Mathematisches Forschungsinstitut Oberwolfach

Report No. 30/2013

DOI: 10.4171/OWR/2013/30

The Arithmetic of Fields

Organised by
Moshe Jarden, Tel Aviv
Florian Pop, Philadelphia

16 June – 22 June 2013

Abstract. This report includes extended abstracts of talks given in a conference on the "Arithmetic of Fields" that was held in Mathematisches Forschung Institute, Oberwolfach during 16–22 June 2013. It also includes extended abstracts of talks delivered in joint sessions by participants of a parallel conference on "Quadratic Forms and Linear Algebraic Groups".

Mathematics Subject Classification (2010): 12E30.

Introduction by the Organisers

The seventh conference on "The Arithmetic of Fields" organized by Moshe Jarden (Tel Aviv) and Florian Pop (Philadelphia) was held on 16 – 22 June 2013. The participants came from 7 countries: USA (8), Germany (7), Israel (6), France (2), Canada (1), England (1), and South Africa (1), All together, 26 people attended the conference, seven were young researchers, and four were women.

Compared to the sixth conference, this time we had only "half a conference", the other half was on "Quadratic Forms and Linear Algebraic Groups". That subject was close enough to "Field Arithmetic" to organize each morning two joint sessions for the two groups. The afternoon sessions were separate.

Most of the talks concentrated on the main theme of Field Arithmetic, namely Galois groups and the interplay with the arithmetic of the fields. Some of the talks had an arithmetical geometry flavour while others concentrated on valuation theory.

Even the plenary talks on quadratic forms given by the other group were well attended by the participants of our conference. We followed them with great interest.

All together, the organizers find the blend of young and experienced researchers and the variety of subjects covered very satisfactory.

Workshop: The Arithmetic of Fields

Table of Contents

Abstracts

Local Global Principles for Galois Cohomology

Julia Hartmann
(joint work with David Harbater, Daniel Krashen)

A classical theorem due to Albert, Brauer, Hasse, and Noether states that a central simple algebra over a global field F is split (i.e., isomorphic to a matrix algebra) if and only if it splits over the completions of F at all places.

It is known that the analog is generally false if one instead considers the function field of a surface over a finite field (for any set of valuations). Kato suggested viewing the theorem as a local global principle for $\mathrm{Br}(F)[m] = H^2(F, \mathbb{Z}/m\mathbb{Z}(1))$ for all m, where $\mathbb{Z}/m\mathbb{Z}(n)$ is defined as $\mu_m^{\otimes n}$ if the characteristic of F does not divide m. He further proposed an analog by considering the local-global map

$$H^n(F, Z/m\mathbb{Z}(n-1)) \to \prod_{v\in\Omega} H^n(F_v, \mathbb{Z}/m\mathbb{Z}(n-1)).$$

Here Ω is a suitable set of valuations, and it should depend on the field F for which n this is expected to be injective. In particular, he proved that this local-global map is injective for $n = 3$ when F is the function field of a surface over a finite field, with Ω the set of all discrete valuations. (Note that the corresponding statement for $n > 3$ is vacuous in this situation.)

In this note, we consider function fields of curves over complete discretely valued fields and show that for such fields, both the original Albert-Brauer-Hasse-Noether theorem as well as Kato's analog hold. More precisely, we show the following two theorems.

Theorem 1 ([3], Theorem 3.3.6). *Let F be a one variable function field over a complete discretely valued field K. Assume that K is equicharacteristic and that* $\mathrm{char}(F) \nmid m$. *Then*

$$H^n(F, Z/m\mathbb{Z}(n-1)) \to \prod_{v\in\Omega} H^n(F_v, \mathbb{Z}/m\mathbb{Z}(n-1))$$

is injective for all $n > 1$. Here Ω is the set of discrete (rank one) valuations of F.

Theorem 1 remains true for certain variations of the set Ω, for example one may instead use the set of valuations that come from codimension one points on a regular model of F over the valuation ring of K. After the talk, it was communicated to us by Parimala and Suresh that they have a different (unpublished) proof of the theorem which does not need the equicharacteristic hypothesis.

Theorem 2 ([4], Corollary 9.13). *Let F be a one variable function field over a complete discretely valued field and let Ω be the set of all discrete (rank one) valuations of F. Then the natural map*

$$\mathrm{Br}(F) \to \prod_{v\in\Omega} \mathrm{Br}(F_v)$$

is injective.

Theorem 2 previously appeared in [1] (Theorem 4.3(ii)). It is used here as an example application of a much more general theorem for nonabelian Galois cohomology, see below.

The results of this note (and details about their proofs) may be found in [3] and [4].

1. Proving Theorem 1

Theorem 1 is a consequence of the following

Theorem 3 ([3], Theorem 3.2.3). *Let F be a one variable function field over a complete discretely valued field K and let $\mathcal{X}$ be a regular model for F with closed fiber X. Then the local-global map*

$$H^n(F, Z/m\mathbb{Z}(n-1)) \to \prod_{P\in X} H^n(F_P, \mathbb{Z}/m\mathbb{Z}(n-1))$$

is injective for all $n > 1$. Here F_P is the fraction field of the complete local ring of $\mathcal{X}$ at the point P (the product is taken over all points of X, including generic points of components of X).

To relate these two theorems, one considers the kernels $Ш^n(F,A)$ and $Ш^n_0(\mathcal{X},A)$ of the local-global maps, where more generally A is any commutative group scheme. If A is a finite commutative group scheme of order not divisible by the residue characteristic of K, these fit into an exact sequence

$$0 \to Ш^n_0(\mathcal{X},A) \to Ш^n(F,A) \to \prod_{P\in X_{(0)}}{}' \, Ш^n(F_P,A) \to 0$$

where the restricted product is taken over all closed points P of X. Using a result of Panin ([5], Theorem C), one can deduce that $Ш^n(F_P,A) = 0$ for all $n > 1$ and all $P \in X_{(0)}$ if K is equicharacteristic. Hence Theorem 1 and Theorem 3 are equivalent under this hypothesis on K.

For the proof of Theorem 3, one considers a finite set of overfields of F that come from patching. Let as before F be a one variable function field over a complete discretely valued field K with ring of integers T, uniformizer t, and residue field k. Let $\mathcal{X}$ be a normal model of F over T. Let $\mathcal{P}$ be a finite nonempty set of closed points of the closed fiber X of $\mathcal{X}$ which contains all points at which X is not unibranched. Let $\mathcal{U}$ denote the set of components of $X \setminus \mathcal{P}$.

For $U \in \mathcal{U}$, we let F_U denote the fraction field of the t-adic completion of the set $\{f \in F | \, f \in \mathcal{O}_{\mathcal{X},Q}$ for all $Q \in U\}$. For $P \in \mathcal{P}$ on the closure of $U \in \mathcal{U}$, consider height one prime ideals $\wp$ in the complete local ring of $\mathcal{X}$ at P which contain t. For each such *branch* $\wp$, let $F_\wp$ denote the fraction field of the completion of the localization of $\mathcal{O}_{\mathcal{X},P}$ at $\wp$. For notational simplicity, we introduce

$$F_1 := \prod_{P\in\mathcal{P}} F_P \qquad F_2 := \prod_{U\in\mathcal{U}} F_U \qquad F_0 := \prod_{\wp\in\mathcal{P}} F_\wp$$

Theorem 3 is then deduced from the following local-global principle

Theorem 4 ([3], Theorem 3.1.5). *With notation as above, the local-global map*

$$H^n(F, \mathbb{Z}/m\mathbb{Z}(n-1)) \to H^n(F_1, \mathbb{Z}/m\mathbb{Z}(n-1)) \times H^n(F_2, \mathbb{Z}/m(n-1))$$

is injective for all m for which $\mathrm{char}(k) \nmid m$ *and for all $n > 1$.*

The key to proving this third version of the local-global principle is the existence of the overfields $F_\wp$. In fact, we show that for $A = \mathbb{Z}/m(n)$, there is a long exact sequence ([3], Theorem 3.1.3)

$$\begin{tikzcd}
0 \arrow[r] & A(F) \arrow[r] & A(F_1) \times A(F_2) \arrow[r] & A(F_0) \arrow[dll, rounded corners] \\
 & H^1(F,A) \arrow[r] & H^1(F_1,A) \times H^1(F_2,A) \arrow[r] & H^1(F_0,A) \cdots
\end{tikzcd}$$

which may be thought of as reminiscent of the usual Mayer-Vietoris sequence. Thus injectivity at some level n comes from surjectivity at the previous level. We explicitly show that

$$H^1(F_1, \mathbb{Z}/m\mathbb{Z}(1)) \times H^1(F_2, \mathbb{Z}/m\mathbb{Z}(1)) \to H^1(F_0, \mathbb{Z}/m\mathbb{Z}(1))$$

is injective, using the geometric origin of the rings F_i. Combining this with the norm residue isomorphism theorem (former Bloch-Kato conjecture) which implies that every element in $H^n(F_0, \mathbb{Z}/m\mathbb{Z}(n))$ is a sum of products of elements in $H^1(F_0, \mathbb{Z}/m\mathbb{Z}(1))$, we obtain the statement of Theorem 4.

2. Proving Theorem 2

In order to prove Theorem 2, we more generally consider the first Galois cohomology $H^1(F,G)$ of a not necessarily commutative linear algebraic group G. Again, the kernel $\text{Ш}(F,G)$ of the local-global map

$$H^1(F,G) \to \prod_{v \in \Omega} H^1(F_v, G)$$

can in many cases be related to the kernel $\text{Ш}_{\mathcal{P}}(\mathcal{X}, G)$ of a local-global map

$$H^1(F,G) \to H^1(F_1,G) \times H^1(F_2,G)$$

coming from patching (the strategy is as in the first part, using a local-global map with respect to points on the closed fiber of a regular model; we omit the details). Via a 6-term exact sequence

$$\begin{tikzcd}
1 \arrow[r] & H^0(F,G) \arrow[r] & H^0(F_1,G) \times H^0(F_2,G) \arrow[r] & H^0(F_0,G) \arrow[dll, rounded corners] \\
 & H^1(F,G) \arrow[r] & H^1(F_1,G) \times H^1(F_2,G) \arrow[r, shift left] \arrow[r, shift right] & H^1(F_0,G).
\end{tikzcd}$$

one can again reduce the injectivity of this finite local-gobal map to the surjectivity on the level of H^0. This surjectivity holds for linear algebraic groups that are rational and connected by [2], Theorem 3.6. More generally, for nonconnected rational linear algebraic groups (i.e. groups whose components are all rational varieties), we give an explicit description of the obstruction in terms of the so called reduction graph Γ of a regular model of F:

Theorem 5 ([4], Corollary 6.5). *Let F be as above and let G be a rational linear algebraic group over F. Then $Ш_{\mathcal{P}}(\mathcal{X}, G) = \mathrm{Hom}(\pi_1(\Gamma), G/G^0)$. In particular, it is finite. It is trivial if and only if Γ is a tree or G is connected.*

For the original obstruction set $Ш(F, G)$ we show the following

Theorem 6 ([4], Theorem 8.10). *Let F be a one variable function field over a complete discretely valued field with residue field k, and let G be a rational linear algebraic group. Suppose either k is algebraically closed of characteristic zero or G^0 is defined and reductive over a regular model $\mathcal{X}$ of F. Then $Ш(F, G) = Ш_{\mathcal{P}}(F, G)$.*

In the special case when $G = \mathrm{PGL}_d$ (for various d), we obtain Theorem 2.

References

[1] J.-L. Colliot-Théène, R. Parimala, and V. Suresh, *Patching and local-global principles for homogeneous spaces over function fields of p-adic curves*, Comment. Math. Helv. **87** (2012), 1011–1033.

[2] D. Harbater, J. Hartmann, and D. Krashen, *Applications of patching to quadratic forms and central simple algebras*, Invent. Math. **178** (2009), 231–263.

[3] D. Harbater, J. Hartmann, and D. Krashen, *Local-global principles for Galois cohomology*, to appear in Comment. Math. Helv.

[4] D. Harbater, J. Hartmann, and D. Krashen, *Local-global principles for torsors over arithmetic curves*, 2013 manuscript, available at ArXiv: 1108.3323.

[5] I. A. Panin, *The equicharacteristic case of the Gersten conjecture*, Tr. Mat. Inst. Steklova **241** (Teor. Chisel, Algebra i Algebr. Geom.), (2003), 169–178. Translation in: Proc. Steklov Inst. Math. **241**, no. 2 (2003), 154–163.

Upper bounds for Euclidean minima of abelian fields

Eva Bayer–Fluckiger
(joint work with Piotr Maciak)

Let K be an algebraic number field, and let O_K be its ring of integers. Let $\mathrm{N} : K \to \mathbf{Q}$ be the absolute value of the norm map. The number field K is said to be *Euclidean* (with respect to the norm) if for every $a, b \in O_K$ with $b \neq 0$ there exist $c, d \in O_K$ such that $a = bc + d$ and $\mathrm{N}(d) < \mathrm{N}(b)$. It is easy to check that K is Euclidean if and only if for every $x \in K$ there exists $c \in O_K$ such that $\mathrm{N}(x - c) < 1$. This suggests to look at

$$M(K) = \mathrm{sup}_{x \in K} \mathrm{inf}_{c \in O_K} \mathrm{N}(x - c),$$

called the *Euclidean minimum* of K.

The determination of Euclidean number fields and Euclidean minima is a classical problem – see for instance the survey of Lemmermeyer [L 95], as well as the tables of Cerri [C 07]. Another classical problem is to find *upper bounds* for $M(K)$ in terms of the degree $n = [K : \mathbf{Q}]$ of the number field K, and of the absolute value d_K of its discriminant. Upper bounds valid for arbitrary number fields exist since the early 1950's, due to work of Clarke and Davenport. In [BF 06], it is proved that

$$M(K) \leq 2^{-n} d_K.$$

If K is totally real, then a conjecture attribruted to Minkowski states that

$$M(K) \leq 2^{-n} \sqrt{d_K}.$$

This is known for $n \leq 8$ (cf. [HGRS 11]). One can also try to prove the conjecture for some families of number fields. This is done in [BF 06], [BFN 05] and [BFS 06] for certain cyclotomic fields. It is natural to ask the same question for *abelian* number fields. We have

Theorem. [BFM 13] *Let p be an odd prime number, and let K be an abelian number field of conductor p^r. If $r \geq 2$, then we have*

$$M(K) \leq 2^{-n} \sqrt{d_K}.$$

In particular, Minkowski's conjecture holds for totally real number fields of conductor p^r, when p is an odd prime and $r \geq 2$.

The proof uses packing and covering invariants of number fields, following a method of [BF 06]. A key ingredient is the determinantion of the *trace form* of the ring of integers.

References

[BF 06] E. Bayer–Fluckiger. Upper bounds for Euclidean minima of algebraic number fields, *J. Number Theory* **121** (2006), 305–323.

[BFM 13] E. Bayer–Fluckiger, P. Maciak. Upper bounds for the Euclidean minima of abelian fields of odd prime power conductor, *Math. Ann.* (to appear).

[BFN 05] E. Bayer–Fluckiger, G. Nebe. On the Euclidean minimum of some real number fields, *Journal dethéorie des nombres de Bordeaux* **17** (2005), 437-454.

[BFS 06] E. Bayer–Fluckiger, I. Suarez. Ideal lattices over totally real number fields and Euclidean minima, *Archiv Math.*, **86** (2006), 217-225.

[C 07] J-P. Cerri. Euclidean minima of totally real number fields: algorithmic determination, *Math. Comp.* **76** (2007), 1547-1575.

[HGRS 11] R. J. Hans-Gill, M. Raka and R. Sehmi. On Conjectures of Minkowski and Woods for $n = 8$, *Acta Arith.* **147** (2011), 337-385.

[L 95] F. Lemmermeyer. The Euclidean algorithm in algebraic number fields, *Expo. Math.* **13** (1995), 385-416.

Independence of ℓ-adic Galois representations

Sebastian Petersen
(joint work with Gebhard Böckle and Wojciech Gajda)

Let K be a field. We denote its absolute Galois group by $\mathrm{Gal}(K)$ and let K_s (resp. $\widetilde{K}$) be a separable (resp. algebraic) closure of K. Let $\mathbb{L}$ be the set of all prime numbers. Let $\mathbb{L}' \subset \mathbb{L}$. Assume we are given for every $\ell \in \mathbb{L}'$ a topological group G_ℓ and a continuous homorphism $\rho_\ell : \mathrm{Gal}(K) \to G_\ell$. Let $\rho : \mathrm{Gal}(K) \to \prod_{\ell\in\mathbb{L}'} G_\ell$ be the homomorphism induced by the ρ_ℓ. Following Serre [6] we call the family $(\rho_\ell)_{\ell\in\mathbb{L}'}$ *independent* if $\rho(\mathrm{Gal}(K)) = \prod_{\ell\in\mathbb{L}'} \rho_\ell(\mathrm{Gal}(K))$. We denote by $K(\rho_\ell)$ the fixed field of $\ker(\rho_\ell)$ in K_s and call $K(\rho_\ell)$ the division field of ρ_ℓ. Note that $(\rho_\ell)_{\ell\in\mathbb{L}'}$ is independent if and only if the sequence $(K(\rho_\ell))_{\ell\in\mathbb{L}'}$ of fields is linearly disjoint over K. We shall say that $(\rho_\ell)_{\ell\in\mathbb{L}'}$ is *almost independent* if there exists an open subgroup H of $\mathrm{Gal}(K)$ such that $\rho(H) = \prod_{\ell\in\mathbb{L}'} \rho_\ell(H)$.

