathcal{O}_{K_\lambda})$ of the prime-to-p fundamental group of a characteristic p fiber $X_{\bar{s}}$. Let $G_{i,\lambda} = \overline{\mathrm{im}(\rho_{i,\lambda,\bar{s}})}^{\mathrm{Zar}}$. Each $\rho_{i,\lambda,\bar{s}}$ descends to an arithmetic monodromy representation $\rho_{i,\lambda,s}$ of $\pi_1^{\text{ét}}(X_s, x_{\bar{s}})$, where now X_s is smooth over $\mathbb{F}_p$ ([KP20, §5]). Work of Lafforgue and Drinfeld, and especially [Dri18], shows that each $\rho_{i,\lambda,s}$ admits a λ'-companion (for any λ' not above p)

$$\rho_{i,\lambda',s}\colon \pi_1^{\text{ét}}(X_s, x_{\bar{s}}) \to G_{i,\lambda'}(\overline{\mathbb{Q}}_{\lambda'}) \subset G(\overline{\mathbb{Q}}_{\lambda'});$$

here $G_{i,\lambda'}$ is "the same group" as $G_{i,\lambda}$ but now over $\overline{\mathbb{Q}}_{\lambda'}$. Of course, these representations have profinite image so land in $G(\overline{\mathbb{Z}}_{\lambda'})$. They are provably tame and so can be “unspecialized" back to characteristic zero: we obtain representations

$$\rho_{i,\lambda'}^{\mathrm{top}}\colon \pi_1^{\mathrm{top}}(X,x)\to G(\overline{\mathbb{Z}}_{\lambda'})\xrightarrow{choose} G(\mathbb{C})$$

that can be shown to be the original list $\{\rho_i\}_{i=1}^N$ ([KP20, §6]). It follows that each ρ_i, and thus ρ, is integral at λ'. The theorem follows from the integrality criterion.

References

[CS08] K. Corlette and C. Simpson, *On the classification of rank-two representations of quasiprojective fundamental groups*, Compos. Math. **144** (2008), no. 5, 1271–1331.

[DR14] M. Dettweiler and S. Reiter, *The classification of orthogonally rigid G_2-local systems and related differential operators*, Trans. Amer. Math. Soc. **366** (2014), no. 11, 5821–5851.

[Dri18] V. Drinfeld, *On the pro-semisimple completion of the fundamental group of a smooth variety over a finite field*, Adv. Math. **327** (2018), 708–788.

[EG18] H. Esnault and M. Groechenig, *Cohomologically rigid local systems and integrality*, Selecta Math. (N.S.) **24** (2018), no. 5, 4279–4292.

[Kat96] N.M. Katz, *Rigid local systems*, Annals of Mathematics Studies, vol. 139, Princeton University Press, Princeton, NJ, 1996.

[KP20] C. Klevdal and S. Patrikis, *G-rigid local systems are integral*, arXiv e-prints (2020), 2009.07350.

[LS18] A. Langer and C. Simpson, *Rank 3 rigid representations of projective fundamental groups*, Compos. Math. **154** (2018), no. 7, 1534–1570.

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

[Yun14] Z. Yun, *Motives with exceptional Galois groups and the inverse Galois problem*, Invent. Math. **196** (2014), no. 2, 267–337.

The minimal ramification problem for function fields

Arno Fehm

(joint work with Lior Bary-Soroker, Alexei Entin)

Let G be a nontrivial finite group. The minimal ramification problem is a refinement of the inverse Galois problem, where one asks for the minimal number $r_{\mathbb{Q}}(G)$ of primes of $\mathbb{Q}$ that ramify in Galois extensions of $\mathbb{Q}$ of group G. Based on class field theory and computations, Boston and Markin [BM09] conjectured that

$$r_{\mathbb{Q}}(G)=\max\{1,d(G^{\mathrm{ab}})\}$$

where G^{ab} is the maximal abelian quotient of G, and d denotes the minimal cardinality of a generating set.

In [BEF21] we try to give evidence for this conjecture by studying its function field analogue. For a finite field $\mathbb{F}_q$ we let $r_{\mathbb{F}_q(T)}(G)$ denote the minimal number of primes of the function field $\mathbb{F}_q(T)$ (corresponding to irreducible polynomials in $\mathbb{F}_q[T]$ and the prime at infinity) that ramify in Galois extensions of $\mathbb{F}_q(T)$ of group G in which $\mathbb{F}_q$ is algebraically closed. Following the Boston–Markin heuristic and taking wild ramification into account, we conjecture that for $q=p^\nu$,

$$r_{\mathbb{F}_q(T)}(G)=\max\{1,d((G/p(G))^{\mathrm{ab}})\},$$

where $G/p(G)$ is the maximal quotient of G of order prime to p. For example, for $n \geq 3$ the conjecture predicts that $r_{\mathbb{F}_q(T)}(A_n) = 1$ and $r_{\mathbb{F}_q(T)}(S_n) = 1$ for every q.

Using class field theory we prove that this conjecture holds for abelian groups G, and therefore the right hand side is always a lower bound. We then prove the conjecture for symmetric and alternating groups (and products of these) in many cases, like the following:

Theorem 1 (S_n over $\mathbb{F}_q(T)$). *Let $n > 2$ and $q = p^\nu$ a prime power. Then*

(1) $r_{\mathbb{F}_q(T)}(S_n) \leq 2$, and
(2) $r_{\mathbb{F}_q(T)}(S_n) = 1$ in each of the following cases:
 (a) The analogue for $\mathbb{F}_q(T)$ of Schinzel's hypothesis H holds.
 (b) $q \not\equiv 3 \bmod 4$
 (c) $p < n-1$ or $p = n$
 (d) $q > (2n-3)^2$

Theorem 2 (A_n over $\mathbb{F}_q(T)$). *Let $n \geq 3$ and $q = p^\nu$ a prime power.*

(1) If $p > 2$ or $4|q$, then $r_{\mathbb{F}_q(T)}(A_n) \leq 2$, and
(2) $r_{\mathbb{F}_q(T)}(A_n) = 1$ in each of the following cases:
 (a) $n \geq 13$ and the analogue for $\mathbb{F}_q(T)$ of Schinzel's hypothesis H holds.
 (b) $2 < p < n-1$ or $p = n$ or $p = n-1, p^2|q$ or $p = 3, n = 4$
 (c) $p = 2$ and $4|q$ or $10 \neq n \geq 8, n \equiv 0, 1, 2, 6, 7 \pmod 8$

Theorem 3 (Powers of S_n, A_n over $\mathbb{F}_q(T)$). *Let $p \geq 2$, $q = p^\nu$, $p < n-1$, $k \geq 1$. Then $r_{\mathbb{F}_q(T)}(S_n^k) = \begin{cases} 1, & p = 2 \\ k, & p > 2 \end{cases}$, and if $p \neq 2$, then also $r_{\mathbb{F}_q(T)}(A_n^k) = 1$.*

Finally, by lifting our realizations of S_n over $\mathbb{F}_p(T)$ for large p to $\mathbb{Q}(T)$ and applying results from [BS20], we are able to improve on a result of Plans [Pla04]:

Theorem 4 (S_n over $\mathbb{Q}$). *Schinzel's hypothesis H implies that $r_{\mathbb{Q}}(S_n) = 1$ for every $n > 1$.*

To achieve these results we apply a variety of different approaches, the main ones being the following:

(a) For $p \leq n$ and certain q, we give explicit polynomials following Abhyankar (e.g. [Abh92]) that give realizations ramified over 0 and ∞, tamely over ∞. A second step then eliminates the ramification over ∞ (see below).
(b) For $p > n$ and certain q, we show the existence of realizations ramified over one finite prime and ∞ using results by Adrianov and Zvonkin [AZ15, Adr17] on the monodromy of rational functions and a number theoretic argument involving Weil's Riemann hypothesis for function fields. A second step eliminates the ramification over ∞ using hypothesis H type arguments.
(c) Also in the range $p > n$, we start with an explicit polynomial that gives a realization ramified over $0, 1, \infty$. A second step then eliminates the ramification over ∞ using recent results from [CHLPT15] on small prime gaps over function fields that apply for all $q \geq 107$.

(d) Finally, we verify a few exceptional cases of small n and q using SAGE.

The elimination of ramification over ∞ in (a),(b) is achieved by the following simple principle: Let $f \in \mathbb{F}_q(T)[X]$ with splitting field ramified only over the finite prime $\pi \in \mathbb{F}_q[T]$ of degree d, and tamely over ∞ with ramification index e. If

($*$) there exists $h \in \mathbb{F}_q[T]$ with $e|\deg(h)$ such that $\pi(h)$ is irreducible,

then $\mathrm{Gal}(f(h(T),X)|\mathbb{F}_q(T)) = \mathrm{Gal}(f(T,X)|\mathbb{F}_q(T))$ and $f(h(T),X)$ has splitting field ramified only over $\pi(h)$. This condition ($*$) is a consequence of the analogue of Schinzel's hypothesis H for $\mathbb{F}_q(T)$. The reason that we get unconditional results using approach (b) is that we are able to prove ($*$) in certain cases:

Proposition 5. *In each of the following cases,* ($*$) *holds:*

(1) q *is sufficiently large with respect to* d *and* e *(*[Ent19]*)*
(2) $\mathrm{rad}'(e)|q^\ell - 1$ *for every prime divisor* ℓ *of* d*, and* $q \geq (d-1)^2(2^{\omega(e)}-1)^2$ *(with* $h = T^e - c$*,* $c \in \mathbb{F}_q$*, using* [Coh10]*)*
(3) $\mathrm{rad}'(e)|q-1$ *and* $\gcd(d,e)=1$ *(with* $h = cT^e$*,* $c \in \mathbb{F}_q^\times$*)*

Here $\mathrm{rad}'(e)$ *is the radical of* e *if* $4 \nmid e$*, and twice the radical of* e *if* $4|e$*, and* $\omega(e)$ *is the number of prime divisors of* e*.*

References

[Abh92] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. **27**(1) (1992), 68–133.

[Adr17] N. Adrianov, *Primitive monodromy groups of rational functions with one multiple pole*, J. Math. Sci. **226**(5) (2017), 548–560.

[AZ15] N. Adrianov and A. Zvonkin, *Weighted trees with primitive edge rotation groups*, J. Math. Sci. **209**(2) (2015), 160–191.

[BEF21] L. Bary-Soroker, A. Entin and A. Fehm, *The minimal ramification problem for rational function fields over finite fields*, manuscript (2021).

[BS20] L. Bary-Soroker and T. Schlank, *Sieves and the minimal ramification problem*, J. Inst. Math. Jussieu **19**(3) (2020), 919–945.

[BM09] N. Boston and N. Markin, *The fewest primes ramified in a G-extension of* $\mathbb{Q}$, Ann. Sci. Math. Québec **33**(2) (2009), 145–154.

[CHLPT15] A. Castillo, C. Hall, R.J. Lemke Oliver, P. Pollack, and L. Thompson, *Bounded gaps between primes in number fields and function fields*, Proc. Amer. Math. Soc. **143** (2015), 2841–2856.

[Coh10] S. D. Cohen, *Primitive elements on lines in extensions of finite fields*, Contemporary Mathematics **518** (2010).

[Ent19] A. Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, Int. Math. Res. Not. (2019).

[Pla04] B. Plans, *On the minimal number of ramified primes in some solvable extensions of* $\mathbb{Q}$, Pacific J. Math. **215**(2) (2004).

The p-adic section conjecture for localisations of curves

Martin Lüdtke

We presented the results of our doctoral dissertation in which we obtained new cases of the section conjecture for certain localisations of curves over p-adic fields, thus making a step from the known birational case towards the open case of complete curves.

1. The section conjecture

In 1983, Grothendieck conjectured in his famous letter to Faltings [Gro97] that rational points of curves can be described in terms of the étale fundamental group in the following way. Let X be a smooth, proper, geometrically connected curve over a field k of characteristic zero, let $\overline{k}/k$ be an algebraic closure, denote by $G_k \coloneqq \mathrm{Gal}(\overline{k}/k)$ the absolute Galois group and let $x_0 \in X(\overline{k})$ be a base point. We have a surjective homomorphism $\mathrm{pr}_*\colon \pi_1(X, x_0) \twoheadrightarrow G_k$ induced by the structural morphism $\mathrm{pr}\colon X \to \mathrm{Spec}(k)$. Using the functoriality of the étale fundamental group, any rational point $x \in X(k)$ induces a section $s_x\colon G_k \to \pi_1(X, x_0)$, which is well-defined up to $\pi_1(X_{\overline{k}}, x_0)$-conjugacy. We have thus a map

$$(*) \qquad X(k) \longrightarrow \left(\begin{matrix} \pi_1(X_{\overline{k}}, x_0)\text{-conjugacy} \\ \text{classes of sections of } \mathrm{pr}_* \end{matrix} \right).$$

Conjecture (Section Conjecture)**.** *If k is a finitely generated field extension of $\mathbb{Q}$ and X/k is a proper hyperbolic curve, then the map $(*)$ is a bijection.*

There is also a variant of the section conjecture for open, not necessarily proper, hyperbolic curves $U \subseteq X$. It is based on the observation that even rational points at infinity (also called *cusps*), i.e. points in $(X \setminus U)(k)$, give rise to sections of the fundamental group in the following way. For $x \in (X \setminus U)(k)$, denote by U_x^{h} the *henselisation* of U at x. It is equal to the spectrum of the henselisation of the function field of X at the valuation v_x and constitutes an algebraic analogue of a small punctured disc in X around x. Denoting by $\mathrm{T}^\circ_{X,x}$ the tangent scheme without origin of X at x, it follows from Deligne's theory of tangential base points that there is an isomorphism of étale fundamental groups $\pi_1(U^{\mathrm{h}}_{X,x}) \cong \pi_1(\mathrm{T}^\circ_{X,x})$. In particular, for each nonzero tangent vector v in $\mathrm{T}^\circ_{X,x}(k) \cong \mathbb{A}^1(k) \setminus \{0\}$, we have a section $s_v\colon G_k \to \pi_1(\mathrm{T}^\circ_{X,x}) \cong \pi_1(U^{\mathrm{h}}_{X,x}) \subseteq \pi_1(U)$.

Conjecture (Section conjecture for open curves)**.** *If U/k is a smooth, not necessarily proper, hyperbolic curve with compactification X, then every section of the map $\pi_1(U) \to G_k$ is induced by a unique k-rational point of X.*

The section conjecture for U becomes a weaker statement as U is shrunk smaller. In the limit over all open subcurves of X, i.e. upon passing to the generic point η_X of X, we end up with a birational variant of the section conjecture. Denote by K the function field of X, let $\overline{K}/K$ be an algebraic closure containing $\overline{k}$ and let $G_K \coloneqq \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group. Each k-rational point $x \in X(k)$ induces sections $s_x\colon G_k \to G_K$ in the manner described above.

Conjecture (Birational section conjecture). *Every section of the map $G_K \to G_k$ is induced by a unique k-rational point of X.*

2. The p-adic section conjecture for localisations of curves

While all the above variants of the section conjecture over finitely generated extensions of $\mathbb{Q}$ are wide open, the birational section conjecture for p-adic base fields is known [Koe05]:

Theorem (p-adic birational section conjecture, Koenigsmann 2005). *The birational section conjecture holds if k is a finite extension of $\mathbb{Q}_p$.*

The proof uses model theory of p-adically closed fields. Pop [Pop10] in 2010 gave a different proof based on his local-to-global principle for Brauer groups [Pop88, Theorem 4.5]. In our work we extended Pop's proof from the birational case to more general localisations of curves.

Let X/k be a smooth, proper curve and let $S \subseteq X_{\mathrm{cl}}$ be an arbitrary set of closed points.

Definition. The *localisation* X_S of X at S is defined as

$$X_S := \bigcap_{U \subseteq S} U,$$

where U ranges over the dense open subsets of X containing S and the intersection is taken in the scheme-theoretic sense, i.e. as a fibre product over X.

For example, the localisation at $S = X_{\mathrm{cl}}$ is the full curve X; the localisation at the empty set $S = \emptyset$ is generic point $X_\emptyset = \{\eta_X\}$. In general, the localisation X_S interpolates between those two extremes. We say that X_S satisfies the section conjecture if every section of the map $\pi_1(X_S) \to G_k$ is induced by a unique k-rational point of X.

3. Main results

We identify conditions on X_S under which Pop's proof generalises from the birational case to X_S. By verifying these conditions in a number of cases, we obtain new examples of localised curves which satisfy the section conjecture:

Theorem (L., 2020). *Assume that*

(a) S is at most countable; or
(b) X is defined over a a subfield $k_0 \subseteq k$ and

$$S = \{\textit{transcendental points over } k_0\} \cup \textit{(finite)}.$$

Then X_S satisfies the section conjecture.

Following Pop's strategy, we are actually proving a "minimalistic" version of the section conjecture which works with very small quotients of the fundamental groups and from which the full version is recovered. For a profinite group Π, denote by Π' the maximal p-elementary abelian quotient and by Π'' the maximal $\mathbb{Z}/p\mathbb{Z}$-metabelian quotient. A section $G'_k \to \pi_1(X_S)'$ on the p-elementary abelian level is called *liftable* if it admits a lift to the $\mathbb{Z}/p\mathbb{Z}$-metabelian level $G_k'' \to \pi_1(X_S)''$. We say that X_S satisfies the *liftable section conjecture* if every liftable section is induced by a unique k-rational point of X.

Theorem (L., 2020)**.** *Let k be a finite extension of $\mathbb{Q}_p$ containing the p-th roots of unity. Let X/k be a smooth, proper, geometrically connected curve and $S \subseteq X_{\mathrm{cl}}$ a set of closed points. Assume that the following four conditions are satisfied:*

(Sep): *For all $x \neq y$ in $X(k)$, the map*

$$\mathcal{O}(X_{S\cup\{x,y\}})^\times \to k^\times/k^{\times p}$$

given by $f \mapsto f(x)/f(y)$ is nontrivial.

(Pic): *Every geometrically connected, finite p-elementary abelian cover $W \to X_S$ satisfies* $\mathrm{Pic}(W)/p = 0$.

(Rat): *For all non-rational closed points $x \in X_{\mathrm{cl}}$ for which* $\deg(x)$ *is not divisible by p, the map*

$$\mathcal{O}(X_{S\cup\{x\}})^\times \to \kappa(x)^\times/\,k^\times\kappa(x)^{\times p}$$

given by $f \mapsto f(x)$ is nontrivial.

(Fin): *For every rank one valuation w on K extending the p-adic valuation on k, the following map has finite cokernel:*

$$\mathcal{O}(X_S)^\times \to (K_w^{\mathrm{h}})^\times/(K_w^{\mathrm{h}})^{\times p}.$$

Then X_S satisfies the liftable section conjecture.

We have descent results for the liftable section conjecture which allow us to perform finite Galois extensions of the base field and hence obtain similar statements over fields not containing the p-th roots of unity. Moreover, by a simple argument already implicit in Pop's work, if the liftable section conjecture holds for all finite étale covers of X_S, then the full section conjecture for X_S itself can be deduced.

References

[Gro97] A. Grothendieck, *Brief an G. Faltings*, In: *Geometric Galois actions*, London Mathematical Society Lecture Note Series (1997), 49–58.

[Koe05] J. Koenigsmann, *On the 'Section Conjecture' in anabelian geometry*, Journal für die reine und angewandte Mathematik **588** (2005), 221–236.

[Pop10] F. Pop, *On the birational p-adic section conjecture*, Compos. Math. **146.3** (2010), 621–637.

[Pop88] ———, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. Reine Angew. Math. **392** (1988), 145–175.

[Lüd20] M. Lüdtke, *The p-adic section conjecture for localisations of curves*, Dissertation (2020), online available at: https://www.uni-frankfurt.de/95494079/dissertation.pdf

On the exceptional set in Hilbert's Irreducibility Theorem

Joachim König
(joint work with Danny Neftin)

Hilbert's Irreducibility Theorem (HIT) is one of the fundamental results in arithmetic geometry. In his famous 1892 paper [Hil92], Hilbert showed (in particular) the following:

Theorem 1 (HIT). *Let $F(t, X) \in \mathbb{Q}[t, X]$ be an irreducible polynomial of degree ≥ 1 in X. Then there exist infinitely many rational numbers t_0 such that $F(t_0, X)$ remains irreducible.*

In fact, the set of t_0 which render the specialized polynomial $F(t_0, X)$ reducible may be seen as exceptional in several precise ways. For example this set is a special case of what is nowadays known as a "thin set in the sense of Serre": it is the union of a finite set and finitely many value sets $\varphi_i(X_i(\mathbb{Q}))$ $(i = 1, \ldots, r)$, where $\varphi_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}$ are nontrivial dominant morphisms.

In recent years, various types of effective versions of Hilbert's Irreducibility Theorem have been shown, yielding, e.g., bounds for the least value $t_0 \in \mathbb{Z}$ yielding the irreducibility conclusion (e.g., [DW08]). For some very specific polynomials F, the exceptional set $\mathcal{R}_F := \{t_0 \in \mathbb{Q} \mid F(t_0, X) \text{ reducible } \}$ has also been determined in full.

However, for general classes of polynomials, the best hope is usually to determine $\mathcal{R}_F$ up to finite set - i.e., explicitly determine all the morphisms φ_i as above. We therefore pose the following general problem:

Problem 1. *For an irreducible polynomial $F(t, X) \in \mathbb{Q}[t, X]$, determine the set $\mathcal{R}_F := \mathcal{R}_F := \{t_0 \in \mathbb{Q} \mid F(t_0, X) \text{ is reducible}\}$ up to a finite set.*

We may of course also ask for the set $\mathcal{R}_F := \mathcal{R}_{F,K}$ for polynomials defined over arbitrary number fields, and then also about variants such as the *integral* exceptional set $\mathcal{R}_F \cap O_K$ (where O_K denotes the ring of integers of the number field K). Regarding the latter, a full description has previously been obtained for certain particular F, notably in the case $F(t, X) = f(X) - t$ with an *indecomposable* polynomial $f \in K[X]$. In particular, Fried showed ([Fri71], [Fri86]) that for an indecomposable polynomial $F = f(X) - t \in \mathbb{Q}[t, X]$ with $\deg(f) > 5$, $\mathcal{R}_F \cap \mathbb{Z}$ is, up to a finite set, simply the value set $f(\mathbb{Q}) \cap \mathbb{Z}$. Müller ([Mül99]) generalized those results to arbitrary indecomposable polynomials $F(t, X)$ of prime degree or of Galois group S_n, showing that in this case $R_F \cap \mathbb{Z}$ is finite unless the curve $F(t, X) = 0$ has infinitely many rational points (t_0, x_0) with $t_0 \in \mathbb{Z}$, i.e., corresponds to a so-called Siegel function, for which [Mül13] yields a classification. Such results were based on permutation-group theoretic investigations, in particular the classification of genus-0 actions of primitive permutation groups (occurring as the monodromy groups of polynomials f as above). The step from primitive actions to arbitrary transitive actions, however, is a considerable one and has not been ventured in any sort of generality, meaning that Problem 1 for arbitrary polynomials has remained widely open so far.

