Mathematisches Forschungsinstitut Oberwolfach

Report No. 05/2009

DOI: 10.4171/OWR/2009/05

The Arithmetic of Fields

Organised by
Moshe Jarden (Tel Aviv)
Florian Pop (Philadelphia)
Leila Schneps (Paris)

February 1st – February 7th, 2009

Abstract. The workshop "The Arithmetic of Fields" focused on a series of problems concerning the interplay between number theory, arithmetic and algebraic geometry, Galois theory, and model theory, such as: the Galois theory of function fields / covers of varieties, rational points on varieties, Galois cohomology, local-global principles, lifting/specializing covers of curves, model theory of finitely generated fields, etc.

Mathematics Subject Classification (2000): 12E30.

Introduction by the Organisers

The sixth conference on "The Arithmetic of Fields" was organized by Moshe Jarden (Tel Aviv), Florian Pop (Philadelphia), and Leila Schneps (Paris), and was held in the week February 1–7, 2009. The participants came from 14 countries: Germany (14), USA (11), France (7), Israel (7), Canada (2), England (2), Austria (1), Brazil (1), Hungary (1), Italy (1), Japan (1), South Africa (1), Switzerland (1), and The Netherlands (1). All together, 51 people attended the conference; among the participants there were thirteen young researchers, and eight women.

Most of the talks concentrated on the main theme of Field Arithmetic, namely Galois theory and its interplay with the arithmetic of the fields. Several talks had an arithmetical geometry flavour.

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

New Fields With Free Absolute Galois Groups

Moshe Jarden

One of the major achievements of Field Arithmetic is the following result:

Theorem 1. *Let K be a countable PAC field. Then* $\mathrm{Gal}(K) \cong \hat{F}_\omega$ *if and only if K is Hilbertian.*

The "only if" part was proved by Roquette. The "if" part was proved first in charactristic 0 by Fried-Völklein using methods of complex analysis, then in the general case by Pop using "rigid patching", and finally also by Haran-Jarden using "algebraic patching".

An easier result of v.d.Dries-Lubotzky gives for each field K and every cardinal number m a regular extension F of K of infinite transcendence degree such that F is PAC and $\mathrm{Gal}(F) \cong \hat{F}_m$.

The aim of this talk is to present one of the major results of the (still in writing) book "Algebraic Patching" by the speaker. It gives for each PAC field K a relatively small (yet infinite) extension F of $K(x)$ such that $\mathrm{Gal}(F) \cong \hat{F}_m$ (with $m = \mathrm{card}(K)$), and F is Hilbertian.

Theorem 2 (Main Theorem)**.** *Let K be a PAC field of characteristic p and cardinality m and let x a variable. Denote the set of all monic irreducible polynomials in $K[x]$ by $\mathcal{F}$. For each $f \in \mathcal{F}$ and every positive integer n with $p \nmid n$ we choose an n-th root $f^{1/n}$ of f such that $(f^{1/n})^d = f^{d/n}$ for each $d|n$. Let F be a field that contains $F_0 = K(f^{1/n})_{f\in\mathcal{F},\ p\nmid n}$ and is contained in $K_{\mathrm{cycl}}(x)_{\mathrm{ab}}^{(p')}$. Then F is Hilbertian and* $\mathrm{Gal}(F) \cong \hat{F}_m$.

Here K_{cycl} is the field obtaind from K by adjoining all roots of unity in K_s to K and $K_{\mathrm{cycl}}(x)_{\mathrm{ab}}^{(p')}$ is the maximal Abelian extension of $K_{\mathrm{cycl}}(x)$ of order not divisible by p.

Remark. Following a suggestion of Florian Pop, we may replace F_0 in the Main Theorem by smaller fields serving the same purpose as the original one. To this end we consider a partition $\mathcal{F} = \coprod_{i=1}^r \mathcal{F}_i$ such that $\mathrm{card}(\mathcal{F}_i) = m$ for each i. Let $\mathcal{F} \to \prod_{i=1}^r \mathcal{F}_i$ be a bijection mapping each $f \in \mathcal{F}$ to the r-tuple $(f_1, \ldots, f_r)$. Then the field $F_0 = K(\sqrt[n]{f_1, \ldots, f_n})_{f\in\mathcal{F},\, p\nmid n}$ satisfies the conclusion of Main Theorem.

We don't know if F_0 is ample.

If $K = K_{\mathrm{cycl}}$, then $\mathrm{Gal}(K(x)_{\mathrm{ab}}^{(p')}) \cong \hat{F}_m$, hence $\mathrm{Gal}(K(x))_{\mathrm{ab}} \cong \hat{F}_m$ (because $K(x)_{\mathrm{ab}}/K(x)_{\mathrm{ab}}^{(p')}$ is an Abelian extension). If on the other hand, $\zeta_l \notin K$ for some prime number $l \neq p$, then $F_0/K(x)$ is not Abelian.

The proof of Main Theorem is based on four results. The first of them is important in its own sake.

Proposition A. *Let K be an ample field and x a variable. Then* $\mathrm{Gal}(K(x))$ *is semi-free.*

Here we say that K is **ample** if for every absolutely irreducible variety V with a K-rational point the set $V(K)$ is Zariski-dense in V ([3, Lemma 5.3.1]). In particular, every PAC field is ample. Alternatively, K is existentially closed in $K((t))$. One may prove that if h is a nonconstant rational function on V, defined over K, then $\mathrm{card}\{h(\mathbf{a}) \mid \mathbf{a} \in V(K)\} = \mathrm{card}(K)$.

We say that a profinite group G of infinite rank m is **semi-free** if every finite split embedding problem

$$(\phi : G \to A,\ \alpha : B \to A)$$

has m **independent solutions** γ_κ, $\kappa < m$. The latter condition means that the family $\{\mathrm{Ker}(\gamma_\kappa) \mid \kappa < m\}$ of open subgroups of $\mathrm{Ker}(\phi)$ is independent with respect to the normalized Haar measure of $\mathrm{Ker}(\phi)$. In other words, if $\kappa_1, \ldots, \kappa_r$ are distinct ordinals smaller than m, then $(\mathrm{Ker}(\phi) : \bigcap_{i=1}^r \mathrm{Ker}(\gamma_{\kappa_i})) = \prod_{i=1}^r (\mathrm{Ker}(\phi) : \mathrm{Ker}(\gamma_{\kappa_i}))$.

We sketch a proof of Proposition A at the end of this note.

Proposition B. **(a):** *Let G be a semi-free profinite group and H a closed subgroup. If H is contained in a G-diamond, then H is semi-free and* $\mathrm{rank}(H) = \mathrm{rank}(G)$.

(b): *Let F/E be a separable algebraic extension of fields. Suppose* $\mathrm{Gal}(E)$ *is semi-free and F is contained in an E-diamond. Then* $\mathrm{Gal}(F)$ *is semi-free and* $\mathrm{rank}(\mathrm{Gal}(F)) = \mathrm{rank}(\mathrm{Gal}(E))$.

(c): *Let F/E be a separable algebraic extension of fields. Suppose E is Hilbertian and F is contained in an E-diamond. Then E is Hilbertian.*

In the notation of Proposition B we say that H is **contained in a G-diamond** if G has closed normal subgroups N_1, N_2 such that $N_1 \not\subseteq H$, $N_2 \not\subseteq H$, and $N_1 \cap N_2 \subseteq H$. Analogously we say that F **is contained in an E-diamond** if E has Galois extensions N_1, N_2 such that $F \not\subseteq N_1$, $F \not\subseteq N_2$, and $F \subseteq N_1N_2$. Proposition B(a) is a recent joint result of Bary-Soroker, Haran, and Harbater. Proposition B(b) is the Galois theoretic interpretation of Proposition B(a). Finally, Proposition B(c) is Haran's diamond theorem for Hilbertian fields. The proof of the result of Bary-Soroker-Haran-Harbater is a clever variant of the proof of Haran's result.

Proposition C. *Let K be a PAC field of characteristic p, x a variable, and F a separable algebraic extension of $K(x)$. Suppose $w(F^\times)$ is a p'-divisible group for every valuation w of F trivial on K. Then* $\mathrm{Gal}(F)$ *is projective.*

Here we say that an Abelian group Γ is p'-divisible, if for each $\gamma \in \Gamma$ and every positive integer n with $p \nmid n$ there exists $\beta \in \Gamma$ such that $n\beta = \gamma$.

We say below something on the proof of Proposition C.

Proposition D. *Let G be a projective semi-free profinite group of infinite rank m. Then $G \cong \hat{F}_m$.*

The proof applies the projectivity of G and the semi-freeness of G to show that every finite embedding problem for G with a nontrivial kernel has m-solutions. By a result proved independently by Melnikov and Chatzidakis, $G \cong \hat{F}_m$ [2, Lemma 25.1.8].