The main examples of such families we are interested in arise as follows: Let $\mathbb{L}' := \mathbb{L} \smallsetminus \{\mathrm{char}(K)\}$.

(a) Let A/K be an abelian variety. Then for $\ell \in \mathbb{L}'$ and $i \in \mathbb{N}$ the Galois group $\mathrm{Gal}(K)$ acts on $A[\ell^i] = A(\widetilde{K})[\ell^i]$ and also on the ℓ-adic Tate module $V_\ell(A) := (\varprojlim_{i\in\mathbb{N}} A[\ell^i]) \otimes \mathbb{Q}_\ell$. We consider the representation

$$\sigma_{\ell,A} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

Then $K(\sigma_{\ell,A})$ is just the field $K(A[\ell^\infty])$ obtained from K by adjoining the coordinates of all division points in $A[\ell^\infty] = \bigcup_{i\in\mathbb{N}} A[\ell^i]$ to K. Note that the family $(\sigma_{\ell,A})_{\ell\in\mathbb{L}'}$ is independent if and only if $(K(A[\ell^\infty])_{\ell\in\mathbb{L}'}$ is a linearly disjoint sequence of extension fields of K. If K is a number field, then $(\sigma_{\ell,A})_{\ell\in\mathbb{L}'}$ is almost independent by a classical result of Serre dating back to the 80's (cf. [5]). Igusa had shown earlier that $(\sigma_{\ell,A})_{\ell\in\mathbb{L}'}$ is almost independent if K is a finitely generated field of characteristic zero and A is an elliptic curve with transcendental j-invariant.

(b) More generally let X/K be a separated algebraic scheme, $d \in \mathbb{Z}$ and $q \in \mathbb{N}$. For $\ell \in \mathbb{L}'$ we denote by

$$\rho_{\ell,X}^{(q)}(d) : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Q}_\ell}(H^q(X_{\widetilde{K}}, \mathbb{Q}_\ell(d)))$$

the representation of the Galois group $\mathrm{Gal}(K)$ on the ℓ-adic étale cohomology group $H^q(X_{\widetilde{K}}, \mathbb{Q}_\ell(d))$ and by

$$\rho_{\ell,X,c}^{(q)}(d) : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Q}_\ell}(H_c^q(X_{\widetilde{K}}, \mathbb{Q}_\ell(d)))$$

the representation of $\mathrm{Gal}(K)$ on the ℓ-adic étale cohomology group with compact support $H_c^q(X_{\widetilde{K}}, \mathbb{Q}_\ell(d))$. We put $\rho_{\ell,X}^{(q)} := \rho_{\ell,X}^{(q)}(0)$ and $\rho_{\ell,X,c}^{(q)} := \rho_{\ell,X,c}^{(q)}(0)$. If X is an abelian variety and $X^\vee$ the dual abelian variety, then there is an isomorphism of $\mathbb{Q}_\ell[\mathrm{Gal}(K)]$-modules

$$V_\ell(X^\vee) \cong H^1(X_{\widetilde{K}}, \mathbb{Q}_\ell(1)),$$

and thus the representations $\sigma_{\ell,X^\vee}$ and $\rho^{(1)}_{\ell,X}(1)$ are isomorphic.

With a view towards generalizations of the results of Igusa and Serre mentioned so far one may wonder in which circumstances the families $(\sigma_{\ell,A})_{\ell\in\mathbb{L}'}$, $(\rho^{(q)}_{\ell,X}(d))_{\ell\in\mathbb{L}'}$ and $(\rho^{(q)}_{\ell,X,c}(d))_{\ell\in\mathbb{L}'}$ in the above examples are almost independent. In general they are not; one needs additional assumptions on K. For example, if $X = \mathbb{P}_1$ and $q = 2$, then $\dim_{\mathbb{Q}_\ell}(H^2(X_{\widetilde{K}}, \mathbb{Q}_\ell)) = 1$ and the action of $\mathrm{Gal}(K)$ is given by the inverse of the cyclotomic character $\varepsilon_\ell : \mathrm{Gal}(K) \to \mathbb{Q}_\ell^\times$ for $\ell \in \mathbb{L}'$. It is a classical result in number theory that $(\varepsilon_\ell)_{\ell\in\mathbb{L}}$ is almost independent provided K is a finitely generated field of characteristic zero. On the other hand $(\varepsilon_\ell)_{\ell\in\mathbb{L}}$ is *not* almost independent if K is a finitely generated field of positive characteristic, and there are even examples of fields K of characteristic zero such that $(\varepsilon_\ell)_{\ell\in\mathbb{L}}$ is *not* almost independent over K.

Also note that if the structure morphism $X \to \mathrm{Spec}(K)$ factors through $\mathrm{Spec}(E)$ for some finite Galois extension E/K and if I denotes the set of K-embeddings $E \to \widetilde{K}$, then $X_{\widetilde{K}} = X \times_K \mathrm{Spec}(\widetilde{K}) = \coprod_{i\in I} X \times_{E,i} \mathrm{Spec}(\widetilde{K})$ and the action of $\mathrm{Gal}(K)$ on $H^0(X_{\widetilde{K}}, \mathbb{Q}_\ell) = \coprod_{i\in I} \mathbb{Q}_\ell$ is given by the natural action of $\mathrm{Gal}(K)$ on I. Thus $E \subset K(\rho^{(0)}_{\ell,X})$ for all $\ell \in \mathbb{L}'$ and consequently $(\rho^{(0)}_{\ell,X})_{\mathbb{L}'\setminus I}$ is *not* independent for every finite subset I of $\mathbb{L}$. This shows that one should hunt for "almost independence results" rather than for "independence results".

Theorem 1. *Let K be a finitely generated field of characteristic zero. Let X/K be a separated algebraic scheme, $d \in \mathbb{Z}$ and $q \in \mathbb{N}$. Then the families $(\rho^{(q)}_{\ell,X}(d))_{\ell\in\mathbb{L}}$ and $(\rho^{(q)}_{\ell,X,c}(d))_{\ell\in\mathbb{L}}$ are both almost independent.*

In the important special case where K is a number field this theorem was recently proved by Serre (cf. [6]) continuing and generalizing his earlier work on abelian varieties over number fields (cf. [5]). In several places in the literature (cf. [6], [4] and [7]) the question came up whether Theorem 1 holds in the case where $\mathrm{trdeg}(K/\mathbb{Q}) > 0$. This question was finally solved in [3] by reducing it to the number field case where it was already known thanks to the work of Serre. The reduction used methods from group theory due to Nori and E. Artin, finiteness theorems in geometric class field due to Katz and Lang, and the generic base change theorem in étale cohomology (cf. [4]) of Katz and Laumon.

The hypothesis on the characteristic of K is crucial in Theorem 1: Let K be a finitely generated field of *positive* characteristic p and $\mathbb{L}' = \mathbb{L} \smallsetminus \{p\}$. We already mentioned that then the family of cyclotomic characters $(\varepsilon_\ell)_{\ell\in\mathbb{L}'}$ over K is *not* almost independent, and hence $(\rho^{(2)}_{\ell,\mathbb{P}_1})_{\ell\in\mathbb{L}'}$ is *not* almost independent. For a separated algebraic K-scheme X and $q \in \mathbb{N}$ one may ask, however, whether the restricted family $(\rho^{(q)}_{\ell,X} | \mathrm{Gal}(\widetilde{\mathbb{F}_p}K))_{\ell\in\mathbb{L}'}$ is almost independent. (The answer is yes.) Note that $\widetilde{\mathbb{F}}_pK/K$ is the rather small infinite algebraic extension of K obtained by adjoining all roots of unity to K. Having gone that far it seemed natural to ask for an analogue of Theorem 1 where the ground field is a geometric function field, i.e. a finitely generated extension of an algebraically closed field. Such a result was independently obtained by Cadoret-Tamagawa (cf. [2]) and by the authors (cf. [1]).

Theorem 2. *Let K_0 be an algebraically closed field of characteristic $p \geq 0$ and K/K_0 a finitely generated extension. Let X/K be a separated algebraic scheme and $q \in \mathbb{N}$. Let $\mathbb{L}' = \mathbb{L} \smallsetminus \{p\}$. Then the families $(\rho_{\ell,X}^{(q)})_{\ell\in\mathbb{L}'}$ and $(\rho_{\ell,X,c}^{(q)})_{\ell\in\mathbb{L}'}$ are both almost independent.*

In the case where K is a geometric function field we can say quite a bit about the images of the representations under consideration.

Theorem 3. *Let K_0 be an algebraically closed field of characteristic $p \geq 0$ and K/K_0 a finitely generated extension. Let X/K be a separated algebraic scheme and $q \in \mathbb{N}$. Let $\mathbb{L}' = \mathbb{L} \smallsetminus \{p\}$. Let either $(\rho_\ell)_{\ell\in\mathbb{L}'} = (\rho_{\ell,X}^{(q)})_{\ell\in\mathbb{L}'}$ or $(\rho_\ell)_{\ell\in\mathbb{L}'} = (\rho_{\ell,X,c}^{(q)})_{\ell\in\mathbb{L}'}$. Then there exists a finite extension K'/K and a constant $c \in \mathbb{N}$ with the following properties.*

- i) *The group $\rho_\ell(\mathrm{Gal}(K'))$ is generated by its ℓ-Sylow subgroups for every $\ell \in \mathbb{L}'$.*
- ii) *For every $\ell \in \mathbb{L}'$ the group $\rho_\ell(\mathrm{Gal}(K'))$ has a normal series*

$$\rho_\ell(\mathrm{Gal}(K')) \rhd N_\ell \rhd P_\ell \rhd \{e\}$$

such that $\rho_\ell(\mathrm{Gal}(K'))/N_\ell$ is a finite product of finite simple groups of Lie type in characteristic ℓ, the group N_ℓ/P_ℓ is a finite abelian group of order prime to ℓ, the index $[N_\ell : P_\ell]$ is (uniformly) bounded by c, and P_ℓ is a pro-ℓ group.

The proof of Theorems 1 and 2 in [1] makes crucial use of group theoretical results of Larsen and Pink and of finiteness properties of étale fundamental groups. Furthermore we had to understand certain (tame) ramification properties of families of the form $(\rho_{\ell,X}^{(q)})_{\ell\in\mathbb{L}'}$ and $(\rho_{\ell,X,c}^{(q)})_{\ell\in\mathbb{L}'}$ where X is a separated algebraic scheme over K and K a function field over $\mathbb{F}_p$. Our proof of the desired ramification properties involves the alteration technique of de Jong and the local Langlands correspondence proved by Lafforgue. Alternatively we could have applied a recent result of Orgogozo in order to get these ramification properties.

In the case of abelian varieties one obtains the following

Corollary 4. *Let either K_0 be an algebraically closed field of arbitrary characteristic or $K_0 = \mathbb{Q}$. Let K/K_0 be a finitely generated field extension. Let A/K be an abelian variety. Then there exists a finite extension E/K such that $(E(A[\ell^\infty]))_{\ell\in\mathbb{L}\smallsetminus\{\mathrm{char}(K)\}}$ is an E-linearly disjoint sequence of fields.*

References

[1] Gebhard Böckle, Wojciech Gajda and Sebastian Petersen. *Independence of ℓ-adic representations of geometric Galois groups.* Preprint available at www.arxiv.org: 1302.6597.

[2] Anna Cadoret and Akio Tamagawa. *On subgroups of* $\mathrm{GL}_n(\mathbb{F}_\ell)$ *and representations of étale fundamental groups.* Preprint.

[3] Wojciech Gajda and Sebastian Petersen. *Independence of ℓ-adic Galois representations over function fields.* Compositio Mathematica, 149(07):1091–1107, 2013.

[4] Luc Illusie. *Constructibilité générique et uniformité en ℓ.* Preprint.
[5] Jean-Pierre Serre. Lettre à Ken Ribet du 7/3/1986. *Collected Papers IV.*
[6] Jean-Pierre Serre. *Une critère d'indépendance pour une famille de représentations ℓ-adiques.* Preprint available at www.arxiv.org: 1006.2442.
[7] Jean-Pierre Serre. Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques. *Proc. Symp. Pure Math.*, (55):377–400, 1994.

Random Galois extensions of Hilbertian fields

Lior Bary-Soroker
(joint work with Arno Fehm)

A central problem in the theory of Hilbertian fields is to find conditions under which a separable extension L of a Hilbertian field K is again Hilbertian (e.g. when $K = \mathbb{Q}$). The talk dealt with Galois extensions whose group has 'finitely many relations,' in a certain sense. The main result presented is that typically, those extensions are Hilbertian.

Theorem 1. *Let K be a countable Hilbertian field and L/K a Galois extension. Then the set of $\sigma \in \mathrm{Gal}(L/K)^n$ for which $L[\sigma]$ is not Hilbertian has Haar measure 0.*

Here $L[\sigma]$ is the fixed field of the minimal normal subgroup $[\sigma]$ that contains $\sigma_1, \dots, \sigma_n$.

This theorem generalizes Jarden's result for $L = K_s$, the separable closure of K and settles a problem stemming from the work of Haran, Jarden, and Pop for $L = \mathbb{Q}_{\mathrm{tot},S}$, the field of totally S-adic numbers, for a finite set of absolute values S of $\mathbb{Q}$.

In the proof, among other things, we use the infinite Ramesy theorem, for the first time, to the best of our knowledge, in Field Arithmetics.

Permanence principles for Hilbertian fields

Arno Fehm
(joint work with Lior Bary-Soroker and Gabor Wiese)

A field K is **Hilbertian** if for every irreducible $f \in K[T, X]$ which is monic and separable in X there exists $\tau \in K$ such that $f(\tau, X)$ is irreducible. Let K be Hilbertian and L/K an algebraic extension. Classical results state that under any of the following conditions, also L is Hilbertian:

(1) L/K is finite;
(2) L/K is small, i.e. for every $n \in \mathbb{N}$ there exist only finitely many fields $K \subseteq M \subseteq L$ with $[M : K] = n$;
(3) L/K is abelian (Kuyk 1970);
(4) there exists a field $K \subseteq M \subseteq L$ with M/K Galois and $1 < [L : M] < \infty$ (Weissauer 1982);

(5) there exist Galois extensions M_1, M_2 of K with $L \subseteq M_1M_2$, $L \not\subseteq M_1$, and $L \not\subseteq M_2$ (Haran 1999);

The work [1] adds a new permanence principle to this list:

(6) there exist fields $K = M_0 \subseteq \cdots \subseteq M_r$ with $L \subseteq M_r$ such that for each i, M_{i+1}/M_i is Galois with group abelian or a product of finite simple groups.

Note that (6) includes (3) as the special case $r = 1$ and M_1/M_0 abelian. Already the case $r = 2$ and M_2/M_1, M_1/M_0 both abelian is new.

Let us call the extension L/K an **$\mathcal{H}$-extension** if every intermediate field $K \subseteq M \subseteq L$ is Hilbertian. Observe that (1), (2), (3) and (6) imply that L/K is such an $\mathcal{H}$-extension, while (4) and (5) do not.

Lemma 1. *If $(K_\ell)_\ell$ is a family of Galois $\mathcal{H}$-extensions of K, and E/K is an $\mathcal{H}$-extension such that the family $(K_\ell E)_\ell$ is linearly disjoint over E, then the compositum $\prod_\ell K_\ell$ is an $\mathcal{H}$-extension of K.*

Proof. Let $K \subseteq M \subseteq \prod_\ell K_\ell$. If for some ℓ, $M \subseteq K_\ell$, then M is Hilbertian because K_ℓ/K is an $\mathcal{H}$-extension. If for some ℓ, $M \not\subseteq K_\ell$ and $M \not\subseteq \prod_{\ell' \neq \ell} K_{\ell'}$, then M is Hilbertian by (5). In the remaining case, $M \subseteq \bigcap_\ell \prod_{\ell' \neq \ell} K_{\ell'} E = E$ by linear disjointness, hence M is Hilbertian because E/K is an $\mathcal{H}$-extension.[1] □

For a profinite group Γ, let $D(\Gamma)$ denote the intersection over all open normal subgroups N of Γ with Γ/N abelian or simple. Define a descending normal series by $\Gamma^{(0)} = \Gamma$, $\Gamma^{(i+1)} = D(\Gamma^{(i)})$, and let $\mathrm{length}(\Gamma) = \inf\{i : \Gamma^{(i)} = 1\}$ be the **abelian-simple length** of Γ.