In joint work with Danny Neftin ([KN20]), we develop for the first time the necessary machinery to attack Problem 1 in general, and in particular for large classes of polynomials of arbitrary composition length. In particular, we obtain the following result ([KN20, Theorem 1.3]).

Theorem 2 (K., Neftin)**.** *There exists $N > 0$ with the following property. Let $f : X_F \to \mathbb{P}^1_{\mathbb{Q}}$ be the projection to t-coordinates from the curve $F(t,x) = 0$ over $\mathbb{Q}$. Suppose that $f = f_1 \circ \cdots \circ f_r$ for geometrically indecomposable coverings f_i of degree $n_i \geq N$, and of monodromy group A_{n_i} or S_{n_i}, $i = 1,\dots,r$. Then, up to a finite set, $\mathcal{R}_F$ is the union of at most $2r$ value sets $h_j(Y_j(\mathbb{Q}))$, $j = 1,\dots,2r$, of coverings $h_j : Y_j \to \mathbb{P}^1_{\mathbb{Q}}$. Moreover, up to finitely many elements, $\mathcal{R}_F$ equals the union of sets $\mathcal{R}_g$,[1] where g runs through the minimal subcoverings of f.*

We note the relevance of the last conclusion. In recent years, classification results for primitive monodromy groups ([Mül95], [Mül13], [GS07] [NZ20a], [NZ20b]) have enabled a complete description of the set $\mathcal{R}_g$ for indecomposable coverings g of sufficiently large degree. Theorem 2 therefore allows, for the first time in such generality, to reduce the general case to the indecomposable case, under the only assumption that the indecomposables f_i have "general" (i.e., alternating or symmetric) monodromy group. Our methods also apply to somewhat more general scenarios, notably the case in which the indecomposables have almost-simple monodromy group.

Of particular relevance is the special case of polynomials $F(t,X) = f(X) - t$, for which we obtain the following more concise conclusion ([KN20, Theorem 1.1]):

Theorem 3 (K., Neftin)**.** *Let $F(t,X) = f(X) - t \in \mathbb{Q}(t)[x]$ where $f = f_1 \circ \ldots \circ f_r$ for indecomposable $f_i \in \mathbb{Q}[x]$, $i = 1,\dots,r$ of degree ≥ 5, none of which is linearly related to a monomial X^n or a Chebyshev polynomial T_n ($n \in \mathbb{N}$). Assume further that $\deg f_1 > 20$. Then $\mathcal{R}_F$ is either the union of $f_1(\mathbb{Q})$ with a finite set, or f_1 is in an explicitly known list and there exists a rational function $\tilde{f}_1 \in \mathbb{Q}(X)$ such that $\mathcal{R}_F$ is the union of $f_1(\mathbb{Q})$, $\tilde{f}_1(\mathbb{Q})$ and a finite set.*
In both cases, $\mathcal{R}_F$ is the union of $\mathcal{R}_{f_1(X)-t}$ and a finite set.

This has direct applications to several arithmetic problems of interest. Firstly, the special case where $f = g^n := g \circ \cdots \circ g$ is the n-th iterate of a polynomial g, is relevant in arithmetic dynamics. As an immediate corollary of Theorem 3, for every given $n \in \mathbb{N}$, there are at most finitely many *newly irreducible* values of g^n, i.e., values $t_0 \in \mathbb{Q}$ for which $g^n(X) - t_0$ is reducible whereas $g^k(X) - t_0$ is irreducible for each $k = 1,\dots,n-1$. Indeed, up to finitely many exceptions, a reducible value of g^n is even already a reducible value for $g_1(X) - t_0$ where $g = g_1 \circ \cdots \circ g_r$ is a decomposition into indecomposables.

A second application (of the theorem and its proof) concerns the so-called Davenport-Lewis-Schinzel problem (see [DLS61]), asking for the classification of

[1] Here, for a cover $g : Y \to \mathbb{P}^1_{\mathbb{Q}}$, we mean by $\mathcal{R}_g$ the set of $t_0 \in \mathbb{P}^1_{\mathbb{Q}}$ with a reducible fiber $g^{-1}(t_0)$; this may be identified with the set $\mathcal{R}_G$ where $G(t,X)$ is any defining polynomial for g, again up to a finite set.

pairs of polynomials $f, g \in \mathbb{C}[X]$ for which $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is reducible. This classification has previously been obtained by Fried in the case where at least one of f, g is assumed indecomposable ([Fri73]), notably showing that, up to equivalence, only a short finite list of non-trivially reducible pairs (f, g) exist. We are able to reach a conclusion of the same kind (see [KN20, Theorem 1.2]) without the indecomposability assumption (i.e., for polynomials f, g of arbitrary composition length), although at the cost of having to exclude indecomposables with exceptional - namely, solvable - monodromy.

A task for future research would be to relax or entirely drop the restrictions (corresponding to group-theoretical nonsolvability assumptions) in the above theorems. In particular, composition of low-degree indecomposables such as quadratic polynomials seem to pose considerable challenges.

References

[DLS61] H. Davenport, D. J. Lewis, A. Schinzel, *Equations of the form* $f(x) = g(y)$. Quarterly J. of Math. 12 (1961), 304–312.

[DW08] P. Dèbes, Y. Walkowiak, *Bounds for Hilbert's irreducibility theorem.* Pure Appl. Math. Q. 4 (2008), no. 4, Special Issue: In honor of Jean-Pierre Serre. 1059–1083.

[Fri71] M.D. Fried, *On the diophantine equation* $f(y) - x = 0$. Acta Arith. 19 (1971), 79–87.

[Fri73] ———, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables.* Illinois J. of Math. 17 (1973), 128–146.

[Fri86] ———, *Applications of the classification of simple groups to monodromy, part ii: Davenport and Hilbert–Siegel problems*, preprint (1986), 1–55.

[GS07] R. Guralnick, J. Shareshian, *Symmetric and Alternating Groups as Monodromy Groups of Riemann Surfaces I: Generic Covers and Covers with Many Branch Points.* Appendix by R. Guralnick and R. Stafford. Mem. Amer. Math. Soc. 189 (2007).

[Hil92] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten.* J. reine angew. Math. 110 (1892), 104–129.

[KN20] J. König, D. Neftin, *Reducible specializations of polynomials: the nonsolvable case*, arXiv:2001.03630 [math.NT] (2020).

[Mül95] P. Müller, *Primitive monodromy groups of polynomials.* Recent developments in the inverse Galois problem, Contemp. Maths. 186, 385–401, Amer. Math. Soc., 1995.

[Mül13] ———, *Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials.* Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) XII (2013), 369–438.

[Mül99] ———, *Hilbert's irreducibility theorem for prime degree and general polynomials.* Israel J. Math. 109 (1999), 319–337.

[NZ20a] D. Neftin, M. Zieve, *Monodromy groups of indecomposable coverings of bounded genus.* Preprint (2020). `https://neftin.net.technion.ac.il/files/2020/11/monodromy-3.pdf`.

[NZ20b] ———, *Monodromy groups of product type.* Preprint (2020). `https://neftin.net.technion.ac.il/files/2020/11/wreath-2.pdf`.

Some aspects of arithmetic functions in Grothendieck-Teichmüller theory

Hiroaki Nakamura

Euler's functional equation for dilogarithms $Li_2(z)+Li_2(1-z)+\log z\log(1-z) = Li_2(1) = \zeta(2) = \pi^2/6$ was generalized for $k \geq 2$ by Oi-Ueno [7] in the form

$$(\#_{\mathbb{C}}) \qquad \sum_{j=0}^{k-1} Li_{k-j}(z)\frac{(-\log z)^j}{j!} + Li_{1,\dots,1,2}(1-z) = \zeta(k),$$

where the multi-index of $Li_{1,\dots,1,2}$ has $k-2$ times of 1 and the multiple polylogarithmic function $Li_{\mathbf{k}}(z)$ for general $\mathbf{k} = (k_1\dots,k_d) \in \mathbb{N}^d$ is by definition the analytic continuation to the universal cover of $\mathbf{P}^1(\mathbb{C}) - \{0,1,\infty\}$ of the power series

$$\sum_{0<n_1<\cdots<n_d} \frac{z^{n_d}}{n_1^{k_1}\cdots n_d^{k_d}}.$$

In this talk, I presented how to derive an l-adic Galois analog of the above functional equation and indicated connections of the Grothendieck-Teichmüller theory to some neighboring topics such as arithmetic covers, homotopic approaches to Diophantine problems and arithmetic topology.

Let z be a (tangential) point on $\mathbf{P}^1(K) - \{0,1,\infty\}$ for a subfield K of $\mathbb{C}$, and $\gamma : \overrightarrow{01} \rightsquigarrow z$ be a path on $\mathbf{P}^1(\mathbb{C}) - \{0,1,\infty\}$. Fix a prime l and write G_K for the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. The l-adic Galois associator $f_\sigma^z (= f_\sigma^{z,\gamma})$ for $\sigma \in G_K$ is, by definition, the composition of paths $\gamma\cdot\sigma(\gamma)^{-1}$ that forms an element of $\pi_1^{\text{pro-}l} := \pi_1^{\text{pro-}l}(\mathbf{P}^1_K - \{0,1,\infty\}, \overrightarrow{01})$. (We often abbreviate a reference path γ in writing 'z' implicitly to mean 'z and $\gamma : \overrightarrow{01} \rightsquigarrow z$'). Write $f_\sigma^z = f_\sigma^z(x,y)$ with x, y being the free generators of $\pi_1^{\text{pro-}l}$ corresponding to standard loops running around the punctures $0, 1$ respectively. Then, setting $x = \exp(X), y = \exp(Y)$, we obtain the Magnus expansion in the non-commutative power series ring $\mathbb{Q}_l\langle\langle X,Y\rangle\rangle$ as

$$f_\sigma^z(x,y) = 1 + \sum_w c_w^z(\sigma)\cdot w,$$

where w runs over all *non-commutative* monomials in X, Y. A project by Anderson-Ihara/Wojtkowiak may be phrased as to describe all coefficient functions (1-cochains) $c_w^z : G_K \to \mathbb{Q}_l$ in some explicit manners.

Remark 1. The l-adic Galois associator $f_\sigma^{\overrightarrow{10}} = f_\sigma^{\overrightarrow{10},p}$ for the unit interval $p : \overrightarrow{01} \rightsquigarrow z = \overrightarrow{10}$ forms the primary component of the image of $G_{\mathbb{Q}}$ in the (pro-l) Grothendieck-Teichmüller group.

Remark 2. As a quick list of sample applications of non-closed 1-cochains (Magnus coefficients) over G_K, we count a circle of ideas found in [Kim12, footnote 25], [Wic12, Remark 2.8] or [NSW17, Part II].

For each multi-index $\mathbf{k} = (k_1 \ldots, k_d) \in \mathbb{N}^d$, we define the l-adic Galois multiple polylogarithm $\mathcal{L}^z_{\mathbf{k}}(= \mathcal{L}^{z,\gamma}_{\mathbf{k}}) : G_K \to \mathbb{Q}_l$ by setting $\mathcal{L}_{\mathbf{k}}(\sigma) = (-1)^d \cdot c^z_{w(\mathbf{k})}(\sigma)$ $(\sigma \in G_K)$, where $w(\mathbf{k}) := (X^{k_d-1}Y)\cdots(X^{k_1-1}Y)$ is the non-commutative monomial associated to $\mathbf{k} \in \mathbb{N}^d$. Note that the collection $\{w(\mathbf{k})\}_{\mathbf{k}}$ with $\mathbf{k} \in \bigcup_{d\geq 1}\mathbb{N}^d$ forms a subfamily of the free monoid generated by X, Y consisting of the monomials having the letter Y at their rightmost ends. Our goal is to present the functional equation (inversion formula):

$$(\#_l) \qquad \sum_{j=0}^{k-1} \mathcal{L}^z_{k-j}(\sigma)\frac{\rho_z(\sigma)^j}{j!} + \mathcal{L}^{1-z}_{1,\ldots,1,2}(\sigma) = \mathcal{L}^{\overrightarrow{10}}_k(\sigma) \quad (\sigma \in G_K)$$

with $\rho_z : G_K \to \mathbb{Z}_l$ the Kummer 1-cocycle along $\{\sqrt[l^n]{z}\}_{n\in\mathbb{N}}$. Here is a key observation: Let $\theta(*) = 1 - *$ be the involution automorphism of $\mathbf{P}^1$, and with a given path $\overrightarrow{01} \rightsquigarrow z$, associate $\gamma' : \overrightarrow{01} \rightsquigarrow 1-z$ to be the composite $p \cdot \theta(\gamma)$ of the unit interval path $p : \overrightarrow{01} \rightsquigarrow \overrightarrow{10}$ to $\theta(\gamma)$. Then, by a simple computation, we observe

$$(*) \qquad f^{z,\gamma}_\sigma(x,y) = f^{1-z,\gamma'}_\sigma(y,x) \cdot f^{\overrightarrow{10}}_\sigma(x,y).$$

The desired inversion formula $(\#_l)$ follows from comparison of the Magnus expansions of both sides of the above key identity $(*)$, after combined with known explicit formulas for some partial coefficients. For the latter and related topics, we refer the reader to [NW02][NW12][NW20][NW20].

Remark 3. The Magnus series $f^z_\sigma(x,y) \in \mathbb{Q}_l\langle\langle X, Y\rangle\rangle$ may be viewed as the l-adic Galois analog of the standard solution of the (complex or p-adic) KZ-equation $\frac{d}{dz}G_0(z) = (\frac{X}{z} + \frac{Y}{z-1})G_0(z)$ determined by the asymptotic condition $G_0(z) \approx z^X$ $(z \to 0)$. Write $G_0(z) = 1 + \sum_w c_w(z) \cdot w$. Using the characterization of $G_0(z)$ in regard to the KZ differential equation, Furusho ([Fur04]) derived explicit formulas that express each $c_w(z)$ as a polynomial of $Li_{\mathbf{k}}(z)$'s and $\log z$, in particular, showed the inclusion $\{c_w(z)\}_w \subset \mathbb{Q}[\{Li_{\mathbf{k}}(z)\}_{\mathbf{k}}, \log z]$. We pose a question for the l-adic Galois analog whether $\{c^z_w\}_w \subset \mathbb{Q}[\{Li^z_{\mathbf{k}}\}_{\mathbf{k}}, \rho_z]$ holds as collections of functions on G_K.

Remark 4. Investigation of analogy between primes and knots is called "arithmetic topology" and has been intensively studied by Mazur, Morishita, Kapranov, Reznikov and others. Recently Hirano-Morishita [HM19], using Ihara theory, related mod l Milnor invariants to l-adic Galois dilogarithms for $l = 2, 3$. In these cases, Shiraishi [Shi21] confirmed a reciprocity law of the mod-l triple Milnor symbols for primes in light of the functional equation of l-adic Galois dilogarithms.

References

[Fur04] H. Furusho, *p-adic multiple polylogarithms and the p-adic KZ equation*, Invent. Math. **155** (2004), 253–286.

[HM19] H. Hirano, M. Morishita, *Arithmetic topology in Ihara theory II: Milnor invariants, dilogarithmic Heisenberg coverings and triple power residue symbols*, J. of Number Theory, **198** (2019), 211–238.

[Kim12] M. Kim, *Galois theory and Diophantine geometry*, in “Non-abelian fundamental groups and Iwasawa theory” (J. Coates, M.Kim, F.Pop, M.Saïdi, P.Schneider eds.) London Math. Soc. Lect. Note Ser. **393** (2012), 162–187.

[NSW17] H. Nakamura, K. Sakugawa, Z. Wojtkowiak *Polylogarithmic analogue of the Coleman-Ihara formula, I*, Osaka J. Math. **54** (2017), 55–74; *Part II*, RIMS Kokyuroku Bessatsu **B64** (2017), 33-54.

[NW02] H. Nakamura, Z. Wojtkowiak, *On explicit formulae for l-adic polylogarithms*, in “Arithmetic Fundamental Groups and Noncommutative Algebra” (M.D.Fried, Y.Ihara eds.) Proc. Symp. Pure Math., **70** (2002), 285-294.

[NW12] ———, *Tensor and homotopy criteria for functional equations of l-adic and classical iterated integrals*, in “Nonabelian Fundamental Groups and Iwasawa Theory” (J.Coates, M.Kim, F.Pop, M.Saidi, P.Schneider eds.), London Math. Soc. Lecture Note Series, **393** (2012), 258–310 (Cambridge UP).

[NW20] ———, *On distribution formula for complex and l-adic polylogarithms*, in “Periods in Quantum Field Theory and Arithmetic” (J.Burgos Gil, K.Ebrahimi-Fard, H.Gangl eds) Springer Proceedings in Mathematics & Statistics **314** (2020), pp.593–619.

[NW20] ———, *On adelic Hurwitz zeta measures*, J. London Math. Society **101**(3), (2020), 938-959.

[OU13] S. Oi, K. Ueno, *The Inversion Formula of Polylogarithms and the Riemann-Hilbert Problem*, in “Symmetries, Integrable Systems and Representations” (K.Iohara, S. Morier-Genoud, B. Rémy eds.), Springer Proceedings in Mathematics & Statistics **40** (2013), pp.491–496.

[Shi21] D. Shiraishi, *On ℓ-adic Galois polylogarithms and triple ℓ-th power residue symbols*, Kyushu J. Math. **75** (2021), 95–113.

[Wic12] K. Wickelgren, *n-nilpotent obstructions to π_1 sections of $\mathbb{P}^1 - \{0, 1, \infty\}$ and Massey products*, in “Galois-Teichmüller Theory and Arithmetic Geometry” (H.Nakamura, F.Pop, L.Schneps, A.Tamagawa eds.) Adv. Stud. Pure Math., **63** (2012), 579–600.

The parametric dimension

Danny Neftin

(joint work with Pierre Débes, Francois Legrand, Joachim König)

A fundamental measure of the complexity of all G-extensions of $\mathbb{Q}$ is the essential dimension $ed(G) = ed_{\mathbb{Q}}(G)$. More precisely, $ed(G)$ is the minimal integer $d \geq 0$ for which there exists a *G-extension* E/F, of a field F of transcendence degree d over $\mathbb{Q}$, such that every G-extension of (étale algebras) over a field L of characteristic 0 is a specialization of E/F.

The *(essential) parametric dimension* $pd(G) = pd_{\mathbb{Q}}(G)$ is the analogous notion in arithmetic geometry which measures the complexity of all G-extensions of $\mathbb{Q}$ itself. More precisely, $pd(G)$ is the minimal integer $d \geq 0$ for which there exist finitely many G-extensions E_i/F_i, $i = 1, \ldots, r$, with F_i of transcendence degree d over $\mathbb{Q}$, such that every G-extension of $\mathbb{Q}$ is a specialization of E_i/F_i for some i. Very little is known about $pd(G)$.

To estimate $pd(G)$ from below, consider the following analogous local measure of complexity. The *(essential) local dimension* $\ell d(G)$ of G is the minimal integer $d \geq 0$ for which there exist finitely many G-extensions E_i/F_i, $i = 1, \ldots, r$, with F_i of transcendence degree d over $\mathbb{Q}$, such that every G-extension of $\mathbb{Q}_p$ is a specialization of some E_i/F_i for all but finitely many rational primes p. One then has $\ell d(G) \le pd(G)$.

In an earlier joint work with König and Legrand [KLN19], we use the notion of local dimension to study the existence of a parametric G-extension E/F of transcendence degree 1 over $\mathbb{Q}$. In particular, we show that $\ell d(G) > 1$, and hence $pd(G) > 1$, when G contains a noncyclic abelian subgroup. In other words, there exists no parametric G-extension E/F of transcendence degree 1 over $\mathbb{Q}$ when G contains a noncyclic abelian subgroup. In a joint work with Dèbes, König, and Legrand [DKLN21, DKLN20], we prove a geometric analogue of this assertion for all groups and consider the relation to generic extensions.

Another motivation for this local approach comes from Grunwald problems, a stronger version of the inverse Galois problem. It is conjectured by Colliot–Thélène, and by Harari for solvable groups, that for every choice of finitely many G-extensions $L^{(p)}/\mathbb{Q}_p$, $p \in S$, there exists a G-extension $L/\mathbb{Q}$ such that $L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong L^{(p)}$ for all $p \in S \setminus T$, where $T = T(G)$ is a finite set of "bad primes" depending only on G. In this setting, the set of G-extensions $L^{(p)}/\mathbb{Q}_p, p \in S$ is called a *Grunwald problem*, and L is called a *solution*. The conjecture is known to hold for many solvable groups, cf. the recent results of Harpaz–Wittenberg [HW20], Harari [Har07] and Demarche, Lucchini Arteche, and myself [DLN17].

The Hilbert–Grunwald problem, that arises from the work of Dèbes–Ghazi [DG12], asks for the minimal integer $d \ge 0$ for which there exist finitely many G-extensions E_i/F_i with F_i of transcendence degree d, such that every Grunwald problem, avoiding a finite set $T = T_G$, has a solution within the specializations of some E_i. This integer $hgd(G) := d$ is called the Hilbert–Grunwald dimension. In [KLN19], we show that $hgd(G) > 1$ when G contains a noncyclic abelian subgroup.

In a recent joint work with König [KN20], we show that, surprisingly, transcendence degree 2 extensions suffice in order to parametrize all local extensions and solve all Grunwald problems. We show that for every finite group G, there exists a G-extension E/F, with F of transcendence degree 2 over $\mathbb{Q}$, such that every G-extension of $\mathbb{Q}_p$ is a specialization of E/F, for every prime p of $\mathbb{Q}$ outside a finite set T. If furthermore G admits a generic extension over $\mathbb{Q}$, then F can be chosen purely transcendental over $\mathbb{Q}$, and every Grunwald problem $L^{(p)}/\mathbb{Q}_p$, $p \in S \setminus T$ has a solution within the set of specializations of E/F.

