Mathematisches Forschungsinstitut Oberwolfach

Report No. 25/2018

DOI: 10.4171/OWR/2018/25

# Field Arithmetic

Organised by
Lior Bary-Soroker, Tel Aviv
Florian Pop, Philadelphia
Jakob Stix, Frankfurt

3 June – 9 June 2018

Abstract. Field Arithmetic studies the interrelation between arithmetic properties of fields and their absolute Galois groups. It is an interdisciplinary area that uses methods of algebraic number theory, commutative algebra, algebraic geometry, arithmetic geometry, finite and profinite groups, and non-archimedean analysis. Some of the results are motivated by questions of model theory and used to establish results in (un-)decidability.

*Mathematics Subject Classification (2010):* 12E30.

## Introduction by the Organisers

This workshop was the 8th MFO Workshop in *Field Arithmetic*, and brought together experts from several related research areas where major progress has been achieved recently. Among the participants were two of the initiators of Field Arithmetic in the 1980's, namely Wulf-Dieter Geyer (Erlangen) and Moshe Jarden (Tel Aviv). The organizers were happy to observe that the blend of young and experienced researchers present at the workshop and the variety of subjects that they covered lead to a stimulating atmosphere with all participants actively contributing to the success of the meeting. The hospitality of the staff at MFO provided for a pleasant meeting environment, and that contributed a lot to a smooth running of the workshop.

Among the prominent areas of research the talks touched upon were number theory in global fields, algebraic geometry, model theory of local fields and of finitely generated fields, first order definability of valuations, anabelian geometry — especially Grothendieck's and Bogomolov's birational anabelian geometry, local global principles, both for the existence of rational points and for (cohomological)

Hasse principles. The talks reflected the richness and the power of results obtained by combining tools from several areas, e.g., valuation theory, Galois theory, group theory, local-global approaches, model theory and logic, which is one of the core characteristics of field arithmetic. The major areas of research and the talks roughly grouped together by area were as follows:

- Anabelian geometry, $K$-theory, and cohomology: talks by Cadoret, Efrat, Ivanov, Karemaker, Topaz.
- Arithmetic geometry: talks by Colliot-Thélène, Jarden, Park, Zywina.
- Local-global principles for points and covers: talks by Harbater, Neftin, Schindler.
- Model theory and definability: talks by Dittmann, Fehm, Poonen.
- Number theory in global fields: talks by Entin, Gorodetsky, Ramiharimanana.

There was also an *evening talk* on Wednesday night by Jochen Koenigsmann, a *problem session* on Thursday night, and as a service to the younger participants also a *historical survey talk* by Wulf-Dieter Geyer on Friday afternoon.

The talks by Cadoret and Topaz were about anabelian type reconstruction based on $K$-theory of function fields and pro-$\ell$ abelian-by-central Galois theory. They hinted at the possibility of using this kind of constructions and results to approach a host of problems in arithmetic and algebraic geometry, e.g., the birational Tate conjectures (for divisors), Iwasawa theory, etc. The talks by Ivanov and Karemaker explored anabelian geometry for rings of integers in number fields. Karemaker spoke about recovering the isomorphy type of number fields from their 2-dimensional representations, whereas Ivanov investigated *infinitesimal Dirichlet densities* which can be used in studying pro-$p$ extensions of number fields unramified outside a given infinite set $S$ of primes. Finally, Efrat's talk was about a conceptual generalization of Massey products using the complexity of words in group generators by constructions in group cohomology.

The talk by Jarden presented a proof of further cases of a long standing conjecture concerning the torsion points of abelian varieties over random subfields $K(\underline{\sigma}) \subset \overline{K}$ for $K$ finitely generated and $\underline{\sigma}$ a finite system of elements of the absolute Galois group $G_K$. Colliot-Thélène reported in his talk about a simplified proof for results concerning families of smooth projective varieties due to Hassett, Pirutka and Tschinkel: such fibrations can have both rational and non-stably rational smooth fibers. Park explained her result about the image of the tropicalization procedure for curves taking into account the metric structure on the tropicalization. Finally, Zywina's talk was about *effective computation* of Mumford–Tate groups of abelian varieties over number fields.

The local global principles (LGP), both for rational points and for cohomology groups, are some of the most powerful tools in arithmetic and algebraic geometry. Schindler spoke about a LGP related to a recent conjecture of Harpaz–Wittenberg concerning rational points on rationally connected varieties. Complete results in this direction would have tremendous consequences in arithmetic geometry and inverse Galois theory. Harbater gave an overview of recent and new results concerning local-global principles for points on homogeneous spaces over function fields of curves over complete DVR's, and indicated how one applies these LGP to differential Galois theory over large fields $k$ of infinite transcendence degree. These results lead to solving a conjecture by Matzat on the existence and nature of the *differential absolute Galois group* of rational function fields $k(t)$, where $k$ is an algebraically closed field of countable transcendence degree. Finally, Neftin's talk was about a weak approximation property and the Grunwald–Wang problem. Particular aspects of this theory are properties and variants of LGP's for rational points on homogeneous spaces of the form $\mathrm{GL}_n/G$ or $\mathrm{SL}_n/G$, where $G$ is a finite subgroup. Recent results by several authors were presented, both for $G$ solvable and non-solvable.

Definability of valuations is at the center of several major open problems (and strategies to tackle such problems) concerning model theory of local fields and of finitely generated fields. This is the case with one of the main open problems in the elementary theory of finitely generated fields, which was the theme of Poonen's talk. Fehm introduced the class of *pseudo-algebraic fields* and sketched the proof that they are dense in their real and $p$-adic closures. Dittmann's talk was about the *p-Pythagoras number* of fields, which is a new very interesting invariant of fields, extending the usual notion of the Pythagoras number of a field. These are very exciting new developments, and their consequences in arithmetic geometry are subject of further intense and extensive research.

Gorodetsky talked about the resolution of a function field analogue of a deep open problem in analytic number theory. The problem concerns the Chebotarev density theorem in short intervals. Entin presented a new geometric method to compute Galois groups. This method is very general, and in particular, it generalizes many of the recent computations of Galois groups coming from number theoretic applications. Ramiharimanana discussed new results on the minimal ramification problem in number fields.

*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-1049268, "US Junior Oberwolfach Fellows".

## Workshop: Field Arithmetic

## Table of Contents

# Abstracts

## The first-order theory of finitely generated fields

Bjorn Poonen

This is a survey on topics surrounding some open questions about the first-order theory of finitely generated fields.

### 1. First-order sentences and formulas

Let $k$ be a field. A first-order sentence in the language of rings, such as

$$(\forall z)(\exists x)(\exists y)\ x^2 + y^2 = z,$$

will be either true or false for $k$. The theory of $k$ is the set of first-order sentences that are true for $k$. Fields $k$ and $\ell$ are elementarily equivalent if their theories coincide. For example, one formulation of the Lefschetz principle is that all algebraically closed fields of characteristic 0 are elementarily equivalent to each other; this implies that theorems proved over $\mathbb{C}$ via analytic methods can be immediately transported to fields such as $\overline{\mathbb{Q}}$, for example.

A first-order formula $\phi$ is like a first-order sentence except that it may involve variables that are free, not bound by quantifiers. If $\phi$ has $m$ free variables, then it has a truth value only after assigning values in $k$ to those variables, and the set of value tuples in $k^m$ that make $\phi$ true for $k$ is called a definable subset of $k^m$. (Strictly speaking, this should be called 0-definable if the formula does not involve symbols for constants in $k$ beyond those present in the language of rings, 0 and 1.) Given definable subsets $D \subset k^m \times k^n$ and $B \subset k^m$ such that the projection $k^m \times k^n \to k^m$ restricts to a map $\pi\colon D \to B$, call $\{\pi^{-1}(b) : b \in B\}$ a definable family of sets.

### 2. Finitely generated fields

Call $K$ finitely generated (f.g.) if it is finitely generated as a field extension of its minimal subfield ($\mathbb{Q}$ or $\mathbb{F}_p$). Alternative descriptions:

- function field of a geometrically integral variety over a number field or finite field;
- finite extension of $\mathbb{Q}(t_1, \dots, t_n)$ or $\mathbb{F}_p(t_1, \dots, t_n)$;
- $\operatorname{Frac} R$, where $R$ is a domain that is f.g. as a $\mathbb{Z}$-algebra.

The Kronecker dimension of such a field $K$ is defined by

$$\operatorname{Kr.dim} K := \text{Krull}\dim R = \begin{cases} \operatorname{tr.deg}(K/\mathbb{F}_p), & \text{if } \operatorname{char} K = p > 0, \\ \operatorname{tr.deg}(K/\mathbb{Q}) + 1, & \text{if } \operatorname{char} K = 0. \end{cases}$$

## 3. Three questions

Each of the following questions asks for more than the previous one:

1. (Sabbagh 1980s, Pop 2002 [2]) Given non-isomorphic f.g. fields $K$ and $L$, is there a sentence that is true for $K$ and false for $L$?
2. Given a f.g. field $K$, is there a sentence that is true for $K$ and false for all f.g. fields not isomorphic to $K$?
3. Is every *reasonable class* of infinite f.g. fields cut out by a single sentence? (See [1, §1.2] for a definition of "reasonable" suggested by Hrushovski.)

## 4. Results

- Rumely [4] proved theorems that imply a positive answer to all three questions restricted to the case of global fields, i.e., f.g. fields $K$ of Kronecker dimension 1. The key was to build on work of J. Robinson and Ershov to find a uniformly 0-definable family of sets that includes all valuation subrings of $K$.
- Pop [2] proved that for each $n \in \mathbb{N}$, there is a sentence $\sigma_n$ that for a f.g. field $K$ holds if and only if $\operatorname{Kr.dim} K = n$. The method was to use the work of Voevodsky and Rost relating isotropy of Pfister forms to cohomological dimension.
- The author [1, Theorem 1.1] proved that there is a first-order sentence that is true for all f.g. fields of characteristic 0 and false for all f.g. fields of positive characteristic. The proof uses the arithmetic of elliptic curves.
- The author [1, Theorem 1.3] proved that there is a first-order formula that in any f.g. field $K$ defines the constant field (the relative algebraic closure of the minimal subfield in $K$).
- The author [1, Theorem 1.4] proved that for each $n \in \mathbb{N}$, there is a first-order formula $\psi_n(t_1, \ldots, t_n)$ that when interpreted in a f.g. field $K$ is true if and only if $t_1, \ldots, t_n$ are algebraically dependent over the constant field.
- The answer to all three questions would be positive if one could find a uniformly definable family containing sufficiently many valuation subrings in every f.g. field; see Scanlon's article [5].
- Pop [3] proved a positive answer to the first two questions restricted to f.g. fields of Kronecker dimension $\leq 2$. He used a higher local-global principle due to Kato.

## References

[1] B. Poonen, *Uniform first-order definitions in finitely generated fields*, Duke Math. J. **138** (2007), 1–22.

[2] F. Pop, *Elementary equivalence versus isomorphism*, Invent. Math. **150** (2002), 385–408.

[3] F. Pop, *Elementary equivalence versus isomorphism, II*, Algebra Number Theory **11** (2017), 2091–2111.

[4] R. S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), 195–217.

[5] T. Scanlon, *Infinite finitely generated fields are biinterpretable with* $\mathbb{N}$, J. Amer. Math. Soc. **21** (2008), 893–908. Erratum in J. Amer. Math. Soc. **24** (2011), 917.

## Chebotarev Density Theorem in Very Short Intervals for Nilpotent Extensions of $\mathbb{F}_q(T)$

Ofir Gorodetsky
(joint work with Lior Bary-Soroker, Taelin Karidi)

One of the main theorems in algebraic number theory is the Chebotarev Density Theorem, which says the following (for base field $\mathbb{Q}$). Let $E$ be a finite Galois extension of $\mathbb{Q}$ with Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$ and with ring of integers $\mathcal{O}_E$. For a prime number $p$, we define

$$\left(\frac{E/\mathbb{Q}}{p}\right) \subseteq G,$$

to be the set of all $\sigma \in G$ for which there exists a prime $\mathfrak{P}$ of $E$ lying above $p$ such that

$$\sigma(x) \equiv x^p \mod \mathfrak{P},$$

for all $x \in \mathcal{O}_E$. If $p$ is unramified in $E$, then $\left(\frac{E/\mathbb{Q}}{p}\right)$ is called the *Frobenius* at $p$ and it is a conjugacy class in $G$. The Chebotarev Density Theorem says that as $p$ varies, the Frobenius equidistributes in the set of conjugacy classes. More precisely, let

$$\pi(x) = \#\{p \leq x : p \text{ prime number}\}$$

be the prime counting function. By the Prime Number Theorem, we know that $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$ well approximates $\pi(x)$. For a conjugacy class $C \subseteq G$, let

$$\pi_C(x;E) = \#\left\{p \leq x : p \text{ prime number and } \left(\frac{E/\mathbb{Q}}{p}\right) = C\right\}$$

be the function that counts primes with Frobenius equal to $C$. The Chebotarev Density Theorem says that

$$\pi_C(x;E) \sim \frac{|C|}{|G|}\mathrm{Li}(x), \qquad x \to \infty.$$

It is both natural and important for applications to consider the Chebotarev Density Theorem in short intervals. Balog and Ono [1] studied the non-vanishing of Fourier coefficients of modular forms in short intervals. For this application they prove that

$$\pi_C(x+y;E) - \pi_C(x;E) \sim \frac{|C|}{|G|}\frac{y}{\log x}, \qquad x \to \infty, \tag{1}$$

for $x^{1-1/c(E)+\varepsilon} \leq y \leq x$, and where $c(E) > 0$ is a constant depending only on $[E:\mathbb{Q}]$. Recently, the range of $y$ was improved by Thorner [11, Corollary 1.1].

A folklore conjecture says that for any fixed $\varepsilon > 0$ and $y = x^\varepsilon$ the formula (1) holds true. The work of Lagarias and Odlyzko [8], which is conditional on the Riemann Hypothesis for the zeta function of $E$, gives this for $\varepsilon > 1/2$. However, the case $\varepsilon \leq 1/2$ falls beyond the known methods, even conditionally. In the talk we discussed our recent work in the function field setting, which establishes the conjecture for any $\varepsilon > 0$ in the large-$q$ limit and under the assumption that $G$ is nilpotent.

We describe what has been known in the function field setting. For a Galois extension $E$ of $\mathbb{F}_q(T)$ with Galois group $G$, the Frobenius at a prime $P$ is defined similarly. Given a conjugacy class $C \subseteq G$, we set

$$\pi_{C;q}(n;E) = \#\left\{P \text{ a degree-}n \text{ prime} : \left(\frac{E/\mathbb{F}_q(T)}{P}\right) = C\right\},$$

the function that counts primes with Frobenius $C$. For simplicity, we assume that $E/\mathbb{F}_q(T)$ is geometric. Thanks to the availability of the Riemann Hypothesis for curves over finite fields, Fried and Jarden proved that [6, Proposition 6.4.8]

$$\left|\pi_{C;q}(n;E) - \frac{|C|}{|G|}\frac{q^n}{n}\right| \ll \frac{|C|}{|G|}\max\{\text{genus}(E), |G|\}\frac{q^{n/2}}{n}, \tag{2}$$

where $\frac{q^n}{n}$ is the function field analogue of $\mathrm{Li}(x)$; this is an effective Chebotarev Density Theorem over $\mathbb{F}_q(T)$.

Following Keating and Rudnick [7, §2.1], we define a short interval around a polynomial $f$ of degree $n$ with parameter $0 \leq m < n$ to be

$$I(f,m) = \{f + g : \deg g \leq m\}.$$

Its size is $I(f,m) = q^{m+1}$. In order to compare with the number field interval $\{x \leq n \leq x + x^\varepsilon\}$, we see that $x$ corresponds to $|f| = q^n$ and $x^\varepsilon$ corresponds to $q^{m+1}$, so $\varepsilon = \frac{m+1}{n}$. Our interest is in the quantity

$$\pi_{C;q}(I(f,m);E) = \#\left\{P \in P_{n,q} \cap I(f,m) : \left(\frac{E/\mathbb{F}_q(T)}{P}\right) = C\right\}.$$

One would naively expect that (2) implies an estimate for $\pi_{C;q}(I(f,m);E)$ whenever $m + 1 > n/2$ (i.e., $\varepsilon > 1/2$). However, this is not always true, as there is an obstruction to Chebotarev in short intervals coming from the fact that $E$ is not necessarily linearly disjoint from the cyclotomic field $L_{n-m-1}$ associated to a power of the prime at infinity (see [10, Chapter 12]). Applying (2) to the compositum of $EL_{n-m-1}$ would yield a Chebotarev in short intervals for $\varepsilon > 1/2$ with *possibly modified* densities. We note that the extensions $L_{n-m-1}$ are wildly ramified at the prime at infinity.

The main result presented in the talk is

**Theorem 1** (Bary-Soroker, G., Karidi)**.** *For every $B > 0$ there exists a constant $M_B$ satisfying the following property. Let $q$ be a prime power. Let $n > m \geq 2$ if $q$ is odd and $n > m \geq 3$ otherwise. Let $G$ be a nilpotent group and let $E/\mathbb{F}_q(T)$ be a geometric $G$-extension that is tamely ramified at the prime at infinity. Assume that* genus$(E), n, |G| \leq B$. *Let $f \in \mathbb{F}_q[T]$ be monic of degree $n$. Then*

$$\left|\frac{1}{q^{m+1}}\pi_{C;q}(I(f,m);E) - \frac{|C|}{|G|}\frac{1}{n}\right| \leq M_B q^{-1/2}. \tag{3}$$

In the talk we introduced the general notion of $G$-factorization arithmetic functions, which are arithmetic functions on $\mathbb{F}_q[T]$, whose value on a polynomial $f(T)$

depends only on the Frobenius at the prime factors of $f(T)$. The indicator of primes with given Frobenius is an instance of such a function. Another example is the indicator of polynomials that are norms of an ideal in $\mathcal{O}_E$. This class of functions generalizes those considered by Bary-Soroker and Fehm [4] for $E = \mathbb{F}_q(\sqrt{-T})$ and Rodgers [9] for $E = \mathbb{F}_q(T)$.

We sketched the method of proof. Given a short interval, we relate such an arithmetic function $\psi$ to a class function $\psi'$ on a *subgroup* of the wreath product $G \wr S_n$. The main property of this association is that the expected value of $\psi$ on the short interval is asymptotically equal to the average of $\psi'$ on the subgroup as $q \to \infty$ – this is a consequence of a multi-dimensional function field Chebotarev Density Theorem. The main technical part of the work is to compute the subgroup: it equals the wreath product $G \wr S_n$ itself. For the group computation we take an algebraic approach, using elementary group theory, Artin-Schreier theory and Kummer theory. Our methods are in the spirit of the works of S. D. Cohen [5] and Bank, Bary-Soroker and Fehm [2], where $G$ was cyclic and $E$ was of genus 0.

## References

[1] A. Balog and K. Ono, *The Chebotarev density theorem in short intervals and some questions of Serre*, Journal of Number Theory 91 (2001), 356–371.

[2] E. Bank and L. Bary-Soroker and A. Fehm, *Sums of two squares in short intervals in polynomial rings over finite fields.* To appear in American Journal of Mathematics.

[3] E. Bank and L. Bary-Soroker and L. Rosenzweig, *Prime polynomials in short intervals and in arithmetic progressions.* Duke Mathematical Journal 164 (2015), 277-295.

[4] L. Bary-Soroker and A. Fehm, *Correlations of Sums of Two Squares and Other Arithmetic Functions in Function Fields.* International Mathematics Research Notices (2017).

[5] S. D. Cohen, *The Galois group of a polynomial with two indeterminate coefficients.* Pacific Journal of Mathematics 90 (1980), 63–76.

[6] M. D. Fried and M. Jarden, *Field arithmetic.* Volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, second edition, 2005.

[7] J. P. Keating and Z. Rudnick, *The variance of the number of prime polynomials in short intervals and in residue classes.* International Mathematics Research Notices, 2014.

[8] J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[9] B. Rodgers, *Arithmetic functions in short intervals and the symmetric group.* To appear in Algebra & Number Theory.

[10] M. Rosen, *Number theory in function fields.* Volume 219 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

[11] J. Thorner, *A variant of the Bombieri–Vinogradov theorem in short intervals and some questions of Serre*, Mathematical Proceedings of the Cambridge Philosophical Society *161* (2016), 53–63.

## Pseudo-algebraic fields are dense in their classical closures

Arno Fehm

(joint work with Sylvy Anscombe, Philip Dittmann)

In this talk I introduced a new class of fields that generalizes several classical concepts from field arithmetic:

**Definition 1.** A field $F$ is **pseudo-algebraic** if it is a model of the common theory of the algebraic fields $K/\mathbb{Q}$ in the language of rings, i.e. $F \models \bigcap_{K/\mathbb{Q} \text{ alg.}} \mathrm{Th}_{\mathcal{L}_{\mathrm{ring}}}(K)$.

Examples of pseudo-algebraic fields are algebraic fields, local fields and non-standard number fields (like in [2]). Also pseudo-algebraically closed (PAC) fields are pseudo-algebraic, as are PRC and P$p$C fields (fields that satisfy a local-global principle for rational points on varieties) by results of Jarden [5, 6].

It seems that apart from a result by Chatzidakis [1] on the cohomological dimension of such fields, not much is known about pseudo-algebraic fields. The theorem presented in this talk is the following:

**Theorem 2.** *Every pseudo-algebraic field $F$ is dense in all its real closures and all its $p$-adic closures.*

This result is trivial in the case of algebraic fields and appears in the literature in the special case of PAC fields, PRC fields [7] and P$p$C fields [4], but it also gives new examples of fields dense in all their real and $p$-adic closures.