Lemma 2. *Fix $m \in \mathbb{N}$. The class of profinite groups Γ with $\mathrm{length}(\Gamma) \leq m$ is closed under taking normal subgroups, quotients, fiber products and inverse limits. If $N \lhd \Gamma$ is a closed normal subgroup, then $\mathrm{length}(\Gamma) \leq \mathrm{length}(N) + \mathrm{length}(\Gamma/N)$.*

With this terminology, we can reformulate (6) as follows:

Theorem 3. *If K is Hilbertian and L/K is a Galois extension of finite abelian-simple length (i.e. $\mathrm{length}(\mathrm{Gal}(L/K)) < \infty$), then L/K is an $\mathcal{H}$-extension.*

About the proof. The proof of this theorem utilizes Haran's twisted wreath product approach [3]. In order to apply it, one has to show that "abelian-simple length grows in wreath products": Let $\Gamma_0 \leq \Gamma$ and $A \neq 1$ be finite groups with Γ_0 acting on A, and denote by $A \wr_{\Gamma_0} \Gamma = \mathrm{Ind}_{\Gamma_0}^{\Gamma}(A) \rtimes \Gamma$ the twisted wreath product. We prove that if $[\Gamma^{(m)}\Gamma_0 : \Gamma_0] > 2^m$, then $(A \wr_{\Gamma_0} \Gamma)^{(m+1)} \cap \mathrm{Ind}_{\Gamma_0}^{\Gamma}(A) \neq 1$. □

We apply Theorem 3 to extensions arising from **Galois representations**: Fix $n \in \mathbb{N}$. For each prime ℓ let $\rho_\ell : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be a continuous homomorphism, let K_ℓ be the fixed field of $\ker(\rho_\ell)$, and $K(\rho) = \prod_\ell K_\ell$ the compositum.

Proposition 4. *If $(\rho_\ell)_\ell$ is as above, then $K(\rho)/K$ is an $\mathcal{H}$-extension.*

[1] This proof is a simplification of the original one published in [2].

Sketch of proof. By a result of Larsen-Pink [5] there is a constant $J(n)$ and, for each ℓ, an intermediate field $K \subseteq K'_\ell \subseteq K_\ell$ such that K_ℓ/K'_ℓ is Galois with $\mathrm{Gal}(K_\ell/K'_\ell)$ pro-ℓ and K'_ℓ/K is Galois with $\mathrm{Gal}(K'_\ell/K)$ an extension of a finite group of order $\leq J(n)$ by an extension of a product of finite simple groups by an abelian group. Let $E = \prod_\ell K'_\ell$. By Lemma 2, one has $\mathrm{length}(\mathrm{Gal}(E/K)) \leq 2 + \log_2 J(n)$, so E/K is an $\mathcal{H}$-extension by Theorem 3. Since each K_ℓ/K is Galois with $\mathrm{Gal}(K_\ell/K)$ a compact subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, hence finitely generated as a profinite group, K_ℓ/K is an $\mathcal{H}$-extension by (2). Since for each ℓ, $\mathrm{Gal}(K_\ell E/E)$ is pro-ℓ, the family $(K_\ell E)_\ell$ is linearly disjoint over E. Therefore, the claim follows from Lemma 1. □

In the special case where the ρ_ℓ arise from representations on the Tate module of an abelian variety, we obtain the following:

Corollary 5 (Jarden's conjecture)**.** *Let K be a Hilbertian field, A/K an abelian variety, and $K(A_{\mathrm{tor}})$ the extension of K obtained by adjoining all torsion points of A. Then $K(A_{\mathrm{tor}})/K$ is an $\mathcal{H}$-extension.*

In [4], this was proven for number fields K and conjectured for Hilbertian fields K in general. Several further applications of Theorem 3 can be found in [1, Section 5].

References

[1] L. Bary-Soroker, A. Fehm and G. Wiese, *Hilbertian fields and Galois representations*, mauscript, arXiv:1203.4217 (2012).

[2] A. Fehm and S. Petersen, *Division fields of commutative algebraic groups*, to appear in Israel Journal of Mathematics (2012).

[3] D. Haran, *Hilbertian fields under separable algebraic extensions*, Invent. Math. **137**(1) (1999), 113–126.

[4] M. Jarden, *Diamonds in torsion of abelian varieties*, Journal of the Institute of Mathematics Jussieu **9** (2010), 477–380.

[5] M. J. Larsen and R. Pink, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. **24**(4) (2011), 1105–1158.

Principal Bundles over Valued Fields

Laurent Moret-Bailly
(joint work with Ofer Gabber and Philippe Gille)

The slides of this talk are available on the author's webpage:
`http://perso.univ-rennes1.fr/laurent.moret-bailly/exposes.html`

1. Notation and conventions; admissible valued fields

A *valued field* (K, v) is a field K equipped with a Krull valuation v of arbitrary positive rank. We denote by $\widehat{K}$ the completion of K.

If K is a field, a *K-variety* is a K-scheme of finite type. A *K-space* is an algebraic space X, of finite type and locally separated over K (recall that the latter condition means that the diagonal map $X \to X \times_K X$ is an immersion; this is always the case if X is a variety). An *algebraic group* over K is a K-group scheme of finite type.

If (K, v) is a valued field and X is a K-variety, the set $X(K)$ of K-rational points of X admits a natural topology, inherited from the valuation topology on K. The resulting topological space will be denoted by X_{top}. This defines a functor from K-varieties to topological spaces, which commutes with fiber products, takes open (closed) immersions to open (closed) topological embeddings, separated varieties to Hausdorff spaces, and the affine line to K with the usual valuation topology.

Assume moreover that (K, v) is Henselian. Then ("implicit function theorem") the above functor takes étale morphisms to local homeomorphisms. Furthermore, the X_{top} construction can be extended to the category of K-spaces, with the same compatibility properties: see [2] for the special case of complete, rank one valuations.

Definition 1. A valued field (K, v) is *admissible* if it is Henselian and its completion $\widehat{K}$ is a separable extension of K.

Admissible valued fields satisfy the following generalization of Greenberg's approximation theorem [5]:

Theorem 2 (strong approximation theorem [6, Theorem 1.2])**.** *Let (K, v) be an admissible valued field, and let $R \subset K$ be the ring of v. Let $\mathscr{X}$ be an R-scheme of finite presentation.*

Then, for each nonzero ideal J of R, there is an ideal J', with $0 \neq J' \subset J$, such that (under the natural maps)

$$\operatorname{Im}\big(\mathscr{X}(R) \to \mathscr{X}(R/J)\big) = \operatorname{Im}\big(\mathscr{X}(R/J') \to \mathscr{X}(R/J)\big).$$

This has important topological consequences. In particular:

Corollary 3 (see [6, Theorem 1.3])**.** *Let (K, v) be admissible, and let $f : X \to Y$ be a* proper *morphism of K-spaces. Then $f_{\text{top}} : X_{\text{top}} \to Y_{\text{top}}$ has closed image.*

(Note that f_{top} is not a closed map in general).

2. Torsors; statement of the main result

Assume (K, v) is an admissible valued field, G is an algebraic K-group, Y is a K-space, and $f : X \to Y$ is a G-torsor (for the fppf topology) over Y. Taking rational points, we get a continuous free action of G_{top} on X_{top} and a continuous, G_{top}-invariant map $f_{\text{top}} : X_{\text{top}} \to Y_{\text{top}}$. We can factor f_{top} as

$$\begin{tikzcd}
X_{\text{top}} \arrow[r, "\alpha", "\text{quotient map}"'] & X_{\text{top}}/G_{\text{top}} \arrow[r, "\beta", "\substack{\text{continuous}\\ \text{bijection}}"'] & \operatorname{Im}(f_{\text{top}}) \arrow[r, "\gamma", "\substack{\text{topological}\\ \text{embedding}}"'] & Y_{\text{top}} .
\end{tikzcd}$$

Our main theorem is:

Theorem 4. *Notations and assumptions are as above.*

(1) $\operatorname{Im}(f_{\text{top}})$ *is* locally closed *in* Y_{top}.

Moreover, it is open and closed if G is smooth, and it is closed if G satisifes Condition (*) (see Definition 5 below; in particular, this holds if G°_{red} is smooth, or if G is commutative)*.*

(2) *The map $\beta \circ \alpha : X_{\text{top}} \to \operatorname{Im}(f_{\text{top}})$ is a principal G_{top}-bundle (i.e. locally isomorphic, with the G_{top}-action, to the projection $\operatorname{Im}(f_{\text{top}}) \times G_{\text{top}} \to \operatorname{Im}(f_{\text{top}})$).*

Equivalently, β is a homeomorphism and α is a principal G_{top}-bundle.

3. Method of proof

3.1. **The group $G^{\dagger}$, condition (*), and Gabber's compactification.** Let G be an algebraic group over an arbitrary field K. Then [3, Lemma C.4.1] G admits a largest smooth subgroup, which we denote by $G^{\dagger}$. It can be constructed as the Zariski closure of the set of all points of G whose residue fields are separable over K. It is functorial in G, and its formation commutes with separable ground field extensions.

Definition 5. With the above assumptions, denote by $\bar{K}$ an algebraic closure of K. We say that *G satisfies condition* (*) if every subtorus of $G_{\bar{K}}$ is contained in $(G^{\dagger})_{\bar{K}}$.

Condition (*) is easily seen to hold if G°_{red} is smooth, or if G is commutative.

The homogeneous space $Q := G/G^{\dagger}$ has a unique K-rational point; more generally, if T is a G-torsor over K, then $T/G^{\dagger}$ has at most one rational point. The following theorem is a special case of a result announced in [4]:

Theorem 6 (O. Gabber)**.** *With the above notation, there exist:*

- *a projective variety Q^c with an action of G, carrying a G-linearized ample line bundle,*
- *a G-equivariant open immersion $Q \hookrightarrow Q^c$* (we identify Q with its image in Q^c)

such that Q^c has a unique rational point (which of course must be the unique point of $Q(K)$).

If, moreover, G satisfies condition (*), we can choose Q^c in such a way that every G-orbit of Q^c defined over K (in the sense of [1, 10.2, Definition 4]) *is contained in Q.*

3.2. **Strategy of proof of Theorem 4.** Starting with $f : X \to Y$ as in Theorem 4, we introduce the quotient $Z := X/G^\dagger$ and we factor f as $X \xrightarrow{\pi} Z \xrightarrow{h} Y$. (Note that even if X and Y are varieties, Z in general only exists as an algebraic space: this is the main reason for stating our theorem with this generality).

First, note that π is a torsor under the smooth group $G^\dagger$. It follows easily that $\mathrm{Im}(\pi_{\mathrm{top}}) \subset Z_{\mathrm{top}}$ is open and closed, and π_{top} is a principal $G^\dagger_{\mathrm{top}}$-bundle over its image. (The assumption that $\widehat{K}$ is separable over K is not used here). Also, observe that $G^\dagger_{\mathrm{top}} = G_{\mathrm{top}}$.

Next, it is easy to see that h_{top} is injective. Moreover, we prove that it is in fact a topological embedding, and its image is locally closed in Y_{top}, and closed under condition (*). This makes essential use of Theorem 6 and the approximation theorem.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete **21** (1990), Springer.

[2] B. Conrad, *Weil and Grothendieck Approaches to Adelic Points*, L'Ens. Math. (2) **58** (2012), 61–97.

[3] B. Conrad, O. Gabber, G. Prasad, *Pseudo-reductive groups*, Cambridge University Press (2010).

[4] O. Gabber, *On pseudo-reductive groups and compactification theorems*, to appear in Oberwolfach Reports.

[5] M.J. Greenberg, *Rational points in Henselian discrete valuation rings.* Pub. Math. I.H.E.S. **31** (1966), 59–64.

[6] L. Moret-Bailly, *An extension of Greenberg's theorem to general valuation rings*, Manusc. Math. **139** (2012) 1, 153–166.

The u-invariant of a rational function field

David Leep

The (classical) u-invariant of a field F, written $u(F)$, is the maximum dimension of an anisotropic quadratic form defined over F. We set $u(F) = \infty$ if no such maximum exists. The main question of this report is the problem of computing $u(k(t))$ where k is a field and $k(t)$ is the rational function field over k. Throughout this report, k denotes a field with $\mathrm{char}\, k \neq 2$.

Proposition 1. $2u(k) \leq 2\sup\{u(E) \mid [E : k] < \infty\} \leq u(k(t))$.

Proof. The first inequality is trivial and the second inequality is proved using standard valuation theory. □

Proposition 2. *Let $[E : k] = r$. Then $u(E) \leq \frac{r+1}{2} u(k)$.*

Proof. See [L], Theorem 2.10. □

Proposition 2, currently the best known upper bound for $u(E)$, is not strong enough to even suggest the finiteness of $u(k(t))$ in Proposition 1. We now pursue a second approach.

Let $u_k(r, m)$ denote the smallest integer such that every system of r quadratic forms defined over k in more than $u_k(r, m)$ variables vanishes on an m-dimensional affine linear space defined over k. Set $u_k(r, m) = \infty$ if no such integer exists. Note that $u_k(1, 1) = u(k)$.

Proposition 3. $2u(k) \leq u_k(2, 1) \leq u(k(t))$.

Proof. Let q_1 and q_2 be two quadratic forms defined over k. Let $q_1 + tq_2$ denote the polynomial sum over $k(t)$. The Amer-Brumer theorem (see [A] and [B]) states that q_1 and q_2 have a nontrivial common zero over k if and only $q_1 + tq_2$ is isotropic over $k(t)$. This immediately implies that $u_k(2, 1) \leq u(k(t))$. The inequality $2u(k) \leq u_k(2, 1)$ comes from considering two anisotropic forms q_1 and q_2 in disjoint variables. □

Proposition 4. *Let Q be a regular quadratic form defined over $k(t)$. There exist quadratic forms q_1, q_2 defined over k and an integer $l \geq 0$ such that $q_1 + tq_2 \simeq_{k(t)} l\mathbb{H} \perp Q$.*

Proposition 5 (Amer's Theorem, [A])**.** *Let q_1 and q_2 be two quadratic forms defined over k. Then q_1 and q_2 vanish on a common m-dimensional affine linear space over k if and only if $q_1 + tq_2$ vanishes on an m-dimensional affine linear space over $k(t)$.*

Lemma 6.

(1) $2u(k) \leq u_k(2, 1) \leq 3u(k)$.
(2) $u_k(2, m) + 2 \leq u_k(2, m + 1) \leq u_k(2, m) + 3$ *for all* $m \geq 1$.
(3) $u_k(2, 1) + 2(m - 1) \leq u_k(2, m) \leq u_k(2, 1) + 3(m - 1)$ *for all* $m \geq 1$.

Proof. Proofs of these inequalities can be found in [L]. □

Theorem 7. $u(k(t)) = \sup_{m\geq 1}\{u_k(2, m) - 2(m - 1)\}$.

Proof. By Lemma 6, we can assume that $u(k)$ is finite and thus $u_k(2, m)$ is finite for all $m \geq 1$.

For arbitrary $m \geq 1$, let q_1, q_2 be two quadratic forms defined over k in $u_k(2, m)$ variables such that q_1, q_2 do not vanish on a common m-dimensional vector space defined over k. By Proposition 5, $q_1 + tq_2$ doesn't vanish on an m-dimensional vector space over $k(t)$. Thus we have $q_1 + tq_2 \simeq_{k(t)} Q \perp l\mathbb{H} \perp \mathrm{rad}(q_1 + tq_2)$, where Q is anisotropic over $k(t)$ and $l + \dim(\mathrm{rad}(q_1 + tq_2)) \leq m - 1$. Then

$$u(k(t)) \geq \dim Q = u_k(2, m) - 2l - \dim(\mathrm{rad}(q_1 + tq_2)) \geq u_k(2, m) - 2(m - 1).$$

Thus, $u(k(t)) \geq \sup_{m\geq 1}\{u_k(2, m) - 2(m - 1)\}$.

Let Q be an anisotropic quadratic form defined over $k(t)$. By Proposition 4, there exist quadratic forms q_1 and q_2 defined over k such that $q_1 + tq_2 \simeq_{k(t)} Q \perp (m-1)\mathbb{H}$ for some integer $m \geq 1$. We have $\dim(q_1 + tq_2) \leq u_k(2, m)$, otherwise q_1 and q_2 would vanish on a common m-dimensional vector space over k and thus $q_1 + tq_2$ would also vanish on an m-dimensional vector space over $k(t)$ by the trivial implication of Proposition 5. Thus

$$\dim(Q) \leq u_k(2,m) - 2(m-1) \leq \sup_{m\geq 1}\{u_k(2,m) - 2(m-1)\}.$$

Therefore, $u(k(t)) \leq \sup_{m\geq 1}\{u_k(2,m) - 2(m-1)\}$. □

The second inequality in Proposition 3 is contained in Theorem 7 when $m = 1$.

Corollary 8. *$u(k(t)) \leq N$ if and only if $u_k(2,m) \leq 2(m-1) + N$ for all $m \geq 1$.*

The estimate in Lemma 6 (3) implies that

$$u_k(2,1) \leq u_k(2,m) - 2(m-1) \leq u_k(2,1) + (m-1)$$

for all $m \geq 1$. By Corollary 8, these estimates are not strong enough to conclude the finiteness of $u(k(t))$.

I have recently improved the estimates in Lemma 6 to obtain the following result.

Theorem 9. *$u_k(2,m) \leq M + \frac{5}{2}(m-1)$ for some positive constant M and for all $m \geq 1$.*

This improvement of Lemma 6, the first improvement since [L], is still not strong enough to prove the finiteness of $u(k(t))$, but there is hope that additional improvements will still be possible.