Proof of the Main Theorem. As a PAC field, K is ample. We set $E = K(x)$. By Proposition A, $\mathrm{Gal}(E)$ is semi-free. By [2, Prop. 13.2.1], E is Hilbertian.

We consider the following diamond of fields:

$$\begin{tikzcd}
 & M_1M_2 = K_{\mathrm{cycl}}(x)_{\mathrm{ab}}^{(p')} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
N_1 = E(\zeta_n, x^{1/n})_{p\nmid n} \arrow[dr, dash] & F_0 \arrow[d, dash] & N_2 = E(\zeta_n f^{1/n})_{f\in\mathcal{F}\setminus\{x\}, p\nmid n} \arrow[dl, dash] \\
 & E = K(x) &
\end{tikzcd}$$

and note that both N_1 and N_2 are Galois extensions of E that do not contain F_0 (even if F_0 is defined as in Remark 1). Hence they do not contain any field F btween F_0 and M_1M_2. It follows from Proposition B, that each such F is Hilbertian and $\mathrm{Gal}(F)$ is semi-free.

By the construction of F_0, the group $w(F^\times)$ is p'-divisible for every valuation w of F trivial on K. Hence, by Proposition C, $\mathrm{Gal}(F)$ is projective. It follows from Proposition D, that $\mathrm{Gal}(F) \cong \hat{F}_m$.

□

On the proof of Proposition C. The proof has two steps. The first one is due to Ido Efrat. It consists of a local-global principle for the Brauer group of each algebraic extension F of $K(x)$ ([3, Prop. 11.4.5], also [1, Lemma 3.3]). The proof depends among others on the fact that if J is an Abelian variety and J' is a principle homogeneous J-space defined over K, then $J' \cong_K J$ (because $J'(K) \neq \emptyset$).

The second one is due to Florian Pop. It says that if an algebraic extension M of $K(x)$ is Henselian with respect to a valuation which is trivial on K and the value group of M is p'-divisible, then the $\mathrm{Br}(M)^{(p')} = 0$ ([3, Lemma 11.1.11]).

□

On the proof of Proposition A. The proof goes through several stages.

STAGE 1: *Cyclic extensions.* First we consider an arbitrary field K, a variable x, a power q of a prime number, and elements $a, b \in K^\times$. We prove that $K(x)$ has a cyclic extension F of degree q such that

$$\mathrm{Branch}(F/K(x)) = \begin{cases} \{a, b\} & \mathrm{ifchar}(K) \nmid q\mathrm{and}\zeta_q \in K \\ \{a\zeta_q^\sigma \mid \sigma \in \mathrm{Gal}(K(\zeta_q)/K)\} & \mathrm{ifchar}(K) \nmid q\mathrm{and}\zeta_q \notin K \\ \{a\} & \mathrm{ifchar}(K) | q. \end{cases}$$

Moreover, each of the branch points is totally ramified in F. In particular, the inertia groups over the branch points coincide with $\mathrm{Gal}(F/K(x))$.

Here we say that an element $a \in \tilde{K} \cup \{\infty\}$ is a **branch point** of $F/K(x)$ if the prime divisor of $K(x)/K$ defined by the specialization $x \to a$ is ramified in F.

STAGE 2: *Embedding problems over a complete field.* Let $\hat{K}/K$ be an extension of fields, x a variable, and $\hat{E}/\hat{K}(x)$ a finite Galois extension. Consider a finite split embedding problem

$$\mathrm{Gal}(\hat{E}/\hat{K}(x)) \ltimes H \to \mathrm{Gal}(\hat{E}/\hat{K}(x)). \tag{1}$$

and finitely many cyclic subgroup G_j, $j \in J$, of H of prime power orders. Suppose $\hat{K}$ is complete under a non-archmedean absolute value $|\ |$, $\mathrm{trans.deg}(\hat{K}/K) = \infty$, and $H = \langle G_j \mid j \in J\rangle$. Then (1) has a solution field $\hat{F}$ and for each $j \in J$ there exists $\hat{b}_j \in \mathrm{Branch}(\hat{F}/\hat{K}(x))$ with G_j as an inertia group. Moreover, $\hat{b}_j$, $j \in J$, are algebraically independent over K.

The proof of that construction uses "algebraic patching".

STAGE 3: *Lifting and descent.* Now suppose, as we do in Proposition A, that K is an ample field. We consider a finite split embedding problem over K,

$$\mathrm{Gal}(E/K(x)) \ltimes H \to \mathrm{Gal}(E/K(x)) \tag{2}$$

and let $\beta < \mathrm{card}(K)$ be an ordinal number. Suppose by transfinite induction that we have constructed for each $\alpha < \beta$ a solution field F_α of (2) such that the set $\{F_\alpha \mid \alpha < \beta\}$ is linearly disjoint over E. Then the cardinality of the set $B = \bigcup_{\alpha<\beta} \mathrm{Branch}(F_\alpha/K(x))$ is less than $\mathrm{card}(K)$. Moreover, $N = K(x, \mathrm{Branch}(F_\alpha/K(x)))_{\alpha<\beta}$ is a Galois extension of $K(x)$ that contains E and $\mathrm{Branch}(N/K(x)) = B$. In order to conclude the proof of Proposition A we have to construct a solution field F_β of (2) such that $F_\beta \cap N = E$.

To construct F_β, we consider the field $\hat{K} = K((t))$ of formal power series over K together with the complete t-adic absolute value. Then we let $\hat{E} = E\hat{K}$ and obtain the finite split embedding problem (1). Let $\hat{F}$ and $\hat{b}_j$, $j \in J$, be the solution field and the corresponding branch points given in Stage 2. Since $\mathrm{trans.deg}(\hat{K}/K) = \infty$, we may choose the $\hat{b}_j$, $j \in J$, to be transcendental over K.

It is possible to choose $u_1, \ldots, u_n \in \hat{K}$ such that $\hat{F} = F_{\mathbf{u}}\hat{K}$, where $F_{\mathbf{u}}$ is a solution of the embedding problem

$$\mathrm{Gal}(E(\mathbf{u})/K(\mathbf{u}, x)) \ltimes H \to \mathrm{Gal}(E(\mathbf{u})/K(\mathbf{u}, x)). \tag{3}$$

Moreover, $\hat{b}_j = h_j(\mathbf{u})$, where $h_j \in K[X_1, \ldots, X_n]$ are polynomials.

STAGE 4: *Reduction.* Using the theorem of Bertini-Noether and the theory of good reduction initiated by Deuring, one can specialize $\mathbf{u}$ to an n-tuple $\mathbf{u}' \in K$ and extend this specialization to a K-place of F_u such that the residue field F_β of $F_{\mathbf{u}}$ solves embedding problem (2). Moreover, for each $j \in J$, $b_j = h_j(\mathbf{u}')$ is a branch point of $F_\beta/K(x)$ that does not belong to B and G_j is contained in an inertia group I_j of $F_\beta/K(x)$ that lies over b_j. In particular, by Stage C, b_j is unramified in N. It follows that $I_j \le \mathrm{Gal}(F_\beta/F_\beta \cap N)$. Since the G_j's generate $\mathrm{Gal}(F_\beta/E)$, so do the I_j's. Consequently, $F_\beta \cap N = E$.

□

References

[1] I. Efrat, *A Hasse principle for function fields over PAC fields,* Israel Journal of Mathematics **122** (2001), 43–60.

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

[3] M. Jarden *Algebraic Patching,* in preparation.

On the period–index problem in light of the section conjecture

Jakob Stix

1. The section conjecture

Let k be a field, k^{sep} a fixed separable closure and $\mathrm{Gal}_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ its absolute Galois group. The étale fundamental group $\pi_1(X, \bar{x})$ of a geometrically connected variety X/k with a geometric point $\bar{x} \in X$ above k^{sep}/k sits naturally in a short exact sequence

$$1 \to \pi_1(X \times_k k^{\mathrm{sep}}, \bar{x}) \to \pi_1(X, \bar{x}) \to \mathrm{Gal}_k \to 1, \tag{1}$$

which we abbreviate by $\pi_1(X/k)$. A k-rational point $a \in X(k)$ yields by functoriality a section s_a of (1), which depends on the choice of an étale path from a to $\bar{x}$ and thus is well defined only up to conjugation by elements from $\pi_1(X \times_k k^{\mathrm{sep}})$. The section conjecture speculates the following.