As immediate consequences one gets properties of the space of orderings and $p$-valuations and on the residue fields of valuations on such fields:

**Corollary 3.** *If $F$ is pseudo-algebraic, then distinct orderings and $p$-valuations induce distinct topologies on $F$.*

**Corollary 4.** *If $F$ is pseudo-algebraic and $v$ is a nontrivial valuation on $F$ such that the residue field $Fv$ admits an ordering or a $p$-valuation, then $Fv$ is real closed respectively $p$-adically closed.*

This second corollary in turn has concrete applications to the study of diophantine subsets in henselian valued fields with residue field algebraic over $\mathbb{Q}$, cf. [3].

The proof of the theorem axiomatizes the property of algebraic fields to be dense in their real and $p$-adic closures and combines techniques from model theory, number theory and arithmetic. A central point is the ability to define the set of totally positive elements (in the real case) respectively totally $p$-integral elements (in the $p$-adic case). In the real case this is achieved by Siegel's four squares theorem (which can be stated as a uniform bound on the *Pythagoras number* $\pi(K)$ of number fields $K$), while in the $p$-adic case it follows from a very recent $p$-adic analogue of Siegel's theorem [3, Theorem 9] (which can be stated as a uniform bound on the so-called *$p$-Pythagoras number* $\pi_p(K)$ of number fields).

*Remark.* For general fields, i.e. without a result like Siegel's theorem and its $p$-adic analogue, it is not possible to axiomatize the property that a field is dense in its real and $p$-adic closures. For example, refining a construction by Prestel [8] one can build a field $F$ that has precisely one ordering, which is archimedean (so $F$ is dense in all its real closures), but $\pi(F) = \infty$ and an elementary extension $F^*$ of $F$ has infinitely many orderings, including some for which $F^*$ is not dense in the corresponding real closures.

However, whenever $\pi(K)$ respectively $\pi_p(K)$ is finite, the denseness in real respectively $p$-adic closures can indeed be axiomatized. While for algebraic fields this can be seen by a reduction to number fields, which have only finitely many orderings or $p$-valuations (for fixed $p$) to which then the weak approximation theorem can be applied, for fields $F$ that are transcendental over $\mathbb{Q}$ we need new types of approximation theorems like the following:

**Theorem 5.** *Let $F$ be a field and assume that distinct orderings induce distinct topologies on $F$ (cf. Corollary 3). Let $f \in F[X]$ and $\epsilon \in F^\times$, and let $S$ be a set of orderings on $F$ that is open-closed (in the Harrison-topology). If for each ordering $\leq \in S$ there exists $x \in F$ such that $|f(x)| \leq |\epsilon|$, then there exists $x \in F$ such that $|f(x)| \leq |\epsilon|$ for each $\leq \in S$.*

*Remark.* Algebraic fields satisfy the stronger property of being dense in all their henselizations. The same holds for all pseudo-algebraically closed fields by a classical result of Frey–Prestel. Pseudo-algebraic fields, however, do not have this stronger property.

## References

[1] Z. Chatzidakis. On the cohomological dimension of non-standard number fields. *J. Pure Appl. Algebra* 69:121–133, 1990.

[2] G. Cherlin. Ideals of integers in nonstandard number fields. In: D. H. Saracino and V. B. Weispfenning (eds.), *Model Theory and Algebra. A Memorial Tribute to Abraham Robinson.*, 1975.

[3] A. Fehm. Diophantine subsets of henselian fields (joint work with Sylvy Anscombe, Philip Dittmann) *Oberwolfach reports* No. 49/2016.

[4] C. Grob. *Die Entscheidbarkeit der Theorie der maximalen pseudo p-adisch abgeschlossenen Körper.* Dissertation, Konstanz, 1987.

[5] M. Jarden. The algebraic nature of the elementary theory of PRC fields. *Manuscripta math.* 60(4):463–476, 1988.

[6] M. Jarden. Algebraic realization of $p$-adically projective groups. *Compositio Math.* 79(1):21–62, 1991.

[7] A. Prestel. Pseudo real closed fields. In R. B. Jensen and A. Prestel, editors, *Set Theory and Model Theory, Proceedings, Bonn 1979*, pages 127–156. Springer, 1981.

[8] A. Prestel. Remarks on the Pythagoras and Hasse number of real fields. *Journal reine angew. Math.* 303/304, 1978.

## On the (generic) cohomology of function fields

Adam Topaz

### 1. Introduction

The *generic cohomology* of a function field is an object which is constructed using a suitable cohomology theory of algebraic varieties. For simplicity, we restrict our attention to *Betti Cohomology* of algebraic varieties over $k$, where $k$ is an algebraically closed subfield of $\mathbb{C}$.

This talk had two primary goals. The first goal was to compare the generic cohomology of a function field with its Galois cohomology, highlighting the similarities between the two theories. The second goal was to discuss an *anabelian* result, showing that a higher-dimensional function field is determined by its generic cohomology ring, with rational coefficients, when endowed with additional *motivic* information on $\mathrm{H}^1$.

1.1. **Notation.** Let $k$ be an algebraically closed subfield of $\mathbb{C}$, and let $\Lambda$ be a subring of $\mathbb{Q}$. For a $k$-variety $Y$, we write $\mathrm{H}^i(Y, \Lambda)$ for the singular cohomology of $Y(\mathbb{C})$ (endowed with the complex topology) with coefficients in $\Lambda$. We will also endow $\mathrm{H}^i(Y, \Lambda)$ with its canonical mixed Hodge structure, and moreover write $\mathrm{H}^i(Y, \Lambda(j)) := \mathrm{H}^i(Y, \Lambda) \otimes \Lambda(j)$ for the corresponding Tate twist.

Let $X$ be an integral $k$-variety with function field $K$. We define

$$\mathrm{H}^i(K|k, \Lambda(j)) := \varinjlim_U \mathrm{H}^i(U, \Lambda(j))$$

where $U$ varies over the open $k$-subvarieties of $X$. We consider $\mathrm{H}^i(K|k, \Lambda(j))$ as a mixed Hodge structure of possibly *infinite rank.*

### 2. Basic Properties

The cohomology groups $\mathrm{H}^i(K|k, \Lambda(j))$, defined above, behave very similarly to the Galois cohomology of the field $K$, albeit with a more *refined* structure that disappears in profinite settings. Many of the basic properties outlined below can be summarized by saying that generic cohomology forms a *cycle module* in the sense of Rost [8]. For a detailed proof of this fact, which works in great generality, we refer the reader to the work of Déglise [4].

2.1. **Functoriality.** Given a $k$-embedding of function fields $L \hookrightarrow K$, one obtains a canonical *restriction map* $\mathrm{H}^i(L|k, \Lambda(j)) \to \mathrm{H}^i(K|k, \Lambda(j))$. This morphism is compatible with the mixed Hodge structure, and, in the obvious sense, with all of the additional structure mentioned below.

2.2. **Cohomological Dimension.** If $K$ has transcendence degree $d$, then one has $\mathrm{H}^i(K|k, \Lambda(j)) = 0$ for all $i > d$. This follows from the classical Andreotti-Frankel Theorem [1].

2.3. **Cup-products.** One has a canonical cup product

$$\mathrm{H}^i(K|k, \Lambda(j)) \otimes_\Lambda \mathrm{H}^{i'}(K|k, \Lambda(j')) \to \mathrm{H}^{i+i'}(K|k, \Lambda(j+j')).$$

This makes $\mathrm{H}^*(K|k, \Lambda(*)) := \bigoplus_i \mathrm{H}^i(K|k, \Lambda(i))$ into a graded-commutative $\Lambda$-algebra, where $\Lambda$ is identified with $\mathrm{H}^0(K|k, \Lambda)$.

2.4. **Kummer Theory.** One has a canonical *Kummer morphism*

$$\kappa : K^\times \to \mathrm{H}^1(K|k, \Lambda(1))$$

which is induced by the identification $\mathrm{H}^1(\mathbb{G}_m, \Lambda(1)) = \Lambda$. Indeed, if $f \in K^\times$ is given, then $f$ corresponds to a morphism

$$f : U \to \mathbb{G}_m$$

where $U$ is any sufficiently small Zariski open subset of the model $X$ of $K|k$. Then $\kappa(f)$ is defined as the pull-back of $1 \in \Lambda$ via the map

$$\Lambda = \mathrm{H}^1(\mathbb{G}_m, \Lambda(1)) \xrightarrow{f^*} \mathrm{H}^1(U, \Lambda(1)) \to \mathrm{H}^1(K|k, \Lambda(1)).$$

The Künneth formula shows that $\kappa$ is indeed a homomorphism.

2.5. **The Norm-Residue Morphism.** By taking cup-products of $\kappa$, one obtains a canonical morphism of graded $\Lambda$-algebras $\mathrm{T}_*(K^\times) \to \mathrm{H}^*(K|k, \Lambda(*))$. Here $\mathrm{T}_*(K^\times)$ denotes the tensor algebra of $K^\times$. Since $\mathrm{H}^2(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}, \Lambda(2)) = 0$, it follows that this morphism factors through the Milnor K-ring of $K$. In other words, we obtain a *norm-residue morphism* $\kappa^* : \mathrm{K}^{\mathrm{M}}_*(K) \to \mathrm{H}^*(K|k, \Lambda(*))$, which extends the Kummer morphism $\kappa = \kappa^1$.

2.6. **Residue Morphisms.** Let $v$ be a *divisorial valuation* of $K|k$, i.e. a valuation of $K$ which arises from a codimension 1 point on some normal model of $K|k$. To such a valuation $v$, one associates so-called *residue morphisms*

$$\partial_v : \mathrm{H}^{i+1}(K|k, \Lambda(j+1)) \to \mathrm{H}^i(Kv|k, \Lambda(j)),$$

where $Kv$ denotes the residue field of $v$. Such morphisms are compatible with the tame symbol in Milnor K-theory via the norm-residue morphisms.

## 3. An Anabelian Result

While the generic cohomology behaves similarly to Galois cohomology, it often comes equipped with additional structure that is closely tied to geometry. In the context of Betti cohomology with rational coefficients, which is endowed with a mixed Hodge structure, this additional structure provides enough additional information to recover the function field itself.

**Theorem 1** (See [9], Theorem A)**.** *Let $k$ be a subfield of $\mathbb{C}$, and let $K$ be a function field over $k$ of transcendence degree $\geq 2$. Then the isomorphism type of $K|k$ is determined by the following data:*

*(1)* $\mathrm{H}^1(K|k, \mathbb{Q}(1))$ *endowed with its mixed Hodge structure.*

*(2) The kernel of* $\cup : \mathrm{H}^1(K|k, \mathbb{Q}(1)) \otimes_\mathbb{Q} \mathrm{H}^1(K|k, \mathbb{Q}(1)) \to \mathrm{H}^2(K|k, \mathbb{Q}(2))$.

3.1. **Sketch of Proof.** The proof of Theorem 1 follows a strategy which is similar to *Bogomolov's programme* in birational anabelian geometry [3]. While Bogomolov's programme is far from being resolved in general, the additional information arising from the mixed Hodge structure of $\mathrm{H}^1(K|k, \mathbb{Q}(1))$ encodes enough additional information to carry through its strategy. In a few words, one reconstructs the function field $K|k$ using the following steps:

(1) $\mathrm{H}^1(K|k, \mathbb{Q}(1))$ contains $(K^\times/k^\times) \otimes_{\mathbb{Z}} \mathbb{Q}$ as a submodule, and the mixed Hodge structure on $\mathrm{H}^1$ is enough to pinpoint this submodule. This relies on the construction of the Hodge realization of a 1-motive, due to Deligne [5], and the calculation of this realization for a Picard 1-motive [2] [7].

(2) The cup-product in $\mathrm{H}^*(K|k, \mathbb{Q}(*))$, when restricted to this submodule, encodes all information about algebraic dependence in $K|k$.

(3) Using a rational analogue of the local theory in almost-abelian birational anabelian geometry, combining ideas from [3] and [6] along with step (2) above, one recovers information about all *divisorial valuations* of $K|k$.

(4) Again using the cup-product in $\mathrm{H}^*(K|k, \mathbb{Q}(*))$, one can determine the so-called *rational submodules* of $\mathrm{H}^1(K|k, \mathbb{Q}(1))$.

(5) One uses the information about divisorial valuations and the rational submodules of $\mathrm{H}^1(K|k, \mathbb{Q}(1))$ to recover $K^\times/k^\times$ (up-to multiplication by $\mathbb{Q}^\times$), considered as a subgroup of $(K^\times/k^\times) \otimes_{\mathbb{Z}} \mathbb{Q}$, along with all subsets of the form
$$\{(ax + by) \cdot k^\times \ : \ (a, b) \in k^2, \ (a, b) \neq (0, 0)\},$$
as $x, y$ vary over the pairs of $k$-linearly independent elements of $K$.

(6) Finally, noting that $K^\times/k^\times$ is the *projectivization* of $K$ as a $k$-vector space, one applies the *fundamental theorem of projective geometry* to recover $K$ as a $k$-module. The compatibility of this projective structure with the multiplicative structure of $K^\times/k^\times$ finally determines $K$ as a field.

## References

[1] A. Andreotti and T. Frankel, *The Lefschetz theorem on hyperplane sections*, Ann. of Math. (2) **69** (1959), 713–717.

[2] L. Barbieri-Viale and V. Srinivas, *Albanese and Picard 1-motives*, Mém. Soc. Math. Fr. **87** (2001), vi+104.

[3] F. Bogomolov, *On two conjectures in birational algebraic geometry*, Algebraic geometry and analytic geometry (Tokyo, 1990), 1991, 26-52.

[4] F. Déglise, *Motifs génériques*, Rend. Semin. Mat. Univ. Padova **119** (2008), 173–244.

[5] P. Deligne, *Théorie de Hodge III*, Publ. Math. Inst. Hautes Études Sci. **44** (1974), 5-77.

[6] F. Pop, *Pro-$\ell$ abelian-by-central Galois theory of prime divisors*, Israel J. Math. **180** (2010), 43-68.

[7] N. Ramachandran, *Duality of Albanese and Picard 1-motives*, K-theory **22** (2001), no. 3, 271-301.

[8] M. Rost, *Chow groups with coefficients*, Doc. Math **1(16)** (1996), 319-393.

[9] A. Topaz, *A Torelli theorem for higher-dimensional function fields*, Preprint (2017), arXiv:1705.01084.

## The local-global principle for rational points and a conjecture of Harpaz and Wittenberg

Damaris Schindler

The goal of this talk is to describe a conjecture of Harpaz and Wittenberg on split values of polynomials [11] which arose in studying local-global principles of rational points over number fields on nice varieties. We then discuss different analytic techniques with which the conjecture has been attacked so far and how the use of these techniques is related to a limitation of the ground field.

In the following let $k$ be a number field and $X$ a nice (i.e. smooth, projective, geometrically irreducible) variety over $k$. A very natural question is when $X$ possesses a $k$-rational point. A first observation is that if $X$ has a $k$-point then it possesses a point in every completion of $k$. Let $\Omega_k$ be the set of all (finite and infinite) places of the number field $k$ and write $k_\nu$ for the $\nu$-adic completion of $k$ for $\nu \in \Omega_k$. We write $\mathbb{A}_k$ for the adeles of $k$ and $X(\mathbb{A}_k)$ for the adelic points of $X$. Since we assumed $X$ to be projective, we have $X(\mathbb{A}_k) \cong \prod_{\nu\in\Omega_k} X(k_\nu)$. The observation above can then be formulated in the following way: if $X(k) \neq \emptyset$ then $X(\mathbb{A}_k) \neq \emptyset$, as $k$ embeds in each of its completions. An important observation is that the question whether $X(\mathbb{A}_k) \neq \emptyset$ can be decided within a finite amount of time and computations. This is one reason why it is a very interesting question when the existence of adelic points on $X$ is sufficient to deduce the existence of a $k$-rational point on $X$.

**Definition 1** (Hasse principle)**.** Let $\mathcal{F}$ be a family of smooth, projective, geometrically irreducible varieties over a number field $k$. We say that the Hasse principle holds for $\mathcal{F}$ if for all $X \in \mathcal{F}$ the property $X(\mathbb{A}_k) \neq \emptyset$ implies that $X(k) \neq \emptyset$.

Moreover, if there are rational points on $X$ one may ask how well a given adelic point in $X(\mathbb{A}_k)$ can be approximated by a $k$-rational point. This motivates the following definition.

**Definition 2** (Weak approximation)**.** Let $\mathcal{F}$ be as above. We say that the family $\mathcal{F}$ satisfies weak approximation if for every $X \in \mathcal{F}$ with $X(\mathbb{A}_k) \neq \emptyset$ the image of the diagonal embedding

$$X(k) \to X(\mathbb{A}_k),$$

is dense in the product topology.

**Examples 3.** *The following families of varieties satisfy both the Hasse principle and weak approximation:*

- *quadrics in any dimension (by the Hasse–Minkowski theorem)*
- *principal homogeneous spaces of semisimple simply connected linear algebraic groups (by work of Kneser, Harder and Tchernousov)*
- *homogenous spaces under commutative linear algebraic groups (by work of Harder)*
- *smooth hypersurfaces in $\mathbb{P}^n$ of small degree and for large $n$ (over the rational numbers by work of Birch)*

In general, both the Hasse principle and weak approximation can fail. In the following we just give two examples for illustrative purposes (and do not go into the much longer list of existing counter-examples and theory around them).

**Examples 4.**

a) *In 1957, Selmer showed that the projective curve given by*

$$3x^3 + 4y^3 + 5z^3 = 0$$

*has local points over every completion of* $\mathbb{Q}$ *but no* $\mathbb{Q}$*-rational point.*

b) *In 1966, Cassels and Guy observed that the cubic surface given by*

$$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$$

*violates the Hasse principle over the ground field* $k = \mathbb{Q}$.

In the 1970s, Manin observed that many of the then known examples and by now both of the examples named above can be explained in a uniform way. Let $\mathrm{Br}(X)$ be the cohomological Brauer group of $X$. Then there is a well-defined pairing

$$\mathrm{Br}(X) \times X(\mathbb{A}_k) \to \mathbb{Q}/\mathbb{Z}.$$

Let $X(\mathbb{A}_k)^{\mathrm{Br}}$ be the set of adelic points of $X$ that are orthogonal to the whole of $\mathrm{Br}(X)$ under this pairing. Manin observed that

$$X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k).$$

In the examples above it turns out that $X(\mathbb{A}_k)$ is non-empty but that $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ and hence that there cannot be any $k$-rational points on $X$. It is a very interesting question for what classes of varieties this is the only obstruction. Colliot-Thélène conjectured the following.

**Conjecture 5** (Colliot-Thélène [2])**.** *Let $X$ be a smooth, proper, geometrically irreducible and rationally connected variety over a number field $k$. Then $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$.*

One way to attack this conjecture is via some form of fibration method. The idea is that one considers a nice variety $X$ over a number field $k$ together with a dominant morphism $f : X \to \mathbb{P}^1_k$ with rationally connected generic fiber (which implies that $X$ is rationally connected). The goal is then to establish the following statement for a large class of such fibrations.

(A) If the smooth fibers of $f$ above rational points of $\mathbb{P}^1_k$ satisfy Conjecture 5, then $X$ satisfies Conjecture 5.

It turns out that part of the difficulty of establishing (A) can be measured by the rank of the fibration $f$, which can be viewed as measuring its number of 'bad' fibers. By a definition of Skorobogatov, a variety $Y$ over $k$ is called split if it contains a geometrically integral open subset. For example the 0-dimensional subscheme in $\mathbb{P}^1_{\mathbb{Q}}$ given by $x^2 - y^2 = 0$ is split whereas the scheme given by $x^2 + y^2 = 0$ is not split (both considered over $\mathbb{Q}$).

Define the rank of the fibration $f$ as the sum of the degrees of closed points $m$ of $\mathbb{P}^1_k$ where the fiber $X_m$ is not split. Then it is for example known that (A) holds for fibrations $f$ with $\mathrm{rank}(f) = 1$ by work of Harari [9], [10] and for fibrations with $\mathrm{rank}(f) = 2$ and such that the fibers satisfy weak approximation by work of Colliot-Thélène and Skorobogatov [4]. In their seminal work [11] Harpaz and Wittenberg established the statement (A) under the assumption of the following conjecture on split values of polynomials.

**Conjecture 6** (Harpaz and Wittenberg)**.** *Let $k$ be a number field and $n \geq 1$. Let $P_1(t), \ldots, P_n(t) \in k[t]$ be pairwise distinct, irreducible, monic polynomials and let $k_i = k[t]/(P_i(t))$ for $1 \leq i \leq n$. Write $a_i \in k_i$ for the class of $t$ in $k_i$. Consider finite Galois extensions $L_i/k_i$ and $b_i \in k_i^*$ for all $1 \leq i \leq n$. Let $S$ be a finite set of places of $k$ that contains all real places of $k$, all places above which one of the $b_i$ is not a unit or the extension $L_i/k_i$ is ramified for some $1 \leq i \leq n$. For each $\nu \in S$ fix some element $t_\nu \in k_\nu$. Assume that for all $1 \leq i \leq n$ and $\nu \in S$ there exists an element $x_{i,\nu} \in (L_i \otimes_k k_\nu)^*$ such that*

$$b_i(t_\nu - a_i) = N_{L_i \otimes_k k_\nu / k_i \otimes_k k_\nu}(x_{i,\nu})$$

*in $k_i \otimes_k k_\nu$. Let $\epsilon > 0$. Then there exists a $t_0 \in k$ such that*

*(1) $|t_0 - t_\nu|_\nu < \epsilon$ in the $\nu$-adic metric for all $\nu \in S$, and*

*(2) If $\nu(P_i(t_0)) > 0$ for some $1 \leq i \leq n$ and some $\nu \notin S$, then $\nu$ splits completely in $L_i$.*

**Remarks 7.**

*a) Harpaz and Wittenberg show that in order to establish (A) for a given fibration $f : X \to \mathbb{P}^1$, one needs to assume Conjecture 6 for polynomials $P_i(t)$ such that the union of the zeros of these polynomials contains all non-split fibers of $f$.*

*b) In conjunction with Conjecture 6, it is enough to assume in statement (A) that the smooth fibers above the closed points of a Hilbert subset satisfy Conjecture 5 (see Theorem 1.3 in* [11]*).*

Conjecture 6 can be seen as a replacement of Schinzel's hypothesis that has previously been applied in fibration theorems of a similar kind. We formulate it here over the rational integers.