References

[A] M. Amer, *Quadratische Formen über Funktionenkörpern*, unpublished dissertation, Johannes Gutenberg-Universität, Mainz (1976).

[B] A. Brumer, *Remarques sur les couples de formes quadratiques*, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 16, A679–A681.

[L] D. Leep, *Systems of quadratic forms*, J. reine angew. Math. **350**, (1984), 109-116.

Strong Approximation Theorem for absolutely irreducible varieties over P$\mathcal{S}$C Galois extensions of number fields

Aharon Razon

(joint work with W.-D. Geyer, M. Jarden)

Let K be a number field, $\mathcal{V}$ an infinite proper subset of the set of all primes of K, and $\mathcal{S}$ a finite subset of $\mathcal{V}$. Denote the maximal Galois extension of K in which each $\mathfrak{p} \in \mathcal{S}$ totally splits by $K_{\mathrm{tot},\mathcal{S}}$. For each $\mathfrak{p} \in \mathcal{V}$, let $\hat{K}_\mathfrak{p}$ be a completion of K at $\mathfrak{p}$. If $\mathfrak{p}$ is non-archimedean, let $\hat{\mathcal{O}}_{K,\mathfrak{p}}$ be its valuation ring and let $\tilde{\hat{\mathcal{O}}}_{K,\mathfrak{p}}$ be the integral closure of $\hat{\mathcal{O}}_{K,\mathfrak{p}}$ in the algebraic closure, $\tilde{\hat{K}}_\mathfrak{p}$, of $\hat{K}_\mathfrak{p}$. For an algebraic extension M

of K and $\mathcal{U} \subseteq \mathcal{V}$, let $\mathcal{O}_{M,\mathcal{U}} = \{z \in M \mid |z^\sigma|_\mathfrak{p} \leq 1 \ \forall \mathfrak{p} \in \mathcal{U} \ \forall \sigma \in \mathrm{Gal}(K)\}$. (The absolute value $| \ |_\mathfrak{p}$ is extended from K to $\hat{K}_\mathfrak{p}$ and then to $\tilde{\hat{K}}_\mathfrak{p}$ in which we embed $\tilde{K}$.)

For $\sigma = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$, let $K_s(\sigma) = \{x \in K_s \mid \sigma_i(x) = x, \, i = 1, \ldots, e\}$ and let $K_s[\sigma]$ be the maximal Galois extension of K contained in $K_s(\sigma)$. Then, for almost all $\sigma \in \mathrm{Gal}(K)^e$ (with respect to the Haar measure), the field $M = K_s[\sigma] \cap K_{\mathrm{tot},\mathcal{S}}$ satisfies the following strong approximation theorem: Let $V \subseteq \mathbb{A}^n$ be an affine absolutely irreducible variety defined over K and let $\mathcal{T} \supseteq \mathcal{S}$ be a finite subset of $\mathcal{V}$ such that the primes in $\mathcal{U} = \mathcal{V} \smallsetminus \mathcal{T}$ are non-archimedean. Suppose that $V(\tilde{\hat{\mathcal{O}}}_{K,\mathfrak{p}}) \neq \emptyset$ for each $\mathfrak{p} \in \mathcal{U}$ and that there exist a finite Galois extension $\hat{L}_\mathfrak{p}$ of $\hat{K}_\mathfrak{p}$ and a nonempty $\mathfrak{p}$-open subset $\Omega_\mathfrak{p}$ of $V_{\mathrm{simp}}(\hat{L}_\mathfrak{p})$ for each $\mathfrak{p} \in \mathcal{T}$ such that $\Omega_\mathfrak{p}$ is invariant under $\mathrm{Gal}(\hat{L}_\mathfrak{p}/\hat{K}_\mathfrak{p})$ and $\hat{L}_\mathfrak{p} = \hat{K}_\mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{S}$. Then, there exists $\mathbf{z} \in V(\mathcal{O}_{M,\mathcal{U}})$ such that $\mathbf{z}^\sigma \in \Omega_\mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{T}$ and each $\sigma \in \mathrm{Gal}(K)$.

Relaxing "$\hat{L}_\mathfrak{p}$ is a finite Galois extension of $\hat{K}_\mathfrak{p}$" to "$\hat{L}_\mathfrak{p} = \tilde{\hat{K}}_\mathfrak{p}$" for $\mathfrak{p} \in \mathcal{T} \smallsetminus \mathcal{S}$ in the local conditions, the strong approximation theorem can be extended to absolutely irreducible affine varieties V defined over M by replacing the field K with a finite subextension of M/K over which V is defined.

Definable henselian valuations

Jochen Koenigsmann

(joint work with Franziska Jahnke)

The arithmetic of henselian valued fields is largely (and in residue characteristic 0 entirely) determined by the arithmetic of residue field and value group. Conversely, in most natural examples, the henselian valuation is encoded in the arithmetic of the field.

In this talk we investigate the question when a henselian field K admits a henselian valuation v encoded in the arithmetic of K in the sense that the valuation ring $\mathcal{O}_v$ be definable by a first-order formula $\phi(x)$ in the language $\mathcal{L}_{ring} = \{+, \cdot; 0, 1\}$:

$$\mathcal{O}_v = \{x \in K \mid \phi(x)\}.$$

Using three technical ingredients

- canonical p-henselian valuations
- topologically henselian fields á la Prestel-Ziegler
- an analysis of regular and *antiregular* ordered abelian groups

we give a complete classification of such fields in residue characteristic $p = 0$. If $p > 0$ the same classification goes through for tame fields, and, modulo a conjectured weak converse Ax-Kochen/Ershov principle, in general.

In any case, almost all henselian valued fields do admit a definable henselian valuation (using at most one, typically zero parameters).

Local points on supersingular elliptic curves over $\mathbb{Z}_p$ extensions

Mirela Ciperiani

Let E be an elliptic curve defined over $\mathbb{Q}$ and p a rational prime such that

- $p \geq 5$,
- E has supersingular reduction at p.

Consider a finite extension $L/\mathbb{Q}_p$ and a $\mathbb{Z}_p$-extension L_∞/L. Denote by L_n the unique subextension of L_∞ such that $\deg(L_n/L) = p^n$. For simplicity, we assume that $E(\mathbb{Q})_{\mathrm{tors}} = 0$.

Following Kobayashi we define

$$E^+(L_n) = \{P \in E(L_n) \mid \mathrm{tr}_{L_n/L_{m+1}} P \in E(L_m) \text{ for all } m \in 2\mathbb{Z}, 0 \leq m < n\},$$
$$E^-(L_n) = \{P \in E(L_n) \mid \mathrm{tr}_{L_n/L_{m+1}} P \in E(L_m) \text{ for all } m \in 2\mathbb{Z}+1, 0 \leq m < n\}.$$

In the case $L = \mathbb{Q}_p$, the following result was proven by Kobayashi for the cyclotomic $\mathbb{Z}_p$-extension $L_\infty/\mathbb{Q}_p$ and then generalized by Iovita and Pollack to cover all totally ramified extensions $L_\infty/\mathbb{Q}_p$.

Theorem 1 (Kobayashi[Ko], Iovita-Pollack[IP])**.** *If $L_\infty/\mathbb{Q}_p$ is a totally ramified $\mathbb{Z}_p$-extension then*

$$E(L_n) = E^+(L_n) + E^-(L_n) \qquad \text{and} \qquad E^+(L_n) \cap E^-(L_n) = E(L_0)$$

for all $n \geq 1$.

Consider

$$E^\pm(L_\infty) = \varinjlim_n E^\pm(L_n) \subseteq E(L_\infty)$$

and then view

$$E^\pm(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq \mathrm{H}^1(L_\infty, E_{p^\infty})$$

as modules over $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(L_\infty/L]]$. The results of Kobayashi and Iovita - Pollack allow us to deduce that

$$\mathrm{corank}_\Lambda\Big(E^+(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cap E^-(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = 0,$$

and their method of proof also implies that

$$\mathrm{corank}_\Lambda E^\pm(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 1 = \frac{1}{2}\mathrm{corank}_\Lambda \mathrm{H}^1(L_\infty, E_{p^\infty}).$$

We would like to show that

$$\mathrm{corank}_\Lambda\Big(E^+(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cap E^-(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = 0,$$
$$\mathrm{corank}_\Lambda E^\pm(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \frac{1}{2}\mathrm{corank}_\Lambda \mathrm{H}^1(L_\infty, E_{p^\infty}).$$

in greater generality and in particular we want to remove the assumption that $L = \mathbb{Q}_p$. In this talk we described how we prove the following result:

Theorem 2 (Çi)**.** *Let L be a quadratic extension of $\mathbb{Q}_p$ and L_∞/L be the unique anticyclotomic $\mathbb{Z}_p$-extension of L. Then*

$$\mathrm{corank}_\Lambda\Big(E^+(L_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p\cap E^-(L_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p\Big)=0,$$

$$\mathrm{corank}_\Lambda E^\pm(L_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p=\frac{1}{2}\mathrm{corank}_\Lambda \mathrm{H}^1(L_\infty,E_{p^\infty})=2.$$

As an application, we then discussed the effect of this local result on the image complex multiplication points in the Selmer group.

References

[IP] A.Iovita and R.Pollack, *Iwasawa Theory of Elliptic Curves at Supersingular Primes over Towers of Extensions of Number Fields*, J. Reine Angew. Math. **598** (2006), 71–103.

[Ko] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

Period-index and u-invariant questions for fields

R. Parimala
(joint work with V. Suresh)

Let F be a field of characteristic not 2. The u-invariant $u(F)$ is defined to be the maximum dimension of anisotropic quadratic forms over F. The behavior of the u-invariant under rational function field extensions is very little understood.

For any field F, the Brauer p-dimension $Br_p dim(F)$ of F is defined as the least positive integer d such that for any central simple algebra A defined over any finite extension of F of exponent a power of p, the index of A divides the dth power of the exponent. The Brauer dimension of F is the maximum of the Brauer p-dimensions of F as p varies over all primes. The behavior of the Brauer dimension of a field again is very little understood under rational function field extensions.

There is a class of fields where there is way to understand the u-invariant and the Brauer dimension under rational function field extensions. Let K be a complete discrete valued field of characteristic zero with residue field κ. Let F be the function field in one variable over K. Suppose $char(\kappa)=p$. Let l be a prime not equal to p. Harbater, Hartmann and Krashen prove that for a prime l not equal to p, if $Br_l dim(\kappa')\leq d$ for every finite extension κ' of κ and if $br_l dim(E)\leq d+1$ for every function field E in one variable over κ, then $Br_l dim(F)\leq d+2$. This result for K a p-adic field is due to Saltman. It remained open whether $Br_p dim(F)$ is finite for function fields of p-adic curves.

Let κ be a field of characteristic $p>0$. The p-rank of κ is d if $[\kappa:\kappa^p]=p^d$. We prove that if K is a complete discrete valued field of characteristic zero with residue field κ of characteristic $p>0$ with p-rank of κ equal to d, then, for a function field F in one variable over K, $Br_p dim(F)\leq 2d+2$. We also prove that if the residue field κ is a perfect field of characteristic 2, $u(F)\leq 8$. For function fields of p-adic curves, it follows that the Brauer dimension is 2. Further the u-invariant of function fields of dyadic curves is 8, a result due to Heath-Brown and Leep.

The main ingredients in the proof are Kato's filtration of the p-part of the Brauer group of a complete discrete valued field of characteristic zero with residue field of characteristic p and the patching theorems of Harbater-Hartmann-Krashen.

The inverse Galois problem and orthogonal groups

David Zywina

The Inverse Galois Problem asks whether every finite group occurs as the Galois group of some extension of $\mathbb{Q}$. This is a very difficult problem, and it is interesting to prove it for special classes of simple groups.

Fix an odd integer $n \geq 5$ and a prime $\ell \geq 5$. Let $\mathrm{O}(V)$ be the group of automorphisms of a non-degenerate quadratic space (V, q) with $\dim_{\mathbb{F}_\ell} V = n$. The commutator subgroup $\Omega(V)$ of $\mathrm{O}(V)$ is then a simple group (up to isomorphism, it depends only on n and ℓ). Our main result is the following:

Theorem 1. *The group $\Omega(V)$ occurs as the Galois group of an extension of $\mathbb{Q}$ (moreover, it occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$).*

Reiter [3] proved Theorem 1 in the special case where 2 or 3 is not a square modulo ℓ. Additional special cases of Theorem 1 for $n = 5$ and 7 were proved by Häfner [1].

Consider the case $n = 5$. In this case, we have an exceptional isomorphism $\Omega(V) \cong \mathrm{PSp}_4(\mathbb{F}_\ell)$. For simplicity, we suppose that $\ell \geq 17$.

For a fixed $s \in \mathbb{Q} - \{0, 1, -1\}$, consider the Weierstrass equation

$$(t-s)y^2 = x^3 + 3(t^2-1)^3 x - 2(t^2-1)^5. \tag{1}$$

This gives rise to an elliptic scheme $E \to U := \mathbb{A}^1_{\mathbb{Q}} - \{0, 1, -1, s\}$. Let $E[\ell]$ be the ℓ-torsion subscheme of E; it can be viewed as a lisse sheaf of $\mathbb{F}_\ell$-modules over U. Taking étale cohomology, we obtain an $\mathbb{F}_\ell$-vector space

$$V_\ell := H^1_{\text{ét}}\big(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(E[\ell])\big),$$

where $j\colon U \hookrightarrow \mathbb{P}^1_{\mathbb{Q}}$ is the inclusion morphism. The $\mathbb{F}_\ell$-vector space V_ℓ has dimension 5 and is acted upon by the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We could have also defined V_ℓ as a factor of the group $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$ for a related algebraic surface $X/\mathbb{Q}$.

Using the Weil pairing on $E[\ell]$ and the cup product, we obtain a non-degenerate symmetric pairing $V_\ell \times V_\ell \to \mathbb{F}_\ell$. The Galois action respects the pairing, and we have a representation

$$\rho_{s,\ell}\colon\ \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{O}(V_\ell).$$

Using big monodromy arguments of Hall from [2], we show that

$$\rho_{s,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \supseteq \Omega(V_\ell)$$

for "most" s.

Fix such an s; we may further assume that it is of the form $(-w^2+3)/(w^2+3)$ for some $w \in \mathbb{Q}$. We show that $\rho_{s,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \pm\Omega(V_\ell)$; this requires some known cases of the Birch and Swinnerton-Dyer conjecture for elliptic curves over global function fields. The connection with $\rho_{s,\ell}$ being that for all but finitely many primes $p \neq \ell$, we have

$$\det(I - \rho_{s,\ell}(\mathrm{Frob}_p)T) \equiv L(T/p, E_{s,p}) \pmod{\ell},$$

where $E_{s,p}$ is the elliptic curve over $\mathbb{F}_p(t)$ defined by (1) and $L(T, E_{s,p}) \in \mathbb{Z}[T]$ is its L-function. More precisely, we use a refined version of BSD to show that $2L(1/p, E_{s,p})$ and $2L(-1/p, E_{s,p})$ are both squares in $\mathbb{Q}$.

Having an $s \in \mathbb{Q} - \{0, 1, -1\}$ for which $\Omega(V_\ell) \subseteq \rho_{s,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \pm\Omega(V_\ell)$, we then obtain $\Omega(V_\ell)$ as the Galois group of an extension of $\mathbb{Q}$ (note that the image of $\Omega(V_\ell)$ and $\pm\Omega(V_\ell)$ in $\mathrm{O}(V_\ell)/\{\pm I\}$ are both isomorphic to $\Omega(V_\ell)$).

References

[1] F. Häfner. Einige orthogonale und symplektische Gruppen als Galoisgruppen über **Q**. *Math. Ann.*, 292(4):587–618, 1992.

[2] C. Hall. Big symplectic or orthogonal monodromy modulo *l*. *Duke Math. J.*, 141(1):179–203, 2008.

[3] S. Reiter. Galoisrealisierungen klassischer Gruppen. *J. Reine Angew. Math.*, 511:193–236, 1999.

On the Oort conjecture

Andrew Obus

(joint work with Stefan Wewers, Florian Pop)

The *lifting problem for branched covers of curves* asks whether a branched Galois cover of smooth projective curves in characteristic p lifts to characteristic zero. While this question appears to be global, it has in fact been shown to be strictly local. That is, it is sufficient to show that every germ of the cover lifts to characteristic zero. This reduces the lifting problem for branched covers of curves to the following *local lifting problem:*

Problem 1 (Local lifting problem)**.** Let k be an algebraically closed field of characteristic p, let $K/k((t))$ be a G-Galois extension, and let A be the integral closure of $k[[t]]$ in K. Does there exist a complete discrete valuation ring (R, π) of characteristic 0 with residue field k and a finite Galois extension of $\mathrm{Frac}(R[[t]])$ with Galois group G in which the integral closure of $R[[t]]$ has reduction modulo π that is $k[[t]]$-isomorphic to A? If so, can we say anything about R?

The *Oort conjecture* (now a theorem of Obus-Wewers and Pop) states that the local lifting problem always has a solution when G is cyclic. If $p^3 \nmid |G|$, it is further known that one can take $R = W(k)(\zeta_{|G|})$. For other cyclic groups G, this is expected to hold, but is an open question.