Conjecture 1 (Grothendieck [2])**.** *The map $a \mapsto s_a$ is a bijection of the set of rational points $X(k)$ with the set of conjugacy classes of sections of $\pi_1(X/k)$ if k is a number field and X is a smooth, projective curve of genus at least* 2.

It was known to Grothendieck, that $a \mapsto s_a$ is injective by an application of the weak Mordell-Weil theorem.

2. Evidence so far

Only bits of evidence for the section conjecture have emerged over the years. The most convincing piece consists perhaps in J. Koenigsmann's proof in [4] of a birational analogue for function fields in one variable over a local p-adic field.

A **neighbourhood** of a section $s : \mathrm{Gal}_k \to \pi_1(X, \bar{x})$ consists of a connected finite étale cover $X' \to X$ together with a lift $t : \mathrm{Gal}_k \to \pi_1(X', \bar{x}')$ of the section. The geometric covers contained in neighbourhoods of a given section form a cofinal system due to $\pi_1(X \times_k k^{\mathrm{sep}})$ being finitely generated and the use of characteristic subgroups.

The technique of neighbourhoods was pioneered in the work of Nakamura and Tamagawa and leeds to the equivalence of the section conjecture with the weak section conjecture, see [4].

Conjecture 2 (weak section conjecture)**.** *Let k be a number field. A smooth projective curve X/k of genus at least 2 has a rational point if and only if its fundamental group extension $\pi_1(X/k)$ splits.*

Indeed, if a section s exists that differs from all the finitely many sections associated to rational points, then it has a neighbourhood $X' \to X$ whose fundamental group extension still allows a section, namely the lift t, but which does not contain rational points. It is most unfortunate that this foundational argument relies on the theorem of Faltings-Mordell, which during the infancy of the conjecture was believed to follow from the section conjecture itself. In case of a local p-adic field, we can replace Faltings-Mordell by a compactness argument.

3. Local obstructions to sections

The aim of the talk was to present new evidence for the section conjecture as provided in the authors note [5]. As the new evidence is purely local we take the courage to respond now to a question asked after the talk by S. Wewers and conjecture the following.

Conjecture 3. *Conjecture 1 holds also for smooth, projective curves over a local p-adic field.*

The index of X/k is the gcd of the degrees of all k-rational divisors on X, the period of X/k is the gcd of all k-rational divisor classes of X/k. For curves of genus g, period divides the index which divides $2g-2$. The index furthermore annihilates the kernel $\mathrm{Br}(X/k)$ of $\mathrm{Br}(k) \to \mathrm{Br}(X)$. A theorem of Roquette asserts that for $k/\mathbb{Q}_p$ finite, the relative Brauer group $\mathrm{Br}(X/k)$ is cyclic of order the index.

Of course, if we have a rational point on X, then period and index equals 1 and $\mathrm{Br}(X/k)$ is trivial. In light of the section conjecture, the same should follow from merely the assumption of having a section of $\pi_1(X/k)$. Using results of Lichtenbaum on the period/index problem for curves over p-adic local fields we manage to prove at least the following theorem, see [5] Thm 16. An alternative proof using the cycle class of a section was later given by Esnault and Wittenberg in [1].

Theorem 1. *Let k be a finite extension of $\mathbb{Q}_p$ and let X/k be a smooth, projective curve of positive genus, such that the fundamental group extension $\pi_1(X/k)$ admits a section.*

(1) For p odd, period of X equals the index of X and both are powers of p.

(2) For $p = 2$, we have period of X and index of X are powers of 2. If we moreover assume that we have an even degree finite étale cover $X \to X_o$ with X_0 of positive genus, then we have also that period equals the index.

So having a section locally at a p-adic place constraints the numerical data of period and index for the curve base changed to the local field at that place.

The analogue for a real place was known before and admits many proofs (Sullivan and Cox, Huisman, Mochizuki, Pal, ...), one of which relies on a theorem of Witt from 1934 and runs parallel to the proof of Theorem 1, see for example [5] Thm 26.

Theorem 2 (Real section conjecture)**.** *Let $X/\mathbb{R}$ be a smooth, projective curve of genus ≥ 1. Then the map*

$$\pi_0\big(X(\mathbb{R})\big) \to \big\{\textit{conjugacy classes of sections of } \pi_1(X/\mathbb{R})\big\},$$

that maps a connected component of the real locus $X(\mathbb{R})$ to the corresponding conjugacy class of sections is a bijection of finite sets.

4. Constructing examples

Examples of curves X over number fields k such that at a place $v|p$ with completion k_v the relative Brauer group of $X \times_k k_v$ over k_v contains nontrivial torsion prime to p can be achieved in several ways. A geometric method using Brauer-Severi varieties is outlined in [5] §7. These lead to the first known examples of curves over number fields where Conjecture 1 holds, albeit for trivial reasons of having neither sections nor rational points. An explicit example is given for $p \equiv 3$ modulo 4 and $n \geq 2$ by the curve in $\mathbb{P}^2_{\mathbb{Q}}$ given as

$$\{X^{2n} + Y^{2n} = pZ^{2n}\}$$

which has neither points nor sections over $\mathbb{Q}$ for local reasons over $\mathbb{Q}_p$. All examples which we can construct are empty in the sense of having neither points nor sections and are obstructed locally. But these examples exist in abundance. For equally empty examples for curves over number fields which are even counter-examples to the Hasse principle (but less abundant) see the talk of T. Szamuely at the same conference and [3] for details.

References

[1] Esnault, H., Wittenberg, O., *Remarks on the pronilpotent completion of the fundamental group*, preprint, arXiv:0807.2963v3[math.AG], July/December 2008. To appear in Moscow Mathematical Journal.

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

[3] Harari, D., Szamuely, T., *Galois sections for abelianized fundamental groups*, with an Appendix by E. V. Flynn, preprint, arXiv:0808.2556v1[math.AG], August 2008. To appear in Math. Annalen.

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

[5] Stix, J., *On the period-index problem in light of the section conjecture*, preprint, arXiv:0802.4125v1[math.AG], Februar 2008. To appear in American Journal of Mathematics.

Patching and Schacher's admissibility conjecture

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

1. Overview

In [8], Schacher defined the notion of admissibility, which concerns a version of the inverse Galois problem relating to division algebras. Namely, a finite group G is *admissible* over a field F if there is a G-Galois field extension E/F and an F-division algebra D containing E such that E is a maximal subfield of D. Equivalently, $[E:F] = \deg_F D := \sqrt{\dim_F D}$. Note that G is admissible over F if and only if F has a crossed product division algebra with respect to G. The inverse problem for admissibility over F asks which finite groups G are admissible over F; i.e. are Galois groups over F of maximal subfields of F-division algebras.

Schacher showed in that paper that if G is admissible over $F = \mathbb{Q}$ then every Sylow subgroup of G is metacyclic. He showed the converse in the case of abelian groups, and conjectured the converse in general. He also showed a similar necessary condition for function fields of curves over finite fields; again the problem of finding a precise necessary and sufficient condition remains open. In both situations, the difficulty is that even if the Sylow subgroups of G are all admissible, it is unknown how to construct a corresponding field extension and division algebra that fit the local data together. This is related to the fact that the inverse Galois problem is open over such fields, even without an extra condition on division algebras.

In our situation [5], we instead consider function fields of curves over complete discretely valued fields K having algebraically closed residue field k. Many results in inverse Galois theory have been shown in this context using patching, a method of constructing objects by doing so "locally" in a compatible way (e.g. see [2]). Analogously, we use patching here to prove that necessary conditions for admissibility are in fact sufficient. Note that if K is of equal characteristic 0 (e.g. $K = \mathbb{C}((t))$), then K is quasi-finite (i.e. perfect with absolute Galois group $\hat{\mathbb{Z}}$); so this case is analogous to that of curves over finite fields.

Theorem 1 (Main theorem)**.** [5] *Let F be the function field of a curve over a complete discretely valued field K whose residue field k is algebraically closed. If G is admissible over F, then for $p \neq \operatorname{char} k$, every Sylow p-subgroup of G is abelian metacyclic (i.e. abelian of rank ≤ 2). Conversely, if $\operatorname{char} k$ does not divide $|G|$, then G is admissible provided that every Sylow subgroup is abelian metacyclic.*

Here the proof of the forward direction is somewhat analogous to that of Schacher's results, and relies on the fact that in these situations the period equals the index in the Brauer group (this being classical for global fields). The converse direction uses patching, a technique not available for global fields. Note in particular that the above theorem gives a necessary and sufficient condition for a finite group to be admissible over a one-variable function field over $K = \mathbb{C}((t))$.