**Conjecture 8** (Schinzel's hypothesis)**.** *Let $P_1(t), \ldots, P_n(t) \in \mathbb{Z}[t]$ be irreducible polynomials with positive leading coefficients such that the product $\prod_{i=1}^n P_i(t)$ has no fixed prime divisor for $t$ ranging over the integers (i.e. for every prime $p$ there exists a value $t \in \mathbb{Z}$ such that $p$ does not divide $\prod_{i=1}^n P_i(t)$). Then there are infinitely many values of $t \in \mathbb{Z}$ such that $P_i(t)$ are prime for every $1 \leq i \leq n$.*

In [11], Harpaz and Wittenberg show that the general number field version of Schinzel's hypothesis implies Conjecture 6 for the case that all the field extensions $L_i/k_i$, $1 \leq i \leq n$, are abelian (or more generally almost abelian).

Note that Schinzel's hypothesis is extremely difficult. For example, it includes the twin prime conjecture if we take $n = 2$, $P_1(t) = t$ and $P_2(t) = t + 2$. For $n = 1$

and $P_1(t)$ a linear polynomial it reduces to finding prime numbers in arithmetic progressions which is well understood by Dirichlet's theorem. However, it is for example not known if the quadratic polynomial $t^2 + 1$ takes on infinitely many prime values.

The conjecture of Harpaz and Wittenberg does not only allow one to work in the fibration method with not necessarily abelian field extensions $L_i/k$, but also seems much more accessible than Schinzel's hypothesis. In the following we name a couple of cases where progress has been made.

**Theorem 9** (Matthiesen [15]). *Conjecture 6 holds for $k = k_1 = \ldots = k_n = \mathbb{Q}$ and arbitrary $n \in \mathbb{N}$.*

The proof of this result builds on a geometric criterion for Conjecture 6 that can be found in Corollary 9.10 in [11]. Let $W \subset \mathbb{A}^2 \times \prod_{i=1}^n R_{L_i/\mathbb{Q}}(\mathbb{A}^1_{L_i})$ be given as the complement of the affine variety

$$N_{L_i/\mathbb{Q}}(\mathbf{x}^{(i)}) = b_i(\lambda - a_i\mu), \quad 1 \leq i \leq n, \quad (\lambda, \mu) \neq (0,0)$$

minus the union of closed subvarieties given by the vanishing of two of the linear factors defining $N_{L_i/\mathbb{Q}}(\mathbf{x}^{(i)})$ for some $1 \leq i \leq n$.

Corollary 9.10 in [11] implies that if $W$ satisfies strong approximation off a finite place $\nu_0$ for all Galois extensions $L_i/\mathbb{Q}$, $a_i \in \mathbb{Q}, b_i \in \mathbb{Q}^*$ (and all the $a_i$ pairwise different), then Conjecture 6 holds for $k = k_1 = \ldots = k_n = \mathbb{Q}$.

The basic strategy to establish strong approximation for $W$ off a finite place $\nu_0$ consists of finding integral solutions to the system of equations defining $W$ and such that the values $b_i(\lambda - a_i\mu)$ are all square-free outside of a finite set of places, together with some congruence conditions at a finite set of places which we omit for a moment. After a process of homogenization, assume that one is given a system of linear forms $l_i(\lambda, \mu) \in \mathbb{Z}[\lambda, \mu]$, $1 \leq i \leq n$, such that no two are linearly dependent. In essence the problem can then be reduced to studying the following counting function. Let $\mathcal{C}$ be a convex domain in $\mathbb{R}^2$ and $B \in \mathbb{R}$ a large real parameter and write $B\mathcal{C} = \{Bv, v \in \mathcal{C}\}$. For $n \in \mathbb{Z}$, let $R_i(n)$ be the representation function of $n$ by an integral norm $n = N_{L_i/\mathbb{Q}}(\mathbf{x})$, with $\mathbf{x} \in \mathcal{O}_{L_i}$ in a fundamental domain of $\mathcal{O}_K$ modulo the positive unit action. Consider the counting function

$$\sum_{(\lambda,\mu)\in\mathbb{Z}^2\cap B\mathcal{C}} \prod_{i=1}^n R_i(l_i(\lambda, \mu))\mu^2(l_i(\lambda, \mu)).$$

Here, $\mu$ is the Möbius function and hence these factors test each of the linear forms $l_i(\lambda, \mu)$ for being square-free.

Matthiesen's work [15] is inspired by work of Green, Tao and Ziegler on linear correlations of the von Mangoldt function $\Lambda(\cdot)$, see in particular [6], [7] and [8]. A related counting function that prominently features in the work of Green, Tao and Ziegler (here we only need the case of linear forms in two variables) is given by

$$\sum_{(\lambda,\mu)\in\mathbb{Z}^2\cap B\mathcal{C}} \prod_{i=1}^n \Lambda(l_i(\lambda, \mu)).$$

As a special case, one could for example consider the $n$ linear forms $l_i(\lambda, \mu) = \lambda + (i-1)\mu$ and then end up with the problem of detecting $n$-term progressions in the primes (after removing the contribution from higher prime powers). The work of Green, Tao and Ziegler is mainly developed over the rational integers $\mathbb{Z}$. However there are some extensions to the Gaussian integers $\mathbb{Z}[i]$ by Tao [18] (and even analogues over function fields [14]).

As a corollary of the work of Matthiesen [15], Harpaz and Wittenberg deduce statement (A) (see Theorem 1.6 in [11]) for fibrations $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ over the field of rational numbers $\mathbb{Q}$ for the case that all non-split fibers lie over rational points of $\mathbb{P}^1_{\mathbb{Q}}$. Here the restriction to the ground field $\mathbb{Q}$ is due to the use of the above described machinery that is currently only available over the rational numbers.

Other techniques with which one can attack Conjecture 6 include the circle method and sieve methods. For example, in the case $n = 3$ the variety $W$ has been considered in work of Swarbrick–Jones [17] and Schindler–Skorobogatov [16] over an arbitrary number field $k$, both building on earlier work Heath-Brown and Skorobogatov [12] and Colliot-Thélène, Harari and Skorobogarov [3]. (Note however that the paper [16] mainly focuses on cases where the base $\mathbb{P}^1_k$ would be replaced by some higher-dimensional $\mathbb{P}^m_k$). In these articles the auxiliary variety $W$ appears after applying the descent method to the variety $\mathcal{V}$ given by

$$0 \neq P(t) = N_{L/k}(\mathbf{x}),$$

where $P(t) \in k[t]$ is a quadratic polynomial that splits over $k$ and $L/k$ is a finite field extension (for a quadratic polynomial that is not-split see work of Derenthal, Smeets and Wei [5]). The authors establish that the Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation for any smooth projective model of $\mathcal{V}$. For this they establish weak approximation for the auxiliary variety $W$ in the case $n = 3$. There do not seem to be any obstacles in extending these results to establishing strong approximation off a finite place $\nu_0$ over any number field in the case $n = 3$.

There is only very little known about Conjecture 6 for cases where not all polynomials are linear. One result that has been established over $k = \mathbb{Q}$ using sieve methods is the following.

**Theorem 10** (Browning-Schindler [1]). *Conjecture 6 holds for $n = 2$, $k = k_1 = \mathbb{Q}$ and $k_2$ a quadratic extension of $\mathbb{Q}$.*

I.e. this theorem corresponds to one quadratic and one linear polynomial in Conjecture 6. The strategy is again to establish strong approximation for an auxiliary variety that is provided through the work of Harpaz and Wittenberg.

Note that Irving [13] established some cases of Conjecture 6 for one linear and one cubic polynomial where $k = \mathbb{Q}$ and the field extensions $L_i$ are restricted to be of a special form.

## References

[1] Browning, T. D. and Schindler, D., *Strong Approximation and a Conjecture of Harpaz and Wittenberg*, IMRN, to appear, DOI: 10.1093/imrn/rnx252

[2] Colliot-Thélène, J-L., *Points rationnels sur les fibrations*, Higher dimensional varieties and rational points (Budapest, 2001), Bolyai Soc. Math. Stud., vol. 12, Springer, Berlin, 2003, pp. 171–221.

[3] Colliot-Thélène, J-L. and Harari, D. and Skorobogatov, A. N., *Valeurs d'un polynome à une variable représentées par une norme*, Number theory and algebraic geometry, 69–89, London Math. Soc. Lecture Note Ser., 303, Cambridge Univ. Press, Cambridge, 2003.

[4] Colliot-Thélène, J-L. and Skorobogatov, A. N., *Descent on fibrations over $\mathbb{P}^1_k$ revisited*, Math. Proc. Cambridge Philos. Soc. 128 (2000), no. 3, 383–393.

[5] Derenthal, U. and Smeets, A. and Wei, D., *Universal torsors and values of quadratic polynomials represented by norms*, Math. Ann. 361 (2015), no. 3-4, 1021–1042.

[6] Green, B. and Tao, T., *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) 167 (2008), no. 2, 481–547.

[7] Green, B. and Tao, T., *Linear equations in primes*, Ann. of Math. (2) 171 (2010), no. 3, 1753–1850.

[8] Green, B, and Tao, T. and Ziegler, T., *An inverse theorem for the Gowers $U^{s+1}[N]$-norm*, Ann. of Math. (2) 176 (2012), no. 2, 1231–1372.

[9] Harari, D., *Méthode des fibrations et obstruction de Manin*, Duke Math. J. 75 (1994), no. 1, 221–260.

[10] Harari, D., *Flèches de spécialisations en cohomologie étale et applications arithmétiques*, Bull. Soc. Math. France 125 (1997), no. 2, 143–166.

[11] Y. Harpaz and O. Wittenberg, *On the fibration method for zero-cycles and rational points*, Ann. of Math. (2) 183 (2016), no. 1, 229–295.

[12] Heath-Brown, R. and Skorobogatov, A. N., *Rational solutions of certain equations involving norms*, Acta Math. 189 (2002), no. 2, 161–177.

[13] Irving, A. J., *Cubic polynomials represented by norm forms*, J. Reine Angew. Math. 723 (2017), 217–250.

[14] Le, T. H., *Green–Tao theorem in function fields*, Acta Arith. 147 (2011), no. 2, 129–152.

[15] Matthiesen, L., *On the square-free representation function of a norm form and nilsequences*, J. Inst. Math. Jussieu 17 (2018), no. 1, 107–135.

[16] Schindler, D. and Skorobogatov, A. N., *Norms as products of linear polynomials*, J. Lond. Math. Soc. (2) 89 (2014), no. 2, 559–580.

[17] Swarbrick Jones, M., *A note on a theorem of Heath-Brown and Skorobogatov*, Q. J. Math. 64 (2013), no. 4, 1239–1251.

[18] Tao, T., *The Gaussian primes contain arbitrarily shaped constellations*, J. Anal. Math. 99 (2006), 109–176.

## Generalized densities of primes and realization of local extensions

Alexander B. Ivanov

In this talk we address the question of generalizing the Dirichlet density on the set of primes of a number field. The results explained here can be found in [Iv2]. We introduce new densities on the set of primes which give an appropriate positive measure to sets of primes with Dirichlet density zero. The original application for which these densities were introduced, is Theorem 1 below. It is about the realization (in the style of the Grunwald–Wang theorem) of local extensions by global ones satisfying certain conditions. A further application (to saturated sets introduced by Wingberg in [Wi]) is discussed in Section 5 of [Iv2].

To begin with, let $K/K_0$ be a finite Galois extension of number fields, i.e., of finite extensions of $\mathbb{Q}$. Let $x \in \mathrm{Gal}_{K/K_0}$ be of order $d$. Let $P^x_{K/K_0}$ denote the set of all primes $\mathfrak{p}$ of $K$ which are unramified in $K/K_0$ and satisfy $\mathrm{Frob}_{\mathfrak{p},K/K_0} = x$. Note that if $x \neq 1$, then $P^x_{K/K_0}$ has Dirichlet density 0. One can then define a density $\delta_{K/K_0,x}$ of a set $S$ of primes of $K$, which measures how big the ratio of the sizes of $S \cap P^x_{K/K_0}$ and $P^x_{K/K_0}$ is. This is done in the same way as for Dirichlet density, with the only difference that one has to take the limit over the ratio of terms of the kind $\sum_{\mathfrak{p}\in *} \mathrm{N}\mathfrak{p}^{-s}$ not over $s \to 1$ but over $s \to d^{-1}$ with $s$ lying in the right half plane $\Re(s) > d^{-1}$. The point is that $\sum_{\mathfrak{p}\in P^x_{K/K_0}} \mathrm{N}\mathfrak{p}^{-s} \to +\infty$ for $s \to d^{-1}$. The so defined density $\delta_{K/K_0,x}$ is essentially independent of the base field $K_0$, so one also could replace $K_0$ once for all time by $\mathbb{Q}$, but it is easier to work with a Galois extension $K/K_0$.

Once introduced, the most interesting thing about such a density is its base change behavior. To explain it, let $L/K$ be an extension such that $L/K_0$ is Galois. Write $H := \mathrm{Gal}_{L/K} \lhd \mathrm{Gal}_{L/K_0} =: G$ and $\pi\colon G \twoheadrightarrow G/H$ for the natural projection. For any $y \in \pi^{-1}(x)$ we have the map induced by restriction of primes $P^y_{L/K_0} \to P^x_{K/K_0}$. It is in general neither injective nor surjective. For $y, z \in \pi^{-1}(x)$ one easily sees that the images of the corresponding maps are either equal or disjoint and that the former is equivalent to $y, z$ being $H$-conjugate. If $C$ is an $H$-conjugacy class in $\pi^{-1}(x)$, let $M_C$ denote the image of $P^y_{L/K_0}$ for some (any) $y \in C$ in $P^x_{K/K_0}$. The following results generalize Chebotarev's density theorem and give a description of the base change behavior of $\delta_{K/K_0,x}$.

**Proposition.** *Let $L/K/K_0, \pi, x$ be as above. Let $C$ be an $H$-conjugacy class in $\pi^{-1}(x)$. Then*

$$\delta_{K/K_0,x}(M_C) = \frac{\sharp C}{\sharp H}.$$

**Corollary.** *Let $y \in \pi^{-1}(x)$ and let $C$ be its $H$-conjugacy class in $\pi^{-1}(x)$. Then*

$$\delta_{L/K_0,y}(S_L) = \frac{\sharp H}{\sharp C}\delta_{K/K_0,x}(S \cap M_C)$$

*if both densities exist.*

**Application to realizing local extensions.** First we fix some notations. Let $\mathfrak{c}$ be a full class of finite groups (in the sense of [NSW] 3.5.2). Let $R \subseteq S$ be two sets of primes of a number field $K$. Then $K^R_S(\mathfrak{c})$ denotes the maximal pro-$\mathfrak{c}$-extension of $K$ which is unramified outside $S$ and completely split in $R$. Moreover, for a prime $\mathfrak{p}$ of $K$ we denote by $K_\mathfrak{p}(\mathfrak{c})$ the completion of the maximal pro-$\mathfrak{c}$-extension of $K_\mathfrak{p}$ and by $K^{nr}_\mathfrak{p}$ the completion of the maximal unramified extension of $K_\mathfrak{p}$. Let $\delta_K$ denote the usual Dirichlet density on primes of $K$. For two sets $S, T$ of primes of $K$ we write $S \overset{\supset}{\sim} T$ if $S$ contains $T$ up to subset of Dirichlet density 0. For a finite Galois extension $M/K$ and $\sigma \in \mathrm{Gal}_{M/K}$ let $P_{M/K}(\sigma)$ denote the set of primes of $K$ unramified in $M/K$ and whose Frobenius class is the conjugacy class of $\sigma$ in $\mathrm{Gal}_{M/K}$.

For $\ell$ a rational prime or $\infty$, let $\mathfrak{c}_{\leq \ell}$ denote the smallest full class of all finite groups, containing the groups $\mathbb{Z}/p\mathbb{Z}$ for all $p \leq \ell$. The following theorem is a generalization of [NSW] 9.4.3, which handles the case of $\delta_K(S) = 1$.

**Theorem 1.** *Let $K$ be a number field, $S \supseteq R$ sets of primes of $K$, such that $R$ is finite and $S \overset{\supset}{\sim} P_{M/K}(\sigma)$ for some finite extension $M/K$ and $\sigma \in \mathrm{Gal}_{M/K}$. For any $\ell \leq \infty$ and any prime $\mathfrak{p}$ of $K$ we have:*

$$(K_S^R(\mathfrak{c}_{\leq \ell}))_{\mathfrak{p}} = \begin{cases} K_{\mathfrak{p}}(\mathfrak{c}_{\leq \ell}) & \textit{if } \mathfrak{p} \in S \smallsetminus R \\ K_{\mathfrak{p}}(\mathfrak{c}_{\leq \ell}) \cap K_{\mathfrak{p}}^{nr} & \textit{if } \mathfrak{p} \notin S \\ K_{\mathfrak{p}} & \textit{if } \mathfrak{p} \in R. \end{cases}$$

*In particular, since absolute Galois groups of local fields are solvable, taking $\ell = \infty$ shows that the maximal solvable subextension of $K_S^R/K$ lies dense in $\overline{K_{\mathfrak{p}}}$ resp. in $K_{\mathfrak{p}}^{nr}$ for $\mathfrak{p} \in S \smallsetminus R$ resp. $\mathfrak{p} \notin S$.*

One part of the proof of Theorem 1, namely to realize a $p$-extension with given local properties, when $S$ satisfies a certain property $(\dagger)_p$ introduced in [Iv], was done in [Iv]. Essentially, $(\dagger)_p$ means that $S$ contains many primes $\mathfrak{p}$, which are completely split in $K(\mu_p)/K$. The remaining and much more delicate case is when $\delta_{K(\mu_p)}(S_{K(\mu_p)}) = 0$ holds. Then the usual methods from [NSW] and [Iv] do not apply anymore. Moreover, in such a case the pro-$p$-version of the theorem easily can fail. For example, suppose that $\mu_p \not\subseteq K$ and $K(\mu_p)/K$ is totally ramified at each $p$-adic prime, let $1 \neq \sigma \in \mathrm{Gal}_{K(\mu_p)/K}$ and set $S := P_{K(\mu_p)/K}(\sigma)$. Then any prime $\mathfrak{p} \in S$ is unramified in $K_S(p)/K$, as $\mathfrak{p} \notin S_p$ and $\mu_p \not\subseteq K_{\mathfrak{p}}$. Hence $K_S(p) = K_\emptyset(p)$. In particular, let $K = \mathbb{Q}$ and $p$ odd. Then $\mathbb{Q}_S(p) = \mathbb{Q}_\emptyset(p) = \mathbb{Q}$, i.e., the maximal possible local $p$-extension is realized nowhere.

However, in the pro-$\mathfrak{c}_{\leq \ell}$-case the theorem holds. For example take in the above example $\ell = 3$. The set $S := P_{\mathbb{Q}(\mu_3)/\mathbb{Q}}(\sigma)$ satisfies $(\dagger)_p$ for all $p \neq 3$, and in particular $(\dagger)_2$. Hence at any $\mathfrak{p} \in S$ the maximal pro-2-extension can be realized, and hence $\mu_3 \subseteq \mathbb{Q}_{S,\mathfrak{p}}$. After going up to an appropriate finite subextension $\mathbb{Q}_S(\mathfrak{c}_{\leq 2})/K/\mathbb{Q}$, the set $P_{\mathbb{Q}(\mu_3)/\mathbb{Q}}(\sigma)_K \cap \mathrm{cs}(K(\mu_3)/K)$ would at least be infinite and not more empty as for $K = \mathbb{Q}$. The main obstruction now is that this set has Dirichlet density 0, and no one of the usual arguments involving Dirichlet density will apply. To overcome this difficulty we use the generalized densities introduced above. Namely, it turns out that certain $x$-density of this set is positive and then one again can apply some density arguments. However, these arguments are in our situation much more subtle than in the situations where one can use Dirichlet density.

Finally, we remark that there are several other appraoches to realization results of similar spirit. As to our knowledge, no one of them covers Theorem 1, and in particular those cases, where one tries to realize $p$-extensions with ramification allowed only outside $\mathrm{cs}(K(\mu_p/K))$. We mention two recent approaches: a certain pro-$p$ version of the theorem above is also known (only for primes in $S$) in the much harder situation of a finite set $S$ by the work of A. Schmidt (cf. e.g. [Sch]) but only after enlarging $S$ by an appropriate finite subset of a fixed set $T$ of primes of density 1 (which, in particular, satisfies $(\dagger)_p$). A further, completely different and very powerful approach using automorphic forms, which deals with the whole pro-finite group and a finite set $S$, was introduced by Chenevier and Clozel [Ch], [CC]. However, compared to results of this paper, the drawback is that one has to forget about solvability conditions and to assume $R = \emptyset$ (no control of the unramified extensions) and that at least one rational prime must lie in $\mathcal{O}^*_{K,S}$.