Moreover, in [KN20] we show that in fact $pd(G) = \ell d(G)$ whenever certain local global principles hold, suggesting that the invariant $pd(G)$ may be much smaller than $ed(G)$.

Replacing G-extensions by G-torsors, the above definition of essential and parametric dimension carry over to algebraic groups G, and measure the complexity of central simple algebras (CSA's), quadratic forms, and many other algebraic objects. In the case $G = PGL_n$, G-torsors over $\mathbb{Q}$ correspond to degree n central simple algebras (CSA's) over $\mathbb{Q}$. Using the mechanism of [KLN19], jointly with First and Krashen, we show that in this case the parametric dimension is in fact 2!

More precisely, we show that there exist finitely many degree n CSA's $A_1, \dots, A_r$ over $\mathbb{Q}(t,s)$ such that every degree n central simple algebra over $\mathbb{Q}$ is a specialization of A_i for some i. This was previously known only in the case $n = 2$, where degree 2 CSA's are quaternion algebras but the latter method does not apply to cyclic algebras, as cyclic groups of order > 3 have parametric dimension > 1. We are currently studying the parametric dimensions of other reductive groups G.

Beyond complexity problems, there is a substantial advantage in finding parametrizing extensions E_i/F with rational base $F = \mathbb{Q}(t_1, \dots, t_d)$, that is, such that every G-extensions of $\mathbb{Q}$ is a specialization of some E_i. The existence of such parametric extension would give the existence of regular lifts of G-extensions, and hence the Beckmann–Black conjecture, as well as the the finiteness of R-equivalence (rational connectedness) classes on a variety that parametrizes G-extensions of $\mathbb{Q}$. It would also explain when finitely-many G-extensions have a simultaneous regular lift. Further research, aims at proving the existence of finitely many parametrizing G-extensions $E_i/\mathbb{Q}(t_1, \dots, t_d)$ for basic examples, such as dihedral groups, wreath products and nilpotency class 2 groups.

References

[DG12] P. Dèbes, N. Ghazi, *Galois covers and the Hilbert-Grunwald property*, Ann. Inst. Fourier (Grenoble) **62** (2012), 989–1013.

[DKLN21] P. Dèbes, J. König, F. Legrand, D. Neftin, *Rational pullbacks of Galois covers*, to appear in Math. Z..

[DKLN20] ———, *On parametric and generic polynomials with one parameter*, J. Pure App. Algebra **25** (2020), 106717.

[DLN17] C. Demarche, G. Lucchini Arteche, D. Neftin, *The Grunwald problem and approximation properties for homogeneous spaces*, Ann. Inst. Fourier **67** (2017), 1009–1033.

[Har07] D. Harari, *Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini.* (French). Bull. Soc. Math. France, **135** (2007), 549–564.

[HW20] Y. Harpaz, O. Wittenberg, *Zero-cycles sur les espaces homogènes et problème de Galois inverse*, J. Amer. Math. Soc. 33 (2020), 775–805.

[KLN19] J. König, F. Legrand, D. Neftin, *On the local behavior of specializations of function field extensions*, IMRN Vol. 2019 Issue 9, 2951–2980.

[KN20] J. König, D. Neftin, *The local dimension of a finite group over a number field*, arXiv:2007.05383 [math.NT] (2020)

Irreducible automorphic representations with prescribed local behaviours

Hongjie Yu

Deligne [Del15] proposed conjectures concerning the number of local systems with fixed local monodromies on a curve defined over a finite field. The global Langlands correspondence, proved by Drinfeld and Lafforgue, gives a canonical bijection between ℓ-adic local systems and automorphic cuspidal representations. In [Yu18], Deligne's conjecture in everywhere unramified case are proved using automorphic methods. Inspired by Deligne's conjectures and Langlands correspondence, we are interested in the counterpart of his conjectures on automorphic forms.

Let X be a smooth and geometrically connected projective curve over a finite field $\mathbb{F}_q$. For simplicity let G be a split semi-simple linear algebraic group defined on $\mathbb{F}_q$ and $\mathfrak{g}$ its Lie algebra.

Let F be the function field of the curve X: $F = \mathbb{F}_q(X)$, and $\mathbb{A}$ the ring of Adèles. We have the space of G-cusp forms $\mathcal{C}_{cusp}(G)$ which is the space of certain functions over $G(F)\backslash G(\mathbb{A})$. It is a moreover linear representation of $G(\mathbb{A})$ that $G(\mathbb{A})$ acts by translation from right.

Let $S = \{x_1, \cdots, x_r\}$ be a set of closed points of X. For each $x_i \in S_1$, we choose a sub-torus T_i of G defined over the residue field $\kappa(x_i)$ of G, and a character in general position θ_i of $T_i(\kappa(x_i))$. After Deligne-Lustig (fixing an isomorphism between $\mathbb{Q}_\ell$ and $\mathbb{C}$), we obtain an irreducible representation $(-1)^{\mathrm{rk}(T_i)-\mathrm{rk}G} R^{G(\kappa(x_i))}_{T_i(\kappa(x_i))}(\theta_i)$ of $G(\kappa(x_i))$. From these we obtain a representation ρ_i of $G(\mathcal{O}_{x_i})$, where $\mathcal{O}_{x_i}$ is the completion of the structure sheaf $\mathcal{O}_{X,x_i}$. Let ρ be the represenation of $\prod_x G(\mathcal{O}_x)$ which at $x \in S$ is given by the construction above and trivial otherwise. We're interested in the ρ-isotypic part of the space of cusp form. In particular, we would like to know the dimension

$$\dim \mathcal{C}_{cusp}(G)_{\rho-isotypic}.$$

We express this dimension by mass of $\mathbb{F}_q$-points of ξ-stable Hitchin moduli stacks defined by Chaudouard-Laumon [CL10].

Our results can only apply to some special class of ρ called generic, although most of (in a certain sense) ρ satisfy this condition. The datum $(\theta_\bullet)$ is called generic if for any sub-torus S of G which is split and defined over $\mathbb{F}_q$ and immersions $\iota_i : S_{\kappa(x_i)} \to T_i$ we have

$$\prod_{x\in S(\mathbb{F}_q)} \prod_i \theta_i(\iota_i(x)) \neq 1$$

For each i $(1 \leq i \leq r)$, we fix a regular semi-simple element in the Lie algebra of T_i: $t_i \in \mathfrak{t}_i(\kappa(x_i))$. Let C_i be the associate adjoint regular orbit in $\mathfrak{g}(\kappa(x_i))$. A Hitchin pair with fixed residue consists of a G-torrent $\mathcal{E}$ on X_1 and a section $\varphi \in H^0(X - S, \mathrm{Ad}(\mathcal{E})(K + D))$, where $D = x_1 + \cdots x_r$ the associated divisor of S, such that for each x_i in S, we have $\mathrm{res}_{x_i}(\varphi) \in C_i$. We denote by $\mathcal{M}_G(C_\bullet)$ the stacks classifying of these pairs. Supposing that $x_1 \in S$ is a $\mathbb{F}_q$ rational point, Chaudouard-Laumon have defined so-called ξ-stability on $\mathcal{M}_G(C_\bullet)$(or rather on an étale covering of $\mathcal{M}_G(C_\bullet)$. We denoted the stable part by

$$\mathcal{M}_G(C_\bullet)^{\xi-st}.$$

Chaudouard-Laumon have proved that this part is a smooth Deligne-Mumford stack which is proper over the Hitchin base (this fibration is crucial for the proof of Ngo on the fundamental lemma [Ngo10]).

Suppose that the characteristic p of the field $\mathbb{F}_q$ is large for G, $(\theta_\bullet)$ generic and $\mathfrak{t}_1$ is split. Then our main result can be stated as following. For each $s \in G(\mathbb{F}_q)$, there is an integer n_s such that

$$\dim \mathcal{C}_{cusp}(G) = \sum_s n_s q^{-\frac{1}{2}\dim \mathcal{M}_{G_s^0}(C_\bullet)} |(\mathcal{M}_{G_s^0}(C_\bullet)^{\xi-st})(\mathbb{F}_q)|,$$

where the sum is taken over elliptic semi-simple element s such that G_s^0, the connected centralizer of s in G, is semi-simple. The integers n_s depend on $(\theta_\bullet)$ and s but do not depend on the curve. If G is of type A then the above sum reduces to the following equality:

$$\dim \mathcal{C}_{cusp}(G) = n_1 q^{-\frac{1}{2}\dim \mathcal{M}_G(C_\bullet)} |(\mathcal{M}_{G_s^0}(C_\bullet)^{\xi-st})(\mathbb{F}_q)|.$$

References

[CL10] P.-H. Chaudouard and G. Laumon, *Le lemme fondamental pondéré. I. Constructions géométriques.* Compos. Math. 146 (2010), no. 6, 1416-1506.

[Del15] P. Deligne, *Comptage de faisceaux l-adiques.* Astérisque No. 369 (2015), 285-312.

[Ngo10] B.C. Ngo, *Le lemme fondamental pour les algèbres de Lie* Publications Mathématiques de l'IHÉS, Volume 111 (2010), p.1-169

[Yu18] H. Yu, *Comptage des systèmes locaux ℓ-adiques sur une courbe*, arXiv:1807.04659 [math.AG] (2018)

Reductions of K3 surfaces over number fields

Yunqing Tang

(joint work with Ananth Shankar, Arul Shankar, Salim Tayou)

Let K be a number field and X/K an algebraic K3 surface; let $\mathcal{X}$ be a smooth projective model of X over an open subscheme of $\operatorname{Spec} \mathcal{O}_K$, where $\mathcal{O}_K$ denotes the ring of integers of K. For a prime $\mathfrak{p}$ of $\mathcal{O}_K$ in the open subscheme (then X has good reduction at $\mathfrak{p}$), there is an injective map between the Picard groups $\operatorname{Pic}(X_{\overline{K}}) \hookrightarrow \operatorname{Pic}(X_{\overline{\mathbb{F}}_\mathfrak{p}})$, where $\overline{K}$ and $\overline{\mathbb{F}}_\mathfrak{p}$ denote algebraic closures of K and the residue field $\mathbb{F}_\mathfrak{p}$ of $\mathfrak{p}$. In particular, $\operatorname{rk}_\mathbb{Z} \operatorname{Pic}(X_{\overline{K}}) \leq \operatorname{rk}_\mathbb{Z} \operatorname{Pic}(X_{\overline{\mathbb{F}}_\mathfrak{p}})$. We consider the set $S(X)$ of primes $\mathfrak{p}$ such that $\operatorname{rk}_\mathbb{Z} \operatorname{Pic}(X_{\overline{K}}) < \operatorname{rk}_\mathbb{Z} \operatorname{Pic}(X_{\overline{\mathbb{F}}_\mathfrak{p}})$.

We may reformulate the condition on Picard groups in terms of Frobenius actions on the ℓ-adic étale cohomology group $H^2_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell(1))$; see for instance [Cha14, Section 3]. More precisely, for a prime $\mathfrak{p}$ at which X has good reduction, by the Tate conjecture for $\mathcal{X}_{\mathbb{F}_\mathfrak{p}}$ (or over finite extensions of $\mathbb{F}_\mathfrak{p}$),[1] for $\ell \neq \operatorname{char} \mathbb{F}_\mathfrak{p}$, we have

$$\operatorname{Pic}(\mathcal{X}_{\overline{\mathbb{F}}_\mathfrak{p}}) \otimes \mathbb{Q}_\ell = H^2_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{Q}_\ell(1))^{\operatorname{Frob}_\mathfrak{p}^{n_\mathfrak{p}}},$$

where $\operatorname{Frob}_\mathfrak{p} \in \operatorname{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$ is the geometric Frobenius and $n_\mathfrak{p}$ is a large enough positive integer. Moreover, since X has good reduction at $\mathfrak{p}$, there exists an isomorphism $H^2_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell(1)) \cong H^2_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}}_\mathfrak{p}}, \mathbb{Q}_\ell(1))$ such that the above mentioned $\operatorname{Frob}_\mathfrak{p}$ is naturally an Frobenius element of the prime $\mathfrak{p}$ in the image of $\operatorname{Gal}(\overline{K}/K)$

[1] The Tate conjecture for K3 surfaces over finite fields is known by the work of Nygaard [Nyg83], Nygaard–Ogus [NO85], Maulik [Mau14], Madapusi Pera [MP15], Charles [Cha16], Ito–Ito–Koshikawa [IIK], and many others.

acting on $H^2_{\text{ét}}(\mathcal{X}_{\overline{K}}, \mathbb{Q}_\ell(1))$. Thus by this isomorphism, the condition $\mathrm{rk}_\mathbb{Z} \operatorname{Pic}(X_{\overline{K}}) < \mathrm{rk}_\mathbb{Z} \operatorname{Pic}(X_{\overline{\mathbb{F}}_\mathfrak{p}})$ is equivalent to that there exists $n_\mathfrak{p}$ such that

$$H^2_{\text{ét}}(\mathcal{X}_{\overline{K}}, \mathbb{Q}_\ell(1))^\Gamma \subsetneq H^2_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell(1))^{\mathrm{Frob}_\mathfrak{p}^{n_\mathfrak{p}}}$$

for any finite index subgroup $\Gamma \subset \mathrm{Gal}(\overline{K}/K)$. Based on this interpretation in terms of Galois group actions, [Cha14, Theorem 1] classified K3 surfaces into two types and proved that for K3 surfaces of the first type, the set $S(X)$ is of density 0 (after possibly extending K by a finite extension) and for those of the second type, the Tate conjecture implies that the set $S(X)$ consists all the primes of $\mathcal{O}_K$.

For K3 surfaces of the first type, Charles's theorem gives an upper bound of the size of $S(X)$. One main application of our main theorem in this case gives a lower bound of $S(X)$ (under the technical assumption that there exists a smooth projective model $\mathcal{X}$ over the entire $\operatorname{Spec} \mathcal{O}_K$); more precisely, we proved that $\#S(X) = \infty$.

Theorem 1 ([SSTT, Theorem 1.1])**.** *For X/K with potentially good reduction everywhere, there are infinitely many $\mathfrak{p}$ such that $\mathrm{rk}_\mathbb{Z} \operatorname{Pic}(X_{\overline{K}}) < \mathrm{rk}_\mathbb{Z} \operatorname{Pic}(\mathcal{X}_{\overline{\mathbb{F}}_\mathfrak{p}})$.*

For a Kummer surface X over K of the first type in Charles's work, the above theorem (without the potentially good reduction everywhere assumption) was proved by Charles [Cha14] and Ananth N. Shankar and myself [ST20]. These two results are formulated in terms of the Néron–Severi groups of the corresponding abelian surfaces.

The complex analytic analogue of our theorem is well-understood. More precisely, for a non-isotrivial family $\mathcal{X}$ of K3 surfaces over a quasi-projective curve $C/\mathbb{C}$, the Noether–Lefschetz locus $\{t \in C(\mathbb{C}) \mid \mathrm{rk}_\mathbb{Z} \operatorname{Pic}(\mathcal{X}_t) > \min_{s\in C(\mathbb{C})} \mathrm{rk}_\mathbb{Z} \operatorname{Pic}(\mathcal{X}_s)\}$ is dense in $C(\mathbb{C})$ with respect to the complex analytic topology by a classical theorem of Green ([Voi02, Proposition 17.20]; see also [Ogu03]). Moreover, Tayou [Tay20] proved that the Noether–Lefschetz locus is equidistributed with respect to a natural measure on $C(\mathbb{C})$.

Indeed, Theorem 1 is a special case of Theorem 2 below formulated in terms of GSpin Shimura varieties and special divisors. More precisely, given a non-degenerate quadratic space (V, Q) over $\mathbb{Q}$ of signature $(b, 2)$, one can define a Shimura variety of Hodge type with canonical model $M/\mathbb{Q}$ (after choosing a suitable level structure); the classical Torelli map of K3 surfaces relates the moduli space of polarized K3 surfaces over $\mathbb{C}$ to $M_\mathbb{C}$ for certain (V, Q) of signature $(19, 2)$; see for instance [MP15, Sections 1.3, 4.4, 5].[2] Moreover, there are special divisors (also known as Heegner divisors) $Z(m), m \in \mathbb{Z}_{>0}$ on $M/\mathbb{Q}$ and the K3 surfaces whose images under the Torelli map lie in $Z(m)$ are those with $\mathrm{rk}_\mathbb{Z} \operatorname{Pic} \geq 2$. By the work of Kisin [Kis10], Madapusi Pera [MP16], Andreatta–Goren–Howard–Madapusi-Pera [AGHMP18],

[2]More precisely, the Torelli map defines an étale morphism of a finite cover of the moduli space of K3 surfaces to the orthogonal Shimura variety attached to (V, Q) over $\mathbb{C}$ and M admits a finite étale map to the orthogonal Shimura variety.

there are nice integral models $\mathcal{M}, \mathcal{Z}(m)$ over $\mathbb{Z}$ (with certain specific level structure) of $M, Z(m)$.

Theorem 2 ([SSTT, Theorem 1.8]). *Let $\mathcal{Y} \in \mathcal{M}(\mathcal{O}_K)$ and assume that $b \geq 3$ and $\mathcal{Y}_K \notin Z(m)$ for all m. Then there are infinitely many $\mathfrak{p}$ such that $\mathcal{Y}_{\overline{\mathbb{F}}_{\mathfrak{p}}} \in \mathcal{Z}(m)$ for some $m \in \mathbb{Z}_{>0}$ (here m depends on $\mathfrak{p}$).*

We deduce Theorem 1 from Theorem 2 by taking (V, Q) to be the transcendence part of the second Betti cohomology group $H^2(X(\mathbb{C}), \mathbb{Q})$ (equipped with the natural quadratic form given by the cup product).[3]

Theorem 2 is proved by comparing the asymptotic of the local intersection number of $\mathcal{Y}$ and $\mathcal{Z}(m)$ at a given finite prime $\mathfrak{p}$ to that of the total finite intersection number of $\mathcal{Y}$ and $\mathcal{Z}(m)$ summing over all primes as $m \to \infty$ (we actually compare the asymptotics on average in terms of m). The idea of using a local-global estimate to establish infinitude of primes goes back to the work of Charles [Cha18], but the techniques in obtaining the desired estimates in the setting of general GSpin Shimura varieties beyond the modular curve case in [Cha18] are different.

More precisely, the total sum of local intersection numbers at all finite places equals to the Arakelov height of $\mathcal{Y}$ minus the contribution from a Green function Φ_m associated to $\mathcal{Z}(m)$. The main term in this part is estimated by using the arithmetic Borcherds theory due to Howard–Madapusi-Pera [HMP] and an explicit description of Φ_m by Bruinier [Bru02].

The computation of the local intersection multiplicity amounts to counting certain special endomorphisms of the abelian surface or Kuga–Satake abelian variety $A \bmod \mathfrak{p}^n$. We use Grothendieck–Messing theory to study the asymptotic behavior of the lattice of special endomorphisms as $n \to \infty$ and then use the circle method to obtain an estimate of the main term. In order to bound the error term, we use the global height formula to obtain an estimate of the asymptotic of the first successive minimum for the lattices of special endomorphisms and then conclude by a geometry-of-numbers argument. An estimate of the error term in the contribution from Green functions is obtained in a way similar to the treatment for finite places.

In [SSTT], we also discussed applications of [SSTT, Theorem 1.8] and its refinement [SSTT, Theorem 2.4] to reductions of abelian varieties over number fields.

References

[AGHMP18] F. Andreatta, E.Z. Goren, B. Howard, and K. Madapusi Pera. Faltings heights of abelian varieties with complex multiplication. *Ann. of Math. (2)*, 187(2):391–531, 2018.

[Bru02] J.H. Bruinier. *Borcherds products on O(2, l) and Chern classes of Heegner divisors*, volume 1780 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.

[Cha14] F. Charles. On the Picard number of K3 surfaces over number fields. *Algebra Number Theory*, 8(1):1–17, 2014.

[Cha16] ———. Birational boundedness for holomorphic symplectic varieties, Zarhin's trick for $K3$ surfaces, and the Tate conjecture. *Ann. of Math. (2)*, 184(2):487–526, 2016.

[3] If $\mathrm{rk}_{\mathbb{Z}} \operatorname{Pic}(X_{\overline{K}}) \geq 18$ and thus we have $b \leq 2$, the arguments in [Cha18] and [ST20] apply.

[Cha18] ______. Exceptional isogenies between reductions of pairs of elliptic curves. *Duke Math. J.*, 167(11):2039–2072, 2018.
[HMP] B. Howard and K. Madapusi Pera. Arithmetic of Borcherds products, arXiv:1710.00347 [math.NT] (2017)
[IIK] K. Ito, T. Ito, and T. Koshikawa. CM liftings of K3 surfaces over finite fields and their applications to the Tate conjecture, arXiv:1809.09604 [math.NT] (2018)
[Kis10] M. Kisin. Integral models for Shimura varieties of abelian type. *J. Amer. Math. Soc.*, 23(4):967–1012, 2010.
[Mau14] D. Maulik. Supersingular K3 surfaces for large primes. *Duke Math. J.*, 163(13):2357–2425, 2014. With an appendix by Andrew Snowden.
[MP15] K. Madapusi Pera. The Tate conjecture for K3 surfaces in odd characteristic. *Invent. Math.*, 201(2):625–668, 2015.
[MP16] ______. Integral canonical models for spin Shimura varieties. *Compos. Math.*, 152(4):769–824, 2016.
[Nyg83] N.O. Nygaard. Tate's conjecture for ordinary $K3$ surfaces over finite fields. *Invent. Math.*, 74(2): 213–237, 1983.
[NO85] N. Nygaard and A. Ogus. Tate's conjecture for $K3$ surfaces of finite height. *Ann. of Math. (2)*, 122(3):461–507, 1985.
[Ogu03] K. Oguiso. Local families of $K3$ surfaces and applications. *J. Algebraic Geom.*, 12(3):405–433, 2003.
[SSTT] A.N. Shankar, A. Shankar, Y. Tang, and S. Tayou. Exceptional jumps of Picard ranks of reductions of K3 surfaces over number fields, arXiv:1909.07473 [math.NT] (2019).
[ST20] A.N. Shankar and Y. Tang. Exceptional splitting of reductions of abelian surfaces. *Duke Math. J.*, 169 (3): 397–434, 2020.
[Tay20] S. Tayou. On the equidistribution of some Hodge loci. *J. Reine Angew. Math.*,762: 167–194, 2020.
[Voi02] C. Voisin. *Théorie de Hodge et géométrie algébrique complexe.* Collection SMF. Société Mathématique de France, 2002.