In the case of non-zero equal characteristic, it seems that there is no condition on the Sylow p-subgroup for p equal to the characteristic; and so a group should be admissible if and only if the other Sylow subgroups are abelian metacyclic. In mixed characteristic, with enough roots of unity, a group is admissible if every Sylow (including at the residue characteristic) is abelian metacyclic.

2. Sketch of the forward direction

Given a set Ω of discrete valuations on a field F, there is a ramification map

$$\mathrm{ram}_\Omega = \prod_{v\in\Omega} \mathrm{ram}_v : \mathrm{Br}(F)' \to \prod_{v\in\Omega} H^1(k_v, \mathbb{Q}/\mathbb{Z})',$$

where $(\ \ )'$ denotes the elements whose order is not divisible by the residue characteristic of any $v \in \Omega$, and k_v is the residue field at v; see [7], Chapter 10. The kernel of this map is called the *unramified Brauer group* $\mathrm{Br}_u(F)'$ with respect to Ω. We say that $\alpha \in \mathrm{Br}(F)'$ is *determined by ramification* if $\mathrm{per}(\alpha)$ is equal to the order of $\mathrm{ram}_v(\alpha)$ for some $v \in\ \Omega$.

Claim A: If $\mathrm{Br}_u(F) = 0$ and $\mathrm{per}(\alpha)$ is a power of a prime p that does not divide any residue characteristic of Ω, then α is determined by ramification.

The proof of the claim uses that the order of an element of a product is the least common multiple of the orders of its entries, which for p-powers is the maximum of its orders.

Now let L/F be a G-Galois field extension such that L is a maximal subfield of an F-division algebra D. We may consider the p-primary part $[D]_p$ of the Brauer class of D; its period is the p-part $(\mathrm{per}\, D)_p$ of the period of D.

Claim B: If $[D]_p$ is determined by ramification and $(\mathrm{per}\, D)_p = (\mathrm{ind}\, D)_p$, then P is metacyclic, and is abelian metacyclic if F contains a primitive $|P|$-th root of unity.

The strategy for the first part of the claim is to study the Galois theory of the extension $\widehat{L}/\widehat{L^P}$, where these are the completions of L and of the fixed field L^P at a valuation v with respect to which $[D]_p$ is determined by ramification. The proof of the second part of the claim then relies on Kummer theory.

These claims are used in proving the forward part of our theorem, viz. that if G is admissible over F then there is a G-Galois field extension E/F with E a maximal subfield of an F-division algebra D. Using Claim A together with [1], Corollary 1.10(b), we first show that $[D]_p$ is determined by ramification. Combining this with the fact that period=index here ([4], Theorem 5.5, or [6], Theorem 5.3), the hypotheses of Claim B are satisfied. The hypotheses on k then allow us to obtain our conclusion.

3. Sketch of the converse direction

Using patching we show the converse direction of the main result, viz. that if G has abelian metacyclic Sylow subgroups then it is admissible over F. Specifically, we use the framework of patching over fields established in [3]. (Previous versions of patching, which mostly work over rings rather than over fields, are less adapted to our setting.)

In this framework, suppose that $F \subseteq F_0$ are fields and that F_1, F_2 are intermediate fields such that $F_1 \cap F_2 = F$. Given a finite dimensional F-vector space V, we obtain F_i-vector spaces $V_i = V \otimes_F F_i$ for $i = 1, 2$, together with an F_0-isomorphism $\phi : V_1 \otimes_{F_1} F_0 \to V_2 \otimes_{F_2} F_0$. Conversely, one can ask whether a choice of (V_1, V_2, ϕ) is necessarily induced by a choice of V. This is the case, and the above association is in fact an equivalence of categories, if and only if each element of $\mathrm{GL}_n(F_0)$ is the product of an element of $\mathrm{GL}_n(F_1)$ and an element of $\mathrm{GL}_n(F_2)$ (e.g. by [3], Proposition 2.1). Moreover this condition is met in the situation we are considering for admissibility. Namely, let F be the function field of a smooth curve $\hat{X}$ over a complete discrete valuation ring T with uniformizer t. Let U_1, U_2 be proper subsets of the closed fiber X such that $U_1 \cup U_2 = X$, and let $U_0 = U_1 \cap U_2$. For $i = 0, 1, 2$ let F_i be the fraction field of the t-adic completion of the subring of F consisting of rational functions that are regular at the points of U_i. Then the above condition holds for the fields F, F_1, F_2, F_0 ([3], Theorem 4.10). Moreover the above assertion holds for more general situations, e.g. for regular curves that need not be smooth, for more than two intermediate fields, etc. In addition, and crucially for our application (as well as for applications to Galois theory), the fact that the assertion for vector spaces is an equivalence of categories implies the corresponding assertion for other algebraic structures, such as Galois field extensions and central simple algebras.

This technique is applied to our situation for a group G with abelian metacyclic Sylow p_i-subgroups P_i. After choosing appropriate fields F_i containing the given function field F, we explicitly construct P_i-Galois field extensions E_i/F_i that are maximal in F_i-division algebras D_i. These are chosen so that they will be split over a common overfield F_0. Using patching over fields we obtain a G-Galois maximal separable commutative F-subalgebra E of a central simple F-algebra D. We then use the fact that the indices of the Sylow subgroups have no common factor to show that D is a division algebra, and from that we obtain that E is a maximal subfield, proving admissibility.

References

[1] Jean-Louis Colliot-Thélène, Manuel Ojanguren and Raman Parimala, *Quadratic forms over fraction fields of two-dimensional Henselian rings and Brauer groups of related schemes.* In: *Proceedings of the International Colloquium on Algebra, Arithmetic and Geometry*, Tata Inst. Fund. Res. Stud. Math., vol. 16, pp. 185–217, Narosa Publ. Co., 2002.

[2] David Harbater, *Patching and Galois theory.* In *Galois Groups and Fundamental Groups* (L. Schneps, ed.), MSRI Publications series, vol. 41, Cambridge Univ. Press, 2003, pp. 313-424.

[3] David Harbater and Julia Hartmann, *Patching over fields.* 2007 manuscript. To appear in Israel Journal of Mathematics. Available at arXiv:0710.1392.

[4] David Harbater, Julia Hartmann, and Daniel Krashen, *Applications of patching to quadratic forms and central simple algebras.* 2008 manuscript. To appear in Inventiones Mathematicae. Available at arXiv:0809.4481.

[5] David Harbater, Julia Hartmann, Daniel Krashen, *Patching subfields of division algebras*, 2009 manuscript. Available at arXiv:0904.1594.

[6] Max Lieblich, *Period and index in the Brauer group of an arithmetic surface, with an appendix by Daniel Krashen.* 2007 manuscript. Available at arXiv:math/0702240.

[7] David J. Saltman, *Lectures on division algebras*, Published by American Mathematical Society, Providence, RI, 1999.

[8] Murray M. Schacher, *Subfields of division rings. I*, J. Algebra **9** (1968), 451–477.

Supported in part by NSF Grant DMS-0500118.

Fully Hilbertian fields I

Lior Bary-Soroker
(joint work with Elad Paran)

The slides of this talk are available at `http://math.huji.ac.il/~barylior`

A field K is called Hilbertian if it satisfies the following property: for every irreducible polynomial $f(X,Y) \in K[X,Y]$ which is separable in Y, there exist infinitely many $a \in K$ for which $f(a,Y)$ is irreducible in $K[Y]$. The name Hilbertian is derived from Hilbert's irreducibility theorem, which asserts that number fields are Hilbertian.

Hilbert's original motivation for his irreducibility theorem was the inverse Galois problem. Even nowadays Hilbert's irreducibility theorem remains the central approach for this problem, see [7, 9]. Moreover, this theorem has numerous other applications in number theory, see e.g. [8, 2].

It is natural to study the interplay of the cardinality $|K|$ of K and the irreducibility propety. We first consider the number of irreducible specializations. A Hilbert set $H = H(f)$ attached to an irreducible polynomial $f(X,Y)$ is the set of all $a \in K$ for which $f(a,Y)$ is irreducible. It follows from the density of Hilbert sets [3], that $|H| = |K|$ for any irreducible polynomial $f(X,Y) \in K[X,Y]$ that is separable in Y.

A more interesting object to study is the number of 'specialized fields'. Let $f(X,Y)$ be an irreducible polynomial that is separable in Y. Let

$$F = K(X)[Y]/(f(X,Y))$$

and let L be the algebraic closure of K in F. Each $a \in H(f)$ provides a specialized field $F_a \cong K[Y]/(f(a,Y))$ that contains L with $[F_a : K] = [F : K]$. If $F = L(X)$, then $L = F_a$ for all a, i.e., L is the unique specialized field. Assume this is not the case, then K Hilbertian implies the existence of infinitely many specialized fields that are linearly disjoint over L. Surprisingly, even if $|K| > \aleph_0$, it does NOT imply that there are more than $\aleph_0$ specialized fields.