## References

[CC] Chenevier G., Clozel L.: *Corps de nombres peu ramifiés et formes automorphes autoduales*, J. of the AMS, vol. 22, no. 2, 2009, p. 467-519.

[Ch] Chenervier G.: *On number fields with given ramification*, Comp. Math. 143 (2007), no. 6, 1359-1373.

[Iv] Ivanov A.: *Stable sets of primes in number fields*, Algebra & Number Theory **10** (2016), No. 1, pp. 1-36.

[Iv2] Ivanov A.: *Densities of primes and realization of local extensions*, Trans. Amer. Math. Soc., electronically published on April 25, 2018, DOI: https://doi.org/10.1090/tran/7449 (to appear in print).

[NSW] Neukirch J., Schmidt A., Wingberg K.: *Cohomology of number fields*, Springer, 2008, second edition.

[Sch] Schmidt A.: *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine u. angew. Math. **640** (2010) 203-235.

[Wi] Wingberg K.: *Sets of completely decomposed primes in extensions of number fields*, preprint, Heidelberg 2013.

## Profinite Cohomology and the Combinatorics of Words

Ido Efrat

We fix a prime number $p$. For a profinite group $G$ let $H^i(G) = H^i(G, \mathbb{Z}/p)$. The *lower p-central filtration* $G^{(i)} = G^{(i,p)}$ of $G$ is defined inductively by $G^{(1)} = G$ and $G^{(i+1)} = (G^{(i)})^p[G, G^{(i)}]$. Given integers $1 \leq s \leq n$, $n \geq 2$, let $\mathbb{U} = \mathbb{U}_{n,s}$ be the group of all unipotent upper-triangular $(s+1) \times (s+1)$-matrices over the ring $R = \mathbb{Z}/p^{n-s+1}$. There is a central extension

$$0 \to \mathbb{Z}/p \to \mathbb{U} \to \mathbb{U}/\mathbb{U}^{(n)} \to 1$$

corresponding to an element $\gamma_{n,s}$ of $H^2(\mathbb{U}/\mathbb{U}^{(n)})$.

Given a profinite group $G$ and a continuous homomorphism $\rho\colon G \to \mathbb{U}/\mathbb{U}^{(n)}$, we consider the pullback $\rho^*\gamma_{n,s} \in H^2(G)$.

**Examples.**

- *When $n = s \geq 2$ these are the elements of the n-fold Massey product $\langle \mathrm{pr}_{12} \circ \rho, \dots, \mathrm{pr}_{n,n+1} \circ \rho \rangle$. In particular, when $n = s = 2$ we recover the cup product.*
- *For $s = 1$ these are the Bockstein elements* $\mathrm{Bock}(\rho)$ *corresponding to the short exact sequence $0 \to \mathbb{Z}/p \to \mathbb{Z}/p^n \to \mathbb{Z}/p^{n-1} \to 0$.*

The full spectrum of the "external" cohomology elements $\rho^*\gamma_{n,s}$ seem fundamental to the understanding of $H^2(G)$. We considered two cases:

## 1. The generic case

Here $G = S/S^{(n)}$ for a free pro-$p$ group $S$ on a totally ordered basis $X$ (finite for simplicity). Let $X^*$ be the monoid of words in the alphabet $X$. A word $\emptyset \neq w \in X^*$ is called a *Lyndon word* if it is lexicographically smaller than all its proper suffixes. The set of all Lyndon words in $X^*$ forms a Hall family. The (pro-$p$) *Magnus homomorphism*

$$\Lambda\colon S \to R\langle\langle X\rangle\rangle^\times, \quad \sigma \mapsto \sum_{w\in X^*} \epsilon_w(\sigma)w,$$

is defined by $x \mapsto 1+x$ for $x \in X$ (Here $R\langle\langle X\rangle\rangle$ is the $R$-algebra of formal power series in the set of non-commuting variables $X$ and with coefficients in $R$).

Next, for a word $w = (x_1 \cdots x_s) \in X^*$ of length $1 \leq s \leq n$, we define a continuous homomorphism

$$\hat{\rho}_w\colon S \to \mathbb{U}, \quad \hat{\rho}_w(\sigma) = (\epsilon_{(x_i\cdots x_{j-1})}(\sigma))_{1\leq i\leq j\leq s+1},$$

and let $\rho_w\colon S/S^{(n)} \to \mathbb{U}/\mathbb{U}^{(n)}$ be the induced homomorphism. Finally, for a Lyndon word $w$, one defines $\tau_w \in S$ inductively, by $\tau_{(x)} = x$ and $\tau_w = [\tau_{w_1}, \tau_{w_2}]$ if $s \geq 2$ and $w$ has the standard decomposition $w = w_1w_2$ (in the sense of Hall families). We have the following duality:

**Theorem 1** ([1]).

*(a) The cosets of $\tau_w^{p^{n-s}}$, where $w$ ranges over all Lyndon words of length $1 \leq s \leq n$, form a linear basis of $S^{(n)}/S^{(n+1)}$.*

*(b) The cohomology elements $\rho_w^*\gamma_{n,s}$, where $w$ ranges over all Lyndon words of length $1 \leq s \leq n$, form a linear basis of $H^2(S/S^{(n)})$.*

*(c) The above linear bases are semi-dual with respect to the canonical pairing*

$$(\cdot,\cdot)\colon S^{(n)}/S^{(n+1)} \times H^2(S/S^{(n)}) \to \mathbb{Z}/p,$$

*(i.e. the matrix $(\tau_w^{p^{n-s}}, \rho_{w'}^*\gamma_{n,s'})_{w,w'}$ is uni-triangular).*

For $n = 2$ this was proved by Labute (following an earlier work of Serre) in the 1960's.

The external cohomology elements $\rho^*\gamma_{n,s}$ give the following formal description of $H^2(S/S^{(n)})$. For this let $(\mathrm{Sh}(X), ш)$ be the shuffle (graded) $\mathbb{Z}$-algebra over $X$, and let $\mathrm{Sh}(X)_{\mathrm{indec}}$ be its quotient by the submodule $\langle u \,ш\, v \mid \emptyset \neq u, v \in X^*\rangle$.

**Theorem 2.** *For $n < p$ there is an isomorphism*

$$\Big(\bigoplus_{s=1}^{n} \mathrm{Sh}(X)_{\mathrm{indec},s}\Big) \otimes (\mathbb{Z}/p) \xrightarrow{\sim} H^2(S/S^{(n)}), \quad \bar{w} \otimes 1 \mapsto \rho_w^*\gamma_{n,s}.$$

The proofs of Theorems 1 and 2 use tools from the *Combinatorics of Words*, such as the triangulation property for Lyndon words, the Radford basis of the free associative algebra $\mathbb{Z}\langle X\rangle$, and results of Chen–Fox–Lyndon relating the Magnus homomorphism to the shuffle product.

## 2. The Galois case

Suppose that $F$ is a field containing a root of unity of order $p$, and let $G$ be its absolute Galois group $G_F$ (alternatively, its maximal pro-$p$ Galois group $G_F(p)$). By the Merkurjev–Suslin theorem, every element of $H^2(G)$ decomposes as a sum of cup products of Kummer elements $(a)_F \in H^1(G)$, where $a \in F^\times$.

**Question:** For a continuous homomorphism $\rho\colon G \to \mathbb{U}/\mathbb{U}^{(n)}$, what is the decomposition of $\rho^*\gamma_{n,s} \in H^2(G)$ as a sum of cup products?

The following decompositions are known:

- $n = s = 2$: Here $\rho^*\gamma_{2,2} = (\mathrm{pr}_{12} \circ \rho) \cup (\mathrm{pr}_{23} \circ \rho)$.
- $n = 2$, $s = 1$: Here $\rho^*\gamma_{2,1} = (\mathrm{pr}_{12} \circ \rho) \cup (\zeta_p)_F$ for some $p$-th root of unity (E–Mináč).
- $n = s = 3$: Here $\rho^*\gamma_{3,3} = (\mathrm{pr}_{12} \circ \rho) \cup \psi_1 + (\mathrm{pr}_{34} \circ \rho) \cup \psi_2$ for some $\psi_1, \psi_2 \in H^1(G)$. Indeed, this is a restatement of the fact that 3-fold Massey products for absolute Galois groups are non-essential (E–Matzri [2], Mináč–Tân [3]) .

## References

[1] I. Efrat, *The cohomology of canonical quotients of free groups and Lyndon words*, Documenta Math. **22** (2017), 973–997.

[2] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. European Math. Soc. (JEMS) **19** (2017), 3629–3640.

[3] J. Mináč and N.D. Tân, *Triple Massey products vanish over all fields*, J. London Math. Soc. **94** (2016), 909–932.

# Reconstructing function fields from Milnor K-theory

Anna Cadoret

(joint work with Alena Pirutka)

## 1. Introduction

This work is motivated by the following general question, for which no counterexample seems to be known.

**Question 1.** Does the Milnor K-ring $K_*^M(F)$ determine the isomorphism class of the field $F$?

One may also ask whether or not the above holds in a functorial way, that is, whether or not the Milnor K-ring functor is fully faithful from the groupoid of fields to the groupoid of $\mathbb{Z}_{\geq 0}$-graded rings.

Since $K_1^M(F) = F^\times$, Question 1 essentially reduces to reconstructing the additive structure of $F$ from the multiplicative group $F^\times$ endowed with additional data that can be detected by the Milnor K-ring. Our main result (Theorem 1) asserts that for a finitely generated regular field extension $F$ of transcendence degree $\geq 2$ over a perfect field $k$, the multiplicative group $F^\times/k^\times$ endowed with the equivalence relation induced by algebraic dependence on $k$ determines the isomorphism class of $F$ in a functorial way. We also show that for a finitely generated regular field extension of a field $k$ which is either algebraically closed or finite, the Milnor K-ring detects algebraic dependence. This is a consequence of deep K-theoretic results – the $n = 2$ case of the Bloch–Kato conjecture [MS82] when $k$ is algebraically closed and the Bass-Tate conjecture [T71] when $k$ is finite. Combined with Theorem 1, this enables us show that the Milnor K-ring modulo the ideal of divisible elements (resp. of torsion elements) determines in a functorial way finitely generated regular field extensions of transcendence degree $\geq 2$ over algebraically closed fields (resp. over finite fields).

## 2. Main Result

**2.1.** Recall that a field extension $F/k$ is *regular* if $k$ is algebraically closed in $F$. Let $F/k$ be a regular field extension. We say that $\overline{x}, \overline{y} \in F^\times/k^\times$ are *algebraically dependent* and write $\overline{x} \equiv \overline{y}$ if either $\overline{x} = \overline{y} = 1$ or $1 \neq \overline{x}, \overline{y}$ and some (equivalently, all) lifts $x, y \in F^\times$ of $\overline{x}, \overline{y} \in F^\times/k^\times$ are algebraically dependent over $k$. The relation $\equiv$ is an equivalence relation on $F^\times/k^\times$.

**2.2.** Let $F/k$ and $F'/k'$ be regular field extensions. We say that a group morphism $\overline{\psi} : F^\times/k^\times \to F'^\times/k'^\times$ *preserves algebraic dependence* if for every $\overline{x}, \overline{y} \in F^\times/k^\times$ the following holds: $\overline{x} \equiv \overline{y}$ if and only if $\overline{\psi}(\overline{x}) \equiv \overline{\psi}(\overline{y})$.

**2.3.** Let $\mathrm{Isom}(F, F')$ denote the set of field isomorphisms $F \tilde{\to} F'$ and

$$\mathrm{Isom}(F/k, F'/k') \subset \mathrm{Isom}(F, F')$$

denote the subset of isomorphisms $F \tilde{\to} F'$ inducing field isomorphisms $k \tilde{\to} k'$.

Let $\mathrm{Isom}(F^\times/k^\times, F'^\times/k'^\times)$ be the set of group isomorphisms $F^\times/k^\times \tilde{\to} F'^\times/k'^\times$ and

$$\mathrm{Isom}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times) \subset \mathrm{Isom}(F^\times/k^\times, F'^\times/k'^\times)$$

the subset of isomorphisms $F^\times/k^\times \tilde{\to} F'^\times/k'^\times$ preserving algebraic dependence. The group $\mathbb{Z}/2$ acts on the set $\mathrm{Isom}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$ by $\overline{\psi} \mapsto \overline{\psi}^{-1}$. Write

$$\overline{\mathrm{Isom}}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$$

for the resulting quotient.

**Theorem 1.** *Let $k, k'$ be perfect fields of characteristic $p \geq 0$ and let $F/k$, $F'/k'$ be finitely generated regular field extensions of transcendence degree $\geq 2$. Then the canonical map*

$$\mathrm{Isom}(F/k, F'/k') \to \overline{\mathrm{Isom}}^{\equiv}(F^\times/k^\times, F'^\times/k'^\times)$$

*is bijective.*

## 3. Comparison with existing results

Question 1 was considered by Bogomolov and Tschinkel in [BT09], where they prove (a variant of) Theorem 1 for finitely generated regular extensions of characteristic 0 fields ([BT09, Thm. 2]) and deduce from it the K-theoretic application for finitely generated field extensions of algebraically closed fields of characteristic 0 ([BT09, Thm. 4]).

Variants of our results were also obtained by Topaz from a smaller amount of $K$-theoretic information – mod-$\ell$ Milnor $K$-rings (for finitely generated field extensions of transcendence degree $\geq 5$ over algebraically closed fields of characteristic $p \neq \ell$ [To16, Thm. B]) and rational Milnor $K$-rings (for finitely generated field extensions of transcendence degree $\geq 2$ over algebraically closed field of characteristic 0 [To17, Thm. 6.1]) but enriched with the additional data of the so-called "rational quotients" of $F/k$. See also [To17, Rem. 6.2] for some cases where the additional data of rational quotients can be removed.

Our strategy follows the one of Bogomolov and Tschinkel in [BT09], where the key idea is to parametrize lines in $F^\times/k^\times$ as intersections of multiplicatively shifted (infinite dimensional) projective subspaces of a specific form arising from relatively algebraically closed subextensions of transcendence degree 1. See Subsection 4 for details. The strategy of Topaz is more sophisticated and goes through the reconstruction of the quasi-divisorial valuations of $F$ *via* avatars of the theory of commuting-liftable pairs as developed in the frame of birational anabelian geometry. Though not explicitly stated in the literature, it is likely that for finitely generated field extensions of algebraically closed fields of characteristic $p > 0$, Theorem 1 and its K-theoretic application could also be recovered from the techniques of birational anabelian geometry as developed by Bogomolov–Tschinkel [BT12], Pop (e.g. [P12a], [P12b]) and Topaz.

To our knowledge, Theorem 1 for finitely generated regular extensions of arbitrary perfect fields of characteristic $p > 0$ and its K-theoretic application for finitely generated field extensions of finite fields are new.

## 4. Strategy of proof

For simplicity, write $F^p \subset F$ for the subfield generated by $k$ and the $x^p$, $x \in F$, and write $F^\times/p := F^\times/F^{p\times}$.

According to the fundamental theorem of projective geometry, it would be enough to show that a group isomorphism $\overline{\psi} : F^\times/k^\times \tilde{\rightarrow} F'^\times/k'^\times$ preserving algebraic dependence induces a bijection from lines in $F^\times/k^\times$ to lines in $F'^\times/k'^\times$. This would reduce the problem to describing lines in $F^\times/k^\times$ using only $\equiv$ and the multiplicative structure of $F^\times/k^\times$. This classical approach works well if $p = 0$. The key observation of Bogomolov and Tschinkel in [BT09] is that every line can be multiplicatively shifted to a line passing through a "good" pair of points and that those lines can be uniquely parametrized as intersections of multiplicatively shifted (infinite dimensional) projective subspaces of a specific form arising from relatively algebraically closed subextensions of transcendence degree 1 [BT09, Thm. 22]. This is the output of elaborate computations in [BT09]. Later, Rovinsky suggested an alternative argument using differential forms; this is sketched in [BT12, Prop. 9].

When $p > 0$, the situation is more involved. The original computations of [BT09] fail due to inseparability phenomena. Instead, we adjust the notion of "good" for the pair of points in order to refine the argument of Rovinsky. In particular, we use the field-theoretic notion of "regular" element rather than the group-theoretic notion of "primitive" element used in [BT09]. To show that every line can be shifted to a line passing through a "good" pair of points, we use Bertini-like arguments; this is classical when $k$ is infinite but, when $k$ is finite (and $F$ of transcendence degree 2 over $k$) it seems we cannot avoid the use of the Charles-Poonen Bertini theorem [CP16]. This gives us a parametrization of lines which, when $p > 0$, is much rougher than in [BT09, Thm. 22] – up to prime-to-$p$ powers and certain homographies with $F^p$-coefficients; this is due to the apparition of constants in $F^p$ when one integrates differential forms. It is however enough to show that there exists a unique $m \in \mathbb{Z}$ normalized as

$$\begin{array}{ll} |m| = 1 & \text{if } p = 0, 2 \\ 1 \leq |m| \leq \frac{p-1}{2} & \text{if } p > 2; \end{array} \tag{1}$$

such that $\overline{\psi}^m$ induces a bijection from lines in $F^\times/p$ to lines in $F'^\times/p$, so that the fundamental theorem of projective geometry gives a unique field isomorphism $\phi : F \tilde{\to} F'$ such that the resulting isomorphism of groups $\phi : F^\times \tilde{\to} F'^\times$ coincides with $\overline{\psi}^m$ on $F^\times/p$. This concludes the proof if $p = 0$. But if $p > 0$, the extension $F/F^p$ is much smaller (finite-dimensional!) and one has to perform an additional descent step to show that $m = \pm 1$ and $\phi$ coincides with $\overline{\psi}^{\pm 1}$ on $F^\times/k^\times$ (not only on $F^\times/p$).

## 5. Questions

(1) Question 1. For a possible counter-example, consider function fields of curves over algebraically closed or finite fields. In the positive direction, one may ask for the extension of our K-theoretic applications to function fields of transcendence degree $\geq 2$ over more general base fields (than algebraically closed or finite fields).

(2) Non-birational analogue of Theorem 1: One can reformulate Theorem 1 (resp. its K-theoretic application) by saying that the birational equivalence class of a normal proper geometrically integral variety $X$ of dimension $\geq 2$ over a perfect field $k$ is determined in a functorial way by the inductive systems of the $K^\times$ for $K$ describing the relatively algebraically closed subextensions in the function field of $X$ (resp. (some quotients of) its Milnor K-ring). Find minimal sets of data determining $X$ not only up to birational equivalence but up to isomorphism.

## References

[BT09] F. Bogomolov and Y. Tschinkel, *Milnor $K_2$ and field homomorphisms.* In Geometry, analysis and algebraic geometry: 40 years of the Journal of Differential Geometry, Surveys in Differential Geometry **13**, p. 223–244, Int. Press, Somerville, MA, 2009.

[BT12] F. Bogomolov and Y. Tschinkel, *Introduction to binational anabelian geometry.* In Current developments in algebraic geometry, Math. Sc. Res. Inst. Publ. **59**, p. 17–63, Cambridge University Press, Cambridge, 2012.

[CP16] F. Charles and B. Poonen, *Bertini irreducibility theorems for finite fields.* J. Amer. Math. Soc. **29**, p. 81–94, 2016.

[MS82] A. Merkurjev and A. Suslin, *K-cohomology of Severi–Brauer varieties and the norm-residue homomorphism.* Izv. Akad. Nauk. SSSR **46**, p. 1011-1046, 1982.

[P12a] F. Pop, *Recovering function fields from their decomposition graphs.* In Number theory, analysis and geom- etry, p. 519–594. Springer, New York, 2012. Invent. Math. **187**, p. 511-533, 2012.

[P12b] F. Pop, *On the birational anabelian program initiated by Bogomolov I.* Invent. Math. **187**, p. 511-533, 2012.

[T71] J. Tate, *Symbols in arithmetic.* In Actes du Congrès International des Mathématiciens (Nice, 1970), Gauthier-Villars, Paris, p. 201–211, 1971.

[To16] A. Topaz, *Reconstructing function fields from rational quotients of mod-ℓ Galois groups.* Math. Annalen **366**, p. 337–385, 2016.

[To17] A. Topaz, *A Torelli theorem for higher-dimensional function fields.* 2017. arXiv:1705.01084

## Torsion on Abelian Varieties over Large Algebraic Extensions of Finitely Generated Extensions of $\mathbb{Q}$

Moshe Jarden

(joint work with Sebastian Petersen)

The goal of the talk was to complete the proof of an old conjecture of Geyer–Jarden in characteristic 0. The conjecture deals with a finitely generated field $K$ over $\mathbb{Q}$. We fix an algebraic closure $\tilde{K}$ of $K$. Then, the **absolute Galois group** $\mathrm{Gal}(K) = \mathrm{Gal}(\tilde{K}/K)$ of $K$ is a profinite group. It is equipped with a unique Haar measure $\mu_K$ with $\mu_K(\mathrm{Gal}(K)) = 1$ [FrJ08, p. 378, Sec. 18.5]. For each positive integer $e \geq 1$, the group $\mathrm{Gal}(K)^e$ is equipped with the product measure, which we also denote by $\mu_K$. We say that a certain statement holds for **almost all $\boldsymbol{\sigma}$** $\in \mathrm{Gal}(K)^e$ if the set of $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ for which that statement holds has $\mu_K$-measure 1. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$, we consider the field $\tilde{K}(\boldsymbol{\sigma}) = \{x \in \tilde{K} \mid \sigma_i x = x,\ i = 1, \ldots, e\}$.