For the proof of the Oort conjecture, one first easily reduces to the case $G \cong \mathbb{Z}/p^n$, for some $n \geq 1$. The proof is divided into two parts. In order to state these parts more precisely, we introduce the concept (due to Pop) of *essential ramification.* A cyclic $\mathbb{Z}/p^n$-extension of $k[[t]]$ has n jumps $(u_1, \ldots, u_n)$ in the higher ramification filtration for the upper numbering, the so-called *upper jumps.* By the Hasse-Arf theorem, these numbers are all integers. In fact, one can show that $u_{i+1} \geq pu_i$ for all $i \leq n-1$, and that if $u_{i+1} \neq pu_i$, then $p \nmid u_{i+1}$.

Definition 2. A $\mathbb{Z}/p^n$-extension of $k[[t]]$ with upper jumps $(u_1, \ldots, u_n)$ is said to have *no essential ramification* if, for every $1 \leq i \leq n-1$, we have $u_{i+1} < pu_i + p$.

Theorem 3 (Obus-Wewers, [OW12]). *If a $\mathbb{Z}/p^n$-extension of $k[[t]]$ has no essential ramification, then it can be lifted to characteristic zero.*

In Pop's paper [Pop12], it is shown that any $\mathbb{Z}/p^n$-extension of $k[[t]]$ has an equicharacteristic deformation to an extension of $k[[t,s]]$, whose generic fiber has no essential ramification (in this case, since the generic fiber is an extension of $k[[t,s]][s^{-1}]$, "no essential ramification" means no essential ramification over each ramified maximal ideal). Pop is then able to use this deformation, together with Theorem 3, to prove

Theorem 4 (Pop, [Pop12]). *The Oort conjecture holds.*

There are several ways of going about this proof. The one discussed in the talk first constructs a $\mathbb{Z}/p^n$-cover of $\mathbb{P}^1_k$ totally ramified at one point, where the germ above the branch point is the original extension of $k[[t]]$ (this technique is due to Katz-Gabber-Harbater). Then, using the equicharacteristic deformation and Theorem 3, it can be shown that this cover lifts over a rank 2, characteristic zero valuation ring $\mathcal{R}$ with residue field k. An application of Robinson's theorem then shows that the lifting can be accomplished over a finite extension $R/W(k)$. Taking the relevant germ of this cover gives a lift of the original extension over R.

If G is a group for which the local lifting problem has a solution for all G-extensions, then G is known as an *Oort group.* By Theorem 4, all cyclic groups are Oort groups. Determining the list of Oort groups is a difficult open problem.

Work of Chinburg-Guralnick-Harbater and Brewis-Wewers has shown that the only possible Oort groups are the cyclic groups, the dihedral groups of order $2p^n$ for some n, and the alternating group A_4 for $p = 2$. It has been asserted by Bouw that A_4 is, in fact, an Oort group. We conjecture:

Conjecture 5. *The dihedral groups D_{p^n} of order $2p^n$ for* odd *p are Oort groups.*

More generally, for metacyclic groups of the form $G = \mathbb{Z}/p^n \rtimes \mathbb{Z}/m$, where $p \nmid m$, there is a known obstruction to lifting, called the *Bertin obstruction*, which involves the higher ramification groups of the given extension. If the upper jumps of the $\mathbb{Z}/p^n$-subextension are $(u_1, \ldots, u_n)$, then the Bertin obstruction vanishes if and only if G is abelian or center-free, and if each $u_i \equiv -1 \pmod{m}$ when G is center-free. This obstruction vanishes when $m = 2$, as all upper jumps must be odd. The following conjecture generalizes Conjecture 5:

Conjecture 6. *For groups of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$, where $p \nmid m$, the Bertin obstruction is the only obstruction to the local lifting problem.*

Proving this conjecture is equivalent to showing that lifts of certain cyclic local extensions can be obtained in "$\mathbb{Z}/m$-equivariant" ways. Preliminary progress toward this conjecture has been made by Obus and Wewers. It should be mentioned that, in the previous literature, to the best of our knowledge, there is not a single non-cyclic $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$-extension with $p \nmid m$ and vanishing Bertin obstruction which is known either to lift or not to lift!

The case of dihedral groups of 2-power order appears to be much more complicated. However, Pagot has shown that $\mathbb{Z}/2 \times \mathbb{Z}/2$ is an Oort group, and Brewis has exhibited an example of a D_4-extension in characteristic 2 that lifts to characteristic zero.

References

[OW12] A. Obus and S. Wewers, Cyclic extensions and the local lifting problem, to appear in *Ann. of Math.*. arXiv:1208.3909

[Pop12] F. Pop, Lifting of curves, preprint, arXiv:1203.1867.

Higher reciprocity laws and rational points

V. Suresh

(joint work with J.-L. Colliot-Thélène and R. Parimala)

Let K be a number field and Ω_K be the set of places of K. For $v \in \Omega_K$, let K_v denote the completion of K at v. A classical theorem of Hasse and Minkowski asserts that a quadratic form q over K is isotropic if it is isotropic over K_v for all $v \in \Omega_K$.

One has more general local-global principles for homogeneous spaces under connected linear algebraic groups. Let X be a projective homogeneous space under a connected linear algebraic group defined over a number field K. A theorem of Harder asserts that if $X(K_v) \neq \varnothing$, $\forall v \in \Omega_K$, then $X(K) \neq \varnothing$. For principle homogeneous spaces under a semisimple simply connected linear algebraic groups, a similar local-global result holds (Kneser, Harder, Chernousov). For a adjoint, quasi-split or K-rational connected linear algebraic groups over K, a similar local-global principle is a theorem of Sansuc.

Let K be a complete discrete valued field with residue field κ algebraically closed. Let X be a smooth projective curve over K and $F = K(X)$. Let Ω_F be the set of all discrete valuations of F. For $\nu \in \Omega_F$, let F_ν denote the completion of F at ν. Let G be a connected linear algebraic group over F and

$$Ш^1(F, G) = ker(H^1(F, G) \to \prod_{\nu \in \Omega} H^1(F_\nu, G)).$$

The set $Ш^1(F, G)$ classifies all principal homogeneous spaces which have rational points over F_ν for all $\nu \in \Omega_F$. A theorem of Harbater-Hartmann-Krashen asserts that if G is a connected linear algebraic group over F which is F-rational, then $Ш^1(F, G) = \{1\}$.

In this talk we construct an example of a torus T over $F = \mathbb{C}((t))(x)$ with $Ш^1(F,T) \neq \{1\}$, thereby showing that the theorem of Harbater-Hartmann-Krashen need not hold if G is not F-rational.

To construct our example we introduce an obstruction using a Bloch-Ogus complex.

The Zassenhaus Filtration & The Structure of Absolute Galois Groups

Ido Efrat

Let G be a profinite group and p a prime number. The lower p-central filtration $G^{(n)}$ and the p-Zassenhaus filtration $G_{(n)}$ of G are defined inductively by:

$$G^{(1)} = G, \quad G^{(n)} = \prod_{i+j=n} [G^{(i)}, G^{(j)}] \cdot (G^{(n-1)})^p$$

$$G_{(1)} = G, \quad G_{(n)} = \prod_{i+j=n} [G_{(i)}, G_{(j)}] \cdot (G_{(\lceil n/p \rceil)})^p.$$

One has $G^{(2)} = G_{(2)} = [G,G]G^p = \bigcap\{N \triangleleft G \mid G/N \cong \mathbb{Z}/p\}$.

When $G = G_F$ is the absolute Galois group of a field F containing a root of unity of order p, the following is known:

Theorem. (1) For $p=2$, $G^{(3)} = G_{(3)} = \bigcap\{N \triangleleft G \mid G/N \cong \mathbb{Z}/2, \mathbb{Z}/4,\ D_4\}$ (Mináč–Spira, Ann. Math. 1996);
(2) For $p > 2$, $G^{(3)} = \bigcap\{N \triangleleft G \mid G/N \cong \mathbb{Z}/p^2,\ M_{p^3}\}$ (E–Mináč, Amer. J. Math. 2011);
(3) For $p > 2$, $G_{(3)} = \bigcap\{N \triangleleft G \mid G/N \cong \mathbb{Z}/p,\ H_{p^3}\}$ (E–Mináč).

Here, for p odd, M_{p^3} (resp., H_{p^3}) is the unique non-abelian group of order p^3 and exponent p^2 (resp., p). The proofs are based on the Merkurjev–Suslin theorem. The importance of $G_{(3)}$ and $G^{(3)}$ is demonstrated by the following result:

Theorem (E–Mináč)**.** For $G = G_F$ as above, $G/G_{(3)}$ determines the cohomology ring $H^*(G) = H^*(G, \mathbb{Z}/p)$ (with the cup product) and vice versa.

Note that when $p > 2$ (resp., $p = 2$), the group $G/G_{(3)}$ has exponent dividing p (resp. ≤ 4). A analogous result for $G/G^{(3)}$ was proved jointly with Chebolu and Mináč (Math. Ann. 2012).

We reported on a generalization of the above intersection theorems for higher terms in the Zassenhaus filtration $G_{(n)}$. In the (much simpler) special case where G is a free pro-p group the result states:

$$\begin{aligned} G_{(n)} &= \bigcap_{\rho} \mathrm{Ker}(\rho), \quad \rho\colon G \to \mathrm{GL}_n(\mathbb{F}_p) \text{ is a continuous homomorphism} \\ &= \bigcap\{N \trianglelefteq G \mid G/N \leq \mathbb{U}_n(\mathbb{F}_p)\}. \end{aligned}$$

Here $\mathbb{U}_n(\mathbb{F}_p)$ denotes the group of all $n \times n$ unipotent upper-triangular matrices over $\mathbb{F}_p$.

More generally, suppose that G is a profinite group satisfying:

(A1) There is a presentation $1 \to N \to S \to G(p) \to 1$, with S a free profinite group and $N \le S_{(n)}$.

(A2) Denoting the subgroup of $H^2(G)$ generated by the image of the n-fold Massey product $H^1(G)^n \to H^2(G)$ by $H^2(G)_{n-\mathrm{Massey}}$, the kernel

$$\mathrm{Ker}\big(H^2(G/G_{(n)})_{n-\mathrm{Massey}} \xrightarrow{\mathrm{inf}} H^2(G)\big)$$

is generated by n-fold Massey products.

We remark that under (A1), the n-fold Massey product is a single-valued map, by results of Vogel (Crelle 2005), so (A2) makes sense.

Main Theorem. Assuming (A1) and (A2),

$$G_{(n+1)} = \bigcap\{N \trianglelefteq G \mid G/N \le \mathbb{U}_{n+1}(\mathbb{F}_p)\}.$$

Assumptions (A1) and (A2) hold e.g., in the following cases:

(a) When $n = 2$ and $G = G_F$ for a field F containing a root of unity of order p;

(b) When $\mathrm{cd}_p(G) \le 1$.

In particular, we recover the previously known intersection theorems for $G_{(3)}$, as well as the above special case.

The 2-fold Massey product is just the cup product, so (A2) in case (a) follows easily from the injectivity of the Galois symbol map $K_2^M(F)/p \to H^2(G)$ (Merkurjev–Suslin). This leads to the following

Problem. Generalize the Merkurjev–Suslin theorem to n-fold Massey products.

On Galois sections for hyperbolic *p*-adic curves

Jakob Stix
(joint work with Florian Pop)

This note advocates a valuation theoretic point of view on Grothendieck's section conjecture in general, and for hyperbolic curves over p-adic fields in particular.

1. Valuative point of view towards the section conjecture

1.1. **Packets of sections.** Let X/k be a normal, geometrically irreducible variety with function field K. Let Gal_K be the absolute Galois group of K, and view the étale fundamental group $\pi_1(X)$ as its maximal quotient unramified over X:

$$\mathrm{Gal}_K \twoheadrightarrow \mathrm{Gal}(\tilde{K}/K) = \pi_1(X).$$

Let w be a Krull k-valuation of K with residue field $\kappa(w) = k$. The decomposition group $D_{\tilde{w}|w} \subseteq \pi_1(X)$ determined by a prolongation $\tilde{w} \mid w$ to $\tilde{K}$ admits a natural projection $D_{\tilde{w}|w} \twoheadrightarrow \mathrm{Gal}_{\kappa(w)}$ that always has a splitting $\sigma : \mathrm{Gal}_{\kappa(w)} \to D_{\tilde{w}|w}$. We obtain a **Galois section**, i.e., a section of $\pi_1(X) \to \mathrm{Gal}_k$, as follows:

$$s_w : \mathrm{Gal}_k = \mathrm{Gal}_{\kappa(w)} \xrightarrow{\sigma} D_{\tilde{w}|w} \to \pi_1(X).$$

The section s_w depends on the choice of splitting σ and on the choice of $\tilde{w}$. The collection of all such s_w associated to w is the **packet** of sections at w.

1.2. **The section conjecture.** Recall that a **hyperbolic** curve is a smooth geometrically connected curve with non-abelian geometric étale fundamental group.

Conjecture 1 (Grothendieck's section conjecture [G83])**.** *Let k be a number field and X/k a hyperbolic curve. Then every Galois section $s : \mathrm{Gal}_k \to \pi_1(X)$ is of the form s_w for a suitable choice of k-valuation w on the function field of X.*

Remark 2. (1) Since the injectivity of the section map for hyperbolic curves

$$X(k) \to \{s : \mathrm{Gal}_k \to \pi_1(X) \ ; \ \text{Galois section}\}, \quad a \mapsto s_a$$

is well known, Conjecture 1 is equivalent to the original version from [G83].

(2) In fact, the valuation theoretic formulation of Conjecture 1 takes care of the necessary correction of the original statement, see already in [G83], due to cuspidal sections coming from rational points from the boundary of the compactification.

(3) With $\mathrm{Gal}_K \to \mathrm{Gal}_k$ instead of $\pi_1(X) \to \mathrm{Gal}_k$ we obtain a birational version of the section conjecture. This is in fact a theorem for the variant where k is a finite extension of $\mathbb{Q}_p$ due to Koenigsmann [K03].

2. Valuations on p-adic fields

2.1. **The main theorem.** We are now concerned with the p-adic version of Conjecture 1. From now on, let $k/\mathbb{Q}_p$ be a finite extension with p-adic valuation v, ring of integers $\mathfrak{o}_k$, and residue field $\mathbb{F}$. The variety X/k will be a hyperbolic curve. We define

$$\mathrm{Val}_v(K) = \{w \ ; \ \text{Krull valuation on } K \text{ extending } v \text{ on } k\}$$

and similarly $\mathrm{Val}_v(\tilde{K})$. Then the main result of [PS09] is the following.

Theorem 3. *Let $k/\mathbb{Q}_p$ be a finite extension and X/k a hyperbolic curve with function field K. Then for every Galois section $s : \mathrm{Gal}_k \to \pi_1(X) = \mathrm{Gal}(\tilde{K}/K)$ there is a valuation $\tilde{w} \in \mathrm{Val}_v(\tilde{K})$ such that with $w = \tilde{w}|_K$*

$$s(\mathrm{Gal}_k) \subseteq D_{\tilde{w}|w} \subseteq \pi_1(X).$$

Remark 4. (1) Theorem 3 confirms a p-adic version of Conjecture 1: every Galois section is of the form s_w for a suitable valuation. Only the class of valuations has to take into account also the more "arithmetic" compactification by flat projective $\mathfrak{o}_k$-models of X, see below for the description of $\mathrm{Val}_v(\tilde{K})$. For an assertion towards the uniqueness of the valuation w in Theorem 3 we refer to [PS09].

(2) We set v_a for the k-valuation of K corresponding to the k-rational point $a \in X(k)$. The composition of valuations $w_a = v \circ v_a$ yields a map

$$X(k) \to \mathrm{Val}_v(K), \quad a \mapsto w_a$$

such that $D_{w_a} = s_a(\mathrm{Gal}_k)$ up to conjugation. The p-adic section conjecture follows from Theorem 3 if only valuations of the form w_a admit sections of $D_{\tilde{w}|w} \to \mathrm{Gal}_k$.

(3) If the p-adic section conjecture turns out to be wrong, then Theorem 3 yields the analogous correction with sections coming from valuations centered at infinity as in the case for affine curves with Grothendieck's original conjecture in [G83].

(4) There are conditional results due to Saïdi to lift Galois sections at least partially towards birational Galois sections, namely to the cuspidally abelian quotient of Gal_K relative X, with the idea in mind to reduce the p-adic section conjecture to Koenigsmann's Theorem recalled above. Further weaker but unconditional lifting results are obtained by Borne/Emsalem together with the author.

(5) Hoshi has shown that the geometrically pro-p version of the section conjecture fails in explicit examples where non-geometric sections exist.

(6) Mochizuki deals with an analogue regarding Galois sections for the tempered fundamental group of André, a group which is pro-discrete rather than pro-finite.

2.2. **An application.** Theorem 3 has the following consequence for Galois sections (trivial for Galois sections coming from k-rational points).