In this work we study fields which have as much and as distinct as possible specialized fields F_a. That is to say, there exists a subset $A \subseteq H(f)$ of cardinality $|K|$ and specialized fields F_a, $a \in A$ such that F_a are linearly disjoint over L. We call a field with this feature **fully Hilbertian**. It is important to note that a *countable* field K is Hilbertian if and only if it is fully Hilbertian.

The objective of this work is to initiate the study of fully Hilbertian fields and to show that this family exhibit the same good behavior as Hilbertian fields. In particular, we show that the basic construction of Hilbertian fields are fully Hilbertian. Also we show that all permanence criteria of Hilbertian fields, also hold for fully Hilbertian fields.

Our main motivation for this study comes from the following Galois theoretic application.

Theorem 1. *Let K be an ample fully Hilbertian field. Then* $\mathrm{Gal}(K)$ *is semi-free.*

(Recall that a profinite group of infinite rank m is called semi-free if every finite split embedding problem has m independent solutions.) An important application of this theorem is considered in Elad Paran's talk.

Maybe the most important part of this work is the proofs that many families of Hilbertian fields are in fact fully Hilbertian. First, as mentioned above, a countable Hilbertian field is fully Hilbertian. Thus number fields are fully Hilbertian. The second basic, and perhaps most interesting, family of fully Hilbertian fields are function fields.

Theorem 2. *Let F be a finitely generated transcendental extension of an arbitrary field K. Then F is fully Hilbertian.*

The next case to consider is algebraic extensions of fully Hilbertian fields. We show that the notion of a fully Hilbertian field is well behaved – exhibiting the same permanence properties of Hilbertian fields.

Any algebraic extension L/K factors to a tower of fields $K \subseteq E \subseteq L$ in which E/K is purely inseparable and L/E is separable. We study each case separately. First fully Hilbertianity is preserved under purely inseparable extensions, as Hilbertian fields do:

Theorem 3. *Let E be a purely inseparable extension of a fully Hilbertian field K. Then E is fully Hilbertian.*

The case of separable extensions is much more interesting. First, it is clear that not every extension of a fully Hilbertian (or Hilbertian) field is Hilbertian. For example, a separably closed field is not Hilbertian, and hence not fully Hilbertian. A lot of research was spent on the Hilbertianity of separable extensions of Hilbertian fields, and perhaps the most general result is Haran's diamond theorem [5]. Haran's work also gave evidence to the so called *twinning principle.*

In [6] Jarden and Lubotzky formulate the **twinning principle**. They suggest a connection between results about freeness of subgroups of free profinite groups and results about Hilbertianity of separable extensions of Hilbertian fields. Furthermore, Jarden and Lubotzky state that the proofs in both cases have analogies. In spite of that they add that *it is difficult to see a real analogy between the proofs of the group theoretic theorems and those of field theory.*

As mentioned, in [4, 5] Haran provides more evidence to the twinning principle by proving his diamond theorem in both cases (see also [2, Theorems 13.8.3 and 25.4.3]). Haran's main tool in both proofs is twisted wreath products. (Using twisted wreath product one can induce embedding problems and then, on the other direction, induce weak solutions via Shapiro's map. Haran shows that under some conditions those weak solutions are in fact solutions, i.e., surjective. We refer to this method henceforth as the **Haran-Shapiro induction**.)

In [1], the speaker, Haran, and Harbater refine the Haran-Shapiro Induction in order to extend the proof to the class of semi-free groups. We feel the the right analog in the twinning principle should be between semi-free groups of rank m and fully Hilbertian fields of cardinality m. In this work we show that all the group theoretic construction of the Haran-Shapiro Induction are in fact 'field theoretic'. This allow us to reduce proofs about permanence criteria of fully Hilbertian fields to the group theoretic case of semi-free groups (which was treated in [1]). Thus we get, e.g.,

Theorem 4. *Let M be a separable extension of a fully Hilbertian field K. Then each of the following conditions suffices for M to be fully Hilbertian.*

(1) *M/K is finite.*
(2) *M is an abelian extension of K.*
(3) *M is a proper finite extension of a Galois extension N of K.*
(4) *(The diamond theorem) there exist Galois extensions M_1, M_2 of K such that $M \subseteq M_1M_2$, but $M \not\subseteq M_i$ for $i = 1, 2$.*

References

[1] Lior Bary-Soroker, Dan Haran, and David Harbater, *Permanence criteria for semi-free profinite groups*, 2008, http://arxiv.org/abs/0810.0845.

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

[3] Wulf Dieter Geyer and Moshe Jarden, *Fields with the density property*, J. Algebra **35** (1975), 178–189.

[4] Dan Haran, *Free subgroups of free profinite groups*, J. Group Theory **2** (1999), no. 3, 307–317.

[5] ———, *Hilbertian fields under separable algebraic extensions*, Invent. Math. **137** (1999), no. 1, 113–126.

[6] Moshe Jarden and Alexander Lubotzky, *Hilbertian fields and free profinite groups*, J. London Math. Soc. (2) **46** (1992), no. 2, 205–227.

[7] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[8] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[9] Helmut Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, An introduction.

Fully Hilbertian Fields II

Elad Paran
(joint work with Lior Bary-Soroker)

Hilbert's motivation for proving his irreducibility theorem was Galois theory over number fields. For countable fields, the notions of Hilbertianity and full Hilbertianity coincide. However, for uncoutable fields, the notion of full Hilbertianity is strictly stronger than that of Hilbertianity, and allows to prove stronger Galois theoretic results. Suppose K is a field, such that every finite split embedding problem is solvable over $K(x)$. For example, this is true if K is ample, by a major theorem of Pop. Moreover, the conjecture of Debes and Deschamps suggests this is true for any field K. If K satisfies this propety and is also Hilbertian, then any finite split embedding problem over K can be lifted to $K(x)$, solved there, and the solution can be specialized to a solution over K.

However, this process does not allow to control the number of solutions over K, since distinct distinct specializations may result in identical specialized fields. If the field K satisfies the stronger property of being fully Hilbertian, then a single solution over $K(x)$ yields $|K|$ solutions over K, linearly disjoint over the field L defining the embedding problem over K. Thus, if K is fully Hilbertian and ample, the Galois group of K is a semi-free profinite group.

In 2006, Harbater and Stevenson essentialy proved that if $K = K_0((X,Y))$ is the field of formal power series in two variables over an arbitrary base field K, then Gal(K) is semi-free. In this talk, we prove that this is true for any number of variables. More generally, if K is the quotient field of a complete local Noetherian domain of dimension exceeding 1, then K is fully Hilbertrian. Since K is ample (by a recent theorem of Pop), this implies that $\mathrm{Gal}(K)$ is semi-free.

We note that this Galois theoretic result was essentialy obtained recently by Pop, and independtly obtained using Patching by the speaker. However, proving that a field is fully Hilbertrian is a strictly stronger result, in terms of the arithemtical properties of the field. That is, there exist ample fields with semi-free Galois groups which are not fully Hilbertian.

Finally, we remark that the notion of Hilbertianity, though orinigally introduced in order to attack Galois theoretic problems, found numberous other applications in number theory. For example, in the construction of elliptic curves of high degree. We hope that in a similar fashion, the notion of full Hilbetrianity could be useful for arithmetical problems over uncoutanble fields, outside the scope of Galois theory.