Given an abelian variety $A$ over $K$ and a positive integer $m$, we denote the kernel of the multiplication on $A$ by $m$ with $A_m$. For a prime number $l$, we write $A_{l^\infty} = \bigcup_{i=1}^{\infty} A_{l^i}$.

**Conjecture A** [GeJ78, p. 260, Conjecture]. *Let $K$ be a finitely generated field over $\mathbb{Q}$, let $A$ be a non-zero abelian variety over $K$, and let $e$ be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the following holds:*

*(a) If $e = 1$, there exist infinitely many prime numbers $l$ with $A_l(\tilde{K}(\boldsymbol{\sigma})) \neq 0$.*

*(b) If $e \geq 2$, there exist only finitely many prime numbers $l$ with $A_l(\tilde{K}(\boldsymbol{\sigma})) \neq 0$.*

*(c) If $e \geq 1$ and $l$ is a prime number, then $A_{l^\infty}(\tilde{K}(\boldsymbol{\sigma}))$ is finite.*

**B. Previous results.** Conjecture A along with its analog in positive characteristics has been proved in [GeJ78, p. 259, Thm. 1.1] when $A$ is an elliptic curve. The analog of the conjecture is true for an arbitrary abelian variety over a finite field [JaJ84, p. 114, Prop. 4.2]. Note that the latter paper contains a proof of Part (a) of Conjecture A and its analog in positive characteristic. Unfortunately, that proof is false as indicated in [JaJ85].

Part (c) of Conjecture A along with its analog in positive characteristic and Part (b) of the conjecture appear in [JaJ01, Main Theorem].

The main result of [GeJ05] considers a non-zero abelian variety $A$ over a number field $K$ and says that there exists a finite Galois extension $L$ of $K$ such that for almost all $\sigma \in \mathrm{Gal}(L)$ there exist infinitely many primes $l$ with $A_l(\tilde{K}(\sigma)) \neq 0$.

Finally, David Zywina [Zyw16] improves [GeJ05] by proving Part (a) of Conjecture A for a number field $K$ not only for almost all $\sigma \in \mathrm{Gal}(L)$ for some $L$ as [GeJ05] does but for almost all $\sigma \in \mathrm{Gal}(K)$.

We generalize Zywina's result to an arbitrary finitely generated extension $K$ of $\mathbb{Q}$:

**Theorem C.** Let $A$ be a non-zero abelian variety over a finitely generated extension $K$ of $\mathbb{Q}$. Then, for almost all $\sigma \in \mathrm{Gal}(K)$ there exist infinitely many prime numbers $l$ with $A_l(\tilde{K}(\sigma)) \neq 0$.

**D. On the proof.** Let $g = \dim(A)$. For each prime number $l$ let

$$\rho_{A,l} \colon \mathrm{Gal}(K) \to \mathrm{GL}_{2g}(\mathbb{F}_l)$$

be the $l$-ic representation (also called the **mod-$l$ representation**) of $\mathrm{Gal}(K)$ induced by the action of $\mathrm{Gal}(K)$ on the vector space $A_l$ over $\mathbb{F}_l$ of dimension $2g$.

**D1. Serre's theorem.** The proof of [GeJ05] uses the main result of [Ser86]. That result deals with a number field $K$. Among others, it gives a finite Galois extension $L$ of $K$, a positive integer $n$, and for each $l$ a connected reductive subgroup $H_l$ of $\mathrm{GL}_{2g,\mathbb{F}_l}$ such that $(H_l(\mathbb{F}_l) : \rho_{A,l}(\mathrm{Gal}(L)))$ divides $n$. In addition, the fields $L(A_l)$ with $l$ ranging over all prime numbers are linearly disjoint over $L$. Another important feature of Serre's theorem is the existence of a set $\Lambda$ of prime numbers of positive Dirichlet density such that $H_l$ splits over $\mathbb{F}_l$ for each $l \in \Lambda$.

**D2. Borel–Cantelli Lemma.** For each $l$ let

$$S_l = \{\sigma \in \mathrm{Gal}(L) \mid \rho_{A,l}(\sigma) \text{ has eigenvalue } 1\}.$$

Then, [GeJ05] proves the existence of a positive constant $c$ and a set $\Lambda$ of positive Dirichlet density such that $\mu_L(S_l) > \frac{c}{l}$ for each $l \in \Lambda$. Thus, $\sum_{l \in \Lambda} \mu_L(S_l) = \infty$. In addition, by D1, the sets $S_l$ with $l$ ranging over $\Lambda$ are $\mu_L$-independent. It follows from the Borel–Cantelli Lemma that almost all $\sigma \in \mathrm{Gal}(L)$ lie in infinitely many $S_l$'s with $l \in \Lambda$. Thus, for almost all $\sigma \in \mathrm{Gal}(L)$ there exist infinitely many $l$'s such that $A_l(\tilde{K}(\sigma)) \neq 0$, which is the desired result over $L$.

**D3. Zywina's combinatorial approach.** Zywina makes a more careful use of the Borel–Cantelli Lemma. In [Zyw16], he chooses a set $B$ of representatives of $\mathrm{Gal}(K)$ modulo $\mathrm{Gal}(L)$. For each $l$ and every $\beta \in B$ he considers the set

$$U_{\beta,l} = \{\sigma \in \beta\,\mathrm{Gal}(L) \mid \rho_{A,l}(\sigma) \text{ has eigenvalue } 1\}.$$

Then, he constructs a positive constant $c$ and a set $\Lambda_\beta$ of prime numbers having positive Dirichlet density such that

$$\mu_K(U_{\beta,l}) \geq \frac{c}{l} \text{ for each } l \in \Lambda_\beta. \tag{1}$$

Again, by the Borel–Cantelli Lemma, this leads to the conclusion that the $\mu_K$-measure of the set $U_\beta$ of all $\sigma \in \mathrm{Gal}(K)$ that belong to infinitely many $U_{\beta,l}$ is $\frac{1}{[L:K]}$. Since the $U_\beta$'s with $\beta \in B$ are disjoint, it follows that for almost all $\sigma \in \mathrm{Gal}(K)$ there are infinitely many $l$'s such that $A_l(\tilde{K}(\sigma)) \neq 0$.

**D4. Function fields.** Now assume that $K$ is a finitely generated extension of $\mathbb{Q}$ of positive transcendence degree and choose a subfield $E$ of $K$ such that $K/E$ is a regular extension of transcendence degree 1. We wish to find a prime divisor of $K/E$ with residue field $\bar{K}$ that induces a good reduction of $A$ onto an abelian variety $\bar{A}$ over $\bar{K}$ such that

$$\mathrm{Gal}(K(A_l)/K) \cong \mathrm{Gal}(\bar{K}(\bar{A}_l)/\bar{K}) \tag{2}$$

for at least every $l$ in a set of positive Dirichlet density.

**D5. Hilbert irreducibility theorem.** The first idea that comes to mind is to use Hilbert Irreducibility Theorem. However, that theorem can take care of only finitely many prime numbers, so it is of no use for our problem.

**D6. Openness theorem.** Instead, we choose a smooth curve $S$ over $E$ whose function field is $K$ such that $A$ has a good reduction along $S$ and set $\hat{K} = \prod_{l\in\mathbb{L}} K(A_l)$, where $\mathbb{L}$ is the set of all prime numbers. Using a combination of results of Anna Cadoret and Akio Tamagawa that goes under the heading "openness theorem", we find a closed point $\mathbf{s}$ of $S$ with an open decomposition group in $\mathrm{Gal}(\hat{K}/K)$. Let $\bar{K}_{\mathbf{s}}$ be the residue field of $K$ at $\mathbf{s}$ and $\hat{K}_{\mathbf{s}} = \prod_{l\in\mathbb{L}} \bar{K}_{\mathbf{s}}(A_{\mathbf{s},l})$, where $A_{\mathbf{s}}$ is the reduction of $A$ at $\mathbf{s}$. Then, there exists a finite extension $K'$ of $K$ in $\hat{K}$ such that the reduction modulo $\mathbf{s}$ induces an isomorphism $\mathrm{Gal}(\hat{K}/K') \cong \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\bar{K}_{\mathbf{s}})$. This gives the desired isomorphism (2) for $K'$ rather than for $K$ and for all prime numbers $l$.

**D7. Serre's theorem over $K$.** Now we use a result of [GaP13] and find a finite Galois extension $L$ of $K$ that contains $K'$ and satisfies the same reduction conditions that $K'$ does and in addition the fields $L(A_l)$, with $l$ ranging over all prime numbers, are linearly disjoint over $L$.

Note that $\bar{K}_{\mathbf{s}}$ is again finitely generated over $\mathbb{Q}$ and the transcendence degree of $\bar{K}_{\mathbf{s}}$ over $\mathbb{Q}$ is one less than that of $K$. Starting with Serre's theorem for number fields mentioned in D1 and using induction on the transcendence degree over $\mathbb{Q}$, we now prove the theorem of Serre over our current field $K$.

**D8. Strongly regular points.** Having Serre's theorem for our function field $K$ at our disposal, we now follow the proof of [Zyw16] to obtain the estimates (1) for our abelian variety $A/K$. The proof contains a careful analysis of regular points of the reductive groups $H_l$ mentioned in Serre's theorem for $l \in \Lambda$. It uses Zywina's crucial observation that if $T$ is an $\mathbb{F}_l$-split maximal torus of $H_l$ and $\mathbf{t} \in T(\mathbb{F}_l)$, then $\mathbf{t}^{n!} \in \rho_{A,l}(\mathrm{Gal}(L))$. Moreover, if $\mathbf{t}$ is a regular element of $H_l$ and $T$ is the unique maximal torus of $H_l$ that contains $\mathbf{t}$, then the number of points $\mathbf{t}' \in T(\mathbb{F}_l)$ with $(\mathbf{t}')^{n!} = \mathbf{t}^{n!}$ is at most $(n!)^r$, where $r = \mathrm{rank}(H_l) = \dim(T)$. Finally, still following [Zyw16], we make use of the Lang–Weil estimates (or rather the more accurate version of these estimates that [Zyw16] provides) to prove that "most of the points" of $\rho_{A,l}(\mathrm{Gal}(K))$ are regular points of $H_l$ whose characteristic polynomials have "maximal numbers of roots in $\mathbb{F}_l$" (We may refer to these points as "strongly regular").

**D9. Serre's density theorem.** At some point of the proof, [Zyw16] uses the Chebotarev density theorem for number fields to choose a prime of $K$ whose Artin class is equal to a previously chosen conjugacy class in $\mathrm{Gal}(L(A_l)/K)$ (where $L$ is the number field mentioned in Serre's theorem for number field). Instead, we use Serre's generalization of the Chebotarev density theorem to our function field $K$ in order to find a prime $\mathfrak{p}$ of $K$ with the same properties as above.

**Acknowledgment.** Part of this work was done during research visits of the first author at the University of Kassel. We thank Wulf-Dieter Geyer and Aharon Razon for careful reading of this work and the referee for helpful comments to an earlier version of it.

## References

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, third edition, revised by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[GaP13] W. Gajda and S. Petersen, *Independence of $l$-adic Galois representations over function fields,* Compositio Mathematica **149** (2013), 1091-1107.

[GeJ78] W.-D. Geyer and M. Jarden, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields,* Israel Journal of Mathematics **31** (1978), 157–197.

[GeJ05] W.-D. Geyer and M. Jarden, *Torsion of Abelian varieties over large algebraic fields,* Finite Field Theory and its Applications **11** (2005), 123–150.

[JaJ84] M. Jacobson and M. Jarden, *On torsion of abelian varieties over large algebraic extensions of finitely generated fields,* Mathematika **31** (1984), 110–116.

[JaJ85] M. Jacobson and M. Jarden, *On torsion of abelian varieties over large algebraic extensions of finitely generated fields: Erratum,* Mathematika **32** (1985), 316.

[JaJ01] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields,* Acta Arithmetica **98** (2001), 15–31.

[Mum74] D. Mumford, *Abelian Varieties,* Oxford University Press, London, 1974.

[Ser86] J.-P. Serre, *Groupes linéaires modulo p et points d'ordere fini des varietés abéliennes,* Note of a cours at Collège de France given in 1986, taken by Eva Bayer-Fluckiger,

[Zyw16] D. Zywina, *Abelian varieties over large algebraic fields with infinite torsion,* Israel Journal of Mathematics **211** (2016), 493–508.

## Recovering fields from local/adelic Hecke algebra isomorphisms

Valentijn Karemaker
(joint work with Gunther Cornelissen)

Let $K$ be a field and let $G_K$ denote its absolute Galois group. First suppose that $K$ is a number field. When $K$ is Galois over $\mathbb{Q}$, Neukirch [13] proved that $G_K$ determines $K$, in the sense that any isomorphism $G_K \cong G_L$ (as profinite groups) induces a unique field isomorphism $K \cong L$. Uchida [18] later proved this result when $K$ is not necessarily Galois; the same result was obtained independently by Iwasawa (unpublished), using results by Ikeda [8]. By contrast, the abelianisation $G_K^{\text{ab}}$, corresponding to the one-dimensional representations of $G_K$, does not determine $K$, cf. [15].

Now suppose that $K$ is a non-archimedean local field of characteristic zero. In this case, Yamagata showed in [20] that the analogous statement of the result by Neukirch and Uchida is false. Jarden and Ritter [9] prove that $G_K$ determines the absolute field degree $[K\colon \mathbb{Q}_p]$ and the maximal abelian subextension of $K$ over $\mathbb{Q}_p$. In addition, Mochizuki [12] proved that the absolute Galois group together with its ramification filtration *does* determine a local field of characteristic 0, and Abrashkin [1], [2] extended this result to any characteristic $p > 0$.

A couple of natural questions then arise: when $K$ is a number field, do irreducible *two-dimensional* (being the "lowest-dimensional non-abelian") representations of $G_K$ determine $K$? When $K$ is a non-archimedean local field of characteristic zero, to what extent does the representation theory of $G_K$ determine $K$?

By the philosophy of the Langlands programme, $n$-dimensional irreducible representations of $G_K$ (or, more generally, of the Weil group $W_K$) should be in correspondence with certain automorphic representations of $\mathrm{GL}_n$.

Over non-archimedean local fields of characteristic zero, the local Langlands correspondence was proven by Harris and Taylor [6] and Henniart [7]. When $K$ is a number field, no analogous result is known, although various special cases have been considered. One believes that irreducible $n$-dimensional representations of $G_K$ should correspond to cuspidal representations of $\mathrm{GL}_n(\mathbb{A}_K)$ "of Galois type" [3, p. 244].

Automorphic (admissible) representations of $\mathrm{GL}_n(\mathbb{A}_K)$ in turn correspond to (admissible) modules over the Hecke algebra $\mathcal{H}_{\mathrm{GL}_n}(K)$. Therefore, our questions inspire the next question.

**Question:** Let $K$ be either a number field or a non-archimedean local field of characteristic zero. To what extent does (the representation theory of) the Hecke algebra $\mathcal{H}_{\mathrm{GL}_n}(K)$ determine $K$?

For $n = 2$, the following result provides a partial answer.

**Theorem A** ([10]). *Let $K$ and $L$ be two non-archimedean local fields of characteristic zero and $G = \mathrm{GL}_2$. Then there is a Morita equivalence $\mathcal{H}_G(K) \sim_M \mathcal{H}_G(L)$.*

The Morita equivalence means that the respective categories of modules over the Hecke algebras of $K$ and $L$ are isomorphic. That is, the module structure of the complex representations of $\mathrm{GL}_2$ over a local field as above does not depend on the local field. The proof uses the Bernstein decomposition of the Hecke algebra.

Hecke algebras exist for any linear algebraic group $G$ over $\mathbb{Q}$. When $K$ is a number field, we will work with the finite-adelic real Hecke algebra, and when $K$ is a non-archimedean local field of characteristic zero, we use the local Hecke algebra. These are defined as follows:

$$\mathcal{H}_G(K) = \begin{cases} C_c^\infty(G(\mathbb{A}_{K,f}), \mathbb{R}) & \text{if } K \text{ is a number field,} \\ C_c^\infty(G(K), \mathbb{C}) & \text{if } K \text{ is non-arch. local of char. 0.} \end{cases}$$

(We could replace $\mathbb{R}$ by $\mathbb{C}$ in the number fields case; this does not affect our results.) Such Hecke algebras are equipped with an $L^1$-norm, which is induced from the Haar measure on the (locally compact) point group; an $L^1$-*isomorphism* will be an algebra isomorphism which respects this norm.

Using Stone–Weierstrass and results by Kawada [11] and Wendel [19], we show in the number field case that there is an $L^1$-isomorphism of finite-adelic Hecke algebras $\mathcal{H}_G(K) \cong_{L^1} \mathcal{H}_G(L)$ if and only if there is an isomorphism of finite-adelic point groups $G(\mathbb{A}_{K,f}) \cong G(\mathbb{A}_{L,f})$, and in the local field case that there is an $L^1$-isomorphism of local Hecke algebras $\mathcal{H}_G(K) \cong_{L^1} \mathcal{H}_G(L)$ if and only if there is an isomorphism of local point groups $G(K) \cong G(L)$.

The question whether $G(R) \cong G(S)$ for algebraic groups $G$ and rings $R, S$ implies a ring isomorphism $R \cong S$ has been considered before (following seminal work of van der Waerden and Schreier from 1928 [17]), most notably when $G = \mathrm{GL}_n$ for $n \geq 3$ or when $G$ is a Chevalley group and $R$ and $S$ are integral domains (see, e.g., [4], [16] and the references therein). The methods employed there make extensive use of root data and Lie algebras.

When $G = \mathrm{GL}_n$ for $n \geq 2$ and $K$ and $L$ are non-archimedean local of characteristic zero, $G(K) \cong G(L)$ implies $K \cong L$ by Theorem 5.6.10 of [14]. That is, the following result provides another partial answer to the Question above for the case of local fields.

**Theorem B** ([5]). *Let $K$ and $L$ be two non-archimedean local fields of characteristic zero and let $G = \mathrm{GL}_n$, $n \geq 2$. Then there is an $L^1$-isomorphism of local Hecke algebras $\mathcal{H}_G(K) \cong_{L^1} \mathcal{H}_G(L)$ if and only if there is a field isomorphism $K \cong L$.*

In the case of number fields, we introduce the following technical condition on the groups $G$: we call $G$ *fertile* for a field $K/\mathbb{Q}$ if $G$ contains a Borel group $B$ which is split over $K$ as $B = T \ltimes U$, such that over $K$, the split maximal torus $T \neq \{1\}$

acts nontrivially by conjugation on the abelianisation of the maximal unipotent group $U \neq \{0\}$. In particular, $\mathrm{GL}_n$ is fertile for any $K$ and all $n \geq 2$.

Then our partial answer to the Question above for global fields is the following result.

**Theorem C** ([5])**.** *Let $K$ and $L$ be two number fields, and let $G$ denote a linear algebraic group over $\mathbb{Q}$ which is fertile for $K$ and $L$. There is a topological group isomorphism of finite-adelic point groups $G(\mathbb{A}_{K,f}) \cong G(\mathbb{A}_{L,f})$ if and only if there is a topological ring isomorphism $\mathbb{A}_K \cong \mathbb{A}_L$.*

We make some remarks on the condition $\mathbb{A}_K \cong \mathbb{A}_L$. When such an isomorphism exists, $K$ and $L$ are said to be locally isomorphic. Local isomorphism implies, but is generally stronger than, arithmetic equivalence of $K$ and $L$. Recall that $K$ and $L$ are arithmetically equivalent if their Dedekind zeta functions coincide: $\zeta_K = \zeta_L$. Moreover, if $K$ or $L$ is Galois over $\mathbb{Q}$, both local isomorphism and arithmetic equivalence imply that $K$ and $L$ are isomorphic as fields.

Therefore, if $K$ and $L$ are Galois over $\mathbb{Q}$, and $G$ is fertile for $K$ and $L$, Theorem C shows that there is an $L^1$-isomorphism of Hecke algebras $\mathcal{H}_G(K) \cong_{L^1} \mathcal{H}_G(L)$ if and only if $K \cong L$. This result can be seen as an automorphic analogue of Neukirch's theorem.

Our proof of Theorem C uses number theory in adele rings and, by not passing to Lie algebras, applies to a more general class of (not necessarily reductive) algebraic groups. First, we prove in general that maximal divisible subgroups $\mathbb{D}$ of $G(\mathbb{A}_{K,f})$ and maximal unipotent point groups are the same up to conjugacy; note that this does not apply at the archimedean places). The torus $\mathbb{T}$ (as a quotient of the normaliser $\mathbb{N}$ of the unipotent point group $\mathbb{D}$ by itself) acts on the abelian group $\mathbb{V} = [\mathbb{N}, \mathbb{D}]/[\mathbb{D}, \mathbb{D}]$, that decomposes as a sum of one-dimensional $\mathbb{T}$-modules, on which $\mathbb{T}$ acts by multiplication with powers. Now we use a formula of Siegel, which allows us to express any adele as a linear combination of fixed powers, to show how this implies that the centre of the endomorphism ring of the $\mathbb{T}$-module $\mathbb{V}$ is a a cartesian power of the finite adele ring. We then use the structure of the maximal principal ideals in the finite adele ring to find from these data the adele ring itself.

## References

[1] V. Abrashkin, *On a local analogue of the Grothendieck conjecture*, Internat. J. Math. **11** no. 2 (2000), 133–175.

[2] V. Abhraskin, *Modified proof of a local analogue of the Grothendieck conjecture*, J. Théor. Nombres Bordeaux **22** no. 1 (2010), 1–50.

[3] D. Bump, J. Cogdell, E. de Shalit, D. Gaitsgory, E. Kowalski and S. Kudla, *An introduction to the Langlands program*, Birkhäuser Boston, Inc. (2003), x+281.