A linear variant of GT

Adam Topaz
(joint work with Florian Pop)

1. Introduction

The *Grothendieck-Teichmüller group*, henceforth denoted $\widehat{\mathbf{GT}}$, was introduced by Drinfeld [Dri91] as a subgroup of $\mathrm{Aut}(\widehat{F_2})$ defined by certain explicit equations. Here $\widehat{F_2}$ denotes the free profinite group on two generators. Amazingly, there is a natural morphism

$$\rho\colon\ \mathrm{Gal}_{\mathbb{Q}} \to \widehat{\mathbf{GT}}$$

arising from the identification of $\widehat{F_2}$ with the geometric étale fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ with respect to the tangential base-point $\overrightarrow{01}$. It is a well-known consequence of Belyi's theorem that the map ρ above is *injective*, although the surjectivity of this map remains one of the most important open problems in modern Galois theory.

1.1. **A functorial description.** The group $\widehat{\mathbf{GT}}$ has several alternative descriptions which highlight the connection with Galois theory. Let $\mathcal{M}_{0,n}$ denote the moduli-space of genus 0 curves with n marked points, and let $\widehat{K}(0,n)$ denote its geometric étale fundamental group. Harbater-Schneps [HS00] showed that $\widehat{\mathbf{GT}}$ can be described as a subgroup of $\mathrm{Out}(\widehat{K}(0,5))$ consisting of elements which commute with the image of the canonical map $S_5 \to \mathrm{Out}(\widehat{K}(0,5))$ arising from the action of S_5 on $\mathcal{M}_{0,5}$, and which are compatible with the conjugacy classes of the inertia groups associated to the boundary components of $\mathcal{M}_{0,5}$.

This result was recently refined in the works of Hoshi-Minamide-Mochizuki [HMM17] and Minamide-Nakamura [MN19]. A consequence of their work shows that $\widehat{\mathbf{GT}}$ can be described as the outer-automorphism group of a certain diagram of profinite groups arising from the genus-zero portion of the Grothendieck-Teichmüller tower. In more precise terms, consider the smallest category of $\mathbb{Q}$-varieties whose objects are $\mathcal{M}_{0,n}$ for $n = 4, 5$, and which contains the following morphisms:

(1) The automorphisms $\mathcal{M}_{0,n}$, $n = 4, 5$, arising from the natural action of S_n obtained by "permuting the n-marked points."
(2) The projections $\mathcal{M}_{0,5} \to \mathcal{M}_{0,4}$ obtained by "forgetting one of the marked points."

Denote this category of $\mathbb{Q}$-varieties by $\mathcal{V}_0$. Consider the functor $\bar{\pi}_1$ from the category of $\mathbb{Q}$-varieties to the category of profinite groups with *outer* morphisms which associates the geometric étale fundamental group to a variety. For any subcategory $\mathcal{V}$ of the category of $\mathbb{Q}$-varieties, there is a natural action of $\mathrm{Gal}_{\mathbb{Q}}$ on the restriction of this functor $\bar{\pi}_1|_{\mathcal{V}}$, arising simply from the canonical outer Galois action on geometric étale fundamental groups. With this terminology, the consequence of [HMM17, MN19] alluded to above can be summarized by saying that $\widehat{\mathbf{GT}}$ is naturally isomorphic to $\mathrm{Aut}(\bar{\pi}_1|_{\mathcal{V}_0})$, and that this isomorphism is compatible with the canonical maps from $\mathrm{Gal}_{\mathbb{Q}}$.

1.2. **Line arrangements.** The starting point of the work reported on in this talk is the observation that

$$\mathcal{M}_{0,4} = \mathbb{P}^1 \setminus \{0, 1, \infty\},\ \mathcal{M}_{0,5} = (\mathcal{M}_{0,4})^2 \setminus \Delta,$$

where Δ denotes the diagonal in the cartesian square. In other words, one has

$$\mathcal{M}_{0,5} = \mathbb{A}^2 \setminus \mathbf{L}_0,$$

where $\mathbf{L}_0$ is the zero-locus of the function $x \cdot (1-x) \cdot y \cdot (1-y) \cdot x - y$ on the $\mathbb{Q}$-variety $\mathbb{A}^2 = \operatorname{Spec} \mathbb{Q}[x, y]$. Note that $\mathbf{L}_0$ is a closed subvariety of $\mathbb{A}^2$ which is (geometrically) a finite union of affine lines. With this in mind, we consider the following category $\mathcal{L}$ of $\mathbb{Q}$-varieties. The objects of $\mathcal{L}$ have one of two forms:

(1) The variety $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.
(2) Complements of the form $\mathcal{U}_{\mathbf{L}} := \mathbb{A}^2 \setminus \mathbf{L}$, where $\mathbf{L}$ is a closed subvariety of $\mathbb{A}^2$ which is geometrically a finite union of affine lines.

The nonidentity morphisms of $\mathcal{L}$ have one of the following two forms:

(1) The inclusions among the $\mathcal{U}_{\mathbf{L}}$.

(2) The projections $\mathcal{U}_{\mathbf{L}} \to \mathbb{P}^1 \setminus \{0,1,\infty\}$ associated to the rational functions $x, y, x-y$, whenever $\mathbf{L}$ is sufficiently large.

1.3. **Results.** Instead of working with profinite fundamental groups, we consider their pro-ℓ two-step nilpotent quotients. To be precise, fix a prime ℓ, write $\bar{\pi}_1(X)^{(\ell)}$ for the maximal pro-ℓ quotient of $\bar{\pi}_1(X)$, and consider

$$\Pi_X^c := \frac{\bar{\pi}_1(X)^{(\ell)}}{[\bar{\pi}_1(X)^\ell, [\bar{\pi}_1(X)^\ell, \bar{\pi}_1(X)^\ell]]}, \ \Pi_X^a := \frac{\bar{\pi}_1(X)^{(\ell)}}{[\bar{\pi}_1(X)^\ell, \bar{\pi}_1(X)^\ell]}.$$

Note that Π_X^c and Π_X^a are both functorial in X, and that Π_X^a is a (functorial) quotient of Π_X^c. Write Π^c and Π^a for these functors and put

$$\mathrm{Aut}^c(\Pi^a|_{\mathcal{L}}) := \mathrm{image}(\mathrm{Aut}(\Pi^c|_{\mathcal{L}}) \to \mathrm{Aut}(\Pi^a|_{\mathcal{L}})).$$

Observe that we have a canonical morphism $\rho : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}^c(\Pi^a|_{\mathcal{L}})$, as well as a natural map $\mathbb{Z}_\ell^\times \to \mathrm{Aut}^c(\Pi^a|_{\mathcal{L}})$ arising from the scalar action of $\mathbb{Z}_\ell^\times$ on Π_X^a. The main theorem of the work presented in this talk can now be stated as follows.

Theorem 1. *The canonical map* $\rho : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}^c(\Pi^a|_{\mathcal{L}})_{/\mathbb{Z}_\ell^\times}$ *is an isomorphism.*

This theorem is a special case of a more general result which generalizes the above statement along the following three axes:

(1) One may consider hyperplane arrangements in $\mathbb{A}^n$ whenever $n \geq 2$, with the above theorem being the special case of $n = 2$.
(2) One may replace Π^c and Π^a with the quotients by the third resp. second terms in the so-called Λ-*Zassenhaus filtration* of $\bar{\pi}_1$, where Λ is any nontrivial quotient of $\mathbb{Z}_\ell$. The above theorem is the special case of $\Lambda = \mathbb{Z}_\ell$.
(3) The field $\mathbb{Q}$ can be replaced with an arbitrary perfect base-field k_0, assuming that $\mathcal{L}$ is generalized accordingly.

2. A brief outline of the argument

We now give a very brief outline of the proof of the theorem mentioned in the previous section. Write $\mathfrak{G} := \mathrm{Aut}^c(\Pi^a|_{\mathcal{L}})$, and put

$$\mathbf{\Pi}^\star := \varprojlim_{\mathbf{L}} \Pi^\star_{\mathcal{U}_{\mathbf{L}}}, \ \star \in \{a, c\}.$$

The group $\mathfrak{G}$ acts on $\mathbf{\Pi}^a$ compatibly with the relation $[-,-] = 0$ where $[-,-]$ refers to the $\mathbb{Z}_\ell$-bilinear commutator on $\mathbf{\Pi}^a$ taking values in the kernel of $\mathbf{\Pi}^c \to \mathbf{\Pi}^a$.

2.1. **The local theory.** In this step we parameterize the affine lines in $\mathbb{A}^2$ via their decomposition and inertia groups in $\mathbf{\Pi}^a$, using only the following data:

(1) The group $\mathbf{\Pi}^a$ and the relation $[-,-] = 0$.
(2) Additional data arising from the projections to $\mathbb{P}^1 \setminus \{0,1,\infty\}$ in $\mathcal{L}$.

The action of $\mathfrak{G}$ is compatible with this data, hence we obtain an action of $\mathfrak{G}$ on the collection of such lines. As a consequence of the construction, it turns out that this action is compatible with the sets of lines which are vertical over the x resp. y-axes of $\mathbb{A}^2$. Identifying points in $\mathbb{A}^2(\overline{\mathbb{Q}})$ with their (x,y)-coordinates, this provides an action of $\mathfrak{G}$ on $\mathbb{A}^2(\overline{\mathbb{Q}})$.

2.2. **The global theory.** In this portion of the argument, we prove that the action of $\mathfrak{G}$ on the collection of affine lines and on $\mathbb{A}^2(\overline{\mathbb{Q}})$ is compatible with *incidence* in $\mathbb{A}^2$. A variant of the *fundamental theorem of projective geometry* is then applied to deduce that $\mathfrak{G}$ acts on $\mathbb{A}^2(\overline{\mathbb{Q}})$ via elements of $\mathrm{Gal}_{\mathbb{Q}}$. This thereby provides a left inverse to the canonical map $\rho\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathfrak{G}$. To conclude the proof of the above theorem, we prove that the kernel of this left inverse agrees with the image of the map $\mathbb{Z}_\ell^\times \to \mathfrak{G}$.

References

[Dri91] V.G. Drinfel'd, *On quasitriangular quasi-Hopf algebras and on a group that is closely connected with* $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, Leningrad Math. J. **2** (1991), no. 4, 829–860.

[HS00] D. Harbater and L. Schneps, *Fundamental groups of moduli and the Grothendieck-Teichmüller group*, Trans. Amer. Math. Soc. **352** (2000), no. 7, 3117–3148.

[HMM17] Y. Hoshi, A. Minamide and S. Mochizuki, *Group-theoreticity of numerical invariants and distinguished subgroups of configuration space groups*, RIMS preprint 1870 (2017).

[MN19] A. Minamide and H. Nakamura, *The automorphism groups of the profinite braid groups*, arXiv:1904.06749 [math.GT], to appear in *Amer. J. Math.* (2019).

Simplicial and homotopical aspects of arithmetic geometry

Benjamin Collas

Following the "Longue marche à travers la théorie de Galois" (1981) and the study of the absolute Galois group of rational via combinatorial group-theoretic properties of the moduli spaces of curves $\mathcal{M}_{g,[m]}$ – now Grothendieck-Teichmüller and anabelian geometry theories, Grothendieck's "À la poursuite des champs" (1983) lays the theoretical and *categorical* foundation for closing further the gap between algebraic topology and algebraic geometry – see now Lurie's ∞-categories and Toën's geometry. As early exploited by T. Oda, this includes the higher consideration of homotopy groups and stack symmetries of the arithmetic of the spaces.

This report reviews results and techniques from *Homotopical Arithmetic Geometry* in relation with the rational, motivic, and arithmetic aspects of the workshop (Topics a, b and c) such as led **(1)** by these higher consideration, and **(2)** by bringing closer spaces, anabelian and abelian geometries – see Fig. 1.

$$\begin{tikzcd}
\mathrm{Sch}_k \arrow[dr, "\{-\}_{et}"] \arrow[drr, bend left, "(-)_{\mathbb{A}^1}"] \arrow[dd] & & & \mathcal{SH}^{et}(\mathbb{Q}) \arrow[dd, shift left, "N"] \\
& \text{Pro-Sp} \arrow[r, shift right, "S"'] & \mathcal{H}^{et}(\mathbb{Q}) \arrow[l, shift right, "R_{et}"'] \arrow[ur, "\Sigma^\infty"] \arrow[dr, dashed] & \\
\mathrm{St}(k) \arrow[ur, dashed, "\{-\}_{et}"] \arrow[urr, dashed, bend right, "(-)_{\mathbb{A}^1}"'] & & & DA^{et}(\mathbb{Q}) \arrow[uu, shift left, "\Gamma"]
\end{tikzcd}$$

Spaces Anab. Geo. $\mathbb{A}^1$-Geo. Motives

Fig 1. Geometries, arithmetic and motives: Friedlander's pro-spaces, Morel-Voevodsky's (un)stable motivic homotopy, and Ayoub's motives.

1. Geometric Galois Action and Anabelian Geometry

Anabelian investigations rely on seminal properties of the arithmetic-geometric exact sequence **(AGS)** and the associated geometric Galois action **(GGA)**:

$$1 \leftarrow \pi_1^{et}(\mathrm{Spec}(k)) \overset{\dashrightarrow}{\leftarrow} \pi_1^{et}(X,*) \leftarrow \pi_1^{et}(X_{\bar{k}},*) \leftarrow 1 \qquad \rightsquigarrow G_k \to \mathrm{Out}[\pi_1^{et}(X_{\bar{k}},*)].$$

Following Grothendieck's original insight, they are expressed in terms of group-theoretic properties (e.g. center-freeness, terminality of inertia-decomposition groups) for *topological* $K(\pi,1)$ varieties over number fields (H. Nakamura, A. Tamagawa) and p-adic fields (S. Mochizuki, Y. Hoshi) – see [IN97] for an overview.

1.1. **Anabelian Geometry & Étale Homotopy Type.** For k sub-p-adic field, X a smooth connected variety and Y a hyperbolic curve over k, a reformulation of Mochizuki's Th. A in terms of $\{X\}_{et}$ is given by [SS16]:

$$\{-\}_{et}\colon \mathrm{Isom}_K(X,Y) \underset{K(\pi,1)}{\xrightarrow{\sim}} \mathrm{Isom}_{\mathrm{Ho(Pro\text{-}Sp)}\downarrow ket}[\{X\}_{et},\{Y\}_{et}] \tag{1}$$

that follows the expected π_1-Hom-property between classifying pro-space BG and pro-group G, and relies on the centre-freeness of G_k.

In higher dimension, assuming a certain factor-dominant immersion $Y \hookrightarrow C_1 \times \cdots \times C_n$ into hyperbolic curves (HC) provides over number fields **(1)** the *existence of a functorial retract* of $\{-\}_{et}$ by application of Tamagawa's Lemma for separating rational points and of Lefschetz counting-points formula, that implies **(2)** that:

> *Every smooth variety over a number field K admits a relative anabelian Zariski basis $\mathcal{U}$,*

i.e. such that Eq. (1) is satisfied for any X, $Y \in \mathcal{U}$ – see ibid.

Note that the later relies on the existence of strongly hyperbolic Artin neighbourhoods in smooth varieties, i.e. for the scheme to be the abutment of some *elementary fibrations* into hyperbolic curves $\{X_i\}_{i=0,\dots,n}$ that satisfy the (HC) property.

1.2. **Higher Anabelian Topological Types.** For $\mathcal{M}$ Deligne-Mumford stacks, and for the moduli of curves $\mathcal{M}_{g,[m]}$ in particular, the stack inertias $I_{\mathcal{M},*} \to \mathcal{M}$ of *cyclic type* share similar properties with the divisorial (anabelian) ones: they are topological generators with a GGA Tate-type [CM14], and Serre's goodness is at once an Artin neighbourhood and a $I_{\mathcal{M}}$-property – that measures the discrepancy between topological and étale $K(\pi,1)$. This motivates *the investigation of stack anabelian obstructions in terms of* $\{\mathcal{M}\}_{et}$ – see $\{-\}_{et}$ in Fig. 1 and §2.

In terms of higher dimensional anabelian geometry, one could investigate some étale topological type Postnikov anabelian obstruction for well-chosen varieties over number fields. We also refer to techniques of p-adic fields which provides natural classes of anabelian spaces beyond curves and schemes (e.g. of Belyi type, quasi-tripod) for absolute (and relative) versions of (2) above – see Y. Hoshi's report in this volume.

1.3. **An Anabelian $\mathbb{A}^1$-geometry?** It follows Isaksen's Quillen adjunction (R_{et}, S) – see also A. Schmidt's work – that $\{-\}_{et}$ factorizes through $(-)_{\mathbb{A}^1}$, thus motivating the investigation of *anabelian obstructions in terms of non-$\mathbb{A}^1$-rigid invariants.*

2. Motives for the Moduli Stack of Curves

Morel-Voevodsky's (unstable) motivic homotopy categories $\mathcal{H}^{et}(k)$ and $\mathcal{SH}^{et}(k)$ of simplicial presheaves – and spectras of – provides a functorial bridge between the arithmetic and motivic properties of spaces – see Fig. 1; from the category of stacks $\mathrm{St}(k)$ to Ayoub's derived weak Tannaka category $DA^{et}(k)$.

2.1. **Algebraic & Topological Circles for Stacks.** Jardine's Quillen categorical $\mathrm{St}(k) = \mathrm{Ho}[sPr_{et}(\mathrm{Aff}_k)]$ leads to the definition of motive for stack $M(\mathcal{M}) := N[\Sigma^\infty(M_{\mathbb{A}^1})]$ with the consequences of: **(1)** recovering the stack inertia as the derived $\mathbb{S}^1$-loop space $I_{\mathcal{M}} = [\mathbb{S}^1, \mathcal{M}]$ in the algebraic-topologic decomposition of the motivic Lefschetz $\mathbb{P}^1 = \mathbb{S}^1 \wedge \mathbb{G}_m$, and **(2)** considering a new homological fiber functor to bypass the pro-unipotent nature of the "scheme" mixed Tate motives.

2.2. **A Stack Inertia Decomposition.** Indeed, the Hochschild homological functor $\mathrm{HH}_\bullet$ applied to the GGA *arithmetic* stack inertia decomposition of the cyclic special loci $\mathcal{M}_{g,[m]}(\gamma)$ of [CM14] provides:

A motivic stack inertia decomposition for $\mathcal{M}_{g,[m]}$:

$$M(\mathcal{M}) = \oplus_\gamma \oplus_{kr} \oplus_i M(\mathcal{M}_{kr})^{(i)}$$

where γ runs among the automorphisms of curves, kr among the irreducible components of $\mathcal{M}_{g,[m]}(\gamma)$ and (i) follows a lambda-cotangent complex decomposition.

Further study should confirm **(1)** the role of $\mathrm{HH}_\bullet$ as a (weak) Tannaka fibre functor in $\mathrm{DA}^{et}(k)$, while **(2)** the $(\mathbb{S}^1, \mathbb{G}_m)$- (translation,filtration) for HH-spectra in $\mathcal{SH}^{et}(k)$ should reflect the stack limit Galois action between distinct stack inertia and divisorial strata of [CM14].

3. Grothendieck Section Conjecture and Homotopic Obstruction

For X smooth variety over a field k and the question of local-global obstruction to the existence of rational points (Topic a), a conceptual breakthrough is given by Harpaz-Schlank's étale homotopy sets $X^\bullet(hk)$ and their adelic rational versions $X(\mathbb{A})^\bullet := \kappa_A^{-1}(\mathrm{Im}(loc))$ of homological and topological types where $\bullet \in \{h; (h,n)\}$ (resp. $\bullet \in \{\mathbb{Z}h; (\mathbb{Z}h, n)\}$) – see [HS13].

$$\begin{array}{ccc} X(k) & \xrightarrow{\kappa} & X(hk)^\bullet \\ \downarrow & & \downarrow{\scriptstyle loc} \\ X(\mathbb{A}) & \xrightarrow{\kappa_A} & \prod X(hk_v)^\bullet \end{array}$$

They altogether provide **(1)** an *unified overview of the classical fin/fin-ab, Brauer-Manin and étale Brauer-Manin descent obstructions*, and **(2)** *an ideal context for Grothendieck's section conjecture* that embraces the anabelian and abelian geometry at once – e.g. (Harari-Stix's Cor. 9.13 ibid.): If $X(\mathbb{A})^{fin} \neq \emptyset$, then (AGS) has a section.

3.1. **Homotopic Obstruction in Family.** Quick's refined construction in a certain model category of Pro-space of $X(hk) = \pi_0(\{X_{\bar{k}}\}_{et}^{\wedge, hG_k})$ – as homotopy fixed points simplicial set [Qu10]– gives access to a homotopy section reformulation where one can incorporate further techniques of classical algebraic geometry.

Let us consider a Friedlander's geometric fibration $X \to S$ of geometrically unibranch schemes, and assume being given some cuspical data C_S and C_s for the basis $S(hk)$ and each k-rational fibres $X_s(hk)$. Under those assumptions, Corwin and Schlank establish that – [CS20]:

> *Let $X \to S$ as above. If the the injective (resp. surjective) section conjecture holds the basis S and the fibres C_s, $s \in S$, endowed with cuspidal data, then it does so for X.*

3.2. $\mathbb{A}^1$**- and Motivic Versions.** Regarding Noether's problem (Topic a; in its rational connectedness variant) and $\mathbb{A}^1$-geometry, we further refer to [AO19] §4.2 for Asok's approach via $\mathbb{A}^1$-connectedness. For Topic b, we refer to a question of Toën regarding a motivic version of $X(hk)$, where one replaces $\{-\}_{et}$ (resp. G_k) by M (resp. a certain motivic Tannaka Galois group G_{MM}) in the homotopy fixed point construction above.

References

[AO19] A. Asok and P.A. Østvær, *$\mathbb{A}^1$-homotopy theory and contractible varieties: a survey*, 52p., arXiv:1903.07851 [math.AG] (2019).