The absolute Galois groups of semi-local fields

Dan Haran
(joint work with Moshe Jarden, Florian Pop)

Let K be a countable Hilbertian field and let $\sigma = (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(K)^e$ be chosen at random (that is, from a set of Haar measure 1). Furthermore let S be a finite set of absolute values on K such that their completions are local fields. For each $\mathfrak{p} \in S$ we choose a **$\mathfrak{p}$-closure** $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$. This is a Henselian closure if $\mathfrak{p}$ is nonarchimedean, a real closure if $\mathfrak{p}$ is real archimedean, and the algebraic closure of K if $\mathfrak{p}$ is complex archimedean. We can associate fields to this data and determine their absolute Galois groups:

- If $M = K_s(\sigma)$, the fixed field of $\sigma_1, \dots, \sigma_e$ in the separable closure K_s of K, then $\mathrm{Gal}(M) \cong \hat{F}_e$ (Ax '67 for $e = 1$ and Jarden '74 in general).
- If $M = K_s[\sigma]$, the maximal Galois extension of K in the above defined $K_s(\sigma)$, then $\mathrm{Gal}(M) \cong \hat{F}_\omega$ (Jarden '97).
- If $M = K_{\mathfrak{p}_1}^{\sigma_1} \cap \cdots \cap K_{\mathfrak{p}_e}^{\sigma_1}$, where $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_e\}$, then $\mathrm{Gal}(M)$ is the free product $\mathop{\boxed{\ast}}_{i=1}^{e} \mathrm{Gal}(K_{\mathfrak{p}_i})^{\sigma_i}$ (Geyer '78).
- If $N = \bigcap_{\mathfrak{p} \in S} \bigcap_{\rho \in \mathrm{Gal}(K)} K_{\mathfrak{p}}^{\rho}$, then $\mathrm{Gal}(N) \cong C$, where C is the profinite group $C = \mathop{\boxed{\ast}}_{\mathfrak{p} \in S} \mathop{\boxed{\ast}}_{\rho \in R_{\mathfrak{p}}} \mathrm{Gal}(K_{\mathfrak{p}}^{\rho})$, for some Cantor space $R_{\mathfrak{p}} \subseteq \mathrm{Gal}(K)$ (Fried-Haran-Völklein '93 for $S = \{\text{real}\}$ and Pop '96 in general).

  Fix N and C as above for the rest of this exposition.
- If $M = N(\sigma) = N \cap K_s(\sigma)$, then $\mathrm{Gal}(M) \cong \hat{F}_e \star C$ (Haran-Jarden-Pop, Nagoya J. Math., to appear).
- If $M = N[\sigma] = N \cap K_s[\sigma]$, then

Theorem 1. $\mathrm{Gal}(M) \cong \hat{F}_\omega \star C$.

Proof of the Theorem (a sketch):

Choose $\tau \in \mathrm{Gal}(K)$ at random and let E be a proper finite extension of $N[\sigma, \tau]$ contained in $N[\sigma]$.

$$\begin{tikzcd} K \arrow[r] & N[\sigma,\tau] \arrow[r] & E \arrow[r] & N[\sigma] \arrow[r] & N \arrow[r] & K_s \end{tikzcd}$$

Then E is Hilbertian, by Weissauer's theorem. Furthermore, $N[\sigma, \tau]$ is PSC (Jarden-Geyer, '02), and hence so is E (Haran-Pop-Jarden, '06). Therefore, by our previous work, $\mathrm{Gal}(E)$ is relatively projective with respect to the family of conjugates of $\mathrm{Gal}(K_{\mathfrak{p}})$, for $\mathfrak{p} \in S$, and hence E is ample.

In this situation, Pop ('96) proves that $\mathrm{Gal}(E) \cong \hat{F}_\omega \star C$, so that the projection $\hat{F}_\omega \star C \to C$ coincides with the restriction $\mathrm{Gal}(E) \to \mathrm{Gal}(N/E)$.

Claim. $\mathrm{Gal}(N/N[\sigma]) \cong \hat{F}_\omega$.

Proof. Indeed, $\mathrm{Gal}(N/N[\sigma]) \triangleleft \mathrm{Gal}(N/E) \cong \hat{F}_\omega$, so by Melnikov it suffices to show that if G is the group of a prime order or a direct product S^n of finitely many copies of a finite non-abelian simple group S, then G is a quotient of $\mathrm{Gal}(N/N[\sigma])$.

We first realize G over E: As $\mathrm{Gal}(N/E) \cong \hat{F}_\omega$, there is $E \subseteq F \subseteq N$ such that $\mathrm{Gal}(F/E) \cong G$. By Colliot-Thélène, Harbater, Moret-Bailly, Haran-Jarden, and others (independently) there is a G-Galois extension $E(x,y)/E(x)$, regular over E and a place φ from $E(x,y)$ onto F such that $\varphi(E(x)) = E$.

This setup is defined already over a finite extension L of K in E. Hence L/K is finite, $L \subseteq N[\sigma]$, $L(x,y)/L(x)$ is a G-Galois extension regular over L, and there is a place $\varphi \colon L(x,y) \to N$ such that $\varphi(L(x) = L$.

Without loss of generality L/K is Galois, otherwise replace L by its Galois closure over K. Now, L is Hilbertian, hence there is a sequence $L_1, L_2, L_3, \ldots$ such that each L_i/K is Galois, $\mathrm{Gal}(L_i/K) \cong G$, $L_i \subseteq K_{\mathfrak{p}}$, for all $\mathfrak{p} \in S$, and hence $L_i \subseteq N$. There is $\lambda \in G$ such that its image $\lambda_i \in \mathrm{Gal}(L_i/L)$ normally generates the whole group. Without loss of generality there is i such that $\sigma_1|_{L_i} = \lambda_i$. It then follows that $L_i \cap N[\sigma] = L$, and hence $\mathrm{Gal}(L_i N[\sigma]/N[\sigma]) \cong G$. □

Finally we use a pure group-theoretical lemma, a profinite version of the Kurosh Subgroup Theorem for a normal subgroup of infinite index of a free product:

Lemma 1. *Let C, F be profinite groups and let $\pi\colon C \star F \to F$ be the projection. Let $F_0 \leq F$. Then $\pi^{-1}(F_0) \cong \big(\mathop{\ast}_{r \in F/F_0} C^r\big) \star F_0$.*

Apply this to our situation; $F = \hat{F}_\omega$, $F_0 \cong \hat{F}_\omega$, and $\pi\colon C \star F \to F$ is the restriction map $\mathrm{Gal}(E) \to \mathrm{Gal}(N/E)$. Thus $\mathrm{Gal}(N[\sigma]) = \pi^{-1}(\mathrm{Gal}(N/N[\sigma]) \cong \big(\mathop{\ast}_{r \in F/F_0} C^r\big) \star \hat{F}_\omega$.

Because C is itself a free product, $\mathop{\ast}_{r \in F/F_0} C^r \cong C$. Thus $\mathrm{Gal}(N[\sigma]) \cong C \star \hat{F}_\omega$. This ends the proof of the Theorem.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Jochen Koenigsmann

1. $\mathbb{Z}$ is universally definable in $\mathbb{Q}$

Hilbert's 10th problem was to find a general algorithm for deciding, given any n and any polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, whether or not f has a zero in $\mathbb{Z}^n$. Building on earlier work by Martin Davis, Hilary Putnam and Julia Robinson, Yuri Matiyasevich proved in 1970 that there can be no such algorithm. In particular, the existential first-order theory $Th_\exists(\mathbb{Z})$ of $\mathbb{Z}$ (in the language of rings $\mathcal{L} := \{+, \cdot; 0, 1\}$) is undecidable. Hilbert's 10th problem over $\mathbb{Q}$, i.e. the question whether $Th_\exists(\mathbb{Q})$ is decidable, is still open.

If one had an **existential** (or **diophantine**) definition of $\mathbb{Z}$ in $\mathbb{Q}$ (i.e. a definition by an existential 1st-order $\mathcal{L}$-formula) then $Th_\exists(\mathbb{Z})$ would be interpretable in $Th_\exists(\mathbb{Q})$, and the answer would, by Matiyasevich's Theorem, again be no. But it is still open whether $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$.

The earliest 1st-order definition of $\mathbb{Z}$ in $\mathbb{Q}$, due to Julia Robinson ([3]) can be expressed by a $\forall\exists\forall$-formula of the shape

$$\phi(t) = \forall x_1 \forall x_2 \exists y_1 \ldots \exists y_7 \forall z_1 \ldots \forall z_6 \; f(t; x_1, x_2; y_1, \ldots, y_7; z_1, \ldots, z_6) = 0$$

for some $f \in \mathbb{Z}[t; x_1, x_2; y_1, \ldots, y_7; z_1, \ldots, z_6]$, so that for any $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \text{ iff } \phi(t) \text{ holds in } \mathbb{Q}.$$

Recently, Bjorn Poonen ([1]) managed to find a $\forall\exists$-definition with 2 universal and 7 existential quantifiers. In this talk we present a $\forall$-definition of $\mathbb{Z}$ in $\mathbb{Q}$:

Theorem 1. *There is a polynomial $g \in \mathbb{Z}[t; x_1, \ldots, x_{58}]$ such that, for all $t \in \mathbb{Q}$,*

$$t \in \mathbb{Z} \textit{ iff } \forall x_1 \ldots \forall x_{58} \in \mathbb{Q}\ g(t; x_1, \ldots, x_{58}) \neq 0.$$

If one measures logical complexity in terms of the number of changes of quantifiers then this is the simplest definition of $\mathbb{Z}$ in $\mathbb{Q}$, and, in fact, it is the simplest possible: there is no quantifier-free definition of $\mathbb{Z}$ in $\mathbb{Q}$.