[4] Y. Chen, *Isomorphisms of adjoint Chevalley groups over integral domains*, Trans. Amer. Math. Soc. **348** no. 2 (1996), 521–541.

[5] G. Cornelissen and V. Karemaker, *Hecke algebra isomorphisms and adelic points on algebraic groups*, Doc. Math. **22** (2017), 851–871.

[6] M. Harris and R. Taylor, *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies **151** (2001), viii+276.

[7] G. Henniart, *Une preuve simple des conjectures de Langlands pour* GL$(n)$ *sur un corps p-adique*, Invent. Math. **139** no. 2 (2000), 439–455.

[8] M. Ikeda, *Completeness of the absolute Galois group of the rational number field*, J. Reine Angew. Math. **291** (1977), 1–22.

[9] M. Jarden and J. Ritter, *On the characterization of local fields by their absolute Galois groups*, J. Number Theory **11** no. 1 (1979), 1–13.

[10] V. Karemaker, *Hecke algebras for* GL$_n$ *over local fields*, Arch. Math. (Basel) **107** no. 4 (2016), 341–353.

[11] Y. Kawada, *On the group ring of a topological group*, Math. Japonicae **1** (1948), 1–5.

[12] S. Mochizuki, *A version of the Grothendieck conjecture for p-adic local fields*, Internat. J. Math. **8** no. 4 (1997), 499–506.

[13] J. Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 296–314.

[14] T. O'Meara, Lectures on linear groups, American Mathematical Society, Providence, R.I. (1974), vii+87.

[15] M. Onabe, *On the isomorphisms of the Galois groups of the maximal Abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. **27** (1976), 155–161.

[16] V. Petechuk, *Automorphisms of matrix groups over commutative rings*, Mat. Sb. (N.S.) **117(159)** no 4 (1982), 534–547, 560.

[17] O. Schreier and B. van der Waerden, *Die Automorphismen der projektiven Gruppen*, Abh. Math. Sem. Univ. Hamburg **6** no. 1 (1928), 303–322.

[18] K. Uchida, *Isomorphisms of Galois groups*, J. Math. Soc. Japan **28** no. 4 (1976), 617–620.

[19] J. Wendel, *On isometric isomorphism of group algebras*, Pacific J. Math. **1** (1951), 305–311.

[20] S. Yamagata, *A counterexample for the local analogy of a theorem by Iwasawa and Uchida*, Proc. Japan Acad. **52** no. 6 (1976), 276–278.

## Points on Varieties in Families of Fields

Philip Dittmann

In this talk I presented a family of existential first-order definable subsets of fields, which is of interest in a variety of contexts. The method of definition is a modification and generalisation of the method used in [6] for a $\forall\exists$-definition of the ring of integers in number fields, and further used in [8] and [7] for a $\forall$-definition, again of the ring of integers.

Let $K$ be a field and $X/K$ a variety which satisfies a local–global principle over all finite extensions of $K$, i.e. for any finite extension $L/K$ the variety has an $L$-point if and only if it has an $L_v$-point for all henselisations or completions $L_v$ of $L$ of a certain kind.

Then we consider the set $S(X/K) \subseteq K$ consisting of those $a \in K$ such that $X$ has a point over all residue fields of of the $K$-algebra $K[X]/(X^2 - aX + 1)$. This should be thought of as considering the behaviour of $X$ along a family of extension fields of $K$.

One shows without difficulty that $S(X/K)$ is existentially definable in $K$, and that it is, in a precise sense, controlled by the henselisations (completions) of $K$. For instance, the method of [6] can be rephrased as the observation that if $K$ is a number field and $X/K$ a plane conic with a point over all real completions of $K$, then the set of pairwise sums $S(X/K) + S(X/K)$ is precisely equal to the intersection of valuation rings of $K$ over whose completion $X$ does not have a point. Similar results hold when one changes the definition of $S$ by considering polynomials of higher degree than 2.

A very attractive feature of these definitions is that they yield not only definable sets of low quantifier complexity with readily understood arithmetic meaning, but that they also behave well when changing the base field $K$, i.e. considering $S(X_L/L)$ instead of $S(X/K)$. This is important for uniformity in several of our results.

Some applications of the sets $S(X/K)$ and generalised variants, in which polynomials of higher degree than 2 are considered, are the following.

(1) The $p$-Pythagoras number of number fields is bounded, i.e. there is a uniform existential definition of the intersection of $p$-valuation rings (of a fixed rank) in all number fields. See [5] and also Fehm's talk at this workshop. The proof works by considering sets $S(X/K)$ for suitable Severi–Brauer varieties $X/\mathbb{Q}$.

(2) Again by consideration of Severi–Brauer varieties, I proved in [1] that irreducibility of a polynomial over a global field is an existential condition on its coefficients. See also [2].

(3) Using local–global principles for Pfister forms, one may make use of sets $S(X/K)$ in finitely generated fields $K$. These principles are based on proven versions of Kato's cohomological local–global principles due to Kerz and Saito ([9]). They have also been applied by Pop in [3]. One obtains for instance that any finitely generated field $K$ of characteristic not 2 does not have embedded residue in the sense of [4], so henselian valuation rings with residue field $K$ are uniformly existentially definable in all fields.

## References

[1] P. Dittmann, *Irreducibility of polynomials over global fields is diophantine*, Compositio Math. **154** (2018), no. 4, 761–772.

[2] P. Dittmann, *Irreducibility of polynomials over number fields is diophantine*, Oberwolfach reports No. 49/2016

[3] F. Pop, *Elementary equivalence versus isomorphism II*, Algebra & Number Theory **11** (2017), 2091–2111

[4] S. Anscombe and A. Fehm, *Characterizing diophantine henselian valuation rings and valuation ideals*, Proc. London Math. Soc. **115** (2017), 293–322.

[5] A. Fehm, *Diophantine subsets of henselian fields (joint work with Sylvy Anscombe, Philip Dittmann)*, Oberwolfach reports No. 49/2016

[6] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682.

[7] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. Math. **183** (2016), 73–93.

[8] J. Park, *A universal first order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), 961–980.

[9] M. Kerz and S. Saito, *Cohomological Hasse principle and motivic cohomology for arithmetic schemes*, Publ. Math. IHES **115** (2012), no. 1, 123–183.

## On finite extensions of decidable fields

Jochen Koenigsmann

In 1973, Abraham Robinson asked the following

**Question 1** ([R]). *Is every finite extension of an undecidable field necessarily undecidable?*

Conversely, one may ask

**Question 2** ([K]). *Is every finite extension of a decidable field necessarily decidable?*

Here a field $K$ is called *decidable* if $\mathrm{Th}(K)$, the first-order theory of $K$ in the language of rings $\mathcal{L}_{ring} = \{+, \cdot, 0, 1\}$, is decidable in the sense that there is an algorithm which, given any first-order $\mathcal{L}_{ring}$-sentence $\phi$, tells you whether or not $\phi$ holds in $K$. Equivalently, by the Completeness Theorem of first-order logic, $K$ is decidable if and only if there is a recursive axiomatization for $\mathrm{Th}(K)$.

Examples of decidable fields are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Q}_p$ and all finite extensions. Examples of undecidable fields are (all finite extensions of) $\mathbb{Q}$, $\mathbb{F}_p(t)$ and $\mathbb{C}(t_1, t_2)$, as well as the field $\mathbb{R}(t)$. The question of decidability is open for $\mathbb{F}_p((t))$, $\mathbb{C}(t)$, $\mathbb{Q}^{ab}$, $\mathbb{Q}^{solv}$ and all finite extensions.

Both of the above two questions have a negative answer. For Question 1, a negative answer was given in [CDM] where an undecidable PAC-field $K$ was constructed with the property that all proper finite extensions $L/K$ are decidable, and they are all isomorphic to each other. In [K], alternative undecidable PAC-fields with decidable finite extensions were found among algebraic extensions of $\mathbb{Q}$. If $\mathbb{C}(t)$ turned out to be decidable then $K = \mathbb{R}(t)$ and $L = \mathbb{C}(t)$ would provide the most natural example of a negative solution to Question 1.

A negative solution to Question 2 (joint work with Kesavan Thanagopal) uses Ershov's *wonderful extension* $W$ of $\mathbb{Q}$ (cf. [E1] and [E2]). $W$ is a field which has, for each $p \in \mathbb{P} \cup \{\infty\}$, an embedding $\lambda_p : W \to \mathbb{Q}_p$ (where $\mathbb{Q}_\infty = \mathbb{R}$) inducing a unique $p$-adic valuation (resp. ordering) $v_p$ on $W$ such that

(i) if $x \in W^\times$ then $x \in \mathcal{O}_{v_p}^\times$ for almost all $p$,
(ii) $W$ satisfies a local-global principle for rational points on smooth algebraic varieties w.r.t. $(v_p)_p$,
(iii) $W$ is algebraically maximal with (i) and (ii).

Such a field $W$ exists, $W$ is decidable and $W \cap \overline{\mathbb{Q}} = \mathbb{Q}$. Now let $K \succeq W$ be a saturated elementary extension, let $\Sigma \subseteq \mathbb{P}$ be a non-recursive set of primes, let $n$ be an integer $> 1$, and let $L/K$ be an extension of degree $n$ which is totally ramified at all $p \in \Sigma$ and totally split at all $p \in \mathbb{P} \setminus \Sigma$. This 'behaviour at $p$' is part of the first-order theory of $L$ (via uniform definability of valuations in global fields). Thus $L$ is undecidable while $K$ is (like $W$) decidable.

## References

[CDM] Gregory Cherlin, Lou van den Dries, Angus Macintyre, *The elementary theory of regularly closed fields*, manuscript, 1980.

[E1] Yuri L. Ershov, *On Surprising Extensions of the Field of Rationals*, Doklady Mathematics **62(1)** (2000), 8–9.

[E2] Yuri L. Ershov, *Multivalued Fields*, Kluwer Academic 2001.

[K] Jochen Koenigsmann, *On a question of Abraham Robinson's*, Israel Journal of Mathematics **214(2)** (2016), 931–943.

[R] Abraham Robinson, *Metamathematical Problems*, J. Symb. Logic **38(3)** (1973), 500–516.

## Rational and nonrational varieties may coexist in smooth projective families (after Hassett–Pirutka–Tschinkel, and Schreieder)

J.-L. Colliot-Thélène

Hassett, Pirutka and Tschinkel [3] (2016) gave the first examples of families $X \to B$ of smooth, projective, connected, complex varieties having some rational fibres and some other fibres which are not even stably rational.

This used the specialisation method of Voisin [7] (2013), as extended by Pirutka and myself [2] (2014). Just as with all previous applications of the method, the paper [3] involved an explicit desingularisation of some singular variety.

Under specific circumstances, a simplified version of the specialisation method was produced by Schreieder [4, 5] (2017), leading to a simpler proof of the HPT example (no explicit resolution of singularities). In the note [1] written on the occasion of the conference Quadratic Forms in Chile 2018, held at IMAFI, Universitad de Talca, 8-12 January 2018, I reported on this simplified approach of [3]. In my talk at Oberwolfach, I went through most details of [1].

For further developments, the reader is invited to read the papers [4, 5, 6] by Schreieder.

## References

[1] J.-L. Colliot-Thélène, Introduction to work of Hassett–Pirutka–Tschinkel and Schreieder, https://arxiv.org/abs/1806.00598

[2] J.-L. Colliot-Thélène et A. Pirutka, Hypersurfaces quartiques de dimension 3 : non rationalité stable, Annales Sc. Éc. Norm. Sup. **49** (2016), 371–397.

[3] B. Hassett, A. Pirutka, Yu. Tschinkel, Stable rationality of quadric surface bundles over surfaces, Acta Mathematica, to appear.

[4] S. Schreieder, On the rationality problem for quadric bundles, preprint 2017, https://arxiv.org/abs/1706.01356v4

[5] S. Schreieder, Quadric surface bundles over surfaces and stable rationality, https://arxiv.org/abs/1706.01358v4, to appear in Algebra & Number Theory.

[6] S. Schreieder, Stably irrational hypersurfaces of small slopes, https://arxiv.org/abs/1801.05397v2

[7] C. Voisin, Unirational threefolds with no universal codimension 2 cycle. Invent. math. **201** (2015), 207–237.

## Approximation and Grunwald problems

Danny Neftin
(joint work with François Legrand, Joachim König)

A classical theorem of Hilbert shows that the quotient $\mathbb{A}^n/S_n$, of the affine space $\mathbb{A}^n$ by the action of the symmetric group $S_n$ which permutes the coordinates, is rational. Given an action of a finite group $G$ on $\mathbb{A}^n$, the study of rationality of the variety $\mathbb{A}^n/G$ is also known as Noether's problem, and is well known to imply the inverse Galois problem for $G$. A much weaker property of $\mathbb{A}^n/G$ is *weak weak approximation (WWA)*: a (geometrically integral algebraic) variety $X$ over a number field $K$ has WWA if there exists a finite set $T$ such that $X(K)$ is dense in $\prod_{v\in S} X(K_v)$ for every finite set $S$ of places disjoint from $T$. Although weaker, the WWA for $\mathbb{A}^n/G$ also implies the inverse Galois problem over $K$, by a correspondence of Colliot-Thélène and Ekedahl [2].

Since $\mathbb{A}^n/G$ and $\mathrm{SL}_n/G$ are unirationally equivalent, by the no-name lemma, $A^n/G$ has WWA if and only if the variety $\mathrm{SL}_n/G$ has WWA. Thus, via Hilbert 90, the property is equivalent to the surjectivity of the map

$$\mathrm{Res}_S : H^1(K,G) \to \prod_{v\in S} H^1(K_v,G)$$

for every finite set $S$ disjoint from a finite set of exceptions $T$. This is a stronger version of the Grunwald problem: given extensions $L^{(v)}/K_v$, $v \in S$, and embeddings $\mathrm{Gal}(L^{(v)}/K_v) \hookrightarrow G$, is there a $G$-extension $L/K$ such that $L_v \cong L^{(v)}$ for every $v \in S$?

In this talk, we survey past results and recent developments concerning the WWA property for the varieties $\mathbb{A}^n/G$. We start by describing Colliot-Thélène's conjecture [1] that the Brauer–Manin obstruction is the only obstruction to WWA for rationally connected varieties and in particular for $\mathbb{A}^n/G$, and continue to the results of Grunwald–Wang for abelian groups; Neukirch [11] for odd order groups and its generalization by Lucchini-Arteche [10]; Saltman's result [12] for groups with a generic extension; results of Harari [6] and Demarche–Lucchini-Arteche–N. [5] for iterated semidirect products of abelian groups; and the recent result of Harpaz–Wittenberg [7] for supersolvable groups. We also describe examples where weak approximation fails but WWA holds.

Finally, we describe a recent approach towards the case of nonsolvable groups of the Grunwald problem which should extend to WWA. Starting with a regular $G$-extension $E/K(t)$, one considers the extensions $E_{t_0}/k$ obtained by specializing at points $t_0 \in K$. The results of Débes–Ghazi [3, 4], suggest that the Grunwald problem can be solved by considering such extensions. Namely, they show that for every $S$ disjoint from a finite set of "bad" primes $T_E$, and unramified Galois extensions $L^{(v)}/K_v$ with $\mathrm{Gal}(L^{(v)}/K_v) \hookrightarrow G$, for $v \in S$, there exists $t_0 \in K$ such that the completion of $E_{t_0}$ at $v$ is $L^{(v)}$.

To obtain ramified extensions, one has to consider specializations that are $v$-adically close to a branch point $t_1 \in K$ of $E/K(t)$. We show [9] that the decomposition group at $v$ of such a specialized extension $E_{t_0}/K$ can be read off of that of

$E_{t_1}/K$. This provides a constraint on all local extensions obtained as completions of specializations $E_{t_0}/k$. Furthermore, we show that the Grunwald problem can be solved for all local extensions $L^{(v)}/K_v$, $v \in S$, satisfying this constraint. This and subsequent work of Knig [8] suggest that the Grunwald problem can be solved by specializing families of regular extensions $E/K(s,t)$.

## References

[1] J.-L. Colliot-Thélène, *Points rationnels sur les fibrations, Higher dimensional varieties and rational points*, (2003) Bolyai Soc. Math. Stud., vol. 12, Springer, Berlin. pp. 171–221.

[2] J.-L. Colliot-Thélène, Ekedahl, Personal correspondence.

[3] P. Dèbes, N. Ghazi. *Specializations of Galois covers of the line,* In "Alexandru Myller" Mathematical Seminar, volume 1329 of AIP Conf. Proc., pages 98–108. Amer. Inst. Phys., Melville, NY, 2011.

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

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

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

[7] Y. Harpaz, O. Wittenberg, *Zero-cycles sur les espaces homogènes et problème de Galois inverse*, (2018) preprint.

[8] J. König, *The Grunwald problem and specialization of families of regular Galois extensions,* (2017) preprint.

[9] J. König, F. Legrand, D. Neftin *On the local behaviour of specializations of function field extensions,* to appear in IMRN, arXiv:1709.03094.

[10] G. Lucchini-Arteche, *Approximation faible et principe de Hasse pour des espaces homogènes à stabilisateur fini résoluble,* Math. Ann., **360** (2014), 1021–1039.

[11] J. Neukirch, *On Solvable Number Fields*, Inven. Math. **53** (1979), 135–164.

[12] D. J. Saltman. *Generic Galois extensions and problems in field theory.* Adv. in Math., **43** (1982), 250–283.

## Solving Embedding Problems with Bounded Ramification

Nantsoina Cynthia Ramiharimanana
(joint work with Moshe Jarden)

A sharpened version of the inverse Galois problem is the so-called embedding problem. Given a Galois extension $K/K_0$ of global fields, a finite group $G$, and an epimorphism $\alpha : G \longrightarrow \mathrm{Gal}(K/K_0)$, one looks for a Galois extension $N$ of $K_0$ that contains $K$ such that $\mathrm{Gal}(K/K_0) \cong G$ and the restriction map $\mathrm{res}_{N/K} : \mathrm{Gal}(N/K_0) \longrightarrow \mathrm{Gal}(K/K_0)$ coincides with $\alpha$. Equivalently, with $K_{0,\mathrm{sep}}$ being the separable algebraic closure of $K_0$, and $\mathrm{Gal}(K_0) = \mathrm{Gal}(K_{0,\mathrm{sep}}/K_0)$, one looks for a continuous epimorphism $\psi : \mathrm{Gal}(K_0) \longrightarrow G$ such that $\alpha \circ \psi = \mathrm{res}_{K_{0,\mathrm{sep}}/K}$. We refer to $\psi$ as proper solution of the embedding problem (whereas, if $\psi$ is only a homomorphism, as above, we say that $\psi$ is a weak solution of the embedding problem). The question about the proper solvability of finite embedding problems over $K_0$ is far from being settled. But, in those cases where an embedding problem as above is solvable, one may ask whether a solution field as above can be found with a bound in the ramification, i.e. with a bound on the cardinality of the set $\mathrm{Ram}(N/K_0)$ of the primes of $K_0$ that are ramified in $N$.

Working with central embedding problems with kernel the cyclic group of order $l$, [1] uses the Scholz–Reichardt method in order to realize for each prime number $l$ every finite $l$-group $G$ over $K$ under the condition $l \neq \mathrm{char}(K)$ and $\zeta_l \notin K$. With $|G| = l^n$, the work [1] constructs a Galois extension $N$ of $K$ such that $\mathrm{Gal}(N/K) \cong G$ and $|\mathrm{Ram}(N/K)| \leq n + r(K)$, where $r(K)$ depends only on arithmetical invariants of $K$. If $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$, then $r(K) = 0$, so the result of [1] reproduces in this case a result of Serre in [4] that $|\mathrm{Ram}(N/K)| \leq n$.

In the case of number fields, Neukirch observes in [2] that for each prime divisor $\mathfrak{p}$ of $K_0$, the completion $\hat{K}_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}}$ gives rise to a local embedding problem. We denote the group of unity in $K$ by $\mu(K)$. In the spirit of Scholz–Reichardt, Neukirch proves that if the kernel $\ker(\alpha)$ of the epimorphism $\alpha : G \longrightarrow \mathrm{Gal}(K/K_0)$ is solvable, $\gcd(|\ker(\alpha)|, |\mu(K)|) = 1$, and each of the local embedding problems is weakly solvable, then the original embedding problem is properly solvable. For each prime $\mathfrak{p}$ of $K_0$ we identify $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ with a closed subgroup of $\mathrm{Gal}(K_0)$. Then, one may find a proper solution that coincides on $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ with a given local weak solution $\varphi_\mathfrak{p}$ for finitely many $\mathfrak{p}$'s. However, [2] gives no bound on the ramification of the proper solution. The results of [2] are generalized to the case of global fields in [3].

It is exactly the latter gap that our work intends to fill. To this end we recall that if $n = \prod_{i=1}^m l_i^{r_i}$ is a decomposition of a positive integer $n$ into a product of powers of distinct primes $l_1, \ldots, l_m$, then $\Omega(n) = \sum_{i=1}^n r_i$. The main result is the following.