[CM14] B. Collas and S. Maugeais, *On Galois action on stack inertia of moduli spaces of curves*, arXiv:1412.4644 [math.AG] (2014).

[CS20] D. Corwin and T.M. Schlank, *Brauer and Etale Homotopy Obstructions to Rational Points on Open Covers*, arXiv:2006.11699 [math.NT] (2020).

[HS13] Y. Harpaz and T.M. Schlank, *Homotopy obstructions to rational points* in Torsors, étale homotopy and applications to rational points, 280–413, London Math. Soc. Lecture Note Ser., 405, Cambridge Univ. Press, Cambridge, 2013.

[IN97] Y. Ihara and H. Nakamura, *Some illustrative examples for anabelian geometry in high dimensions*, in Geometric Galois actions, 1, 127–138, London Math. Soc. Lecture Note Ser., 242, Cambridge Univ. Press, Cambridge, 1997.

[Qu10] G. Quick, *Continuous group actions on profinite spaces.* J. Pure Appl. Algebra **215**, 1024–1039 (2011)

[SS16] A. Schmidt and J. Stix, *Anabelian geometry with étale homotopy types*, Ann. of Math. **(2)** 184, no. 3, 817–868 (2016)

Reconstruction of invariants of configuration spaces of a hyperbolic curves from associated Lie algebras

Koichiro Sawada

Let K be a field of characteristic zero, X a hyperbolic curve of type (g, r) over K, n a positive integer, l a prime number, and Σ a set of prime numbers which coincides with either $\{l\}$ or the set of all prime numbers. Write X_n for the n-th configuration space of X over K, i.e., the complement of the union of various weak diagonals in the product of n copies of X. If K is algebraically closed, then write Π_n^{Σ} for the maximal pro-Σ quotient of the étale fundamental group $\pi_1(X_n)$.

In [HMM17], certain explicit group-theoretic algorithms for reconstructing some objects from Π_n^Σ are given. For instance, the dimension n and the set of generalized fiber subgroups (of co-length m for a given m) of Π_n^Σ (that is, the kernel of the natural outer surjection $\Pi_n^\Sigma \to \Pi_m^\Sigma$ induced by a "generalized projection morphism" $X_n \to X_m$) can be reconstructed from Π_n^Σ, and, moreover, if $n \geq 2$, then (g, r) can be reconstructed from Π_n^Σ (cf. [HMM17] Theorem 2.5).

In the present talk, we consider "Lie algebra analogues", i.e., we give algorithms for reconstructing some objects from the Lie algebra $\mathrm{Gr}(\Pi_n^l)$ (see e.g. [NT98](2.6) or [Saw18] Definition 1.5) associated to the configuration space of a hyperbolic curve. More precisely, we give explicit reconstruction algorithms for reconstructing n and "generalized fiber ideals" (which are defined in the same way as generalized fiber subgroups), and, moreover, if $n \geq 2$, then we give an explicit reconstruction algorithm for reconstructing (g, r).

The most important part of the reconstruction algorithms is, by using an explicit presentation of $\mathrm{Gr}(\Pi_n^l)$ (cf. e.g. [NT98](3.2)), the classification of surjective homomorphisms (as abstract Lie algebras over $\mathbb{Z}_l$) from $\mathrm{Gr}(\Pi_n^l)$ to a "surface algebra" over $\mathbb{Z}_l$, that is, a Lie algebra over $\mathbb{Z}_l$ isomorphic to "$\mathrm{Gr}(\Pi_1^l)$" for some hyperbolic curve. As an application of this classification, we can classify surjective homomorphisms of groups from Π_n^Σ to a surface group under a certain condition. We remark that recently it has been found that this classification can be done without any conditions (cf. [Saw20] Theorem B).

As an application to anabelian geometry, the above classification of surjective homomorphisms of groups yields a Grothendieck's anabelian conjecture-type result between a hyperbolic polycurve (cf. [Hos14] Definition 2.1) and a configuration space of a hyperbolic curve of genus $g \geq 1$. Since a configuration space of a hyperbolic curve is a hyperbolic polycurve, this result can be seen as a special case of the Grothendieck conjecture for hyperbolic polycurves, which is still open. (In [Hos14], the Grothendieck conjecture for hyperbolic polycurves of dimension ≤ 4 over a sub-l-adic field was proved. Moreover, in [SS16], the Grothendieck conjecture for strongly hyperbolic Artin neighborhoods of arbitrary dimension over a finitely generated field over $\mathbb{Q}$ was proved.) Note that the case $g = 0$ is still unsolved, that is, it is unknown that whether a hyperbolic polycurve and a configuration space of a hyperbolic curve of genus 0 (over a certain field) are isomorphic if their étale fundamental groups are isomorphic.

References

[Hos14] Y. Hoshi, The Grothendieck conjecture for hyperbolic polycurves of lower dimension, *J. Math. Sci. Univ. Tokyo* **21** (2014), no. 2, 153–219.

[HMM17] Y. Hoshi, A. Minamide, and S. Mochizuki, Group-theoreticity of numerical invariants and distinguished subgroups of configuration space groups, RIMS preprint **1870** (2017).

[NT98] H. Nakamura and N. Takao, Galois rigidity of pro-l pure braid groups of algebraic curves, *Trans. Amer. Math. Soc.* **350** (1998), no. 3, 1079–1102.

[Saw18] K. Sawada, Reconstruction of invariants of configuration spaces of hyperbolic curves from associated Lie algebras, RIMS preprint **1896** (2018).

[Saw20] K. Sawada, On surjective homomorphisms from a configuration space group to a surface group, RIMS preprint **1921** (2020).

[SS16] A. Schmidt and J. Stix, Anabelian geometry with étale homotopy types, *Ann. of Math.* (2) **184** (2016), no. 3, 817–868.

The outer automorphism groups of the profinite braid groups

Arata Minamide
(joint work with Hiroaki Nakamura)

In this talk, we discussed a computation of the outer automorphism groups of the profinite braid groups (cf. [MN21]).

In this article, for any group Γ, we shall write $\mathrm{Aut}(\Gamma)$ (respectively, $\mathrm{Out}(\Gamma)$) for the group of automorphisms (respectively, group of outer automorphisms) of Γ. (Note that any automorphism of a topologically finitely generated profinite group is continuous (cf. [NS03]).) We shall denote by $\widehat{\Gamma}$ the profinite completion of Γ.

1. The discrete case

Let $n > 3$ be a positive integer. We shall write B_n for the (Artin) braid group on n strings. It is well-known that B_n has the following presentation:

$$B_n \;=\; \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{l} \sigma_i \cdot \sigma_{i+1} \cdot \sigma_i \;=\; \sigma_{i+1} \cdot \sigma_i \cdot \sigma_{i+1} \\ \sigma_i \cdot \sigma_j \;=\; \sigma_j \cdot \sigma_i \quad (|i-j| \;\geq\; 2) \end{array} \right\rangle.$$

In the discrete case, one example of a nontrivial outer automorphism of B_n is obtained as follows. Write $\iota \in \mathrm{Aut}(B_n)$ for the automorphism (of order 2) of B_n determined by the formula $\sigma_i \mapsto \sigma_i^{-1}$ $(i = 1, 2, \ldots, n-1)$. Then one verifies easily that the image of ι via the natural surjection $\mathrm{Aut}(B_n) \to \mathrm{Out}(B_n)$ is nontrivial. In fact, this is the only one nontrivial outer automorphism of B_n.

Theorem 1 (Dyer-Grossman [DG81])**.** *The natural surjection* $\mathrm{Aut}(B_n) \to \mathrm{Out}(B_n)$ *induces an isomorphism*

$$\langle \iota \rangle \;\xrightarrow{\sim}\; \mathrm{Out}(B_n).$$

2. The profinite case

In the profinite case, we have much more examples of nontrivial outer automorphisms. Indeed, let us consider the n-th configuration space

$$(\mathbb{A}^1_{\mathbb{Q}})_n \;\stackrel{\text{def}}{=}\; \{(x_1, \ldots, x_n) \in (\mathbb{A}^1_{\mathbb{Q}})^n \mid x_i \neq x_j \ (i \neq j)\}$$

of the affine line $\mathbb{A}^1_{\mathbb{Q}}$ over $\mathbb{Q}$. Here, we note that we have a natural action of the symmetric group $\mathfrak{S}_n$ (on n letters) on this variety. Then the structure morphism $(\mathbb{A}^1_{\mathbb{Q}})_n/\mathfrak{S}_n \to \mathrm{Spec}(\mathbb{Q})$ induces a natural faithful outer action

$$\rho : G_{\mathbb{Q}} \;\stackrel{\text{def}}{=}\; \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \;\hookrightarrow\; \mathrm{Out}(\pi_1(((\mathbb{A}^1_{\mathbb{Q}})_n/\mathfrak{S}_n) \times_{\mathbb{Q}} \overline{\mathbb{Q}})) \;\cong\; \mathrm{Out}(\widehat{B}_n),$$

where we write "$\pi_1(-)$" for the étale fundamental group of $(-)$.

Moreover, one can "extend" this natural outer action. Drinfeld [Dri90] and Ihara [Iha90] introduced the (profinite) *Grothendieck-Teichmüller group* $\widehat{\mathrm{GT}}$, which is defined as a certain explicit subgroup of the automorphism group of a free profinite group of rank 2, and observed the following:

– There exists a natural faithful outer action $\overline{\rho} : \widehat{\mathrm{GT}} \hookrightarrow \mathrm{Out}(\widehat{B}_n)$.
– It holds that $\mathrm{Im}(\rho) \subseteq \mathrm{Im}(\overline{\rho})$.

(For a rigorous justification of these observations, we refer to [Iha94] and [IM95].)

Remark 1. By identifying $G_{\mathbb{Q}}$ (respectively, $\widehat{\mathrm{GT}}$) with $\mathrm{Im}(\rho)$ (respectively, $\mathrm{Im}(\overline{\rho})$), we obtain an inclusion $G_{\mathbb{Q}} \subseteq \widehat{\mathrm{GT}}$ ($\subseteq \mathrm{Out}(\widehat{B}_n)$). An open problem asks whether this inclusion is an equality.

On the other hand, in [MN21], we newly introduced another natural faithful outer action. Write

$$Z_n \stackrel{\mathrm{def}}{=} \mathrm{Ker}(\widehat{\mathbb{Z}}^{\times} \to (\widehat{\mathbb{Z}}/n(n-1)\widehat{\mathbb{Z}})^{\times}).$$

Then one may define a natural homomorphism

$$\phi : Z_n \ \to \ \mathrm{Aut}(\widehat{B}_n)$$

(whose composite with $\mathrm{Aut}(\widehat{B}_n) \to \mathrm{Out}(\widehat{B}_n)$ is injective). Our main result shows that any outer automorphism of $\widehat{B}_n$ arises from $\overline{\rho}$ and ϕ.

Theorem 2 (Minamide-Nakamura [MN21])**.** *The natural outer actions of $\widehat{\mathrm{GT}}$ and Z_n on $\widehat{B}_n$ induce an isomorphism*

$$\widehat{\mathrm{GT}} \times Z_n \ \stackrel{\sim}{\to} \ \mathrm{Out}(\widehat{B}_n).$$

Remark 2. In particular, if $G_{\mathbb{Q}} = \widehat{\mathrm{GT}}$, then we have $G_{\mathbb{Q}} \times Z_n \stackrel{\sim}{\to} \mathrm{Out}(\widehat{B}_n)$.

3. A computation related to anabelian geometry

In our proof of this theorem, we apply a computation related to anabelian geometry. Let k be an algebraically closed field of characteristic zero. For any positive integer $r > 3$, we shall write $\mathcal{M}_{0,r}$ for the moduli stack over k of proper smooth curves of genus zero with r-ordered marked points. Here, we note that

$$\mathrm{Ker}(\widehat{B}_n/(\mathrm{center}) \to \mathfrak{S}_n) \text{ may be identified with } \pi_1(\mathcal{M}_{0,n+1}).$$

In particular, via this identification, we obtain a natural faithful outer action of $\widehat{\mathrm{GT}}$ on $\pi_1(\mathcal{M}_{0,n+1})$. In our proof, we apply the following computation, which may be regarded as a refinement of [HS00], Main Theorem, (b):

Theorem 3 (Hoshi-Minamide-Mochizuki [HMM17])**.** *The natural outer actions of $\widehat{\mathrm{GT}}$ and $\mathfrak{S}_{n+1}$ on $\pi_1(\mathcal{M}_{0,n+1})$ induce an isomorphism*

$$\widehat{\mathrm{GT}} \times \mathfrak{S}_{n+1} \ \stackrel{\sim}{\to} \ \mathrm{Out}(\pi_1(\mathcal{M}_{0,n+1})).$$

One of the key ingredients of this computation is the following anabelian result:

Proposition 4 (Hoshi-Minamide-Mochizuki [HMM17])**.** *Let $F \subseteq \pi_1(\mathcal{M}_{0,n+1})$ be a fiber subgroup, i.e., the kernel of the natural outer surjection $\pi_1(\mathcal{M}_{0,n+1}) \to \pi_1(\mathcal{M}_{0,m})$ ($3 < m < n+1$) induced by a projection $\mathcal{M}_{0,n+1} \to \mathcal{M}_{0,m}$ obtained by "forgetting marked points". Then there exists a purely group-theoretic characterization of F. In particular, for any $\alpha \in \mathrm{Aut}(\pi_1(\mathcal{M}_{0,n+1}))$, $\alpha(F)$ is a fiber subgroup.*

References

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

[DG81] J.L Dyer, E.K. Grossman, The Automorphism Groups of the Braid Groups, *Amer. J. Math.* **103** (1981), 1151–1169.

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

[HMM17] Y. Hoshi, A. Minamide, S. Mochizuki, *Group-theoreticity of numerical invariants and distinguished subgroups of configuration space groups*, RIMS Preprint **1870** (March 2017).

[Iha90] Y. Ihara, Braids, Galois groups, and some arithmetic functions, Proc. Intern. Congress of Math. Kyoto 1990, 99–120.

[Iha94] Y. Ihara, On the embedding of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) into $\widehat{GT}$, in *The Grothendieck Theory of Dessins d'Enfants*, *London Math. Soc. Lecture Note Series* **200**, Cambridge Univ. Press (1994), 289–305.

[IM95] Y. Ihara, M. Matsumoto, On Galois Actions on Profinite Completions of Braid Groups, *Recent Developments in the Inverse Galois Problem*, *Contemp. Math.* **186**, AMS (1995), 173–200.

[MN21] A. Minamide, H. Nakamura, *The automorphism groups of the profinite braid groups*, to appear in *Amer. J. Math.*

[NS03] N. Nikolov, D. Segal, Finite index subgroups in profinite groups, *wC. R. Math. Acad. Sci. Paris* **337** (2003), 303–308.

Iterated p-adic integration and rational points on curves

Jennifer S. Balakrishnan

The Chabauty–Coleman method can be used to determine the finite set of rational points on certain curves of genus at least 2, using the construction of Coleman's p-adic line integrals.

Let X be a smooth projective curve of genus g over $\mathbf{Q}$, let J denote its Jacobian, and let r denote the rank of $J(\mathbf{Q})$. The Chabauty–Coleman method produces a finite set of p-adic points containing the set $X(\mathbf{Q})$ when $r < g$. This finite set of p-adic points is computed as the zero locus of a Coleman integral.

When $r \geq g$, less is known. One promising technique is Kim's nonabelian extension [Kim05, Kim09, Kim10] of Chabauty. Some progress has been made on the first nonabelian step of this, the *quadratic Chabauty method*, developed in a few directions in joint work with A. Besser, N. Dogra, S. Müller, J. Tuitman, and J. Vonk [BBM16, BD18, BD20, BDMTV19], which can apply when the rank is equal to the genus. Here a finite set of p-adic points containing $X(\mathbf{Q})$ is cut out using iterated p-adic integrals. There are some examples of modular curves $X/\mathbf{Q}$ where we have been able to use quadratic Chabauty to determine $X(\mathbf{Q})$.

We present a selection of examples, from the "cursed" split Cartan modular curve $X_s(13)$ to the genus 3 curves of prime level ℓ in the family of Atkin–Lehner quotient curves $X_0^+(\ell)$, all joint work with N. Dogra, S. Müller, J. Tuitman, and J. Vonk [BDMTV21].

References

[BBM16] J.S. Balakrishnan, A. Besser, and J. S. Müller. Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves. *J. Reine Angew. Math.*, 720:51–79, 2016.

[BD18] J.S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller.

[BD20] ______. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *IMRN*, 2020. rnz362.

[BDMTV19] J.S. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[BDMTV21] ______. Quadratic Chabauty for modular curves: Algorithms and examples. 2021.

[Kim05] M. Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

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

[Kim10] ______. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23:725–747, 2010.

Tannakian Cebotarev density theorems

Anna Cadoret (joint work with Akio Tamagawa)

1. Introduction and main result

Let X be a smooth, geometrically connected variety over a finite field k of char $p > 0$; let η denote its generic point. The classical Cebotarev density theorem asserts that for every finite continous quotient $\pi_1(X) \twoheadrightarrow \Pi$ and union of conjugacy classes $\Delta \subset \Pi$, the set $S_\Delta \subset |X|$ of closed points $x \in |X|$ such that the corresponding Frobenii elements $\varphi_x \in \pi_1(X)$ map to Δ has (Dirichlet) density $\delta(S_\Delta) = |\Delta|/|\Pi|$. Passing to the limit, one gets that for every $S \subset |X|$ with upper density $\delta^u(S) = 1$ the union of the $\pi_1(X)$-conjugacy classes of the $\varphi_x \in \pi_1(X)$, $x \in S$ is dense in $\pi_1(X)$ for the profinite topology. This implies that for a $\overline{\mathbb{Q}}_\ell$-local system ($\ell \neq p$) $\mathcal{C}$ on X, if $G(\mathcal{C})^{an}$ denotes the image of the corresponding representation of $\pi_1(X)$ on $\mathcal{C}_{\overline{\eta}}$ and if, for $x \in |X|$, $\Phi_x^{\mathcal{C}\,an} \subset G(\mathcal{C})^{an}$ denotes the $G(\mathcal{C})^{an}$-conjugacy class of the image of φ_x in $G(\mathcal{C})^{an}$ then the union of the $\Phi_x^{\mathcal{C}\,an}$, $x \in S$ is ℓ-adically dense in $G(\mathcal{C})^{an}$. In particular, for every $S \subset |X|$ with $\delta^u(S) = 1$ (resp. > 0) the following holds:

A) If $G(\mathcal{C})$ denotes the Zariski closure of $G(\mathcal{C})^{an}$ in $\mathrm{GL}_{\mathcal{C}_{\overline{\eta}}}$ and if for $x \in |X|$, $\Phi_x^{\mathcal{C}} \subset G(\mathcal{C})$ denotes the conjugacy class generated by $\Phi_x^{\mathcal{C}\,an}$ in $G(\mathcal{C})$ then (resp. the Zariski-closure of) the union of the $\Phi_x^{\mathcal{C}}$, $x \in S$ is Zariski-dense in $G(\mathcal{C})$ (resp. contains a connected component of $G(\mathcal{C})$);

B) If $\mathcal{C}'$ is another $\overline{\mathbb{Q}}_\ell$-local system on X such that $(x^*\mathcal{C})^{ss} \simeq (x^*\mathcal{C}')^{ss}$, $x \in S$ then $\mathcal{C}^{ss} \simeq \mathcal{C}'^{\,ss}$ (where $(-)^{ss}$ stands for semisimplification).

The Cebotarev density theorem plays a fundamental part in arithmetic geometry in that it often enables to reduce problems about $\overline{\mathbb{Q}}_\ell$-local systems on X to problems about semisimple $\overline{\mathbb{Q}}_\ell$-local systems on points (that is the datum of a vector space with a semisimple automorphism). This prompts the question of similar statements for local systems with other coefficients such as p-adic (*i.e.* convergent or overconvergent $\overline{\mathbb{Q}}_p$-F-isocrystals) or ultraproduct ones (*i.e.* quasi-tame $\overline{\mathbb{Q}}_{\mathfrak{u}}$-local systems). Such coefficients share with $\overline{\mathbb{Q}}_\ell$-local systems the property that they form a Tannakian category with good functorial properties with respect to morphisms of varieties (in particular, inclusions of closed points so that there is a well-defined notion of conjugacy class of Frobenii at $\in |X|$). But, except in the unit-root case (Crew), the Tannakian structure on $\overline{\mathbb{Q}}_p$-local systems does not upgrade to a category of finite-dimensional continuous $\overline{\mathbb{Q}}_p$-representations of $\pi_1(X)$ while, if the Tannakian structure on $\overline{\mathbb{Q}}_{\mathfrak{u}}$-local systems does upgrade to a category of finite-dimensional continuous $\overline{\mathbb{Q}}_{\mathfrak{u}}$-representations of $\pi_1(X)$, the ultraproduct topology is not Hausdorff so that the classical Cebotarev density theorem is useless. Still, for such coefficients, the weaker statements A), B) make sense and are already of significant importance (*e.g.* Statement B) for pure local systems is a key ingredient in the proof of the Langlands' correspondance).

Of course, A) implies B) and, as observed by Tsuzuki and Abe, one can prove B) by a simple L-function argument using weights provided one has a suitable"à la Weil II" formalism of Frobenius weights, which is the case for overconvergent $\overline{\mathbb{Q}}_p$- and $\overline{\mathbb{Q}}_{\mathfrak{u}}$-local systems. In this work, we consider the *a priori* stronger statement A) and obtain

Theorem 1 (Tannakian Cebotarev)**.** *Statement A) holds for $\mathcal{F}$ one of the following:*
(1) a $\overline{\mathbb{Q}}_\ell$-, $\overline{\mathbb{Q}}_{\mathfrak{u}}$- or an overconvergent $\overline{\mathbb{Q}}_p$-local system;
(2) a †-extendable convergent $\overline{\mathbb{Q}}_p$-local system (and, more generally, for a convergent $\overline{\mathbb{Q}}_p$-local system satisfying a weak form of the (generalized) parabolicity conjecture of Crew).

Here "†-extendable" means lying in the essential image of the natural (fully faithful by Kedlaya) functor $\mathcal{F}^\dagger \to \mathcal{F}$ from overconvergent to convergent $\overline{\mathbb{Q}}_p$-local systems.