Corollary 1. *$\mathbb{Q} \setminus \mathbb{Z}$ is diophantine in $\mathbb{Q}$.*

Corollary 2. *$Th_{\forall\exists}(\mathbb{Q})$ is undecidable.*

2. Key steps in the proof of Theorem 1

Like all previous definitions of $\mathbb{Z}$ in $\mathbb{Q}$, we use local class field theory and Hasse's Local-Global-Principle for quadratic forms. What is new in our approach is the use of the Quadratic Reciprocity Law and, inspired by the model theory of local fields, the transformation of some existential formulas into universal formulas.

Step 1: **Poonen's diophantine definition of quaternionic semi-local rings.** The first step essentially copies Poonen's proof ([1]). We adopt his terminology:

Definition 1. For $a, b \in \mathbb{Q}^\times$, let

- $H_{a,b} := \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \alpha \oplus \mathbb{Q} \cdot \beta \oplus \mathbb{Q} \cdot \alpha\beta$ be the quaternion algebra over $\mathbb{Q}$ with multiplication defined by $\alpha^2 = a$, $\beta^2 = b$ and $\alpha\beta = -\beta\alpha$,
- $\Delta_{a,b} := \{l \in \mathbb{P} \cup \{\infty\} \mid H_{a,b} \otimes \mathbb{Q}_l \not\cong M_2(\mathbb{Q}_l)\}$ the set of primes (including ∞) where $H_{a,b}$ does not split locally ($\mathbb{Q}_\infty = \mathbb{R}$ and $\mathbb{P}$ denotes the set of rational primes) — $\Delta_{a,b}$ is always finite, and $\Delta_{a,b} = \emptyset$ iff $a \in N(b)$, i.e. a is in the image of the norm map $\mathbb{Q}(\sqrt{b}) \to \mathbb{Q}$,
- $S_{a,b} := \{2x_1 \in \mathbb{Q} \mid \exists x_2, x_3, x_4 \in \mathbb{Q} : x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$ the set of traces of norm-1 elements of $H_{a,b}$, and
- $T_{a,b} := S_{a,b} + S_{a,b} + \{0, 1, \ldots, 2309\}$ – note that $T_{a,b}$ is an existentially defined subset of $\mathbb{Q}$, and that $2309 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 - 1$.

Lemma 1. *$T_{a,b} = \bigcap_{l \in \Delta_{a,b}} \mathbb{Z}_{(l)}$, where $\mathbb{Z}_{(\infty)} := \{x \in \mathbb{Q} \mid -4 \leq x \leq 2313\}$.*

The proof follows essentially that of [1], Lemma 2.5, using Hensel's Lemma, the Hasse bound for the number of rational points on genus-1 curves over finite fields, and the local-global principle for quadratic forms. Poonen then obtains his $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$ from the fact that

$$\mathbb{Z} = \bigcap_{l \in \mathbb{P}} \mathbb{Z}_{(l)} = \bigcap_{a,b>0} T_{a,b}.$$

Note that $a > 0$ or $b > 0$ implies that $\infty \notin \Delta_{a,b}$.

***Step 2:* Towards a uniform diophantine definition of all $\mathbb{Z}_{(p)}$'s in $\mathbb{Q}$.** We will present a diophantine definition for the local rings $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$ depending on the congruence of the prime p modulo 8, and involving p (and if $p \equiv 1 \texttt{ mod } 8$ an auxiliary prime q) as a parameter. However, since in any first-order definition of a subset of $\mathbb{Q}$ we can only quantify over the elements of $\mathbb{Q}$, and not e.g. over all primes, we will allow arbitrary (non-zero) rationals p and q as parameters in the following definition.

Definition 2. For $p, q \in \mathbb{Q}^\times$ let

- $R_p^{[3]} := T_{-p,-p} + T_{2p,-p}$
- $R_p^{[5]} := T_{-2p,-p} + T_{2p,-p}$
- $R_p^{[7]} := T_{-p,-p} + T_{2p,p}$
- $R_{p,q}^{[1]} := T_{2pq,q} + T_{-2pq,q}$

Note that the R's are all existentially defined subrings of $\mathbb{Q}$ containing $\mathbb{Z}$.

Definition 3. (a) $\mathbb{P}^{[k]} := \{l \in \mathbb{P} \mid l \equiv k \texttt{ mod } 8\}$, where $k = 1, 3, 5$ or 7

(b) For $p \in \mathbb{Q}^\times$, define

- $\mathbb{P}(p) := \{l \in \mathbb{P} \mid v_l(p) \text{ is odd}\}$, where v_l denotes the l-adic valuation on $\mathbb{Q}$
- $\mathbb{P}^{[k]}(p) := \mathbb{P}(p) \cap \mathbb{P}^{[k]}$, where $k = 1, 3, 5$ or 7
- $p \equiv_2 k \texttt{ mod } 8$ iff $p \in k + \mathbb{Z}_{(2)}$, where $k \in \{0, 1, 2, \ldots, 7\}$
- for l a prime, the **generalized Legendre symbol** $\left(\!\!\left(\begin{array}{c} p \\ l \end{array}\right)\!\!\right) = \pm 1$ to indicate whether or not the l-adic unit $pl^{-v_l(p)}$ is a square modulo l.

Lemma 2. (a) $\mathbb{Z}_{(2)} = T_{3,3} + T_{2,5}$

(b) *For $p \in \mathbb{Q}^\times$ and $k = 3, 5$ or 7, if $p \equiv_2 k \texttt{ mod } 8$ then*

$$R_p^{[k]} = \begin{cases} \bigcap_{l \in \mathbb{P}^{[k]}(p)} \mathbb{Z}_{(l)} & \text{if } \mathbb{P}^{[k]}(p) \neq \emptyset \\ \mathbb{Q} & \text{if } \mathbb{P}^{[k]}(p) = \emptyset \end{cases}$$

In particular, if p is a prime ($\equiv k \texttt{ mod } 8$) then $\mathbb{Z}_{(p)} = R_p^{[k]}$.

(c) *For $p, q \in \mathbb{Q}^\times$ with $p \equiv_2 1 \texttt{ mod } 8$ and $q \equiv_2 3 \texttt{ mod } 8$,*

$$R_{p,q}^{[1]} = \begin{cases} \bigcap_{l \in \mathbb{P}(p,q)} \mathbb{Z}_{(l)} & \text{if } \mathbb{P}(p,q) \neq \emptyset \\ \mathbb{Q} & \text{if } \mathbb{P}(p,q) = \emptyset \end{cases}$$

where

$$l \in \mathbb{P}(p,q) :\Leftrightarrow l \in \begin{cases} \mathbb{P}(p) \setminus \mathbb{P}(q) \text{ with } \left(\!\!\left(\begin{array}{c} q \\ l \end{array}\right)\!\!\right) = -1, \text{ or} \\ \mathbb{P}(q) \setminus \mathbb{P}(p) \text{ with } \left(\!\!\left(\begin{array}{c} 2p \\ l \end{array}\right)\!\!\right) = \left(\!\!\left(\begin{array}{c} -2p \\ l \end{array}\right)\!\!\right) = -1, \text{ or} \\ \mathbb{P}(p) \cap \mathbb{P}(q) \text{ with } \left(\!\!\left(\begin{array}{c} 2pq \\ l \end{array}\right)\!\!\right) = \left(\!\!\left(\begin{array}{c} -2pq \\ l \end{array}\right)\!\!\right) = -1 \end{cases}$$

In particular, if p is a prime $\equiv 1 \texttt{ mod } 8$ and q is a prime $\equiv 3 \texttt{ mod } 8$ with $\left(\begin{array}{c} q \\ p \end{array}\right) = -1$ then $\mathbb{Z}_{(p)} = R_{p,q}^{[1]}$.