Theorem 5. *Let $k/\mathbb{Q}_p$ be a finite extension and X/k a proper hyperbolic curve with proper flat model $\mathscr{X} \to \mathrm{Spec}(\mathfrak{o}_k)$. Let $Y = \mathscr{X}_{\mathbb{F}}$ be the special fibre.*

1. *If there is a Galois section $s : \mathrm{Gal}_k \to \pi_1(X)$, then the geometric specialisation map $\overline{\mathrm{sp}} : \pi_1(X \otimes k^{\mathrm{alg}}) \twoheadrightarrow \pi_1(Y \otimes \mathbb{F}^{\mathrm{alg}})$ is surjective.*
2. *Every Galois section $s : \mathrm{Gal}_k \to \pi_1(X)$ specialises to a unique Galois section $t : \mathrm{Gal}_{\mathbb{F}} \to \pi_1(Y)$, i.e., there is a commutative diagram*

$$\begin{tikzcd}
\pi_1(X) \arrow[r, two heads, "\mathrm{sp}"] \arrow[d, shift left] & \pi_1(Y) \arrow[d, shift right] \\
\mathrm{Gal}_k \arrow[r, two heads] \arrow[u, dotted, shift left, "s"] & \mathrm{Gal}_{\mathbb{F}} . \arrow[u, dotted, shift right, "t"']
\end{tikzcd}$$

2.3. **The Riemann–Zariski space.** The space of valuations $\mathrm{Val}_v(\tilde{K})$ can be more geometrically understood as the Riemann–Zariski pro-space of (the closed fibres of) all models. Let $X_H \to X$ be the finite étale cover corresponding to an open subgroup $H \subseteq \pi_1(X)$, and let $\mathscr{X}_H$ be a proper flat $\mathfrak{o}_k$-model of X_H. Any $\tilde{w} \in \mathrm{Val}_v(\tilde{K})$ has a unique center in the special fibre $\mathscr{X}_{H,\mathbb{F}}$ by the valuative criterion of properness, i.e., a point $z_{\tilde{w}}$ such that the valuation ring of $\tilde{w}$ dominates the local ring $\mathcal{O}_{\mathscr{X},z_{\tilde{w}}}$. In fact, the map assigning the compatible system of centers

$$(\star) \qquad \mathrm{Val}_v(\tilde{K}) \xrightarrow{\sim} \varprojlim_{H,\mathscr{X}_H} \mathscr{X}_{H,\mathbb{F}}, \quad \tilde{w} \mapsto z_{\tilde{w}}$$

is a homeomorphism of pro-finite spaces (for the patch topology on the left and the constructible topology on the right).

2.4. **Fixed points.** The map ($\star$) is equivariant under $\pi_1(X) = \mathrm{Gal}(\tilde{K}/K)$ and $D_{\tilde{w}|w}$ is precisely the stabilizer of $\tilde{w}$. By the usual compactness argument with projective limits it suffices for Theorem 3 to show that $\Sigma = s(\mathrm{Gal}_k) \subset \pi_1(X)$ has a fixed point (generic or closed)

$$(\mathscr{X}_{H,\mathbb{F}})^{\Sigma} \neq \emptyset$$

for a cofinal set of open normal subgroups $H \lhd \pi_1(X)$ and equivariant models $\mathscr{X}_H$ on which Σ acts via a finite subgroup of $\pi_1(X)/H$. Thus we first may assume $\mathscr{X}_H$ is a regular semistable model. The fibres of the projection to the stable model

$$\mathscr{X}_H \to \mathscr{X}_{H,\mathrm{stable}}$$

are trees of projective lines. Since a tree is a CAT(0)-space, any action by a finite group on a tree has fixed points. It follows that the fibre over a Σ-fixed point of $(\mathscr{X}_{H,\mathrm{stable}})_{\mathbb{F}}$ again has a Σ-fixed point. We may therefore restrict to stable models.

3. The ℓ-adic Brauer group method

3.1. **The locus of a Brauer class.** Although it is counterintuitive that ℓ-adic methods actually are able to detect the arithmetic in a Galois section, we next fix a prime $\ell \neq p$. The Brauer group method going back to Neukirch in the study of absolute Galois groups of number fields is here based on the following.

The relative Brauer group $\ker(\mathrm{Br}(k) \to \mathrm{Br}(X))$ is cyclic of order the index of X due to Roquette and Lichtenbaum. By [S10] the presence of a section implies that the index is in fact a power of p, so that the map on ℓ-torsion

$$\mathrm{Br}(k)[\ell] \hookrightarrow \mathrm{Br}(X)[\ell] \subseteq \mathrm{Br}(K)[\ell]$$

is injective. In the limit over all neighbourhoods of s, i.e., for the fixed field $M = \tilde{K}^{\Sigma}$, the map $\mathrm{Br}(k)[\ell] \hookrightarrow \mathrm{Br}(M)[\ell]$ remains injective. We now need a fine local–global principle for the Brauer group due to Pop:

Theorem 6 ([P88] Thm 4.5)**.** *Let $k/\mathbb{Q}_p$ be a finite extension and M/k a function field of transcendence degree 1 over k. Then the restriction map*

$$\mathrm{Br}(M) \hookrightarrow \prod_{w \in \mathrm{Val}_v(M)} \mathrm{Br}(M_w^{\mathrm{h}})$$

is injective. Here M_w^{h} denotes the henselisation of M in the valuation w.

It follows that there is a valuation $w_M \in \mathrm{Val}_v(M)$ such that $\mathrm{Br}(k)[\ell]$ survives in $\mathrm{Br}(M_{w_M}^{\mathrm{h}})$. Let $\tilde{w}$ be an extension of w_M to $\tilde{K}$. Since $\mathrm{Gal}(\tilde{K}/M) = \Sigma \simeq \mathrm{Gal}_k$, all intermediate fields are composita with extensions k'/k of the same degree. It follows that $[(\tilde{K} \cap M_{w_M}^{\mathrm{h}}) : M]$ is prime to ℓ since otherwise $\mathrm{Br}(k)[\ell]$ would not survive. Therefore a suitable choice of ℓ-Sylow subgroup $\Sigma_\ell \subset \Sigma$ is contained in

$$(\star\star) \qquad \Sigma_\ell \subseteq \mathrm{Gal}(\tilde{K}/\tilde{K} \cap M_{w_M}^{\mathrm{h}}) = D_{\tilde{w}|w_M} \subseteq D_{\tilde{w}|w}.$$

3.2. **Inertia.** Let $\Theta \subseteq \Sigma$ be the image under s of the inertia group $I_k \subseteq \mathrm{Gal}_k$ and let $I_{\tilde{w}|w} \subseteq D_{\tilde{w}|w}$ denote the inertia group of $\tilde{w}$. Based on ($\star\star$) with considerable more work for valuations $\tilde{w}$ associated to generic points of components of the special fibre one may show the following.

Proposition 7. *It is possible to choose $\tilde{w}$ such that $\Theta_\ell \subseteq I_{\tilde{w}|w}$, where Θ_ℓ is a choice of ℓ-Sylow group of Θ.*

4. Independence of ℓ-adic ramification

4.1. **The kernel of specialisation.** Let $H \lhd \pi_1(X)$ be an open normal subgroup such that X_H has a stable model $\mathscr{X}_{H,\mathrm{stable}}$. We write $Y = \bigcup_\alpha Y_\alpha$ for the union of irreducible components of its reduced special fibre and may further assume that all Y_α are smooth and have genus ≥ 1. We consider the kernel of specialisation

$$N_H := \ker\big(H = \pi_1(X_H) \twoheadrightarrow \pi_1(\mathscr{X}_H)\big)$$

which contains $I_{\tilde{w}|w} \cap H$ for every valuation $\tilde{w} \in \mathrm{Val}_v(\tilde{K})$. We further set

$$V_H = N_H^{\mathrm{ab}} \widehat{\otimes} \mathbb{Q}_\ell$$

and for each $\tilde{w} \in \mathrm{Val}_v(\tilde{K})$ we define a set of cardinality 1 or 2

$$A_{\tilde{w}} = \{\alpha \ ; \ Y_\alpha \text{ contains the center of } \tilde{w} \text{ on } \mathscr{X}_{H,\mathrm{stable}}\}.$$

By ℓ-adic étale cohomology computations and logarithmic geometry we show the following statement on independence of ℓ-adic inertia. For simplicity of notation we denote the discrete rank 1 valuation of $\tilde{K}^H$ associated to Y_α by α.

Proposition 8. (1) *For any choice of prolongation $\tilde{\alpha} \in \mathrm{Val}_v(\tilde{K})$ of each α, the natural map*

$$\bigoplus_\alpha I_{\tilde{\alpha}|\alpha}^{\mathrm{ab}} \otimes \mathbb{Q}_\ell \hookrightarrow V_H$$

is injective.

(2) *For every $\tilde{w} \in \mathrm{Val}_v(\tilde{K})$ the map $I_{\tilde{w}|w} \cap H \to N_H \to V_H$ factors as*

$$I_{\tilde{w}|w} \cap H \to \bigoplus_{\alpha \in A_{\tilde{w}}} I_{\tilde{\alpha}|\alpha}^{\mathrm{ab}} \otimes \mathbb{Q}_\ell \hookrightarrow V_H.$$

4.2. **Sketch of proof for the existence of fixed points.** Let $\sigma \in \Sigma = s(\mathrm{Gal}_k)$ be arbitrary. Since Θ is a normal subgroup in Σ we obtain a commutative diagram

$$\begin{tikzcd}
\Theta_\ell \cap H \arrow[drr] & \subseteq & I_{\tilde{w}|w} \cap H \arrow[dr] & \\
 & & \Theta \cap N_H \arrow[r] & V_H \\
\sigma\Theta_\ell\sigma^{-1} \cap H \arrow[urr] & \subseteq & I_{\sigma(\tilde{w})|w} \cap H \arrow[ur] &
\end{tikzcd}$$

Because s is a Galois section, the composition

$$\mathbb{Z}_\ell(1) \simeq \Theta_\ell \cap H \to V_H \to I_k^{\mathrm{ab}} \otimes \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell(1)$$

is non-trivial. On the other hand, the image of $\Theta \cap N_H$ in V_H spans at most a 1-dimensional subspace, since any closed subgroup of I_k has pro-ℓ completion of rank at most 1. It follows from Proposition 8 that $\Theta \cap N_H$ maps to the subspace

$$\bigcup_{A_{\tilde{w}} \cap A_{\sigma(\tilde{w})}} I^{\mathrm{ab}}_{\tilde{\alpha}|\alpha} \otimes \mathbb{Q}_\ell \hookrightarrow V_H$$

whence $A_{\tilde{w}} \cap A_{\sigma(\tilde{w})} \neq \emptyset$. A combinatorial argument relying again on Proposition 8 shows that either an $\alpha \in A_{\tilde{w}}$ is fixed by Σ, or $A_{\tilde{w}}$ is fixed by Σ as a set and consists of two elements corresponding to components meeting in a unique node. In this way we have found a fixed point under Σ on $\mathscr{X}_{H,\mathrm{stable}}$ and the sketch of the proof of Theorem 3 is complete.

References

[G83] A. Grothendieck, *Brief an Faltings (27/06/1983)*, in: Geometric Galois Action 1 (editors L. Schneps, P. Lochak), LMS Lecture Notes **242**, Cambridge 1997, 49–58.

[K03] J. Koenigsmann, *On the 'section conjecture' in anabelian geometry*, J. Reine Angew. Math. **588** (2005), 221–235.

[P88] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. Reine Angew. Math. **392** (1988), 145–175.

[PS09] F. Pop, J. Stix, *Arithmetic in the fundamental group of a p-adic curve: on the p-adic section conjecture for curves*, `arXiv:1111.1354v1[math.AG]`, December 2009.

[S10] J. Stix, *On the period-index problem in light of the section conjecture*, American Journal of Mathematics **132** (2010), no. 1, 157–180.

The Birational Anabelian Theorem for Surfaces over $\overline{\mathbb{Q}}$

Aaron Michael Silberstein

A. Grothendieck first coined the term "anabelian geometry" in a letter to G. Faltings [Gro97a] as a response to Faltings' proof of the Mordell conjecture and in his celebrated *Esquisse d'un Programme* [Gro97b]. The "yoga" of Grothendieck's anabelian geometry is that if the étale fundamental group $\pi_1^{\text{ét}}(X, \overline{x})$ of a variety X at a geometric point $\overline{x}$ is rich enough, then it should encode much of the information about X as a variety; such varieties X are called **anabelian in the sense of Grothendieck**, and have the property that two anabelian varieties have isomorphic étale fundamental groups if and only if they are isomorphic; and that the isomorphisms between their étale fundamental groups are precisely the isomorphisms between the varieties. Grothendieck did not specify how much extra information should be encoded, and even to this day, there is not a consensus as to how far we expect to be able to push anabelian phenomena. An **anabelian theorem (or conjecture)** is a theorem (or conjecture) which asserts that a class of varieties are anabelian.

Grothendieck wrote in [Gro97a] about a number of anabelian conjectures: one regarding the moduli of curves, defined over global fields (which is still open);

one regarding hyperbolic curves, defined over global fields; and a birational anabelian conjecture, which asserts that Spec of finitely-generated, infinite fields are anabelian (in this case, we say the fields themselves are anabelian). The anabelian conjecture for hyperbolic curves was proved in the 1990's by A. Tamagawa and S. Mochizuki ([Tam97], [Moc99]). The birational anabelian conjecture for finitely-generated, infinite fields is a vast generalization of the pioneering Neukirch-Ikeda-Uchida theorem for global fields ([Neu69], [Uch77], [Ike77], [Neu77]), and is now a theorem due to F. Pop [Pop94].

Grothendieck remarked that "the reason for [anabelian phenomena] seems... to lie in the extraordinary *rigidity* of the full fundamental group, which in turn springs from the fact that the (outer) action of the 'arithmetic' part of this group... is extraordinarily strong" [Gro97a].

F. Bogomolov had the surprising insight [Bog91] that as long as the dimension of a variety is ≥ 2, anabelian phenomena can be exhibited — at least birationally — over an algebraically closed field, *even in the complete absence of the "arithmetic" part of the group Grothendieck referenced.*

Given a field K, we let G_K denote the absolute Galois group of K, the profinite group of field automorphisms of its algebraic closure $\overline{K}$ (see [NSW08] for more details). Given two fields F_1 and F_2, we let $\mathrm{Isom}^i(F_1, F_2)$ denote the set of isomorphisms between the pure inseparable (perfect) closures of F_1 and F_2, up to Frobenius twists. Given two profinite groups Γ_1 and Γ_2, we let $\mathrm{Isom}^{\mathrm{Out}}_{\mathrm{cont}}(\Gamma_1, \Gamma_2)$ denote the set of equivalence classes of *continuous* isomorphisms from Γ_1 to Γ_2, modulo conjugation by elements of Γ_2. There is a canonical map

$$\varphi_{F_1,F_2} : \mathrm{Isom}^i(F_1, F_2) \to \mathrm{Isom}^{\mathrm{Out}}_{\mathrm{cont}}(G_{F_2}, G_{F_1}) \tag{1}$$

which, in general, is neither injective nor surjective.

The birational theory of a variety of dimension n over K is encoded in its field of rational functions, and every field finitely-generated over K and of transcendence degree n arises as the field of rational functions of a K-variety of dimension n. F. Pop, developing Bogomolov's insight, conjectured an anabelian theorem for fields, finitely-generated and of transcendence degree $n \geq 2$ over an algebraically closed field k. We complete the proof of:

Theorem 1 (The Conjecture of Bogomolov-Pop for $k = \overline{\mathbb{Q}}, \overline{\mathbb{F}}_p$)**.** *Let F_1 and F_2 be fields finitely-generated and of transcendence degree ≥ 2 over k_1 and k_2, respectively, where k_1 is either $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}}_p$, and k_2 is algebraically closed. Then φ_{F_1,F_2} is a bijection. Thus, function fields of varieties of dimension ≥ 2 over algebraic closures of prime fields are anabelian.*

In [Pop11b], Pop proved that if $G_{F_1} \simeq G_{F_2}$ then F_1 and F_2 have the same characteristic and transcendence degree. Thus, the conjecture reduces to the case when F_1 and F_2 are of the same characteristic and transcendence degree. Bogomolov and Tschinkel [BT08] provide a proof in the case of transcendence degree $= 2$ when $k = \overline{\mathbb{F}}_p$. Pop proved that φ is a bijection when F_1 has transcendence degree ≥ 2 and $k = \overline{\mathbb{F}}_p$ [Pop12a]; and when F_1 has transcendence degree ≥ 3 and $k = \overline{\mathbb{Q}}$ [Pop11a]. We prove the missing case in [Sil13]:

Theorem 2 (The Birational Anabelian Theorem for Surfaces over $\overline{\mathbb{Q}}$)**.** *Let F_1 and F_2 be fields finitely-generated and of transcendence degree 2 over $\overline{\mathbb{Q}}$. Then φ_{F_1,F_2} is a bijection.*

The proof of Theorem 2 is substantially different in structure from the proofs of the other cases of Theorem 1. They both have the same starting point, two theorems due to Pop from [Pop11a]. To state these theorems, we need a definition:

Definition 3. A **valuative prime divisor** v on F is a discrete valuation, trivial on $K(F)$, such that

$$\text{tr. deg.}_{K(F)} Fv = \text{tr. deg.}_{K(F)} F - 1. \tag{2}$$

The valuation ring $\mathcal{O}_v$ is a discrete valuation ring. not every discrete valuation ring gives rise to a prime divisor. For a general discrete valuation, $\text{tr. deg.}_{K(F)} Fv \leq \text{tr. deg.}_{K(F)} F - 1$. When the equality is strict, we say that v has **no transcendence defect**, and this condition is important in the proof of the birational anabelian conjecture for finitely generated fields; see [Pop94] for more details.