2. Strategy of the proof

2.1. **Proof of (1) *via* companions.** We call local systems appearing in (1) "motivic" Q-local systems (Q one of $\overline{\mathbb{Q}}_\ell$ ($\ell \neq p$), $\overline{\mathbb{Q}}_{\mathfrak{u}}$ or $\overline{\mathbb{Q}}_p$). A motivic Q-local system $\mathcal{F}$ and a motivic Q'-local system $\mathcal{F}'$ are said to be compatible or companions (with respect to a fixed isomorphism $Q \simeq Q'$) if for every $x \in |X|$ the characteristic polynomials of φ_x acting on $\mathcal{F}_{\overline{x}}$, $\mathcal{F}'_{\overline{x}}$ coincide. Let $\mathcal{F}$ be a semisimple motivic Q-local system. The conjectural formalism of pure motives predicts that there should exist a reductive group $G(\mathcal{F}^{mot})$ over $\overline{\mathbb{Q}}$ together with a faithfull finite-dimensional $\overline{\mathbb{Q}}$-representation $\mathcal{F}^{mot}$ and, for every $x \in |X|$, a (semisimple) conjugacy classes $\Phi_x^{\mathcal{F}^{mot}} \subset G(\mathcal{F}^{mot})$ such that for every semisimple motivic Q'-local system $\mathcal{F}'$ which is compatible with $\mathcal{F}$ and $x \in |X|$, the conjugacy class $\Phi_x^{\mathcal{F}'} \subset G(\mathcal{F}')$ arises from $\Phi_x^{\mathcal{F}^{mot}} \subset G(\mathcal{F}^{mot})$ by base-change from $\overline{\mathbb{Q}}$ to Q'. In particular, if $\mathcal{F}$ admits a $\overline{\mathbb{Q}}_\ell$-companion $\mathcal{F}_\ell$ which is étale, then A) for $\mathcal{F}_\ell \Leftrightarrow$ A) for $\mathcal{F}^{mot} \Leftrightarrow$ A) for $\mathcal{F}$.

Though the existence of $G(\mathcal{F}^{mot})$ and $\Phi_x^{\mathcal{F}^{mot}} \subset G(\mathcal{F}^{mot})$, $x \in |X|$ is still completely conjectural, one now knows that, provided X is smooth over k, $\mathcal{F}$ always admits a motivic $\overline{\mathbb{Q}}_\ell$-companion $\mathcal{F}_\ell$ which is étale for $\ell \gg 0$; this is a consequence of the companion conjecture of Deligne (L. Lafforgue, Deligne, Drinfeld, Abe-Esnault, Kedlaya, Cadoret - see *e.g* [Ca19b] for a survey and [Ca19a] for the ultraproduct setting). The first issue is thus to show that A) for $\mathcal{F}_\ell$ transfers "automatically" to $\mathcal{F}$ only by means of the compatibility property. For this, we reformulate A) in terms of the image of the characteristic polynomial map attached to $\mathcal{F}$ and reduce A) for motivic semisimple Q-coefficients to showing that the image of the characteristic polynomial map is independent of the companions. We deduce this independance result from (the companion conjecture and) a theorem of Kazhdan-Larsen-Varshavsky [KLV14] which asserts that a connected reductive group G over an algebraically closed field Q of characteristic 0 can be reconstructed from its semiring of finite-dimensional semisimple Q-rational representations. Using the weight filtration on $\mathcal{F}$ (another by-product of the companion conjecture), we then reduce A) for arbitrary motivic Q-coefficients to motivic Q-coefficients $\mathcal{F}$ which are direct sums of pure motivic Q-coefficients. Such a $\mathcal{F}$ is not semisimple in general but its restriction to $X \times_k \overline{k}$ is (by the formalism of Frobenius weights), which forces $G(\mathcal{F}) \simeq \mathbb{G}_{a,Q}^{\epsilon} \times G(\mathcal{F}^{ss})$ with $\epsilon = 0$ or 1 and A) for such a $\mathcal{F}$ then easily follows from A) for $\mathcal{F}^{ss}$.

2.2. **$\overline{\mathbb{Q}}_p$-coefficients and proof of (2).** From the motivic point of view, the proof of 2.1 is "the" natural one but considering the deepness of the theory of companions, one may ask for an alternative more "elementary" (*i.e.* not resorting to the "à la Weil II" formalism of Frobenius weights nor automorphic techniques *via* the Langlands correspondance) proof of A). Also, the arguments in 2.1 do not extend *a priori* to prove A) for convergent $\overline{\mathbb{Q}}_p$-local systems. But actually one can adjust the arguments of 2.1 to reduce A) for an arbitrary $\overline{\mathbb{Q}}_p$-local system to A) for direct sums of isoclinic convergent $\overline{\mathbb{Q}}_p$-F-isocrystals. This reduction relies on the theory of slopes - a specific feature of the theory of convergent $\overline{\mathbb{Q}}_p$-local systems. More precisely, given a (convergent) $\overline{\mathbb{Q}}_p$-local system $\mathcal{F}$ on X, there always exists a dense open subscheme $U \subset X$ such that $\mathcal{F}|_U$ admits a slope filtration (Grothendieck, Katz). The slope filtration behaves like the weight filtration with respect to Frobenii so that one can apply the same group-theoretic argument as in 2.1 to reduce A) for $\mathcal{F}|_U$ to A) for direct sums of isoclinic convergent $\overline{\mathbb{Q}}_p$-local systems on U. As an isoclinic convergent $\overline{\mathbb{Q}}_p$-local system is a twist of a unit-root one, one can reduce A) to the case of unit-root $\overline{\mathbb{Q}}_p$-local systems, which follows from the classical Cebotarev density theorem *via* Crew's equivalence of categories mentionned above. This reduction is elementary but quite subtle; it is due to Hartl-Pàl [HP18, Thm. 1.8]. This shows A) for $\mathcal{F}|_U$ but this does not automatically imply A) for $\mathcal{F}$ (contrary to what happens for motivic local systems) since the closed immersion $G(\mathcal{F}|_U) \subset G(\mathcal{F})$ is not an isomorphism in general. However, a weak form of the (generalized) parabolicity conjecture of Crew predicts that $G(\mathcal{F}|_U)$ should contain the centralizer in $G(\mathcal{F})$ of the cocharacter $\omega\colon \mathbb{G}_{m,Q} \to G(\mathcal{F})$ defining the slope filtration on $\mathcal{F}|_U$ and we show this is enough to deduce A) for $\mathcal{F}$ from A) for $\mathcal{F}|_U$. As the parabolicity conjecture is now known for †-extendable $\overline{\mathbb{Q}}_p$-local systems by recent works of D'Addezio and Tsuzuki [D'A20], this yields a purely p-adic and "elementary" proof of (2) (and by one more Tannakian reduction, also a purely p-adic and "elementary" proof of (1) for overconvergent $\overline{\mathbb{Q}}_p$-local systems).

2.3. **Tannakian arguments.** Aside from the arithmetico-geometric inputs and the KLV theorem, the main technical difficulties are in the Tannakian reduction steps, for which we need a series of lemmas (of possibly independent interest) to transfer Zariski-density properties of conjugacy invariant subsets. The general situation is the following. Fix an algebraic group $\widehat{G}$ over an algebraically closed field Q of characteristic 0. Assume $\widehat{G}$ is given with a faithfull, r-dimensional Q-representation V and that V is endowed with a filtration $S_\bullet V$: $V =: S_1V \supsetneq \cdots \supsetneq S_sV \supsetneq S_{s+1}V = 0$ defined by a cocharacter $\omega : \mathbb{G}_{m,Q} \to \widehat{G}$. Let $G \subset \widehat{G}$ be a subgroup of the stabilizer of $S_\bullet V$ in $\widehat{G}$ containing the centralizer of ω in $\widehat{G}$ and consider the G-representation $\widetilde{V} := \oplus_i S_iV/S_{i+1}V$. Let $\widetilde{G}$ denote the image of G acting on $\widetilde{V}$ and $R := \ker(G \twoheadrightarrow \widetilde{G})$. Fix also a union $\Phi \subset G$ of G-conjugacy classes, let $\widetilde{\Phi} \subset \widetilde{G}$ (resp. $\widehat{\Phi} \subset \widehat{G}$) denote (resp. the conjugacy-invariant subset generated by) its image in $\widetilde{G}$ (resp. $\widehat{G}$). Eventually, let $\chi : GL_{\widetilde{V}} \to \mathbb{P}_{r,Q} := \mathbb{G}_{m,Q} \times \mathbb{A}^{r-1}_Q$ denote the characteristic polynomial map. Fix a $g \in \Phi$ with image $\widetilde{g} \in \widetilde{G}$. We have:

i) If $\widetilde{G} = R_u(\widetilde{G}) \times \widetilde{G}^{red}$ and $\Psi := Id \times \chi : \widetilde{G} = R_u(\widetilde{G}) \times \widetilde{G}^{red} \to R_u(\widetilde{G}) \times \mathbb{P}_{r,Q}$ then $\overline{\widetilde{\Phi}}^{zar} \supset \widetilde{G}^\circ \widetilde{g}$ iff $\overline{\Psi(\widetilde{\Phi})}^{zar} \supset \Psi(\widetilde{G}^\circ \widetilde{g})$

ii) If for every $\gamma \in \Phi$, $R^{\gamma^{ss}} = 1$ then $\overline{\Phi}^{zar} \supset G^\circ g$ iff $\overline{\widetilde{\Phi}}^{zar} \supset \widetilde{G}^\circ \widetilde{g}$;

iii) If $\overline{\Phi}^{zar} \supset G^\circ g$ then $\overline{\widehat{\Phi}}^{zar} \supset \widehat{G}^\circ g$.

Here $R_u(G) \subset G$ denotes the unipotent radical and $G \twoheadrightarrow G^{red} := G/R_u(G)$ the maximal reductive quotient and for an element $\gamma \in G$, $\gamma = \gamma^u \gamma^{ss} = \gamma^{ss} \gamma^u$ denotes the multiplicative Jordan decomposition of γ in G. I do not elaborate on the proofs of these results but I would like to point out that they are significantly simpler if G is connected. To treat the non-connected case, we introduce the notion of quasi-Cartan subgroup, which is a well-behaved generalization for non-connected algebraic groups of the classical notion of Cartan subgroup. For a reductive G the theory of quasi-Cartan subgroups (then called maximal quasi-tori) is due to Hartl-Pàl; our theory of quasi-Cartan subgroups for arbitrary G is a mild enhancement of theirs.

2.4. The following diagram provides a synthetical overview of the architecture of our proofs.

$$\begin{tikzcd}[column sep=large]
\text{Direct sums of isoclinic } \overline{\mathbb{Q}}_p\text{-coeff.} \arrow[r, Rightarrow, "\substack{\text{Slope}\\ \text{filtration}}", "ii)"'] & \substack{\overline{\mathbb{Q}}_p\text{-coeff. over}\\ \text{dense open } U \subset X} \arrow[r, Rightarrow, "iii)", "\substack{\text{Parabolicity}\\ \text{Conj.}}"'] \arrow[rd, Rightarrow, "iii)"'] & \overline{\mathbb{Q}}_p\text{-coeff.} \\
\text{Classical Cebotarev} \arrow[u, Rightarrow, "\text{Hartl-Pàl}"] \arrow[d, Rightarrow] & & \text{motivic } \overline{\mathbb{Q}}_p\text{-coeff.} \\
\text{Etale } \overline{\mathbb{Q}}_\ell\text{-coeff.} \arrow[r, Rightarrow, "i)", "\substack{\text{Companion}\\ \text{Conj.}}"'] & \substack{\text{Direct sums of pure}\\ \text{motivic } Q\text{-coeff.}} \arrow[r, Rightarrow, "ii)", "\substack{\text{Weight}\\ \text{filtration}}"'] & \text{motivic } Q\text{-coeff.} \arrow[u, Rightarrow]
\end{tikzcd}$$

3. Comparison with Hartl-Pàl

As mentioned, our work owes a lot to [HP18]. In particular, they treat the core case of direct sums of isoclinic convergent $\overline{\mathbb{Q}}_p$-local systems [HP18, Thm. 1.8] and they built the theory of maximal quasi-tori, which lead us to introduce quasi-Cartan subgroups. They also provide a third (chronologically the first) proof of A) for semisimple overconvergent $\overline{\mathbb{Q}}_p$-local systems [HP18, Thm. 1.12] *via* equidistribution - a formal consequence of the "à la Weil II" formalism of Frobenius weights. It is quite different in spirit from ours though it also uses indirectly the companion conjecture for $\overline{\mathbb{Q}}_p$-coefficients through the fact that an irreducible motivic $\overline{\mathbb{Q}}_p$-coefficient with finite determinant is pure of weight 0 (to make the unitarian trick work in the equidistribution argument of Deligne). They also treat some special cases of (2) [HP18, Thm. 1.10].

Remark 1. For the time being, we do not have an "elementary" proof of (1) for ultraproduct local systems.

References

[Ca19a] A. Cadoret, *Ultraproduct Weil II for curves and integral models in compatible families of ℓ-adic local systems*, Preprint, 2019.

[Ca19b] A. Cadoret, *La conjecture des compagnons (d'après Deligne, Drinfeld, L. Lafforgue, T. Abe,...)*, Séminaire Bourbaki 71e année, 2018-2019, no. 1156, 2019.

[D'A20] M. D'Addezio, *Parabolicity conjecture of F-isocrystals*, arXiv:2012.12879 [math.AG] (2020).

[HP18] U. Hartl and H. Pál, *Crystalline Chebotarëv density theorems*, arXiv:1811.07084 [math.NT] (2018).

[KLV14] D. Kazhdan, M. Larsen and Y. Varshavsky, *The Tannakian formalism and the Langlands conjectures*, Algebra Number Theory **8**, p. 243–256, 2014.

Galois theory, patching, and local-global principles

David Harbater

(joint work with Jean-Louis Colliot-Thélène, Julia Hartmann, Daniel Krashen, R. Parimala, V. Suresh)

Patching has been used in inverse Galois theory to realize finite groups as Galois groups, to solve embedding problems, and to study the structure of absolute Galois groups of fields F. A key case is when F is *semi-global field*; i.e., a one-variable function field over a complete discretely valued field K. There, patching makes it possible to construct Galois extensions of F by doing so "locally" (e.g., see [Har03]). More recently, patching has been used in direct Galois theory, especially for local-global principles. In this situation, one analyzes a given extension of F by doing so locally, in the patching framework; and this is the focus here.

For G finite, the spectrum of a G-Galois extension of F is a G-*torsor*; i.e., a principal homogeneous G-space over F. These are classified by the Galois cohomology set $H^1(F,G)$. For G finite (possibly non-constant), torsors were used in [CT20] and [MB01] to solve embedding problems. One can also consider torsors under other linear algebraic groups (smooth subgroups of GL_n) over F. These groups arise, e.g., in differential Galois theory; and in combination with patching, this approach has led to results in inverse differential Galois theory (see [BHHW18] and sequels).

A classical local-global principle (LGP) says that a variety V over a global field F has an F-point if it has an F_v-point for each completion F_v. The key case is V a homogenous space (e.g., a torsor) under a linear algebraic group G; it is known that if G is a connected rational F-variety then LGP holds for G-torsors ([San81], [Che89]). This yields other classical LGP's, e.g. the theorems of Hasse-Minkowski (on isotropy of quadratic forms, via $G = \mathrm{SO}_n$) and Albert-Brauer-Hasse-Noether (on splitting of central simple algebras, via $G = \mathrm{PGL}_n$). Over a global field, LGP's for torsors under a *finite* group always hold, by Tchebotarev density. For a more general group G, the Tate-Shafarevich set $\text{Ш}(F,G) = \ker\left[H^1(F,G) \to \prod_v H^1(F_v,G)\right]$ is the obstruction to LGP for G-torsors.

Now consider the focus of this talk: LGP's over semi-global fields F. Thus F is a one-variable function field over a complete discretely valued field K, say with valuation ring $T = \mathcal{O}_K$, having uniformizer t and residue field k (e.g., $K = k((t))$, $T = k[[t]]$, $F = K(x)$). Let $\mathcal{X}$ be a regular model of F over T, with closed fiber X, which we may assume is a normal crossings divisor (e.g. $\mathcal{X} = \mathbb{P}^1_T$, $X = \mathbb{P}^1_k$).

To each point $P \in X$, let $\widehat{R}_P$ be the complete local ring of $\mathcal{X}$ at P, and let F_P be its fraction field. For each irreducible affine curve $U \in X$, let $\widehat{R}_U$ be the completion of the subring of F consisting of functions regular along U, and let F_U be its fraction field. Here $F \subset F_U, F_P$. To use these *patches* in Galois theory, we pick a finite set $\mathcal{P}$ of closed points $P \in X$ including all the singular points of X, and let $\mathcal{U}$ be the finite set of connected components U of $X - \mathcal{P}$.

If E/F is Galois with (finite) group G, and if E becomes trivial over each F_U and each F_P, must E/F be trivial? This is a LGP for the G-torsor $\mathrm{Spec}(E)$ over F, and $\text{Ш}_{\mathcal{P}}(F,G) = \ker[H^1(F,G) \to \prod_{P\in\mathcal{P}} H^1(F_P,G) \times \prod_{U\in\mathcal{U}} H^1(F_U,G)]$ is the corresponding obstruction. A closer analog of the classical LGP is this: if E becomes trivial over F_v for each completion of F at a discrete valuation v, must E be trivial over F? The corresponding obstruction $\text{Ш}(F,G)$ is given by the same expression as in the global field case. Here $\text{Ш}_{\mathcal{P}}(F,G) \subseteq \text{Ш}(F,G)$; and if G is finite then $\text{Ш}_{\mathcal{P}}(F,G) = \text{Ш}(F,G)$ by Purity of Branch Locus.

Question 1. *Under what circumstances will LGP hold, for F a semi-global field? What is an explicit description of the obstruction?*

To address this question, consider the *reduction graph* associated to $\mathcal{P}$: it is the bipartite graph Γ whose vertices are $\mathcal{P} \cup \mathcal{U}$ and whose edges are pairs (P,U) where $P \in \mathcal{P}$, $U \in \mathcal{U}$, and $P \in \bar{U}$. (This is homotopy equivalent to the dual graph in Deligne-Mumford [DM69].) Viewing Γ as a topological space, we can take $\pi_1(\Gamma)$.

Call a linear algebraic group G *rational* if each connected component of G is a rational F-variety; e.g., constant finite groups and connected rational groups. The quotient G/G^0 by the identity component is then a constant finite group $\bar{G}$.

Theorem 1. [HHK15] *For G rational, $\text{Ш}_{\mathcal{P}}(F,G) \cong \mathrm{Hom}(\pi_1(\Gamma),\bar{G})/{\sim} \cong \bar{G}^m/{\sim}$, where $\sim$ is conjugation by G and m is the number of loops in Γ. Thus LGP holds if and only if Γ is a tree or G is connected.*

This is proven by generalizing Cartan's Lemma on matrix factorization from GL_n to rational groups G. As examples, we have LGP for SO_n and PGL_n, providing analogs of Hasse-Minkowski and Albert-Brauer-Hasse-Noether for semi-global fields. When G is a constant finite group (as in Galois theory), the theorem says that LGP holds if and only if either Γ is a tree or G is trivial. Thus the analog of Tchebotarev density holds for finite groups precisely in those two situations.

For non-rational groups over semi-global fields F, in the finite case we have:

Proposition 2. [CHHKPS21] *Let G be a smooth finite group scheme over F, and F'/F a finite Galois extension splitting G. Suppose the reduction graph Γ' associated to F' is a tree. Then LGP holds for G over F; i.e., $\text{Ш}(F,G) = \text{Ш}_{\mathcal{P}}(F,G)$ is trivial.*

The proof considers the action of $\mathrm{Gal}(F'/F)$ on Γ', and uses Serre's result [Ser03, Section I.3.1] on group actions on trees. For groups that are not assumed finite:

Theorem 3. [CHHKPS21] *Let G be a linear algebraic group over a field k of characteristic 0, and F a semi-global field over $K := k((t))$. Assume the closed fiber of a regular model is reduced, and the reduction graph Γ is a geometric tree (i.e., remains a tree over each finite k'/k). Then $\text{Ш}_{\mathcal{P}}(F,G) = 1$; also $\text{Ш}(F,G)$ if G is connected.*

The proof reduces to the case of connected groups by Prop. 2; then reduces to reductive groups, using that the unipotent radical has trivial cohomology in characteristic 0 ([Ser00, Section I.5.3]). There $\text{Ш}(F,G) = \text{Ш}_{\mathcal{P}}(F,G)$, so it suffices to treat $\text{Ш}_{\mathcal{P}}(F,G)$. To prove triviality of a torsor in $\text{Ш}_{\mathcal{P}}(F,G)$, we use [GPS19], for which it suffices to check that the torsor over F is induced by a torsor over $\mathcal{X}$ that is trivial over X. This is done via a factorization result, proven using the Bruhat decomposition together with an equivalent form of the assumption on Γ: that Γ is a *monotonic tree*; i.e., with respect to some vertex v_0 (the root of the tree), the field of definition stays the same or enlarges as one moves on a path away from v_0.

The LGP for connected reductive groups G carries over to residue characteristic p under some additional hypotheses. But without the tree hypothesis on Γ, LGP can fail even for semisimple simply connected (sssc) groups in characteristic 0:

Example 1. [CHHKPS21] Failure of LGP when Γ is not a tree: Suppose the closed fiber X consists of copies of $\mathbb{P}^1_k$ meeting at k-points, with m loops in Γ. If G is reductive over T then $\text{Ш}(F,G) \cong \mathrm{Hom}(\pi_1(\Gamma), G(k)/\mathrm{R})/\!\sim\ \cong (G(k)/\mathrm{R})^m/\!\sim$. Here $G(k)/\mathrm{R}$ is the group of R-equivalence classes in $G(k)$, where $g_0, g_1 \in G(k)$ are R-*equivalent* if they are connected by an open subset of $\mathbb{A}^1_k$ contained in G_k. (If G is moreover rational, this agrees with Theorem 1, since $G(k)/\mathrm{R} = G/G^0$ there.)

There exist sssc groups G over fields k of characteristic 0 with non-trivial $G(k)/\mathrm{R}$. These then lead to counterexamples to LGP. In fact, by enlarging k we can enlarge $G(k)/\mathrm{R}$, yielding examples with $\text{Ш}(F,G)$ infinite.