**Theorem 1.** *Let $K/K_0$ be a finite Galois extension of global fields with Galois group $\Gamma = \mathrm{Gal}(K/K_0)$, and consider a finite embedding problem*

(1)
$$\begin{tikzcd} & & & \mathrm{Gal}(K_0) \arrow[d, "\rho"] & \\ 1 \arrow[r] & H \arrow[r] & G \arrow[r, "\alpha"] & \Gamma \arrow[r] & 1 \end{tikzcd}$$

*with a solvable kernel $H$. Suppose that*

- *(a)* $\mathrm{char}(K_0) \nmid |H|$, $\gcd(|H|, |\mu(K)|) = 1$, *and*
- *(b) for each prime $\mathfrak{p}$ of $K_0$, there exists a homomorphism $\psi_\mathfrak{p} : \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \longrightarrow G$ such that $\alpha \circ \psi_\mathfrak{p} = \rho|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$ (we call $\psi_\mathfrak{p}$ a local solution).*

*Let $T$ be a finite set of primes of $K_0$ that contains* $\mathrm{Ram}(K/K_0)$ *and for each $\mathfrak{p} \in T$ let $\varphi_\mathfrak{p}$ be a local solution. Then, there exists an epimorphism $\psi : \mathrm{Gal}(K_0) \longrightarrow G$ such that $\alpha \circ \psi = \rho$, and there exists a set of primes $R$ of $K_0$ with $R \cap T = \emptyset$ and $|R| = \Omega(|H|)$ that satisfies the following conditions:*

(1) *for each* $\mathfrak{p} \in T$ *there exists* $a \in H$ *such that* $\psi(\sigma) = a^{-1}\varphi_{\mathfrak{p}}(\sigma)a$ *for all* $\sigma \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$*;*

(2) *the fixed field* $N$ *in* $K_{0,\mathrm{sep}}$ *of* $\ker(\psi)$ *satisfies* $\mathrm{Ram}(N/K_0) \subseteq T \cup R$*, hence* $|\mathrm{Ram}(N/K_0)| \leq |T| + \Omega(|H|)$*.*

Note that if the short exact sequence in (1) splits, then the condition in Theorem 1 about the local solvability is automatically satisfied. Thus, in this case, Theorem 1 holds under the mere conditions that $H$ is solvable, $\mathrm{char}(K_0) \nmid |H|$, and $\gcd(|H|, |\mu(K)|) = 1$.

Also, we note that if $K = K_0$, $T = \emptyset$, and $|G| = l^n$, where $l$ is a prime number such that $l \neq \mathrm{char}(K)$ and $\zeta_l \notin K$, in Theorem 1, then we get a Galois extension $N$ of $K$ with Galois group $G$ such that $|\mathrm{Ram}(N/K)| \leq n$. This improves the estimate $|\mathrm{Ram}(N/K)| \leq n + r(K)$ of the main result of [1] mentioned above.

In a forthcoming work, we plan to remove the condition $\mathrm{char}(K_0) \nmid |H|$ from (a) of Theorem 1, keeping $\gcd(|H|, |\mu(K)|) = 1$ as the only condition on the solvable group $H$ in the theorem.

## References

[1] W. Geyer and M. Jarden, *Bounded realization of l-groups over global fields*, Nagoya Mathematical Journal **150** (1998), 13–62.

[2] J. Neukirch, *On solvable number fields*, Inventiones Mathematicae **53** (1979), 135–164.

[3] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, Heidelberg, Second Edition, corrected version 2.2, July 2015.

[4] J. P. Serre, *Topics in Galois Theory*, Jones and Barlett, Boston (1992).

## Faithful Realizability of Tropical Curves

Jennifer Park

(joint work with Man-Wai Cheung, Lorenzo Fantini, Martin Ulirsch)

A tropical curve is a balanced weighted 1-dimensional rational polyhedral complex. Any algebraic curve $C$ in a toric variety over a non-archimedean field $K$ can be "tropicalized" to obtain a tropical curve ([1]), denoted $\mathrm{Trop}(C)$.

It is then natural to ask which tropical curves can be realized as the tropicalization of an algebraic curve in toric varieties; this is known as the problem of realizability of tropical curves. In this talk, we study a refined version of this problem.

Let $T$ be the split algebraic torus, and let $T^{\mathrm{an}}$ be the non-archimedean analytic space associated to $T$ in the sense of [2]. Then one can define a continuous tropicalization map $\mathrm{trop} : T^{\mathrm{an}} \longrightarrow \mathbb{R}^n$ (for a suitable $n$), and the image of any algebraic curve $C$ (more precisely, its Berkovich analytification $C^{\mathrm{an}}$) in $T$ under this map agrees with $\mathrm{Trop}(C)$.

Furthermore, $C^{\text{an}}$ has the homotopy type of a finite metric graph ([2]); that is, there is a subset of $C^{\text{an}}$, denoted $\Sigma_C$, which is a deformation retract of $C^{\text{an}}$. This is called the skeleton of $C$.

Thus, given an embedding of $C$ into a toric variety $X$ with big torus $T$, we say that the corresponding tropicalization is *faithful* with respect to a skeleton $\Sigma_C$ if trop induces an isometric homeomorphism from $\Sigma_C \cap T^{\text{an}}$ onto its image in $\text{Trop}(C \cap T)$.

We study whether a given tropical curve $\Gamma$ in $\mathbb{R}^n$ can be realized as the tropicalization of an algebraic curve whose non-archimedean skeleton is faithfully represented by $\Gamma$. In this talk, we give an affirmative answer to this question for a large class of tropical curves that includes all trivalent tropical curves, but also many tropical curves of higher valence. Our approach is based on a combination of the theory of toric schemes over discrete valuation rings and logarithmically smooth deformation theory, expanding on a framework introduced by Nishinou and Siebert.

## References

[1] W. Gubler, *The Bogomolov conjecture for totally degenerate abelian varieties*, Inventiones Mathematicae **169** (2007), 377–400.

[2] V. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Mathematical Surveys and Monographs **33** (1990).

# Group realization and embedding problems in differential Galois theory

David Harbater

(joint work with Annette Bachmayr, Julia Hartmann, Florian Pop, Michael Wibmer)

## 1. Introduction and background

This talk presents analogs in differential Galois theory of results in usual Galois theory over a rational function field $F = k(x)$. These results concern the inverse Galois problem, solutions to embedding problems, and the structure of absolute Galois groups. The results presented here appear in a series of joint papers with overlapping authors, as indicated below.

*Prior results in usual Galois theory*

Concerning the inverse Galois problem, if $k$ is algebraically closed then every finite group is a Galois group over $k(x)$. This was shown in characteristic zero in [7]; and in positive characteristic in [8], by deducing this from the corresponding assertion for $K(x)$ with $K = k((t))$ (which in turn was proven using patching).

Embedding problems concern how Galois extensions fit together, and their solvability provides structural information about the absolute Galois group. Generalizing the above inverse Galois assertion, it was shown in [14] that every finite split embedding problem over $K(x)$ is solvable if $K$ is any large (ample) field, by first proving this in the special case that $K$ is a Laurent series field. In the special case of $K$ being algebraically closed, it holds even without assuming splitness.

In [9] and [13], it was shown that if $k$ is any algebraically closed field, then the absolute Galois group $\mathrm{Gal}(k(x))$ is a free profinite group of rank equal to the cardinality of $k$ (generalizing the characteristic zero case, shown in [5]). The countable case relied on a theorem of Iwasawa ([11]) that gives a criterion for freeness in terms of solvability of embedding problems; and the uncountable case relied on a related result of Melnikov and Chatzidakis (see [12]).

*Differential Galois theory*

Differential Galois theory is an analog of usual Galois theory for linear ordinary differential equations. Let $(F, \partial)$ be a differential field of characteristic zero; e.g., $F = k(x)$, $\partial = \frac{d}{dx}$. The *field of constants* of $F$ is $C_F := \{a \in F \mid \partial a = 0\}$ (and similarly for a differential ring). A linear differential equation of order $n$ over $F$ can be written in the form $y' = Ay$, where $y$ is the transpose of $(y_1, \dots, y_n)$ and $A$ is an $n \times n$ matrix over $F$. An analog of a splitting field is a *Picard–Vessiot (PV) ring* $R$ containing $F$. This is a differential ring containing $n$ linearly independent solutions $(y_1, \dots, y_n)$ to the differential equation, forming an $n \times n$ invertible matrix $Y$ whose entries, together with $\det(Y)^{-1}$, generate $R$ over $F$; such that $R$ is differentially simple; and such that $C_R = C_F$. There is an associated differential Galois group $\mathrm{Gal}_\partial(R/F)$, which is a linear algebraic group contained in $\mathrm{GL}_{n,F}$. The differential inverse Galois problem over $F$ asks if every linear algebraic group over $F$ is the differential Galois group of a Picard–Vessiot ring over $F$. This was shown to hold for $\mathbb{C}(x)$ in [15]; and following work by a number of authors in special cases, it was shown for $k(x)$ with $k$ any algebraically closed field of characteristic zero in [10].

Motivated by the above results in usual Galois theory, we can ask about differential Galois realization over $F = k(x)$ for $k$ a Laurent series field, or more generally a large field. We can also ask if (split) differential embedding problems over $F$ have solutions; and if the absolute differential Galois group of $F$ is free if $k$ is algebraically closed. We discuss these questions below.

## 2. Differential inverse Galois problem

We showed in [1] that if $K = k((t))$ has characteristic zero, then every linear algebraic group over $K$ is a differential Galois group over $K(x)$ with respect to $\partial = \frac{d}{dx}$. The proof involved the patching of differential modules. As in usual Galois theory, the argument involves solving the problem locally for certain subgroups $H_1, \dots, H_r$ of the given group $G$. Instead of just using finite cyclic groups as in usual Galois theory, the argument here also uses subgroups of the form $\mathbb{G}_a$ and $\mathbb{G}_m$; after enlarging $K$, the group $G$ is generated by such subgroups and finite cyclic groups, and we then descend back to $K$.

Drawing on this, we showed in [4] that if $k$ is a large field of infinite transcendence degree over $\mathbb{Q}$, then every linear algebraic group $G$ over $k$ is a differential Galois group over $(k(x), d/dx)$. The proof begins by observing that $G$ is induced by a linear algebraic group $G_0$ over a finitely generated field $k_0/\mathbb{Q}$. The Laurent series case implies that $(G_0)_K$ is a differential Galois group over $K(x)$, where

$K = k_0((t))$. The associated PV ring $R$ is then induced by a Picard–Vessiot ring $R_1$ over $k_1(x)$ for some finitely generated field extension $k_1/k_0$ with $k_1 \subset K$. By the hypotheses on $k$, [6, Theorem 1, Lemma 4] implies there is a $k_0$-embedding $k_1 \hookrightarrow k$; and then $R_1 \otimes_{k_1} k$ is the desired PV ring over $k(x)$.

### 3. Differential embedding problems

A *differential embedding problem* over a differential field $F$ consists of a surjection $G \to H$ of linear algebraic groups over $K = C_F$ together with a PV ring $R$ for $H$ over $F$. A *solution* consists of a PV ring for $G$ over $F$ into which $R$ embeds compatibly. In [2], we proved that every differential embedding problem over $\mathbb{C}(x)$ has a solution, using patching in the complex topology.

As in usual Galois theory, one would also like to know that if $K$ is large (of characteristic zero), then split differential embedding problems over $F = K(x)$ (i.e., those for which $G \to H$ has a section) have solutions. Following the strategy in usual Galois theory, to prove this one would first like to prove the special case that the constant field $K$ is a Laurent series field $k((t))$. Actually, to carry out this strategy, it suffices to prove the result for linear algebraic groups over $k$ (rather than over $K$). We proved that case in [3], by using results in [2] that make it possible to use patching to solve split differential embedding problems over Laurent series fields. Then, in [4], this Laurent case was used to prove the desired assertion for $F = K(x)$ where $K$ is a large field of infinite transcendence degree over $\mathbb{Q}$; this built not just on the Laurent case and the strategy from usual Galois theory, but also on the ideas in [4] that were used to solve the differential inverse problem.

### 4. Absolute differential Galois groups: freeness

A differential analog of the Galois closure of a field is the *universal Picard–Vessiot* ring over a differential field $(F, \partial)$; this is a minimal differential extension of $F$ that has the same constant field and such that every linear differential equation has a fundamental solution matrix $Y$ with coefficients in the ring (though the ring is not differentially closed). Associated to this ring is the *universal* (or *absolute*) differential Galois group of $F$; this is a pro-algebraic group $\Gamma_F$. (See [16, Section 4.3], which considers the fraction field of the universal Picard–Vessiot ring.) Usual Galois theory suggests that $\Gamma_F$ is free (in an appropriate sense) if $F = k(x)$ and $\partial = d/dx$, for $k$ algebraically closed (of characteristic zero).

This problem is considered in current joint work with A. Bachmayr, J. Hartmann, and M. Wibmer. We call a pro-algebraic group $\Gamma$ over a field $k$ *free* on a *generating set* $X$ if there is a map $X \to \Gamma(k)$ satisfying a universal mapping property: for every linear algebraic $k$-group $G$ and every map $X \to G(k)$, there is a unique homomorphism $\Gamma(k) \to G(k)$ such that the associated triangle commutes. We have an analog of the result of Iwasawa mentioned above: If $\Gamma$ is a pro-algebraic $k$-group of countably infinite rank, and if every differential embedding problem for $\Gamma$ (with respect to a surjection of linear algebraic $k$-groups) is solvable, then $\Gamma$ is free. Applying this to the previous result about embedding problems over large fields, we obtain that if $k$ is algebraically closed of countably infinite transcendence degree over $\mathbb{Q}$, then the absolute differential Galois group of $k(x)$ is the free pro-algebraic group over $k$ of countable rank.

*Acknowledgment*: The speaker was supported in part by NSF Grant DMS-1463733.

## References

[1] Annette Bachmayr, David Harbater, and Julia Hartmann. Differential Galois groups over Laurent series fields. Proc. London Math. Soc. (3) **1**12 (2016), 455–476.

[2] Annette Bachmayr, David Harbater, Julia Hartmann, and Michael Wibmer. Differential embedding problems over complex function fields. 2016 manuscript, to appear in Documenta Mathematica. Available at arXiv:1610.09336.

[3] Annette Bachmayr, David Harbater, and Julia Hartmann. Differential Embedding Problems over Laurent series fields. 2017 manuscript. Available at arXiv:1710.02502.

[4] Annette Bachmayr, David Harbater, Julia Hartmann, and Florian Pop. Large Fields in Differential Galois Theory. 2017 manuscript. Available at arXiv:1710.03183.

[5] Adrien Douady. Détermination d'un groupe de Galois. C.R. Acad. Sci. Paris **2**58 (1964), 5305–5308.

[6] Arno Fehm. Embeddings of function fields into ample fields. Manuscripta Math. **1**34 (2011), 533–544.

[7] Alexander Grothendieck. Revêtements étales et groupe fondamental (SGA 1). Lecture Notes in Math., vol. 224, Springer, Berlin, 1971.

[8] David Harbater. Mock covers and Galois extensions. J. Algebra, **9**1 (1984), 281–293.

[9] David Harbater. Fundamental groups and embedding problems in characteristic p. In: Recent developments in the inverse Galois problem (M. Fried, et al., eds.), AMS Contemporary Mathematics Series, vol. 186, 1995, 353–369.

[10] Julia Hartmann. On the inverse problem in differential Galois theory. J. reine angew. Math. **5**86 (2005), 21–44.

[11] Kenkichi Iwasawa. On solvable extensions of algebraic number fields. Annals of Math. **5**8 (1953), 548–572.

[12] Moshe Jarden. On free profinite groups of uncountable rank. In: Recent developments in the inverse Galois problem (M. Fried, et al., eds.), AMS Contemporary Mathematics Series, vol. 186, 1995, 371–383.

[13] Florian Pop. Étale Galois covers of affine smooth curves. Invent. Math., **1**20 (1995), 555–578.

[14] Florian Pop. Embedding problems over large fields. Ann. Math., **1**44 (1996), 1–34.

[15] Carol Tretkoff and Marvin Tretkoff, Solution of the inverse problem of differential Galois theory in the classical case, Amer. J. Math. **1**01 (1979), 1327–1332.

[16] Marius van der Put. Galois theory and algorithms for linear differential equations. Journal of Symbolic Computation **3**9 (2005), 451–463.

## A Geometric Approach to Computing Galois Groups of Function Fields

Alexei Entin

Part of the work presented in the lecture can be found in [8].

Let $k$ be a field and let $a_1, \dots, a_n$ be a set of $n$ independent variables over $k$. Denote $K = k(a_1, \dots, a_n)$. Given an explicit finite separable extension $L/K$, a natural problem is to compute the Galois group of its Galois closure. Many instances of this problem have been studied in the past. For example in the 70's, Uchida [10], Smith [9] and S. D. Cohen [6] have studied the Galois groups of (extensions defined by) trinomials of the form $t^n + a_1 t^m + a_2$ and some further generalizations.

There has been renewed interest in this problem over the last decade since computing a Galois group as above has become a central tool in studying decomposition statistics in function fields over $\mathbf{F}_q$ in the $q \to \infty$ regime (e.g. in proofs of the analogues of the classical Hardy–Littlewood and Bateman–Horn conjectures in this setting). Many special instances of the above general problem have been solved by several authors including Bank, Bary-Soroker, Carmon, Gorodetsky, Entin, Fehm, Jarden, Karidi, Rosenzweig and others as part of this program [3][5] [2][7][4][1].

We present an extremely general method for computing Galois groups of a certain class of extensions which generalizes all of the results referred to above. Our method is based on a geometric reinterpretation of the problem.

For simplicity assume that $k$ is algebraically closed (usually it isn't difficult to pass from this to the general case). Let $C$ be a smooth projective curve over $k$, possibly reducible with connected components $C_1, \dots, C_m$ and let $f_1, \dots, f_n$ be elements of the ring

$$k(C) \coloneqq \bigoplus_{i=1}^{m} k(C_i)$$

(they can be viewed as algebraic functions defined on $C$). Extending the base field from $k$ to $K = k(a_1, \dots, a_n)$, we may consider the element

$$f = 1 + a_1 f_1 + \ldots + a_n f_n \in K(C)$$

and its divisor of zeros $\mathrm{div}(f)_0$. Assume that the residue fields of points appearing in $\mathrm{div}(f)_0$ are all separable extensions of $K$. Let $L$ be the Galois closure of their compositum. Under some fairly mild assumptions which are usually not hard to verify we will compute $\mathrm{Gal}(f) \coloneqq \mathrm{Gal}(L/K)$. All of the Galois groups appearing in the work referred to above are special cases of this problem.

We accomplish this by viewing the problem more geometrically. Consider the rational map $\phi : C \to \mathbf{P}^n$ defined by $x \mapsto (1 : f_1(x) : \ldots : f_n(x))$, which can be extended to a morphism. Let $C' = \phi(C)$ be its image. It turns out that computing the group $\mathrm{Gal}(f)$ is equivalent to computing the monodromy of hyperplane sections of $C'$ pulled back to $C$, which we denote by $\mathrm{Mon}(C)$. Our main result is the following, which for simplicity we only state in the irreducible case and in a form useful only if $\mathrm{char}(k) \neq 2$.

**Theorem 1.** *Assume that $C$ is irreducible. Assume further that $C'$ is a reflexive curve in $\mathbf{P}^n$ and that the Galois group $G$ of (the Galois closure of) the extension $k(C)/k(C')$ is generated by the inertia groups of ramification points of the map $C \to C'$ lying over smooth or nodal points of $C'$. Then* $\mathrm{Mon}(C) \cong G \wr S_d$, *where $d = \deg C'$ (we denote by $\wr$ the permutational wreath product).*

Among the new applications of this result is a proof of a Chebotarev density theorem in short intervals over $\mathbf{F}_q[t]$ in the $q \to \infty$ limit (with fixed degrees). This has been recently established by Bary-Soroker, Gorodetsky and Karidi in the case of extensions with solvable Galois group (we remove the solvability restriction).

## References

[1] E. Bank, L. Bary-Soroker, A. Fehm, *Sums of two squares in short intervals in polynomial rings over finite fields*, Amer. J. Math., vol. 140 no. 4 (2018), pp. 1113-1131.

[2] E. Bank, L. Bary-Soroker, L. Rosenzweig, *Prime polynomials in short intervals and in arithmetic progressions*, Duke Math. J., vol. 164 no. 2 (2015), pp. 277-295.

[3] L. Bary-Soroker, *Irreducible values of polynomials*, Adv. in Math., vol. 229 no. 2 (2012), pp. 854 - 874.

[4] L. Bary-Soroker, A. Fehm, *Correlations of sums of two squares and other arithmetic functions in function fields"*, IMRN, rnx250 (2017), https://doi.org/10.1093/imrn/rnx250.

[5] L. Bary-Soroker, M. Jarden, *On the Bateman–Horn conjecture about polynomial rings*, Munster J. Math, vol. 5(2012), pp. 41-58.

[6] S. D. Cohen, *The Galois group of a polynomial with two indeterminate coefficients*, Pacific J. Math., vol. 90 no. 1 (1980), pp. 63-76.

[7] A. Entin, *On the Bateman-Horn conjecture for polynomials over large finite fields*, Comp. Math., vol. 152 no. 12 (2016), pp. 2525-2544.

[8] A. Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, arXiv:1805.05454 [math.NT].

[9] J. H. Smith, *General trinomials having symmetric Galois Group*, Proc. Amer. Math. Soc., vol. 63 no. 2 (1977), pp. 208-212.

[10] K. Uchida, *Galois group of an equation $X^n - aX + b$*, Tohoku Math J. (2), vol. 22 no. 4 (1970), pp. 670-678.

## Computing $\ell$-adic Monodromy Groups

David Zywina

Consider an abelian variety $A$ of dimension $g \geq 1$ defined over a number field $K$. For a prime $\ell$, define

$$V_\ell = \Big(\varprojlim_{e} A[\ell^e]\Big) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

where $A[\ell^e]$ is the group of $\ell^e$-torsion in $A(\overline{K})$. It is a $\mathbb{Q}_\ell$-vector space of dimension $2g$ with a natural action of $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$. We express this action in terms of a Galois representation

$$\rho_\ell : \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell) = \mathrm{GL}_{V_\ell}(\mathbb{Q}_\ell).$$

The $\ell$-adic monodromy group $G_\ell$ is the Zariski closure of $\rho_\ell(\mathrm{Gal}_K)$ in $\mathrm{GL}_{V_\ell}$. For simplicity, assume that all the $G_\ell$ are connected. We describe a way to compute $G_\ell$ under several well-known conjectures.