Definition 4. A **rank-**1 **Parshin chain** on F is a prime divisor. A **rank-**i **Parshin chain** is a composite $w \circ v$, where v is a rank-$(i-1)$ Parshin chain, and w is a prime divisor on Fv.

Pop's theorems are then:

Theorem 5 (Pop, [Pop11a])**.** *Let F be a function field with $K(F) = \overline{\mathbb{Q}}$ and $\text{tr. deg.}_{\overline{\mathbb{Q}}} F \geq 2$. Let $\Gamma \subseteq G_F$ be a closed subgroup, up to conjugacy. Then there is a topological group-theoretic criterion, given one of the representatives of Γ to determine whether there exists i and a rank-i Parshin chain v such that Γ is the inertia group or decomposition group of v, and what this i is, if it exists.*

Theorem 6 (Pop, [Pop12b])**.**

1. *If $\mathcal{S}$ is a geometric set of prime divisors on F, then a (possibly different) set $\mathcal{S}'$ of prime divisors on F is a geometric set if and only if it has finite symmetric difference with $\mathcal{S}$.*
2. *There exists a group-theoretic recipe to recover*

$$\text{Geom}(F) =_{\text{def}} \{\{(T_v, D_v) \mid v \in \mathcal{S}\} \mid \mathcal{S} \textit{ a geometric set}\}$$

directly from G_F.

Previous results took data such as these and reconstructed F directly, in a process which we now term **birational reconstruction**. However, in our approach, we instead take the pair $(G_F, \mathcal{S})$ and reconstruct a model $\mathcal{M}(\mathcal{S})$ of F for which $\mathcal{S}$ is the collection of inertia subgroups of all prime divisors on $\mathcal{M}(\mathcal{S})$. We obtain a description of the geometry of $\mathcal{M}(\mathcal{S})$ without first reconstructing F, and we call this approach **geometric reconstruction**. The main tool is the ability to interpret intersection theory on $\mathcal{M}(\mathcal{S})$ using only group theoretic recipes applied to $\mathcal{S}$ and G_F, without any knowledge of $\mathcal{M}(\mathcal{S})$ other than its existence; this technique is the **anabelian intersection theory**.

References

[Bog91] Fedor A. Bogomolov. On two conjectures in birational algebraic geometry. In *Algebraic geometry and analytic geometry (Tokyo, 1990)*, ICM-90 Satell. Conf. Proc., pages 26–52. Springer, Tokyo, 1991.

[BT08] Fedor Bogomolov and Yuri Tschinkel. Reconstruction of function fields. *Geom. Funct. Anal.*, 18(2):400–462, 2008.

[Gro97a] Alexander Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 49–58. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 285–293.

[Gro97b] Alexandre Grothendieck. Esquisse d'un programme. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 5–48. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 243–283.

[Ike77] Masatoshi Ikeda. Completeness of the absolute Galois group of the rational number field. *J. Reine Angew. Math.*, 291:1–22, 1977.

[Moc99] Shinichi Mochizuki. The local pro-p anabelian geometry of curves. *Invent. Math.*, 138(2):319–423, 1999.

[Neu69] Jürgen Neukirch. Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. *Invent. Math.*, 6:296–314, 1969.

[Neu77] Jürgen Neukirch. Über die absoluten Galoisgruppen algebraischer Zahlkörper. In *Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976)*, pages 67–79. Astérisque, No. 41–42. Soc. Math. France, Paris, 1977.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Pop94] Florian Pop. On Grothendieck's conjecture of birational anabelian geometry. *Ann. of Math. (2)*, 139(1):145–182, 1994.

[Pop11a] Florian Pop. On Bogomolov's birational anabelian program II. Accessible at `www.math.upenn.edu/~pop/Research/Papers.html`, 2011.

[Pop11b] Florian Pop. On I/OM. Accessible at `www.math.upenn.edu/~pop/Research/Papers.html`, 2011.

[Pop12a] Florian Pop. On the birational anabelian program initiated by Bogomolov I. *Invent. Math.*, 187(3):511–533, 2012.

[Pop12b] Florian Pop. Recovering fields from their decomposition graphs. In *Number theory, analysis and geometry*, pages 519–594. Springer, New York, 2012. Accessible at `www.math.upenn.edu/~pop/Research/Papers.html`.

[Sil13] Aaron Michael Silberstein. Anabelian intersection theory I: The conjecture of Bogomolov-Pop and applications. *Submitted*, July 2013.

[Tam97] Akio Tamagawa. The Grothendieck conjecture for affine curves. *Compositio Math.*, 109(2):135–194, 1997.

[Uch77] Kôji Uchida. Isomorphisms of Galois groups of algebraic function fields. *Ann. Math. (2)*, 106(3):589–598, 1977.

Pro-ℓ Galois Groups and Valuations

Adam Topaz

A central problem in birational anabelian geometry is to detect decomposition and inertia subgroups of valuations in a given Galois group. Detecting decomposition and inertia subgroups of *large* Galois groups (i.e. maximal pro-ℓ Galois groups resp. absolute Galois groups) of almost arbitrary fields is essentially completely understood and well-established in the literature; see [7], [4], [6] for the maximal pro-ℓ case resp. [10] for the absolute Galois group case. The techniques employed by the references mentioned above rely on the theory of rigid elements which was first developed by Ware [12] then further expanded by Arason-Elman-Jacob [1] and others [5], [8].

On the other hand, Bogomolov-Tschinkel [2], [3] developed a method to detect decomposition/inertia groups using very small *almost-abelian* pro-ℓ Galois groups under the added assumption that the base field contains an algebraically closed field.

The main result presented in this talk unifies the two approaches above. In particular, we are able to detect so-called "minimized inertia/decomposition" groups (which in many cases agree with the usual notion of inertia/decomposition) using *almost-abelian* pro-ℓ Galois groups of essentially arbitrary fields. For further details concerning the history above and the results below, refer to [11].

For simplicity in exposition, we assume that ℓ is an odd prime, but analogous results hold true also for $\ell = 2$. Let K be a field with $\operatorname{char} K \neq \ell$ and let n denote either a positive integer or ∞. We denote by $\mathcal{G}_K = \operatorname{Gal}(K(\ell)|K)$, the maximal pro-$\ell$ Galois group of K. Furthermore, we denote

$$\mathcal{G}_K^{a,n} := \mathcal{G}_K/[\mathcal{G}_K,\mathcal{G}_K]\cdot\mathcal{G}_K^{\ell^n}, \text{ and } \mathcal{G}_K^{c,n} := \mathcal{G}_K/[\mathcal{G}_K,[\mathcal{G}_K,\mathcal{G}_K]]\cdot \mathcal{G}_K^{\ell^n}.$$

Given $\sigma,\tau \in \mathcal{G}_K^{a,n}$, we denote by $[\sigma,\tau] = \tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}$ where $\tilde{\sigma},\tilde{\tau} \in \mathcal{G}_K^{c,n}$ are lifts of σ,τ. Since $\mathcal{G}_K^{c,n} \to \mathcal{G}_K^{a,n}$ is a central extension, $[\sigma,\tau]$ doesn't depend on the choice of lifts. A pair of elements $\sigma,\tau \in \mathcal{G}_K^{a,n}$ will be called **commuting-liftable** provided that $[\sigma,\tau] = 0$. Similarly, a subgroup $\Sigma \leq \mathcal{G}_K^{a,n}$ will be called **commuting-liftable** provided that all pairs $\sigma,\tau \in \Sigma$ are commuting-liftable.

Denote by $K^{a,n}$ the Galois extension of K with $\operatorname{Gal}(K^{a,n}|K) = \mathcal{G}_K^{a,n}$. For a valuation v of K with valuation ring $(\mathcal{O}_v,\mathfrak{m}_v)$, we introduce the **minimized decomposition** resp. **inertia** group of v:

$$D_v^n := \operatorname{Gal}(K^{a,n}|K(\sqrt[\ell^n]{1+\mathfrak{m}_v})),\quad I_v^n := \operatorname{Gal}(K^{a,n}|K(\sqrt[\ell^n]{\mathcal{O}_v^\times})).$$

If Z_v resp. T_v denote the (usual) decomposition resp. inertia group of (some prolongation to $K^{a,n}$ of) v in $\mathcal{G}_K^{a,n}$, then the following inequalities hold: $D_v^n \leq Z_v$, and $I_v^n \leq T_v$. Moreover, these inequalities are actually *equalities* provided that the residue characteristic of v is different from ℓ. Regardless of the residue characteristic of v, however, the structure (relative to $(\mathcal{G}_K^{a,n},[\bullet,\bullet])$) of the minimized inertia/decomposition groups of v resembles that of the usual inertia/decomposition of a valuation whose residue characteristic is not ℓ, as illustrated by the following:

Theorem 1 ([11] Remark 7.7)**.** *In the notation above, let $\sigma \in I_v^n$ and $\tau \in D_v^n$ be given. Then $[\sigma,\tau] = 0$.*

In particular, if Σ is a subgroup of D_v^n such that $\Sigma/(\Sigma \cap I_v^n)$ is cyclic, then Σ is a commuting-liftable subgroup of $\mathcal{G}_K^{a,n}$. We are now ready to introduce the main theorem of the talk:

Theorem 2 (Main Theorem)**.** *For all $N \gg n$ the following hold. Let K be a field with $\mu_{\ell^N} \subset K$ and let $\Sigma \leq \mathcal{G}_K^{a,n}$ be given. Then following are equivalent:*

(1) *There exists a valuation v of K such that $\Sigma \leq D_v^n$ and $\Sigma/(\Sigma \cap I_v^n)$ is cyclic.*
(2) *There exists a commuting-liftable subgroup $\Sigma' \leq \mathcal{G}_K^{a,N}$ whose image under the canonical map $\mathcal{G}_K^{a,N} \twoheadrightarrow \mathcal{G}_K^{a,n}$ is Σ.*

Moreover, if $n = 1$ then $N = 1$ suffices and if $n \neq \infty$, one can find an explicit $N \neq \infty$ which suffices.

The proof of the main theorem has three main ingredients which we describe below: (1) Galois Cohomology and Milnor K-theory, (2) Valuation Theory, and (3) the theory of Rigid Elements. Below we give a sketch of each ingredient and how it it fits in to the proof of the Main Theorem.

Galois Cohomology and Milnor K-theory. In this part of the proof, we provide a classification of commuting-liftable pairs directly in terms of the arithmetic structure of the field via Kummer theory. This is done in the following theorem:

Theorem 3 (see [11] Theorem 11)**.** *Let K be a field with $\operatorname{char} K \neq \ell$ and $\mu_{\ell^n} \subset K$. Choose an isomorphism $\mu_{\ell^n} \cong \mathbb{Z}/\ell^n$ and consider $\sigma, \tau \in \mathcal{G}_K^{a,n}$ as homomorphisms $K^\times \to \mathbb{Z}/\ell^n$ using Kummer theory and this isomorphism. Then the following are equivalent:*

(1) $[\sigma, \tau] = 0$.
(2) $\sigma(x) \cdot \tau(1-x) = \sigma(1-x) \cdot \tau(x)$ *for all* $x \in K \smallsetminus \{0, 1\}$.

Idea of Proof. This theorem is a group-theoretical interpretation of the Merkurjev-Suslin theorem and its compatibility with Kummer theory. □

Valuation Theory. Suppose that the Main Theorem holds for subgroups $\Sigma^0 \leq \mathcal{G}_K^{a,n}$ whose rank is two. Given a Σ as in the Main Theorem, we consider all rank-two subgroups $\Sigma^0 \leq \Sigma$ and to each one associate a valuation v_{Σ^0}. Using techniques from valuation theory, in this step we deduce that these v_{Σ^0} are all comparable valuations which proves the validity of the Main Theorem for Σ. Thereby, this reduces the proof of the Main Theorem to proving the following:

Theorem 4 ([11] Theorem 3)**.** *For all $N \gg n$ the following hold. Let K be a field with $\mu_{\ell^N} \subset K$ and let $f, g \in \mathcal{G}_K^{a,n}$ be given. Then the following are equivalent:*

(1) *There exist lifts $f', g' \in \mathcal{G}_K^{a,N}$ of f, g such that $[f', g] = 0$.*
(2) *There exists a valuation v of K such that $f, g \in D_v^n$ and $\langle f, g \rangle / (\langle f, g \rangle \cap I_v^n)$ is cyclic.*

Moreover, if $n = 1$ then $N = 1$ suffices and if $n \neq \infty$, one can find an explicit $N \neq \infty$ which suffices.

Rigid Elements. The goal now is to prove Theorem 4. The implication (2) ⇒ (1) in Theorem 4 follows from Theorem 1, which follows from Theorem 3.

In the notation of Theorem 4, denote by $T = \ker f \cap \ker g$ where we consider f, g as homomorphisms $K^\times \to \mathbb{Z}/\ell^n$ via Kummer theory. Assume furthermore the existence of a commuting-liftable pair $f', g' \in \mathcal{G}_K^{a,N}$ which is a lifting for $f, g \in \mathcal{G}_K^{a,n}$. Denote by H the subgroup of $K^\times$ generated by T and all $x \notin T$ such that $1 + x \neq 1, x \mod T$. It is a consequence of the theory of *Rigid Elements* (cf. [1]), that there exists a valuation v of K such that $1 + \mathfrak{m}_v \subset T$ and $\mathcal{O}_v^\times \subset H$. Note that, if $H = K^\times$, this valuation v might be trivial. Thus, it suffices to prove:

Lemma 5 (Key Lemma). *In the notation above, H/T is cyclic.*

Remarks about the Proof. In the case where $n = 1$, the Key Lemma follows from [9] Lemma 3.3 (a slightly weaker version of this lemma also appears in [8]). On the other hand, if $n = \infty$ and K contains an ℓ-closed subfield, the Key Lemma can be deduced in a similar fashion to [3] Proposition 4.1.2.

The general case is much more involved, and uses the restrictions imposed by the existence of f', g', along with Theorem 3, to show that H/T must be cyclic. For the precise details concerning the general case, we refer the reader to [11] Theorem 3. □

References

[1] J. Arason, R. Elman, and B. Jacob. Rigid elements, valuations, and realization of Witt rings. *J. Algebra*, 110(2):449–467, 1987.

[2] F. A. Bogomolov. On two conjectures in birational algebraic geometry. In *Algebraic geometry and analytic geometry (Tokyo, 1990)*, ICM-90 Satell. Conf. Proc., pages 26–52. Springer, Tokyo, 1991.

[3] F. A. Bogomolov and Y. Tschinkel. Commuting elements of Galois groups of function fields. In *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, volume 3 of *Int. Press Lect. Ser.*, pages 75–120. Int. Press, Somerville, MA, 2002.

[4] I. Efrat. Abelian subgroups of pro-2 Galois groups. *Proc. Amer. Math. Soc.*, 123(4):1031–1035, 1995.

[5] I. Efrat. Construction of valuations from K-theory. *Math. Res. Lett.*, 6(3-4):335–343, 1999.

[6] A. J. Engler and J. Koenigsmann. Abelian subgroups of pro-p Galois groups. *Trans. Amer. Math. Soc.*, 350(6):2473–2485, 1998.

[7] A. J. Engler and J. B. Nogueira. Maximal abelian normal subgroups of Galois pro-2-groups. *J. Algebra*, 166(3):481–505, 1994.

[8] J. Koenigsmann. From p-rigid elements to valuations (with a Galois-characterization of p-adic fields). *J. Reine Angew. Math.*, 465:165–182, 1995. With an appendix by Florian Pop.

[9] J. Koenigsmann. Pro-p Galois groups of rank ≤ 4. *Manuscripta Math.*, 95(2):251–271, 1998.

[10] J. Koenigsmann. Encoding valuations in absolute Galois groups. In *Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999)*, volume 33 of *Fields Inst. Commun.*, pages 107–132. Amer. Math. Soc., Providence, RI, 2003.

[11] A. Topaz. Commuting-liftable subgroups of Galois groups II. *Preprint*, 2012. Available at: `arXiv:1208.0583`

[12] R. Ware. Valuation rings and rigid elements in fields. *Canad. J. Math.*, 33(6):1338–1355, 1981.

Groups as Galois groups with local conditions

Pierre Dèbes

Fix a finite group G that we assume to be a *regular Galois group over* $\mathbb{Q}$, that is, there exists a Galois (field) extension $F/\mathbb{Q}(T)$ of group G with $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$. The goal of the talk was to explain the following result jointly due to Nour Ghazi and the speaker [1], to discuss some implications in Inverse Galois Theory and to show some recent developments.