Example 2. [CHHKPS21] Failure of LGP for a non-geometric tree: Suppose the closed fiber X of a model $\mathcal{X}$ of F consists of two copies of $\mathbb{P}^1_k$ meeting at a single closed point, where the residue field is k' (with k, k' of characteristic 0, and k' strictly containing k). So Γ is a tree, but not a geometric tree (the base change to k' is not a tree). If $G(k)/\mathrm{R}$ is trivial and $G(k')/\mathrm{R}$ is non-trivial, then $\text{Ш}(F,G)$ is non-trivial. There are sssc groups where this occurs, and so LGP fails there.

Acknowledgment: The speaker was supported in part by NSF grant DMS-1805439.

References

[BHHW18] A. Bachmayr, D. Harbater, J. Hartmann, M. Wibmer, *Differential embedding problems over complex function fields*, Doc. Math. **23** (2018), 241–291.

[Che89] V.I. Chernousov, *The Hasse principle for groups of type E8*, Doklady Akademii Nauk SSSR **360** (1989), 1059–1063; translation in Soviet Math. Doklady **39** (1989), 592–596.

[CT20] J.-L. Colliot-Thélène, *Rational connectedness and Galois covers of the projective line*, Ann. of Math. **151** (2000), 359–373.

[CHHKPS21] J.-L. Colliot-Thélène, D. Harbater, J. Hartmann, D. Krashen, R. Parimala, V. Suresh. *Local-global principles for constant reductive groups over semi-global fields*, 2021 manuscript.

[DM69] P. Deligne, D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.

[GPS19] P. Gille, R. Parimala, V. Suresh, *Local triviality for G-torsors*, arXiv:1901.04722 [math.AG] (2019).

[Har03] D. Harbater, *Patching and Galois theory*, Galois groups and fundamental groups, 313–424, Math. Sci. Res. Inst. Publ., vol. 41, Cambridge Univ. Press, Cambridge, 2003.

[HHK15] D. Harbater, J. Hartmann, D. Krashen, *Local-global principles for torsors over arithmetic curves*, Amer. J. Math. **137** (2015), 1559–1612.

[MB01] L. Moret-Bailly, *Construction de revêtements de courbes pointées*, J. Algebra **240** (2001), 505–534.

[San81] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. Reine Angew. Math. **327** (1981), 12–80.

[Ser00] J.-P. Serre, *Galois Cohomology*, Springer Monographs in Mathematics, Berlin, Heidelberg, New York, 2000.

[Ser03] ———, *Trees.* Translated by John Stillwell. Corrected 2nd printing of the 1980 English translation. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003.

Probabilistic Galois theory

Lior Bary-Soroker

The main question discussed in this talk was what is the distribution of the Galois group of a random polynomial with integral coefficients. We introduced several models of randomness.

The first model is the so called large box model, in which we fix the degree and choose the coefficients from a large box. Here the classical result is of van der Waerden that with probability going to 1 with the size of the box, the Galois group will be the full symmetric group. We discussed the progress that has been done in the last 90 years about upper bounds on the complement, namely on polynomials with smaller groups. We also discussed subtler questions of hierarchy of subgroups according to their probability to occur as a Galois group, and other interesting questions.

Next we discussed the restricted coefficient model. In its simplest case, we fix a distribution μ for the coefficients of the polynomial, choose the coefficients independently and take the degree to infinity. If μ is a Bernoulli probability taking the values ± 1 with equal probabilities, it is still open whether with probability tending to one the polynomial is irreducible. We discussed the recent progress by the speaker with Kozma, and with Kozma and Koukoulopoulos and by Breuillard and Varju on this problem. The former groups prove that under mild assumptions on μ, for example $\mu \sim \mathcal{U}(\{1, \ldots, L\})$ and $L \geq 35$ fixed, with probability going 1 the polynomial is irreducible and the latter is conditioned on the *general Riemann hypothesis* and prove the same result for any non-degenerate μ that is supported on a finite set.

Lastly we discussed two models coming from random matrix theory in which the polynomial is the characteristic polynomial of a matrix. The first coming from a random walks on the Cayley graph of an arithmetic group and the second is taking a matrix with entries ± 1 (or other measures). We surveyed the results of Rivin, Kowalski, Lubotzky-Rosenzweig on the former model and of Eberhard on the latter.

The Grothendieck-Teichmüller group in topology

Geoffroy Horel

A famous result due to Belyi asserts that the absolute Galois group of $\mathbb{Q}$ acts faithfully on a free profinite group on two generators by outer automorphisms. This actions comes from the identification of the latter group with the étale geometric fundamental group on the variety $\mathbb{P}^1 - \{0, 1, \infty\}$. Based on this theorem, Grothendieck suggested in [Gro97] to describe the absolute Galois group of $\mathbb{Q}$ in terms of this action. From this idea emerged a group, called *the Grothendieck-Teichmüller group* which is conjecturally isomorphic to the absolute Galois group of $\mathbb{Q}$. Independently of this question, this group is of high importance in homotopy theory and geometric topology. The purpose of this talk was to explain some of these applications.

1. $\widehat{GT}$: from operads to configuration category

The starting point of this relationship comes from the identification $\widehat{GT} \simeq \mathrm{hAut}(E_2^\wedge)$ of this group with the group of homotopy automorphisms of the profinite completion of the little 2-disks operad E_2 proved in [Hor17].

1.1. **Little 2-disks operad.** The profinite completion that is considered here is a homotopical generalization of the profinite completion of groups. The little 2-disks operad is a homotopical gadget that controls the operations on a double loop space.

This object also plays an important role in category theory as it controls the structure of a braided monoidal category. This theorem admits a purely combinatorial proof. However, it suggests *an algebro-geometric origin of the little 2-disks operad*. This has been recently done by Vaintrob (see [Vai19]).

1.2. **Two-dimensional configuration category.** Using this action, we can obtain actions of the Grothendieck-Teichmüller group on the configuration category of certain manifolds. The configuration category is a category that can be associated to any manifold M. It was introduced by Boavida de Brito and Weiss in [BW18a]. Its objects are pairs (S, ϕ) with S a finite set and $\phi : S \to M$ an embedding. A morphism from (S, ϕ) to (T, ψ) is a pair (u, p) with $u : S \to T$ a map of finite sets and p a "sticky" path connecting ϕ to $\psi \circ u$ in the space M^S. The sticky condition means that points are allowed to collide along the path but once this has happened, they remain stuck together for the rest of the path.

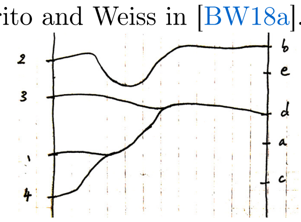

Fig 1. Sticky paths.

Boavida de Brito and Weiss have shown that there is a very close relationship between the configuration category of $\mathbb{R}^2$ and the little 2-disks operad. Using their work, the main theorem of [Hor17] can be equivalently rephrased as:

> *The Grothendieck-Teichmüller group is the group of homotopy automorphisms of the profinite completion of the configuration category of* $\mathbb{R}^2$.

2. $\widehat{GT}$: higher dimensions, manifold calculus and knot theory

In [BW18b], Boavida de Brito and Weiss have given a construction of the configuration category of the product of two manifolds from the data of the configuration category of each factor. Using this result, Boavida Brito and I have *constructed a non-trivial action of the Grothendieck-Teichmüller group on the configuration category of* $\mathbb{R}^d$ *for any* $d \geq 2$ (see [BH19]).

2.1. Goodwillie-Weiss manifold calculus. This action produces interesting consequences when combined with the technique of manifold calculus of Goodwillie and Weiss . The idea of manifold calculus is to produce homotopical approximations of spaces of embeddings between smooth manifolds. This is done by mapping the space of embeddings to the space of maps between the two configuration categories.

Using these ideas, in [BH20], we are able to obtain new results in classical and higher dimensional knot theory.

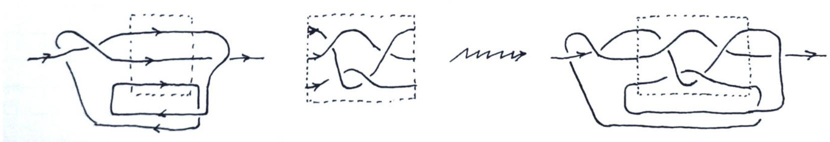

Fig 2. Pure braid infection and additive knot invariant.

2.2. Universal additive invariant of knots. In the case of knots in $\mathbb{R}^d$ with $d \geq 4$, we are able to compute the higher homotopy groups of the space of knots localized at a prime and in a range of degrees that grows to infinity with the prime that we are considering. In the case of classical knots in $\mathbb{R}^3$, we are able to show, using the recent PhD thesis of Danica Kosanović (see [Kos20]), that:

> *The* n*-th Goodwillie-Weiss approximation is the universal type* $(n-1)$*-invariant of knots after localizing at a prime which is larger than* n*.*

Our result extends a result of Kontsevich who showed that this result holds after inverting all primes, via a construction called the Kontsevich integral. On the other hand, it is conjectured that this result holds integrally (i.e. without inverting any primes). Our result can be seen as a small step towards this integral conjecture.

References

[BH20] P. Boavida de Brito, G. Horel, *Galois symmetries of knot spaces*, arXiv:2002.01470 [math.AT] (2020), to appear in Compositio Mathematica.

[BH19] P. Boavida de Brito, G. Horel, *On the formality of the little disks operad in positive characteristic*, arXiv:1903.09191 [math.AT] (2019), to appear in Jour. of London Math. Soc.

[BW18a] P. Boavida de Brito, M. Weiss, *Spaces of smooth embeddings and configuration categories*, Journal of Topology **11** (2018) 65–143.

[BW18b] P. Boavida de Brito, M. Weiss, *The configuration category of a product*, Proc. Amer. Math. Soc. **146** (2018), 4497–4512.

[Gro97] A. Grothendieck, Esquisse d'un programme, in *Around Grothendieck's Esquisse D'un Programme*, London Math. Soc. Lecture Note Series **242** (1997), 5–48.

[Hor17] G. Horel, *Profinite completion of operads and the Grothendieck-Teichmüller group*, Advances in Math. **321** (2017), 326–390.

[Kos20] D. Kosanović, *A geometric approach to the embedding calculus knot invariants*, PhD Thesis at the University of Bonn, 2020.
[Vai19] D. Vaintrob, *Moduli of framed formal curves*, arXiv:1910.11550 [math.AG] (2019).

The absolute anabelian geometry of quasi-tripods

Yuichiro Hoshi

The notion of a quasi-tripod (cf. Definition 4 below) may be regarded as one natural generalization of the notion of a hyperbolic curve of Belyi-type (cf. Remark 5, (1), below). In the present talk, we discuss the absolute anabelian geometry of quasi-tripods.

1. Main result

Definition 1. Let k be a field and p a prime number.

– We shall say that the field k is *algebraic* (respectively, *sub-p-adic*; *generalized sub-p-adic*) if k is isomorphic to a subfield of an algebraic closure of $\mathbb{Q}$ (respectively, to a subfield of a finitely generated extension of $\mathbb{Q}_p$; to a subfield of a finitely generated extension of the p-adic completion of a (not necessarily finite) unramified extension of $\mathbb{Q}_p$).
– We shall say that the field k is *strictly sub-p-adic* if k is sub-p-adic and contains a subfield isomorphic to $\mathbb{Q}_p$.

Definition 2.

(1) Let k be a field and $X_\circ$, $X_\bullet$ orbivarieties over k. Then we shall say that the pair $(X_\circ, X_\bullet)$ is *relatively anabelian* if, for each separable closure $\overline{k}$ of k, the natural map
$$\mathrm{Isom}_k(X_\circ, X_\bullet) \to \mathrm{Isom}_{\mathrm{Gal}(\overline{k}/k)}\big(\pi_1(X_\circ), \pi_1(X_\bullet)\big)/\mathrm{Inn}\big(\pi_1(X_\bullet \times_k \overline{k})\big)$$
is bijective.

(2) For each $\square \in \{\circ, \bullet\}$, let $k_\square$ be a field and $X_\square$ an orbivariety over $k_\square$. Then we shall say that the pair $(X_\circ, X_\bullet)$ is *absolutely anabelian* if the natural map
$$\mathrm{Isom}(X_\circ, X_\bullet) \to \mathrm{Isom}\big(\pi_1(X_\circ), \pi_1(X_\bullet)\big)/\mathrm{Inn}\big(\pi_1(X_\bullet)\big)$$
is bijective.

Remark 3. One fundamental result with respect to the notion defined in Definition 2, (1), is the following result proved by S. Mochizuki (cf. [Moc03], Theorem 4.12): Let k be a generalized sub-p-adic field for some prime number p and $X_\circ$, $X_\bullet$ hyperbolic orbicurves over k. Then the pair $(X_\circ, X_\bullet)$ is relatively anabelian.

Definition 4. Let k be a field of characteristic zero and X a hyperbolic orbicurve over k. Then we shall say that X is a *quasi-tripod* if there exist finitely many hyperbolic orbicurves $X_1, X_2, \ldots, X_n$ such that X_1 is isomorphic to X, X_n is isomorphic to the split tripod $\mathbb{P}^1_k \setminus \{0, 1, \infty\}$ over k, and, moreover, for each $i \in \{1, 2, \cdots, n-1\}$, X_{i+1} is related to X_i in one of the following four ways:

– There exists a finite étale morphism $X_{i+1} \to X_i$.
– There exists a finite étale morphism $X_i \to X_{i+1}$.
– There exists an open immersion $X_i \hookrightarrow X_{i+1}$.
– There exists a partial coarsification morphism $X_i \to X_{i+1}$.

Remark 5.

(1) One verifies immediately that, for a finite extension k of $\mathbb{Q}_p$ and a hyperbolic curve over k, the hyperbolic curve is of Belyi type (cf. [Moc07], Definition 2.3, (ii)) if and only if the hyperbolic curve is a quasi-tripod and, moreover, may be descended to a subfield of k finite over $\mathbb{Q}$.
(2) One also verifies immediately that every hyperbolic curve over a field of characteristic zero whose smooth compactification is of genus less than two is a quasi-tripod.

The main result of the present talk is as follows (cf. [Hos21], Theorem A):

Theorem 1. *For each $\Box \in \{\circ, \bullet\}$, let $p_\Box$ be a prime number, $k_\Box$ a field of characteristic zero, and $X_\Box$ a hyperbolic orbicurve over $k_\Box$. Suppose that the following two conditions* (1), (2) *are satisfied:*

(1) Either $X_\circ$ or $X_\bullet$ is a quasi-tripod.
(2) One of the following three conditions (a), (b), (c) *is satisfied:*
  (a) For each $\Box \in \{\circ, \bullet\}$, the field $k_\Box$ is algebraic, generalized sub-$p_\Box$-adic, and Hilbertian.
  (b) For each $\Box \in \{\circ, \bullet\}$, the field $k_\Box$ is transcendental and finitely generated over some algebraic and sub-$p_\Box$-adic field.
  (c) For each $\Box \in \{\circ, \bullet\}$, the field $k_\Box$ is strictly sub-$p_\Box$-adic.

Then the pair $(X_\circ, X_\bullet)$ is absolutely anabelian.

Remark 6.

– Theorem 1 in the case where either (a) or (b) is satisfied partially generalizes the following result proved by A. Tamagawa (cf. [Tam97], Theorem 0.4): For each $\Box \in \{\circ, \bullet\}$, let $k_\Box$ be a finitely generated extension of $\mathbb{Q}$ and $X_\Box$ an affine hyperbolic curve over $k_\Box$. Then the pair $(X_\circ, X_\bullet)$ is absolutely anabelian.
– Theorem 1 in the case where (c) is satisfied generalizes the following result proved by S. Mochizuki (cf. [Moc07], Corollary 2.3): For each $\Box \in \{\circ, \bullet\}$, let $p_\Box$ be a prime number, $k_\Box$ a finite extension of $\mathbb{Q}_{p_\Box}$, and $X_\Box$ a hyperbolic curve over $k_\Box$. Suppose that either $X_\circ$ or $X_\bullet$ is of Belyi-type (cf. Remark 5, (1)). Then the pair $(X_\circ, X_\bullet)$ is absolutely anabelian.

2. Two applications

The following result is one application of the main result (cf. [Hos21], Theorem B):

Theorem 2. *For each $\Box \in \{\circ, \bullet\}$, let $n_\Box$ be a positive integer, $p_\Box$ a prime number, $k_\Box$ a field of characteristic zero, and $X_\Box$ a hyperbolic curve over $k_\Box$; write $(X_\Box)_{n_\Box}$ for the $n_\Box$-th configuration space of $X_\Box$. Suppose that the following two conditions* (1), (2) *are satisfied:*

(1) One of the following two conditions is satisfied:
- *The inequality* $1 < \max\{n_\circ, n_\bullet\}$ *holds, and, moreover, either* $X_\circ$ *or* $X_\bullet$ *is affine.*
- *The inequality* $2 < \max\{n_\circ, n_\bullet\}$ *holds.*

(2) One of the following three conditions (a), (b), (c) *is satisfied:*
- *(a) For each* $\Box \in \{\circ, \bullet\}$*, the field* $k_\Box$ *is algebraic, generalized sub-*$p_\Box$*-adic, and Hilbertian.*
- *(b) For each* $\Box \in \{\circ, \bullet\}$*, the field* $k_\Box$ *is transcendental and finitely generated over some algebraic and sub-*$p_\Box$*-adic field.*
- *(c) For each* $\Box \in \{\circ, \bullet\}$*, the field* $k_\Box$ *is strictly sub-*$p_\Box$*-adic.*

Then the pair $((X_\circ)_{n_\circ}, (X_\bullet)_{n_\bullet})$ *is absolutely anabelian.*

Definition 7. We shall say that an open basis for the Zariski topology of a given smooth variety over a field is *relatively anabelian* (respectively, *absolutely anabelian*) if, for each members U and V of the open basis, the pair (U, V) is relatively anabelian (respectively, absolutely anabelian).

Remark 8. One fundamental result with respect to the notion defined in Definition 7 is the following result proved by the author (cf. [Hos20], Theorem A): Let k be a generalized sub-p-adic field for some prime number p. Then an arbitrary smooth variety over k has a relatively anabelian open basis.

The following result is one application of the main result (cf. [Hos21], Theorem C):

Theorem 3. *Let* k *be a field and* p *a prime number. Suppose that one of the following three conditions* (a), (b), (c) *is satisfied:*
- *(a) The field* k *is algebraic, generalized sub-*p*-adic, and Hilbertian.*
- *(b) The field* k *is transcendental and finitely generated over some algebraic and sub-*p*-adic field.*
- *(c) The field* k *is strictly sub-*p*-adic.*

Then an arbitrary smooth variety of positive dimension over k *has an absolutely anabelian open basis.*

Remark 9. Theorem 3 in the case where either (a) or (b) is satisfied, together with the result discussed in Remark 8, generalizes the following result proved by A. Schmidt and J. Stix (cf. [SS16], Corollary 1.7): Let k be a finitely generated extension of $\mathbb{Q}$. Then an arbitrary smooth variety over k has a relatively anabelian open basis and absolutely anabelian open basis.

References

[Hos21] Y. Hoshi, The absolute anabelian geometry of quasi-tripods, to appear in *Kyoto J. Math.*

[Hos20] Y. Hoshi, A note on an anabelian open basis for a smooth variety, *Tohoku Math. J.* (2) **72** (2020), 537–550.

[Moc03] S. Mochizuki, Topics surrounding the anabelian geometry of hyperbolic curves, *Galois groups and fundamental groups*, 119–165, Math. Sci. Res. Inst. Publ., **41**, Cambridge Univ. Press, Cambridge, 2003.

[Moc07] S. Mochizuki, Absolute anabelian cuspidalizations of proper hyperbolic curves, *J. Math. Kyoto Univ.* **47** (2007), 451–539.

[SS16] A. Schmidt and J. Stix, Anabelian geometry with étale homotopy types, *Ann. of Math.* (2) **184** (2016), 817–868.
[Tam97] A. Tamagawa, The Grothendieck conjecture for affine curves, *Compositio Math.* **109** (1997), 135–194.

Galois action on the étale fundamental group of the Fermat curve

Rachel Pries
(joint work with Rachel Davis, Vesna Stojanoska, Kirsten Wickelgren)

If X is a curve over a number field K, then we are motivated to understand the action of the absolute Galois group G_K on the étale fundamental group $\pi_1(X)$. When X is the Fermat curve of degree p and K is the cyclotomic field containing a pth root of unity, Anderson proved theorems about this action on the homology of X, with coefficients mod p. In earlier work, we extended Anderson's results to give explicit formulas for this action on the homology. Recently, we use a cup product in cohomology to determine the action of G_K on the lower central series of $\pi_1(X)$, with coefficients mod p. The proof involves some fun Galois theory and combinatorics.

1. Description of talk

In this talk, I first provided motivation and background about the inverse Galois problem and the Fermat curve X. Then I described a result of Anderson about homology of Fermat curves.

There were two main results in this talk. The first is about providing explicit formulas for the Galois action of Anderson. A key point is to determine the finite extension of the cyclotomic field through which the action of the absolute Galois group factors. Another key point is to use motivic homology, logarithmic differential maps, and Kummer maps to express the Galois action.

The second main result is about finding the Galois action on the lower central series of the fundamental group of the $\pi_1(X)$. The ideas in the proof use Galois theory and topology. Throughout the talk, I gave explicit examples and applications for small primes.

Fix $n \geq 3$. Let ζ be a primitive nth root of unity. Let X be the Fermat curve: $x^n + y^n = z^n$. It has genus $g = (n-1)(n-2)/2$. The points of $Z = \{z = 0\}$ and $Y = \{xy = 0\}$ are defined over the cyclotomic field $K = \mathbb{Q}(\zeta)$. Let $U = X - Z$. In $\pi_1(U)$, we define loops $E_{i,j}$ going through the points (x, y): $(0, 1) \to (1, 0) \to (0, \zeta^i) \to (\zeta^j, 0) \to (0, 1)$.

2. First main result

Anderson [And87] proved the following: for $n = p$ an odd prime, let L be the splitting field of $1 - (1 - x^p)^p$. Let $J_Z(X)$ be the generalized Jacobian of X with conductor Z. Then the number field generated by the pth roots of $\beta =$ "$(1, 0) - (0, 1)$" in $J_Z(X)(\overline{\mathbb{Q}})$ is L.