Our main result is that, under two conjectures (Mumford–Tate and $A$ has ordinary reduction at most primes), given "random" primes $\mathfrak{p}$ and $\mathfrak{q}$, the Frobenius polynomials $P_\mathfrak{p}(x)$ and $P_\mathfrak{q}(x)$ determine the group $G_\ell$ and its representation $V_\ell$, up to isomorphism, for all sufficiently large $\ell$.

The group $G_\ell$ and its representation are described in terms of a root datum and an action of $\mathrm{Gal}_{\mathbb{Q}_\ell}$ on it. Unconditionally, computing $G_\ell$ requires proving the existence of certain algebraic cycles.

## Prehistory of Field Arithmetic

Wulf-Dieter Geyer

The organizers of this conference, all of whom I thank for the invitation, asked me to give a report about how our area, the Field Arithmetic, started. There is no canonical way to describe this and any talk about this will be personal and given from a special point of view. So I apologize from the beginning that I will leave out important people and important lines of development. I will just restrict to give my way of looking at this theme and hope to give at least one answer to the question posed by the organizers.

Answering the question would be simpler if I modify and restrict the question to a view at the eight conferences which until today were hosted at the Mathematische Forschungsinstitut Oberwolfach under the name "Field Arithmetic", the first one having taken place 21–27 of October 1990. Such a procedure would miss the point about "prehistory", so I will stop long before this date. But I will mention the fact that several types of Oberwolfach conferences gave space for problems which can be included in the body of Field Arithmetic. For me the most important one in this respect is the conference on Algebraic Number Theory. The first time I participated at this conference was in the year 1964, when Hasse, Roquette, Leopoldt, Kneser, Zassenhaus, Cassels, Fröhlich, Néron were among the senior members, but also Shafarevich, Kostrikin, Koch and some other people from the Eastern Bloc took part which were not allowed to come for the next decades to Oberwolfach. These people were open minded for neighbouring disciplines as the title of my talk "On Galois cohomology of Jacobians" shows. In the following years, slowly, step by step, people came to this conference who in the year 1990 started their own conference "Field Arithmetic".

"Field Arithmetic" is an interaction between different mathematical topics with different histories. To speak about prehistory of "Field Arithmetic" I also have to have a look at the history of these topics, given in the following list:

**1. Arithmetic:** This is one of the oldest parts of mathematics. I have no time to say anything about its history.

**2. Theory of fields:** This topic started with the paper of **Steinitz** from 1912.

**3. Galois theory:** This topic arises from the study of polynomial equations in one variable over a field. I will just mention three important facts from the 19th century history of this area:

**Gauss** computed in 1801 the Galois group of the maximal cyclotomic extension of the rationals as the unit group of the adic completion of the integers (expressed in modern language). His aim was to decide which regular $n$-gons can be constructed by ruler and compass and give explicit constructions if possible.

**Galois** died in 1832 and developed the notion of groups, solvable groups and the Galois group of a polynomial. His aim was to decide which polynomials can be reduced to pure equations, i.e. can be solved by just taking roots and rational operations. Only 12 years after his death this was published, and it took at least the same time until the importance of his ideas become clear to the mathematicians in Europe.

**Hilbert** published in 1892 his irreducibility theorem, showing e.g. that the Galois group of a separable polynomial in one variable over $\mathbb{Q}(t)$ remains (with probability one) the same over $\mathbb{Q}$ after specializing $t$ to an integer. Several talks at this conference bear witness that this fact is one of the corner stones of Field Arithmetic. Hilbert used it to show that the symmetric and alternating groups are Galois groups over $\mathbb{Q}$, in this way starting the Inverse Galois Problem.

**4. Algebraic Geometry:** This topic arises from the study of polynomial equations in several variables over a field. It started in the 19th century with base field $\mathbb{C}$.

**5. Model theory:** A part of mathematical logic which began to bloom in the mid of the 20th century.

**6. Arithmetical Algebraic Geometry:** A child of Arithmetic and Algebraic Geometry, stimulated essentially by the work of **Grothendieck**. This wide area is closely related to Field Arithmetic with another focus, but since it is not involved in the beginning of Field Arithmetic, it is out of my talk.

The prehistory of Field Arithmetic is strongly connected to an earlier interaction between Algebraic Geometry and Model theory, called **Elimination theory**. This was started at the end of the 19th century, the aim was to look for a procedure to solve systems of polynomial equations over $\mathbb{C}$ by quantifier elimination. Some of the pioneers were:

**Kronecker** who published in 1882 a general program which some people consider as a first glimpse into Grothendieck's world of schemes.

**Macaulay** who wrote in 1916 a book on the ideal theory of polynomial rings, which was the base of later work of E. Noether, Krull and others.

**Emmy Noether** whose most important impulse for Field Arithmetic was her irreducibility theorem from 1922 about the reduction of the coefficients of absolutely irreducible polynomials, an easy consequence of elimination theory over algebraically closed fields.

**Grete Hermann** who started in 1925 under E. Noether the algorithmical treatment of Algebraic Geometry using results of Macaulay and Noether[1].

That this area, the elimination theory, can be viewed from a totally different point of view, was made clear by Alfred **Tarski**, an eminent logician of the 20th century, in his booklet

*A decision method for elementary algebra and geometry*

which should appear in 1939 in Paris, but because of the war (Tarski just by chance escaped the holocaust) only a second improved edition appeared in 1951. In this booklet, Tarski showed that the (elementary) theory of real closed fields

[1] To the celebration of Emmy Noethers 100th birthday in 1982 at her birthplace Erlangen I could get van der Waerden to give a nice talk about his teacher. Unfortunately G. Hermann, only a little older than van der Waerden, could not come because of health problems. Both women, Noether and Hermann, are fascinating characters.

is complete and has a quantifier elimination in the language of ordered fields. In the appendix, he claims that the same is true (in the language of fields) for algebraically closed fields of given characteristic. In particular, these theories are decidable.

Tarski's ideas were put into a nice frame of concepts by A. **Robinson** in his book *Complete Theories* in 1956, and its successor in 1963. James **Ax** and Simon **Kochen** used his concepts to give a totally new example of fields which are decidable due to a quantifier elimination. These are the $p$-adically closed fields, the fields elementarily equivalent to Hensel's field $\mathbb{Q}_p$ of $p$-adic numbers. They could show that the theory is axiomatizable and decidable by a quantifier elimination in an appropriate language. Their starting point was a simple diophantine problem, a conjecture of E. Artin: If $f \in \mathbb{Q}_p[X_1, \ldots, X_n]$ is a form of degree $d$ in $n > d^2$ variables, then $f$ has a nontrivial zero in $\mathbb{Q}_p^n$. This is true over the analoguous power series field $\mathbb{F}_p((t))$, and for $d = 2$ it is a classical theorem about quadratic forms. Although the conjecture turned out to be false, Ax–Kochen could show that it is almost true: For each $d$ there is a constant $p(d)$ such that the conjecture is true for all prime numbers $p > p(d)$. They proved this by showing that the nontrivial ultra products of the $\mathbb{Q}_p$ resp. the $\mathbb{F}_p((t))$ are elementarily equivalent. This paper in three parts (1965/66) contains more such results which made clear that model theoretic methods can be important for algebraic and arithmetic questions.

### Towards Field Arithmetic

In 1967, **Ax** published as forerunner of his 1968 paper, which proved that the theory of finite fields is decidable, the paper

*Solving diophantine problems modulo every prime.*

Here he showed that the nontrivial ultraproducts

$$K = \prod_p \mathbb{F}_p \,/\, \mathcal{D}$$

are PAC fields [2]. The algebraic part $K \cap \tilde{\mathbb{Q}}$ determines $\mathcal{D}$, it is the fixed field $\tilde{\mathbb{Q}}(\sigma)$ of a single automorphism $\sigma$ of $\tilde{\mathbb{Q}}$, but not always PAC.

At that time Moshe Jarden was looking at the Hebrew University in Jerusalem for a PhD subject. When he came to Hillel Fürstenberg, he was asked to give a presentation of this paper of Ax. Then Fürstenberg asked him if Ax's example of a non-PAC field $\tilde{\mathbb{Q}}(\sigma)$ was an exception or if this happens often.

In 1969, Moshe finished his PhD thesis under Fürstenberg, combining Ax's ideas with Hilbert's irreducibility theorem. It contains two main results:

(1) Let $\sigma = (\sigma_1, \ldots, \sigma_e) \in G_{\mathbb{Q}}^e$ be an $e$-tuple of automorphisms of $\tilde{\mathbb{Q}}$. Then the fixed field $\tilde{\mathbb{Q}}(\sigma) = \bigcap \tilde{\mathbb{Q}}(\sigma_i)$ of $\sigma$ in $\tilde{\mathbb{Q}}$ is PAC up to exceptional $\sigma$'s which form a set of measure 0 in the compact group $G_{\mathbb{Q}}^e$.

[2] The name "pseudo algebraically closed" was coined by Moshe and appeared first in a paper of G. Frey in 1973.

(2) Let $E$ be a statement about rings, let $\mu$ be the Haar measure of the Galois group $G_{\mathbb{Q}}$ and let $\delta$ be the Dirichlet density on the set $\mathbf{P}$ of prime numbers. Then

$$\mu\{\sigma \in G_{\mathbb{Q}}\,;\; \tilde{\mathbb{Q}}(\sigma) \models E\} \;=\; \delta\{p \in \mathbf{P}\,;\; \mathbb{F}_p \models E\} \;\in \mathbb{Q}\,.$$

Then Moshe had to look for a postdoc position. He got no offer from American universities, but in England he got offers from Cassels, Fröhlich and Birch, in Germany offers from Hirzebruch, Neukirch and Roquette (Heidelberg). Moshe's teacher A. Robinson suggested to go to Heidelberg because there is some Geyer with similar mathematical interests. Robinson knew me from his stays in Tübingen and in Heidelberg. So, in September 1971, Moshe came to Heidelberg. But at that time I already had a call to Erlangen and in February 1972 I had my first permanent position there. Moshe stayed in Heidelberg and profited a lot by the ken of my teacher Roquette.

The distance did not prevent a cooperation. In 1973, we proved that varieties $V$, $\dim V > 0$, over $\mathbb{Q}(\sigma)$ for most $\sigma \in G^e_{\mathbb{Q}}$ do not only have infinitely many rational points, but $V(\tilde{\mathbb{Q}}(\sigma))$ is dense in $V(\tilde{\mathbb{Q}})$ for a given topology. This result was several times improved, the final result was given by Kollár (2006) saying that for any PAC field $K$ the set $V(K)$ is dense for every valuation topology.

In 1977, we wrote a paper named *Torsion of elliptic curves over* $\tilde{\mathbb{Q}}(\sigma)$ which again had lots of successors, the final version is still open.

Now another important figure on the way towards "Field Arithmetic" appeared. Michael Fried, who in 1973 gave a report about Moshe's thesis in the Mathematical Reviews, wrote in 1974 together with G. Sacerdote the paper *Solving diophantine problems over all finite fields* where they improved the Ax papers from 1967/68, giving a primitive recursive decision method for the theory of all finite fields. They replaced Ax's logical methods which only give a recursive decision procedure, by an explicit quantifier elimination by Galois stratification. Moshe was a referee of this paper which appeared in 1976. The cooperation between Moshe and Mike had already begun, in 1975 they showed an improvement of the cited density result of Geyer–Jarden. More important was their joint paper *Diophantine properties of subfields of* $\tilde{\mathbb{Q}}$ from 1976. Here they proved that for any function field $F/K$ of one variable in characteristic 0, $F$ linearly disjoint from $\tilde{K}$ over $K$, there is a $t \in F$ with $[F : K(t)] = n$ for some $n$ such that the Galois group of the normal closure of $F\tilde{K}$ over $\tilde{K}(t)$ is the symmetric group $S_n$. To prove this "stability" result in prime characteristic several papers were written until the final result was done by K. Neumann in a PhD thesis in Erlangen 1996. Using this result Mike and Moshe found in 1976 a new PAC-subfield $K$ of $\tilde{\mathbb{Q}}$, Galois over $\mathbb{Q}$. More precisely the Galois group of $K$ over $\mathbb{Q}$ is an infinite product of finite groups, which implies that $K$ is Hilbertian. From these facts follows (by a later result of Fried–Völklein) that the absolute Galois group of $K$ is the free profinite group of countable rank. The "construction" of $K$ was done by Zorn's lemma. Recently, A. Razon, Moshe and I gave a canonical Galois Hilbertian PAC subfield $K$ of $\tilde{\mathbb{Q}}$, the compositum of all symmetric extensions of $\mathbb{Q}$, such that the Galois group of $\tilde{\mathbb{Q}}/K$ is again free of countable rank, and the Galois group of $K/\mathbb{Q}$ is free of countable rank with respect to the smallest formation of finite groups, containing the symmetric groups.

In 1979, Moshe was for a longer period in Irvine together with Mike. Mike suggested that they should write a book together about Galois stratification, containing all necessary prerequisites: from Galois theory and Profinite Groups, Arithmetic (including curves over finite fields and Čebotarev's density theorem), Algebraic Geometry, Mathematical Logic, Model Theory and Nonstandard Structures, Field Theory (especially Hilbertian Fields), Measure Theory and so on. Mike had already a title for the book: "Field Arithmetic". Here ends the prehistory of "Field Arithmetic", the book was finished in 1986.

## Problem Session

**Question 1** (Lior Bary-Soroker)**.** Consider the set $M_n = \{f = X^n + \sum_{i=0}^{n-1} \pm X^i\}$ of size $2^n$. Can we prove that

$$\#\{f \in M_n \ : \ \mathrm{disc}(f) \text{ is a square}\} = o(1) \text{ as } n \to \infty?$$

It is allowed to replace ±1 by $\{1, \dots, 210\}$, or by any finite set. If the set contains 0, add a restriction that the free coefficient is non-zero. Currently nothing is known about this.

**Question 2** (Lior Bary-Soroker)**.** Motivation: minimal ramification problem (variant of the inverse Galois problem). Let $G$ be a finite group and let $m(G)$ be the minimal $m$ such that there exists a $G$-Galois extension $N/\mathbb{Q}$ with $\leq m$ ramification points ($\mathbb{C}/\mathbb{R}$ is considered ramified). For an abelian group $G$, we known the answer from the Kronecker-Webber theorem: $m(G) = d(G) :=$ minimal number of generators. This yields the general lower bound $m(G) \geq d(G/[G,G])$.

**Conjecture** (Boston–Markin)**.** *If $G \neq 1$, then $m(G) = \max\big(d(G/[G,G]), 1\big)$.*

Not a lot is known about this conjecture. If we restrict to $p$-groups, then Kisilevsky, Neftin, and Sonn proved the conjecture for semi-abelian $p$-groups, i.e, groups that can be constructed inductively by taking semi-direct products with abelian $p$-groups.

(1) Let $G$ be a group such that $\#G = p^n$ for some odd prime $p$ and such that $G$ is exactly 2-generated ($G$ general, $n$ large). We know by the Scholz–Reichardt method that $2 \leq m(G) \leq n - 1$. Can we improve the upper bound to $O(1)$?

(2) Let $G = A_5 \times \ldots \times A_5$ ($n$ copies). The best upper bound known is $m(G) \leq n + O(1)$ due to Bary-Soroker and Schlank, while the conjecture says that $m(G) = 1$. Is the conjecture true in this case?

**Question 3** (Danny Neftin)**.** Given $C_1, \dots, C_{m(G)+r}$ conjugacy classes of cyclic subgroups generating a finite group $G$, is there an extension $L/\mathbb{Q}$ which is tame with Galois group $G$ and inertia groups $C_1, \dots, C_{m(G)+r}$?

In this question, $G$ can be any finite group, so it subsumes the inverse Galois problem. Moreover, a positive answer implies a positive answer to a weaker question asked by Birch in the 1990's: If $G$ is realizable over $\mathbb{Q}$, is it tamely realizable? An affirmative answer to Birch's question is known for solvable groups and some simple groups.

**Question 4** (Florian Pop)**.** Can we realize every finite $p$-group as a *regular* Galois group $\mathrm{Gal}(K/\mathbb{Q}(t))$ where $K \cap \overline{\mathbb{Q}} = \mathbb{Q}$?

Apparently, there are results over $\mathbb{Q}^{\mathrm{ab}}(t)$ in a PhD thesis, according to Danny Neftin. By Kummer theory, regular realizability of abelian groups is known, e.g., over $\mathbb{F}_p(t)$ but not over $\mathbb{Q}(t)$. David Harbater remarks that the statement is known for all semi-abelian groups, so for all $G$ with $\#G < 64$.

**Question 5** (Florian Pop)**.**

(1) Find a smooth projective curve $X$ over $\mathbb{Q}^{\mathrm{ab}}$ such that $X(\mathbb{Q}^{\mathrm{ab}})$ is nonempty finite.

(2) Find a smooth projective curve $X$ over $\mathbb{Q}^{\mathrm{solv}}$ such that $X(\mathbb{Q}^{\mathrm{solv}})$ is nonempty finite.

**Question 6** (Adam Topaz)**.** Let $g \geq 2$, $\Sigma_g = \langle a_1, b_1, \dots, a_g, b_g \mid \prod_{i=1}^{g} [a_i, b_i] = 1 \rangle$.

(1) Does there exist a field $F$ such that $\mathrm{Gal}(F) \cong \hat{\Sigma}_g$ (profinite completion)?

(2) Does there exist a field $F$ of $\mathrm{char}(F) \neq p$ such that $\mathrm{Gal}(F)(p)$ is the pro-$p$ completion of $\Sigma_g$?

Motivation: this group satisfies the (analogue of the) Bloch–Kato conjecture, i.e. there are no cohomological obstructions. (Yet, Adam Topaz expects the answer to be no in both cases.) Part (2) is connected to the elementary type conjecture (which is only known for $p = 2$), also pointing to the answers 'no', according to Ido Efrat. In particular, the cyclotomic character should be nontrivial.

**Question 7** (Jochen Koenigsmann)**.** Is there a projective profinite group $G$ which is decidable but which has an open subgroup $H$ which is undecidable? Here, decidable means in the sense of limits of finite quotients. Projective means cohomological dimension 1, or equivalently, embeddable in a free group. For non-projective groups, there may already be an example.
Motivation: for abelian torsion-free groups, the answer is 'no' by using invariants. Do such invariants exist for projective groups? For finitely generated groups, the answer is also 'no'. It will help to find a PAC field which is decidable and has an undecidable finite extension (but the two statements are not equivalent).

**Question 8** (Florian Pop)**.** One can prove that if $X_g$ is a smooth projective curve over $\mathbb{C}$, then $\pi_1^{\mathrm{alg}}(X_g) \cong \hat{\Sigma}_g$, notation as above. Can this result be proved with algebraic methods?

So far, the cohomology of $\hat{\Sigma}_g$ can only be computed by comparison results. More generally, for an affine curve $X_g \supseteq U = X_g \setminus \{x_1, \dots, x_r\}$, we have the fundamental group $\pi_1^{\mathrm{alg}}(U) \cong \hat{\Sigma}_{g,r} \twoheadrightarrow \hat{\Sigma}_g$ where

$$\Sigma_{g,r} = \Big\langle a_1, b_1, \ldots, a_g, b_g, c_1, \ldots, c_r \mid \prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{r} c_j = 1 \Big\rangle,$$

and the $c_i$ are inertia generators. Can we prove this isomorphism with algebraic methods?

Special cases of special interest are: for $U = \mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}$, prove

$$\pi_1^{\mathrm{alg}}(U) = \langle c_0, c_1, c_\infty \mid c_0 c_1 c_\infty = 1 \rangle^\wedge$$

using algebraic methods. Or, for $U = X_2$, prove

$$\pi_1^{\mathrm{alg}}(U) \cong \hat{\Sigma}_2 = \langle a_1, b_1, a_2, b_2 \mid \prod_{i=1}^{2} [a_i, b_i] = 1 \rangle^\wedge$$

with algebraic methods.

**Question 9** (David Harbater)**.** We have $\pi_1^{\mathrm{top}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}) = F_2 = \langle a, b \rangle$. For any finite $G \twoheadleftarrow F_2$ with generators $a, b$, consider the $G$-cover $Z \to \mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}$. By Grothendieck, we can replace $\mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}$ by $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}$, hence by the curve $\mathbb{P}^1_K \setminus \{0, 1, \infty\}$ for some number field $K/\mathbb{Q}$. Can you determine $K$ (as a field of definition or the field of moduli of the cover)? Richard Parker had a conjecture about this: $K$ should be generated over $\mathbb{Q}$ by the eigenvalues of the linear operator on the group ring $\mathbb{Q}[G \times G]$ (viewed as a $\mathbb{Q}$-vector space) given by left multiplication by the element $\displaystyle\sum_{g \in G} (g^{-1} a g, g^{-1} b g) \in \mathbb{Q}[G \times G]$. Bjorn Poonen remarks that by computability theory, there is a computer algorithm to find a field of definition that is recursive (though not necessarily primitive recursive). But there is the question of whether there is an explicit formula (such as the one proposed by Parker). Note that by Belyi's theorem, for every number field $F$ there is a $G$ and a $G$-cover as above such that its field of moduli $K$ contains $F$.

*Reporter: Martin Lüdtke*