In the statement, given $t_0 \in \mathbb{P}^1(\mathbb{Q})$, we use the notation $F_{t_0}/\mathbb{Q}$ for the *specialization $F/\mathbb{Q}(T)$ at t_0*, *i.e.*, the residue field of any prime above $\langle T - t_0\rangle$ in the integral closure of $\mathbb{Q}[T]_{\langle T-t_0\rangle}$ in F (as usual use $\mathbb{Q}[1/T]_{\langle 1/T\rangle}$ instead if $t_0 = \infty$).

Also, a Grunwald problem for G (over $\mathbb{Q}$) is a collection $(E^p/\mathbb{Q}_p)_{p\in S}$ of Galois extensions of $\mathbb{Q}_p$ of group contained in G, indexed by a prime p varying in a finite set S of finite places of K, and a *solution* to this problem is a Galois extension $E/\mathbb{Q}$ of group G such that for each $p \in S$, we have $E\mathbb{Q}_p/\mathbb{Q}_p = E^p/\mathbb{Q}_p$ (in a fixed algebraic closure of $\mathbb{Q}_p$). The Grunwald problem $(E^p/\mathbb{Q}_p)_{p\in S}$ is said to be *unramified* if each extension $E^p/\mathbb{Q}_p$ is unramified ($p \in S$).

Theorem 1. *There exist two integers $m_0, \beta > 0$ such that for every $x > 0$ and every unramified Grunwald problem $(E^p/\mathbb{Q}_p)_{m_0<p\leq x}$ for G, there is $t_0 \in \mathbb{Z}$ such that the following holds. For all integers $t \equiv t_0$ modulo $(\beta\prod_{m_0<p\leq x} p)$, t is not in the finite list of branch points of $F/\mathbb{Q}(T)$ and the specialization $F_t/\mathbb{Q}$ is a solution to the Grunwald problem $(E^p/\mathbb{Q}_p)_{p\in S}$.*

Recall that
(a) from a famous counter-example of Wang [7], the unique unramified extension $E^2/\mathbb{Q}_2$ of group $G = \mathbb{Z}/8\mathbb{Z}$, viewed as a Grunwald problem, has no solution. This shows that the restriction $p > m_0$ cannot be totally removed in theorem 1.
(b) from a result due to Neukirch [5], if G is solvable of odd order, then every Grunwald problem (unramified or not) has a solution (the special case "G cyclic" being originally due to Grunwald, with a correction of Wang).

Definition 2. Given a real number $\ell \geq 0$, we say that the group G is of Tchebotarev order $\leq \ell$, which we write $\mathrm{tch}(G) \leq \ell$, if there exist real numbers $m, \delta > 0$ such that for every $x > 0$ and every unramified Grunwald problem $(E^p/\mathbb{Q}_p)_{m_0<p\leq x}$ for G, there exists a Galois extension $E/\mathbb{Q}$ such that these two conditions hold:
1. the extension $E/\mathbb{Q}$ is a solution to the Grunwald problem $(E^p/\mathbb{Q}_p)_{m_0<p\leq x}$,
2. $\log |d_E| \leq \delta x^\ell$, where d_E is the discriminant of $E/\mathbb{Q}$.

Set $B(x) = (\beta\prod_{m_0<p\leq x} p)$. Theorem 1 conjoined to the observation that one can take $0 < t_0 \leq B(x)$, and that then we have $\log |d_{F_{t_0}}| \leq \delta \log(B(x))$ for some $\delta > 0$ and finally that $\log(B(x))$ is classically asymptotic to x when $x \to +\infty$, we obtain the following.

Corollary 3. *If a finite group G is a regular Galois group over $\mathbb{Q}$, then* $\mathrm{tch}(G) \leq 1$.

On the other hand, some famous estimates on the Tchebotarev density theorem due to Lagarias, Montgomery and Odlyzko [3] show that, under the General Riemann Hypothesis, for every finite group G, we have

$$\mathrm{tch(G)} > (1/2) - \varepsilon, \text{ for every } \varepsilon > 0$$

This raises the question of whether $\mathrm{tch}(G) > 1$ for some group G, in which case this group G would not be a regular Galois group over $\mathbb{Q}$. At the moment, it cannot even be excluded that $\mathrm{tch}(G) = \infty$ for some group G, even under strong forms of the classical (*i.e.* over $\mathbb{Q}$) Inverse Galois Problem.

The method of proof of theorem 1 provides in fact several specializations t_0 satisfying the conclusion of theorem 1 and such that $0 < t_0 \leq B(x)$. More precisely a lower bound of the form

$$\frac{B(x)}{\beta}\left(\frac{1}{3|G|}\right)^{x/\log(x)}$$

can be obtained for the number of these specializations t_0. A next question is to bound the corresponding specializations $F_{t_0}/\mathbb{Q}$ that are non-isomorphic. This can be achieved, first by reducing the question to counting integral points of given size on a curve, thanks to some “twisting lemma”, and second, by using a result about this last question that was obtained by Y. Walkowiak [7] by refining a method of Heath-Brown [2] in the special case of curves.

The outcome is the following result.

Theorem 4. *Assume $G \neq \{1\}$ is a regular Galois group over $\mathbb{Q}$ and fix a regular realization $F/\mathbb{Q}(T)$ of G. Then there exist an integer $m_0 > 0$ and a constant $\alpha \in]0,1[$ such that the following holds. For every suitably large real number y and every unramified Grunwald problem $(E^p/\mathbb{Q}_p)_{m_0 < p \leq \alpha\log(y)}$, specializations of $F/\mathbb{Q}(T)$ at integers provide at least y^α non-isomorphic Galois extensions $E/\mathbb{Q}$ of group G that are solution to the Grunwald problem and of discriminant $\leq y$.*

More precisely the constant α can be taken to be $\alpha = (4|G|\deg_T(P))^{-1}$, where $P(t,y) = 0$ with $P \in \mathbb{Q}[T,Y]$ monic in Y, is an affine model of the regular extension $F/\mathbb{Q}(T)$. From [6, §2.2], this value of α can be bounded from below by these more intrinsic quantities: $(6(2g+1)|G|^2\log|G|)^{-1}$ and $(6r|G|^3\log|G|)^{-1}$ where g is the genus of the function field F and r the number of branch points of $F/\mathbb{Q}(T)$.

Theorem 4 can be compared to the Malle conjecture [4] which gives some asymptotic formula, namely $c(G)\, y^{a(G)}\, (\log(y))^{b(G)}$ for the number of non-isomorphic Galois extensions $E/\mathbb{Q}$ of group G and discriminant $\leq y$ (for some constants $a(G) \in]0,1]$ and $b(G) \geq 1$ precisely defined by Malle and some constant $c(G) > 0$). Malle even conjectures that his asymptotic formula still holds if some further local conditions are prescribed at finitely many primes, with the same exponents $a(G)$ and $b(G)$ but for some different constant $c(G)$. Our result is thus a weak form of this local Malle conjecture for regular Galois groups over $\mathbb{Q}$.

References

[1] P. Dèbes and N. Ghazi, *Galois Covers and the Hilbert-Grunwald property*, Ann. Inst. Fourier **62/3** (2012), 989–1013.

[2] D. R. Heath-Brown, “The density of rational points on curves and surfaces”, Ann. of Math., **155**, (2002), 553–595.

[3] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, *A Bound for the Least Prime Ideal in the Chebotarev Density Theorem*, Invent. Math. **54** (1979), 279–296.

[4] G. Malle, *On the distribution of Galois groups*, J. Number Theory **92/2** (2002), 315–329.

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

[6] B. Sadi, *Descente effective du corps de dd́efinition des revêtements*, Thesis, Univ. Lille 1, (1999).

[7] Y. Walkowiak, “Théorème d’irréductibilité de Hilbert effectif”, Acta Arithmetica, **116/4**, (2005), 343–362.

Valuations on real function fields and lower bounds for the pythagoras number

David Grimm

The pythagoras number $p_2(F)$ of a field F is by definition the smallest $n \in \mathbb{N}$ such that every sum of squares in F is equal to a sum of n squares in F, or ∞ if no such n exists. When F is the function field of a variety V over $\mathbb{R}$ (or any real closed field), A. Pfister showed that $p_2(F) \leq 2^d$. Finding the exact value of $p_2(F)$ (or just good lower bounds) is an open problem.

W. Kucharz showed in [K1] for real function fields $F/\mathbb{R}$ in d variables that $p_2(F) \geq d+1$, and he obtains the same lower bound more generally for real closed base fields in [K2]. He derives this bound from a more general result on minimal sets of generators for certain finitely generated ideals in the so called *real holomorphy ring* of $F/\mathbb{R}$ as defined in [B, p. 148]. The latter relies on Hironaka’s resolution of singularities and of points of indeterminacy of rational functions. Furthermore, computations of Chern classes of vector bundles are used, and this part of the proof does not seem to generalize to the situation of varieties V over arbitrary formally real base fields K with formally real function field $F = K(V)$ (unless V contains a smooth K-rational point, or a closed point of odd degree).

I presented a more elementary proof for the lower bound $p_2(F) \geq d+1$ that does not need to assume that the base field K of F/K is real closed. Furthermore, Hironaka’s resolution results or computations of Chern classes of vector bundles are not needed.

The case $d \geq 3$ is easily dealt with. We use the fact that if $F = K(V)$ is formally real, then V contains a smooth closed point P with formally real residue field $K(P)$. The generic point of the exceptional fiber of the blowing-up of V along P then yields a discrete valuation with real residue field $K(P)(X_1, \ldots, X_{d-1})$. Simple valuation theoretic considerations show that $p_2(F) \geq p_2(K(P)(X_1, \ldots, X_{d-1}))$, and for real rational function fields in at least two variables we have the better lower bound $p_2(K(P)(X_1, \ldots, X_{d-1})) \geq (d-1)+2 = d+1$ due to an iteration argument based on the *Cassels-Pfister theorem* and the fact that the bound holds when $d-1=2$ due to [CEP].

If $d=2$, the same argument yields that $p_2(F) \geq p_2(K(P)(X))$. However, it is known that $p_2(K(P)(X)) < 3$ can occur even when K is not real closed (e.g. for $K = \mathbb{R}((t))$). So we need a different argument when $d=2$. The key is the observation that it is sufficient to find a discrete valuation on F with nonreal residue field in which -1 is not a square (a well chosen lift of a nontrivial representation of zero as a sum of three squares then exhibits the lower bound $p_2(F) \geq 3$). In geometric terms, it is sufficient to find a geometrically irreducible curve C on the surface V (which we can assume to be projective and normal) that does not contain points with formally real residue field. The generic point of C in V will then yield a valuation with residue field $K(C)$. The way to obtain the existence of such a curve is by considering hyperplane sections of V with respect to some well chosen embedding in projective space. After enlarging the embedding dimension via a Veronese map if necessary, we have V embedded in a larger variety W that is defined over $\mathbb{Q}$ inside projective space while finding at the same time a hyperplane H defined over $\mathbb{Q}$ that has no common $\mathbb{R}$-points with W (and hence in particular with V). The completeness of the first order theory of real closed fields together with Bertini's theorem for generic hyperplane sections shows that after some (rational) small ϵ-variation of the coefficients of H, we have that $C = H \cap V$ is a smooth geometrically connected curve over K (and hence in particular geometrically irreducible) that contains no point with formally real residue field.

In the case $d = 1$, we have in the rational case obviously that $p_2(K(X)) > 1$, as the pythagorean closure of a non-pythagorean field is always an infinite field extension as was shown by Diller and Dress [B, Theorem 3.8].

Kucharz' result on finitely generated ideals of the real holomorphy ring of a function field $F/\mathbb{R}$ does not only yield the lower bound $p_2(F) \geq d + 1$ for the pythagoras number of a function field $F/\mathbb{R}$ in d variables, but in fact for all higher even pythagoras numbers $p_{2m}(F)$ as well (which is by definition the smallest $n \in \mathbb{N}$ such that every sum of $2m$-th powers is a sum of n such powers). In fact, my more elementary approach generalizes also to the $2m$-th pythagoras number. However, since the proof for dimension $d \geq 3$ is a mere reduction to the case of a rational function field $p_{2m}(F) \geq p_{2m}(K(P)(X_1, \ldots, X_{d-1}))$, it remains the task to find good lower bounds for the $2m$-th pythagoras number of the latter kind. One such lower bound (also for base fields that are not real closed) can be obtained by adapting Kucharz' proof to the situation of varieties over formally real fields that contain a smooth rational point. The resulting lower bound $p_{2m}(K(P)(X_1, \ldots, X_{d-1})) \geq (d-1)+1 = d$ in the rational case is slightly too bad to prove Kucharz' bound $p_{2m}(F) \geq d+1$ for arbitrary real d-dimensional function field F over general formally real fields. Summarized we obtain:

Theorem. *Let F/K a real function field in d variables and let $m \in \mathbb{N}$. Then $p_{2m}(F) \geq d + 1$ when $m = 1$, or $d \leq 2$, or when the embedding $K \hookrightarrow F$ admits a section $F \to K \cup \{\infty\}$. In the remaining cases we have $p_{2m}(F) \geq d$.*

Idealy, I would like to show $p_{2m}(F) \geq d + 1$ unconditionally, which with my method of proof would require a better lower bound for rational function fields. Note that the *Cassels-Pfister theorem* for quadratic forms does not generalize to higher degree forms, so it is not evident how one can obtain better lower bounds for the $2m$-th pythagoras number of higher dimensional rational function fields from a good lower bound in small dimensions when $m \geq 2$.

References

[B] E. Becker.*The real holomorphy ring and sums of $2n$th powers*, Real algebraic geometry and quadratic forms (Rennes, 1981), Lecture Notes in Math. 959, (1982), 139–181

[CEP] J.W.S. Cassels, W.J. Ellison, A. Pfister. *On sums of squares and on elliptic curves over function fields*, Journal of Number Theory 3, (1971), 125–149

[K1] W. Kucharz. *Invertible ideals in real holomorphy rings*, J. Reine Angew. Math. 395 (1989), 171–185

[K2] W. Kucharz. *Generating ideals in real holomorphy rings*, J. Algebra 144 (1991), 1–7

Reporter: Adam Topaz

Participants

Dr. Lior Bary-Soroker
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

Prof. Dr. Mirela Ciperiani
Department of Mathematics
The University of Texas at Austin
1 University Station C1200
Austin, TX 78712-1082
UNITED STATES

Prof. Dr. Pierre Dèbes
U.F.R. de Mathématiques
Université de Lille 1
59655 Villeneuve d'Ascq Cedex
FRANCE

Prof. Dr. Ido Efrat
Department of Mathematics
Ben-Gurion University of the Negev
Beer Sheva 84 105
ISRAEL

Dr. Arno Fehm
Fachbereich Mathematik u. Statistik
Universität Konstanz
Universitätsstr. 10
78457 Konstanz
GERMANY

Prof. Dr. Wulf-Dieter Geyer
Department Mathematik
Universität Erlangen-Nürnberg
Cauerstr. 11
91058 Erlangen
GERMANY

Prof. Dr. Barry William Green
Department of Mathematics
University of Stellenbosch
7602 Stellenbosch
SOUTH AFRICA

Prof. Dr. Dan Haran
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

Prof. Dr. Julia Hartmann
Lehrstuhl für Mathematik (Algebra)
RWTH Aachen
Templergraben 64
52062 Aachen
GERMANY

Dr. Armin Holschbach
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg
GERMANY

Prof. Dr. Moshe Jarden
School of Mathematics
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

Dr. Jochen Koenigsmann
Mathematical Institute
University of Oxford
24-29 St Giles
Oxford OX1 3LB
UNITED KINGDOM

Prof. Dr. Laurent Moret-Bailly
U. F. R. Mathématiques
I. R. M. A. R.
Université de Rennes I
Campus de Beaulieu
35042 Rennes Cedex
FRANCE

Dr. Andrew S. Obus
Department of Mathematics
Columbia University
2990 Broadway
New York, NY 10027
UNITED STATES

Dr. Elad Paran
Department of Mathematics
The Open University of Israel
16, Klausner st.
P. O. Box 39 328
Tel Aviv 61392
ISRAEL

Dr. Sebastian Petersen
Institut für Theoretische Informatik,
Mathematik & Operations Research
Universität der Bundeswehr
85577 Neubiberg
GERMANY

Prof. Dr. Bjorn Poonen
Department of Mathematics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Prof. Dr. Florian Pop
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
UNITED STATES

Prof. Dr. Alexander Prestel
Fachbereich Mathematik u. Statistik
Universität Konstanz
Postfach 5560
78434 Konstanz
GERMANY

Dr. Aharon Razon
3 Bet-Zuri st.
Tel-Aviv 6912203
ISRAEL

Dr. Aaron Silberstein
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
UNITED STATES

Prof. Dr. Katherine F. Stevenson
Department of Mathematics
California State University at
Northridge
Northridge CA 91330-8313
UNITED STATES

Dr. Jakob Stix
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg
GERMANY

Dr. Adam Topaz
Department of Mathematics
David Rittenhouse Laboratory
University of Pennsylvania
209 South 33rd Street
Philadelphia PA 19104-6395
UNITED STATES

Dr. Kirsten Wickelgren
Department of Mathematics
Harvard University
One Oxford Street
Cambridge, MA 02138
UNITED STATES

Dr. David Zywina
Department of Mathematics
Queen's University
Jeffery Hall
99 University Avenue
Kingston ONT K7L 3N6
CANADA