To prove this result, Anderson considers Galois actions on étale homology groups. There are similar results by Coleman [Col89] and Ihara [AI88], [Iha86]. The relative homology $H_1(U, Y)$ has dimension n^2 and is a free $\Lambda_1 = \mathbb{Z}[\mu_n \times \mu_n]$-module. We fix a generator $e_{0,0} \in H_1(U, Y)$ to be the path (singular 1-simplex) in X from $(0,1)$ to $(1,0)$ given by $t \mapsto [\sqrt[n]{t} : \sqrt[n]{1-t} : 1]$.

Let K be the cyclotomic field $\mathbb{Q}(\zeta)$ and G_K its absolute Galois group. For all odd primes p satisfying Vandiver's conjecture, our first main result is to explicitly determine the action of G_K on $H_1(X) \otimes \mathbb{Z}/p\mathbb{Z}$ by finding the action on $e_{0,0}$. The action is defined by determining an element $B_q \in \Lambda_1$ for each $q \in Q := \mathrm{Gal}(L/K)$ such that $q \cdot e_{0,0} = B_q e_{0,0}$. See [DPSW16] and [DPSW18] for the formula.

3. Second main result

We consider the Galois action on the lower central series of the étale fundamental group $\pi_1(X)$ of X.

Define the lower central series: For $m \geq 2$, let $[\pi_1(X)]_m$ be the closure of the subgroup generated by $[\pi_1(X), [\pi_1(X)]_{m-1}]$. So $[\pi_1(X)]_2 = [\pi_1(X), \pi_1(X)]$ is the commutator subgroup of $\pi_1(X)$. Then $H_1(X) = \pi_1(X)/[\pi_1(X)]_2$ is first quotient in the LCS of $\pi_1(X)$. It characterizes abelian unramified covers of X. Let $[\pi_1(X)]_3 = [\pi_1(X), [\pi_1(X)]_2]$. Then $[\pi_1(X)]_2/[\pi_1(X)]_3$ is the second quotient in the LCS. It gives information about the 2-nilpotent quotient of $\pi_1(X)$.

Let $\mathrm{gr}(\pi) = \sum_{m \geq 1} [\pi]_m/[\pi]_{m+1}$ be the graded Lie algebra for the lower central series for π. Let F be the free group on $2g$ generators, with graded Lie algebra $\mathrm{gr}(F)$. By work of Lazard [Laz54], Serre [Ser65], and Labute [Lab70], the structure of the graded Lie algebra of $\pi_1(X)$ depends only some element Δ_X of weight 2:

$$\mathrm{gr}(\pi) = \sum_{m \geq 1} [\pi]_m/[\pi]_{m+1} \simeq \mathrm{gr}(F)/\langle \Delta_X \rangle.$$

By work of Hain [Hai97], there is an isomorphism of $G_{\mathbb{Q}}$-modules $[\pi]_2/[\pi]_3 \simeq (H_1(X) \wedge H_1(X))/\mathrm{Im}(C)$. Here $C : H_2(X) \to H_1(X) \wedge H_1(X)$ is the dual map to the cup product $H^1(X) \wedge H^1(X) \to H^2(X)$. Let Δ_X denote a generator of $\mathrm{Im}(C)$. Then $\Delta_X = \sum_{i=1}^{g} a_i \wedge b_i$ for a good presentation

$$\pi_1(U) = \langle a_i, b_i, c_j \mid 1 \leq i \leq g,\ 1 \leq j \leq n \rangle / (\prod [a_i, b_i] \prod c_j).$$

For our second main result, let X be the Fermat curve of exponent n, with $n \geq 3$. We explicitly determine the image $\langle \Delta_X \rangle$ of $H_2(X) \to H_1(X) \wedge H_1(X)$ (coefficients in $\mathbb{Z}$). This gives an explicit characterization of $[\pi_1(X)]_m/[\pi_1(X)]_{m+1}$, for $m \geq 2$. With this formula for Δ_X, when $n = p$ is an odd prime satisfying Vandiver's conjecture, we can compute the action of G_K on $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z}$.

Theorem (Davis/P/Wickelgren [DPW])**.** *For $n \geq 3$, Δ_X is the image in $H_1(X) \wedge H_1(X)$ of*

$$\Delta_U = \sum_{1 \leq i_1 < i_2 \leq n-1} \epsilon(i_1, j_1, i_2, j_2) E_{i_1, j_1} \wedge E_{i_2, j_2} \in H_1(U) \wedge H_1(U),$$

where

$$\epsilon(i_1, j_1, i_2, j_2) = \begin{cases} 1 & j_2 - j_1 \equiv i_2 - i_1 \not\equiv 0 \mod n-1 \\ -1 & j_2 - j_1 + 1 \equiv i_2 - i_1 \not\equiv 0 \mod n-1 \\ 0 & \textit{otherwise.} \end{cases}$$

To prove the formula, we study the $\mathbb{Z}/n$-Galois cover $f : X \to \mathbb{P}^1$ given by $(x, y) \mapsto x$ using topology. We describe a loop around the cusps as a product of commutators of loops.

4. Applications and open questions

First, when $p = 5$, we show that the formula for Δ_X can also be determined by invariance properties under the geometric and arithmetic automorphisms of the curve. We wonder whether that is also true for $p \geq 7$.

Second, when $p = 5$, we can prove a coboundary map application. When $p = 5$, note that $\dim(H_1(X)) = 12$ and $K = \mathbb{Q}(\zeta_5)$. We can reprove a result due to Rohrlich and Tzermias [Roh77] and [Tze97]: the G_K-invariant subspace of $H_1(X) \otimes \mathbb{Z}/5$ has dimension 8; the $G_{\mathbb{Q}}$-invariant subspace of $H_1(X) \otimes \mathbb{Z}/5$ has dimension 2. Also, $\dim(H_1(X) \wedge H_1(X)) = 66$ so $\dim([\pi_1(X)]_2/[\pi_1(X)]_3) = 65$. Using our second main result, we show that the G_K-invariant subspace of $[\pi_1(X)]_2/[\pi_1(X)]_3 \otimes \mathbb{Z}/5$ has dimension 34.

This yields the following coboundary map application. Let $H = H_1(X) \otimes \mathbb{Z}/p$ and $\pi_2/\pi_3 = [\pi_1(X)]_2/[\pi_1(X)]_3 \otimes \mathbb{Z}/p$. There is a short exact sequence

$$0 \to (\mathbb{Z}/p)\Delta_X \to H \wedge H \to \pi_2/\pi_3 \to 0.$$

Since Q fixes Δ_X, this leads to a long exact sequence

$$(\mathbb{Z}/p)\Delta_X \hookrightarrow H^0(Q; H \wedge H) \to H^0(Q; \pi_2/\pi_3) \xrightarrow{\delta} H^1(Q; (\mathbb{Z}/p)\Delta_X)...$$

When $p = 5$, our computations show that δ is trivial. We wonder whether the analogous statement is true for $p \geq 7$.

Acknowledgement: Pries was supported by NSF grants DMS-15-02227 and DMS-19-01819. This project was supported by AIM through a Square collaboration grant.

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.

[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.

[Col89] R.F. Coleman, *Anderson-Ihara theory: Gauss sums and circular units*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 55–72.

[DPSW16] R. Davis, R. Pries, V. Stojanoska, and K. Wickelgren, *Galois action on the homology of Fermat curves*, Directions in number theory, Assoc. Women Math. Ser., vol. 3, Springer, [Cham], 2016, pp. 57–86.

[DPSW18] ———, *The Galois action and cohomology of a relative homology group of Fermat curves*, J. Algebra **505** (2018), 33–69.

[DPW] R. Davis, R. Pries, and K. Wickelgren, *The Galois action on the lower central series of the fundamental group of the Fermat curve*, arXiv:1808.04917 [math.NT] (2018).

[Hai97] R. Hain, *Infinitesimal presentations of the Torelli groups*, J. Amer. Math. Soc. **10** (1997), no. 3, 597–651.

[Iha86] Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106. MR 825839 (87c:11055)

[Lab70] J.P. Labute, *On the descending central series of groups with a single defining relation*, J. Algebra **14** (1970), 16–23.

[Laz54] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190.

[Roh77] D.E. Rohrlich, *Points at infinity on the Fermat curves*, Invent. Math. **39** (1977), no. 2, 95–127.

[Ser65] J.-P. Serre, *Lie algebras and Lie groups*, Lectures given at Harvard University, vol. 1964, W. A. Benjamin, Inc., New York-Amsterdam, 1965.

[Tze97] ———, *Mordell-Weil groups of the Jacobian of the 5th Fermat curve*, Proc. Amer. Math. Soc. **125** (1997), no. 3, 663–668.

Towards minimalistic Neukirch and Uchida theorems

Florian Pop

(joint work with Adam Topaz)

1. Introduction/Motivation

For global fields K_0, let $\mathbb{P}(K_0)$ denote places of K_0, and $G_{K_0} = \mathrm{Aut}(K_0^{\mathrm{sep}}|K_0)$ be the absolute Galois group, with its several variants, e.g. $G_{K_0}^{\mathrm{sol}} = \mathrm{Aut}(K_0^{\mathrm{sol}}|K_0)$, $G_{K_0}^{\mathrm{ab}} = \mathrm{Aut}(K_0^{\mathrm{ab}}|K_0)$. For Galois extensions $K|K_0$, $L|L_0$, let $\mathrm{Isom}^{\mathrm{F}}(L|L_0, K|K_0)$ be the isomorphisms of field extensions up to Frobenius twists. Recall the famous result by Neukirch and Uchida (with contributions by Ikeda, Komatsu, Iwasawa):

Theorem 1 (Classical N & U Thm)**.** *One has a canonical bijection*

$$\mathrm{Isom}^{\mathrm{F}}(L_0^{\mathrm{sep}}|L_0, K_0^{\mathrm{sep}}|K_0) \to \mathrm{Isom}(G_{K_0}, G_{L_0}).$$

Recall that the fundamental technical tool in the proof is Neukirch's *local theory* developed in the 1960's, which is a nutshell asserts that the set $\mathcal{D}_{K_0}$ of maximal closed subgroups $G \subset G_{K_0}$ which are isomorphic to decomposition groups of finite place of global fields is the set of decomposition groups of finite places of K_0. Hence every $\Phi \in \mathrm{Isom}(G_{K_0}, G_{L_0})$ defines a canonical bijection $\mathcal{D}_{K_0} \to \mathcal{D}_{L_0}$. Moreover, Uchida (1976+) gave a *constructive proof* of global function fields K_0 from G_{K_0}. Further, all assertions above hold correspondingly for $G_{\bullet}^{\mathrm{sol}}$, that is:

$$\mathrm{Isom}^{\mathrm{F}}(L_0^{\mathrm{sol}}|L_0, K_0^{\mathrm{sol}}|K_0) \to \mathrm{Isom}(G_{K_0}^{\mathrm{sol}}, G_{L_0}^{\mathrm{sol}}).$$

In the 1990's the above results became special cases of Grothendieck's conjecture of birational anabelian geometry, resolved by Pop (1995), and the results about global function fields were sharpened by Tamagawa (1997), Stix (2002), and Mochizuki (2007), by proving that if X_0, Y_0 are hyperbolic curves over finitely generated fields k_0, and $K_0 = k_0(X_0)$, $L_0 = k_0(Y_0)$, then one has:

$$\mathrm{Isom}^{\mathrm{F}}(X_0, Y_0) \cong \mathrm{Out}\big(\pi_1(X_0), \pi_1(Y_0)\big).$$

Quite recently, Saïdi–Tamagawa (2017), showed that Uchida's Thm holds for the pro-Σ_{K_0} completion $G_{K_0}^{\Sigma_{K_0}}$ of the absolute Galois group, where Σ_{K_0} is non-slim. Further, Hoshi (2019) gave an effective reconstruction of *number fields* K_0 from $G_{K_0}^{\mathrm{sol}}$, thus proving Uchida type results for number fields. (Unfortunately, Hoshi is using the previous results, thus he does not give a new proof of the Neukirch and Uchida Theorem.) And very recently, Saïdi–Tamagawa (2019+ϵ) proved the *m-step solvable* ***N & U Thm*** *for number fields*:

Theorem 2 (Saïdi-Tamagawa)**.** $\mathrm{Isom}(\overset{m}{L_0}|L_0, \overset{m}{K_0}|K_0) \to \mathrm{Isom}\big(G_{K_0}^{m+3}, G_{L_0}^{m+3}\big)/\!\sim$ *is a bijection for $m > 0$, where $\Phi^{m+3} \sim \Phi'^{\,m+3}$ if their "restrictions" to $G_{K_0}^{m}$ are equal.*

To complete this very brief introduction to the topic Neukirch and Uchida Theorem, let me recall the "non-anabelian type results" by Cornelissen, de Smit, Marcolli, Harry Smit and others, which recover $\mathrm{Isom}(L_0, K_0)$ from "decorated" isomorphisms of the character groups $\mathrm{Isom}^*(\widehat{G}_{K_0}, \widehat{G}_{L_0})$.

2. The work in progress (Pop–Topaz)

The work in progress I reported on is about "how much Galois theory characterizes number fields up to canonical isomorphism?"

We consider notations as follows:

- Let $\Lambda = \mathbb{Z}/\ell$ or $\Lambda = \mathbb{Z}_\ell$ (with $\ell > 2$), or $\Lambda = \prod_{\ell' \in S} \mathbb{Z}/\ell'$, $S \subset$ **Primes** infinite.
- For fields F, let $F^c|F^a|F$ be the Λ *abelian-by-central,* resp. *abelian extensions.*
- **Note**: If $F|F_0$ Galois, $F^c|F^a|F|F_0$ are Galois, and one has the exact sequence:

$$1 \to \mathcal{G}_F^{\bullet} \to \mathcal{G}_{F^\bullet|F_0} := \mathrm{Gal}(F^\bullet|F_0) \to \mathcal{G}_{F|F_0} := \mathrm{Gal}(F|F_0) \to 1, \quad \bullet = c, a$$

- For $F|F_0$, $E|E_0$ Galois, consider $\mathcal{G}_{F^c|F_0} \to \mathcal{G}_{F|F_0}$, $\mathcal{G}_{E^c|E_0} \to \mathcal{G}_{E|E_0}$. Denote:

$$\mathrm{Isom}^c(\mathcal{G}_{F|F_0}, \mathcal{G}_{E|E_0}) = \big\{\Phi \in \mathrm{Isom}(\mathcal{G}_{F^c|F_0}, \mathcal{G}_{E^c|E_0}) \mid \Phi(\mathcal{G}_F^c) = \mathcal{G}_E^c\big\}\big/\!\sim$$

- For $\Sigma \subset$ **Primes**, $\delta(\Sigma) = 1$, let $\Sigma_{F_0} \subset \Sigma$ be the totally split part of Σ in F_0.
- Given Σ, consider Galois extensions $F|F_0$ satisfying the following:

Hypothesis $(\mathrm{H})_\Sigma$: *One has $\mu_\Lambda \subset F$, and for almost all $p \in \Sigma_{F_0}$, all the prolongations $v|p$ of p to F satisfy $\mathbb{Q}_p^{\mathrm{ab}} \subset F_v$. Further, if $\Lambda = \mathbb{Z}/\ell$, one has:*

$$(*) \qquad \sqrt[n_p]{p} \in F_v, \text{ where } n_p = \ell(p-1).$$

Example. Suppose that $\mu_{p^\infty} \subset F$ for almost all $p \in \Sigma$, e.g. $F_0^{\mathrm{ab}} \subset F$. One has:

- If $\Lambda \neq \mathbb{Z}/\ell$, then $F|F_0$ satisfies $(\mathrm{H})_\Sigma$.
- If $\sqrt[n_p]{p} \in F$ for almost all $p \in \Sigma_{F_0}$, then $F|F_0$ satisfies $(\mathrm{H})_\Sigma$.

Main Result [P-Topaz/work in progress]. *For $K|K_0$, $L|L_0$ satisfying Hypothesis* $(\mathrm{H})_\Sigma$*, the canonical map below is a bijection:*

$$\mathrm{Isom}(L|L_0, K|K_0) \to \mathrm{Isom}^c(\mathcal{G}_{K|K_0}, \mathcal{G}_{L|L_0}).$$

Comments. Let $K = K_0^{\mathrm{ab}}$, $L = L_0^{\mathrm{ab}}$. Then $\Phi^c(\mathcal{G}_K^c) = \mathcal{G}_L^c \ \forall\, \Phi^c \in \mathrm{Isom}(\mathcal{G}_{K^c|K_0}, \mathcal{G}_{L^c|L_0})$. Therefore, $\mathrm{Isom}^c(\mathcal{G}_{K|K_0}, \mathcal{G}_{L|L_0}) = \mathrm{Isom}(\mathcal{G}_{K^c|K_0}, \mathcal{G}_{L^c|L_0})/\!\sim$. Similar assertions hold for any "*verbal*" Galois extension $K|K_0$ satisfying $(\mathrm{H})_\Sigma$. *In particular*:

(1) $K_0^{\mathrm{ab}}|K_0$ *is* functorially *encoded in its* pro-ℓ abelian-by-central *extension.*
(2) **Minimalistic N & U Thm.** *Let $K|K_0^{\mathrm{ab}}$ be the $\mathbb{Z}/\ell$ elementary abelian extension. Then the isomorphism type of $K|K_0$ is* functorially *encoded in its* $\mathbb{Z}/\ell$ abelian-by-central *extension.*
(3) The above results hold in the same form for $K_0^{\mathrm{cycl}}|K_0$.
(4) The result (1) holds for finitely generated fields F_0 with $\mathrm{char}(F_0) = 0$.

Unfortunately, we cannot **(yet?)** prove (2) for all fin. gen. F_0, $\mathrm{char}(F_0) = 0$.

3. Work in progress/Methods

Two main Steps: (1) **Local Theory**(LT); (2) **Global Theory** (GT).

To (1). The main technical tool is the (long) story of *c.l.p.*: Ware, followed by Jacob, Arason, Bogomolov, B-Tschinkel, Koenigsmann, Efrat, Minac, **Topaz**,...

Theorem 3. *Let $\mu_\ell \subset F$, and $\sigma, \tau \in \mathcal{G}_F^a$ be independent. If σ, τ have commuting liftings to $\mathcal{G}_F^c$ under $\mathcal{G}_F^c \to \mathcal{G}_F^a$, there is $w \in \mathrm{Val}(F)$ such that $\sigma, \tau \in D_w^a$.*

Fact. *If $w \in \mathrm{Val}(F)$ is minimal with $D_w^a \neq 1$, then* $D_{w|w_0} = \mathrm{Stab}_{\mathcal{G}_{F|F_0}}(D_w^a)$.

- Note that the above recipies are invariant under all $\Phi \in \mathrm{Isom}^c(\mathcal{G}_{K|K_0}, \mathcal{G}_{L|L_0})$.
- Let $K_0'|K_0 \hookrightarrow K|K_0$, $L_0'|L_0 \hookrightarrow L|L_0$ correspond under $\Phi \in \mathrm{Isom}^c(\mathcal{G}_{K|K_0}, \mathcal{G}_{L|L_0})$.
- Then $\Phi' : \mathcal{G}_{K|K_0'} \to \mathcal{G}_{L|L_0'}$ gives rise to $\varphi_{\Phi'} : \Sigma(K_0') \to \Sigma(L_0')$ + extra info...

To (2). This is inspired by / uses work of **Harry Smit**. In a nutshell:

For every finite Galois subextension $K_0'|K_0$ of $K|K_0$, let $p \in \Sigma_{K_0'} \subset \Sigma$ be the totally split p in K_0', and $\Sigma(K_0')$ be the prolongation of $\Sigma_{K_0'}$ to K_0'. TFH:

- $\Sigma_{K_0'}$ can be *effectively* described via the (LT).
- In particular, for $p \in \Sigma$, one can detect $\Sigma(K_0') \cap \mathbb{P}_p(K_0')$, hence $[K_0' : \mathbb{Q}]$.
- For $v' \in \Sigma(K_0')$, one can *effectively* detect $\mathrm{Frob}_{v',\ell}$ via the (LT).
- Hence one can effectively detect the ℓ-character group $\widehat{G}_{K_0'}$, etc.
- By (LT), everything is invariant under $\Phi \in \mathrm{Isom}^c(\mathcal{G}_{K|K_0}, \mathcal{G}_{L|L_0})$.

Conclude by applying techniques from work of Harry Smit.

References

[BT02] F. Bogomolov nd Y. Tschinkel, Commuting elements of Galois groups of function fields. *Motives, polylogarithms and Hodge theory, Part I* (Irvine, CA, 1998), 75–120, Int. Press Lect. Ser., **3**, I, 2002.

[CSLMS19] G .Cornelissen, B. de Smit, X. Li, M. Marcolli and H. Smit, Characterization of global fields by Dirichlet L-series, *Research in Number Theory* vol. 5, **7** (2019).

[Hos19] Y. Hoshi, Mono-anabelian reconstruction of number fields, *On the examination and further development of inter-universal Teichmüller theory 2015*, 1–77, RIMS Kôkyûroku Bessatsu, **B76**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2019.

[Pop94] F. Pop, On Grothendieck's conjecture of birational anabelian geometry. *Ann. of Math.* **(2)** 139 (1994), no. 1, 145–182.

[Pop12] F. Pop, $\mathbb{Z}/\ell$ abelian-by-central Galois theory of prime divisors. The arithmetic of fundamental groups—PIA 2010, 225–244, *Contrib. Math. Comput. Sci.*, **2**, Springer, Heidelberg, 2012.

[ST17] M. Saïdi and A. Tamagawa, A refined version of Grothendieck's birational anabelian conjecture for curves over finite fields. *Adv. Math.* **310** (2017), 610–662.

[ST19] M. Saïdi and A Tamagawa, The m-step solvable anabelian geometry of number fields, arXiv:1909.08829 [math.NT] (2019).

[Smit19] H. Smit, L-series and isomorphisms of number fields, arXiv:1901.06198 [math.NT] (2019).

[Top17] A. Topaz, Commuting-Liftable Subgroups of Galois Groups II. *J. reine angew. Math.* (2017) **730**, pg. 65-133

Reporters: Séverin Philip, Densuke Shiraishi