Corollary 3.

$$\mathbb{Z} = \mathbb{Z}_{(2)} \cap \bigcap_{p,q\in\mathbb{Q}^\times} (R_p^{[3]} \cap R_p^{[5]} \cap R_p^{[7]} \cap R_{p,q}^{[1]})$$

The proof of the Lemma uses explicit norm computations for quadratic extensions of $\mathbb{Q}_2$, the Quadratic Reciprocity Law and the following

Observation. *For $a, b \in \mathbb{Q}^\times$ and for an odd prime l,*

$$l \in \Delta_{a,b} \Leftrightarrow \begin{cases} v_l(a) \text{ is odd, } v_l(b) \text{ is even, and } \left(\!\!\left(\begin{matrix} b \\ l \end{matrix}\right)\!\!\right) = -1, \text{ or} \\ v_l(a) \text{ is even, } v_l(b) \text{ is odd, and } \left(\!\!\left(\begin{matrix} a \\ l \end{matrix}\right)\!\!\right) = -1, \text{ or} \\ v_l(a) \text{ is odd, } v_l(b) \text{ is odd, and } \left(\!\!\left(\begin{matrix} -ab \\ l \end{matrix}\right)\!\!\right) = -1 \end{cases}$$

Corollary 4. *The following properties are diophantine properties for any $p \in \mathbb{Q}^\times$:*

- $p \equiv_2 k \texttt{ mod } 8$ *for* $k \in \{0, 1, 2, \ldots, 7\}$
- $\mathbb{P}(p) \subseteq \mathbb{P}^{[1]} \cup \mathbb{P}^{[k]}$ *for* $k = 3, 5$ *or* 7
- $\mathbb{P}(p) \subseteq \mathbb{P}^{[1]}$

Step 3: **From existential to universal.** In Step 3, we try to find universal definitions for the R's occuring in Corollary 3 immitating the local situation: First one observes that for $R = \mathbb{Z}_{(2)}$, or for $R = R_p^{[k]}$ with $k = 3, 5$ or 7, or for $R = R_{p,q}^{[1]}$, the Jacobson radical $J(R)$ can be defined by an existential formula using Observation 2. Now let

$$\widetilde{R} := \{x \in \mathbb{Q} \mid \neg\exists y \in J(R) \text{ with } x \cdot y = 1\}.$$

Proposition 1. (a) *$\widetilde{R}$ is defined by a* universal *formula in $\mathbb{Q}$.*

(b) *If $R = \bigcap_{l\in\mathbb{P}\setminus R^\times} \mathbb{Z}_{(l)}$ then $\widetilde{R} = \bigcup_{l\in\mathbb{P}\setminus R^\times} \mathbb{Z}_{(l)}$, provided $\mathbb{P} \setminus R^\times \neq \emptyset$, i.e. provided $R \neq \mathbb{Q}$.*

(c) *In particular, if $R = \mathbb{Z}_{(l)}$ then $\widetilde{R} = R$.*

The proviso in (b), however, can be guaranteed by diophantinely definable conditions on the parameters p, q:

Lemma 3. *(a) Define for $k = 1, 3, 5$ and 7,*

$$\begin{aligned} \Phi_k &:= \{p \in \mathbb{Q}^\times \mid p \equiv_2 k \texttt{ mod } 8 \text{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{[1]} \cup \mathbb{P}^{[k]}\} \\ \Psi &:= \{(p, q) \in \Phi_1 \times \Phi_3 \mid p \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_q^{[3]}))\}. \end{aligned}$$

Then Φ_k and Ψ are diophantine in $\mathbb{Q}$.

(b) Assume that

- $R = R_p^{[k]}$ *for $k = 3, 5$ or 7, where $p \in \Phi_k$, or*
- $R = R_{p,q}^{[1]}$ *where $(p, q) \in \Psi$.*

Then $R \neq Q$.

The proof of this lemma is somewhat involved, though purely combinatorial, playing with the Quadaratic Reciprocity Law and Observation 2.

The universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ can now be read off the equation

$$\mathbb{Z} = \widetilde{\mathbb{Z}_{(2)}} \cap \Big(\bigcap_{k=3,5,7} \bigcap_{p\in\Phi_k} \widetilde{R_p^{[k]}} \Big) \cap \bigcap_{(p,q)\in\Psi} \widetilde{R_{p,q}^{[1]}},$$

where Φ_k and Ψ are the diophantine sets defined in Lemma 3.

The equation is valid by Lemma 2, Proposition 1(b), (c) and Lemma 3(b). The definition is universal as one can see by spelling out the equation and applying Lemma 1(a) and Corollary 4: for any $t \in \mathbb{Q}$,

$$\begin{aligned} t \in \mathbb{Q} \quad \Leftrightarrow \quad & t \in \widetilde{\mathbb{Z}_{(2)}} \wedge \\ & \forall p \textstyle\bigwedge_{k=3,5,7} (t \in \widetilde{R_p^{[k]}} \vee p \notin \Phi_k) \wedge \\ & \forall p, q (t \in \widetilde{R_{p,q}^{[1]}} \vee (p,q) \notin \Psi) \end{aligned}$$

Theorem 1 is now obtained by diophantine routine arguments and counting quantifiers.

3. A $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$ with just one $\forall$

Using the terminology and the results of the previous section and defining for $p \in \Phi_1$ the subring

$$R_p^{[1]} := \{x \in \mathbb{Q} \mid \exists q \text{ with } (p,q) \in \Psi, q \in (R_{p,q}^{[1]})^{\times} \text{ and } x \in R_{p,q}^{[1]}\},$$

we can also show that there is a $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$ with just one universal quantifier (such a definition was independently given by Alexandra Shlapentokh using an entirely different elliptic curve method in [4]):

Corollary 5. *For all $t \in \mathbb{Q}$:*

$$t \in \mathbb{Z} \leftrightarrow \forall p \bigvee_{k=1,3,5,7} t \in \mathbb{Z}_{(2)} \wedge (t \in R_p^{[k]} \wedge p \in \Phi_k)$$

Writing this in prenex normal form gives a formula with one universal and 58 existential quantifiers.

4. More diophantine predicates in $\mathbb{Q}$

¿From the results and techniques of section 2, one obtains new diophantine predicates in $\mathbb{Q}$. Among them are

- $x \notin \mathbb{Q}^2$
- $x \notin N(y)$, where $N(y)$ is the image of the norm $\mathbb{Q}(\sqrt{y}) \to \mathbb{Q}$

The first was also obtained in [2], using a deep result of Colliot-Thélène et al. on Châtelet surfaces - our techniques are purely elementary.

5. Why $\mathbb{Z}$ should not be diophantine in $\mathbb{Q}$

It is well known that it follows from Mazur's Conjecture about the topological closure of diophantine subsets of $\mathbb{Q}$ in $\mathbb{R}$ that $\mathbb{Z}$ is not diophantine (= existentially definable) in $\mathbb{Q}$. Using model theoretic arguments we draw the same conclusion from a much weaker conjecture:

Conjecture 1. `Non-Integrality Conjecture` **NIC**$_n$ **(for** $n \geq 2$**)**
If $V \subseteq \mathbb{A}^n$ is a hypersurface defined over $\mathbb{Q}$ such that $V(\mathbb{Q})$ is Zariski dense, then so is $V(\mathbb{Q}) \cap (\mathbb{Q} \setminus \mathbb{Z} \cap \mathbb{Q}^{n-1})$.

Note that, by Siegel's Theorem on the finiteness of integral points on curves over $\mathbb{Q}$, the conjecture is true for $n = 2$.

Theorem 2. *If* **NIC**$_n$ *holds for all $n \geq 2$ then $\mathbb{Z}$ is not diophantine in $\mathbb{Q}$.*

References

[1] Bjorn Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, http://www-math.mit.edu/~poonen/, 2008.

[2] Bjorn Poonen, *The set of nonsquares in a number field is diophantine*, http://www-math.mit.edu/~poonen/, 2008.

[3] Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14(2)** (1949), 98-114.

[4] Alexandra Shlapentokh, *Using indices of points on an elliptic curve to construct a diophantine model of $\mathbb{Z}$ and define $\mathbb{Z}$ using one universal quantifier in very large subrings of number fields, including* $\mathbb{Q}$, arXiv:0901.4168v1 [math.NT], 7 Jan 2009.

A Local-Global Principle for Homogeneous Spaces and Applications

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

In recent joint work with D. Harbater [4], we modified the method of patching to make it applicable to objects over fields. This modification, originally intended for use in inverse differential Galois theory (see [2] and [3]), leads to several other interesting applications. Among them is a local-global principle for homogeneous spaces under rational connected linear algebraic groups, which in turn yields results about quadratic forms and central simple algebras. The results of this note can be found in [5].

1. Patching over Fields

The simplest objects that patching techniques over fields can be applied to are vector spaces. Given a quadruple of fields $F \leq F_1, F_2 \leq F_0$, we consider the base change functor

$$\Theta : \mathrm{Vect}(F) \to \mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2).$$

Here Vect$(-)$ denotes the category of finite dimensional vector spaces. The base change functor maps to the two-fibre product category $\mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$, an object of which is a triple (V_1, V_2, ϕ) consisting of an F_i-vector space V_i $(i = 1, 2)$ and an isomorphism $\phi : V_1 \otimes_{F_1} F_0 \to V_2 \otimes_{F_2} F_0$. Such an object is also called a *patching problem*, and a preimage under Θ is a *solution*. We are interested in situations when Θ is an equivalence of categories (then every patching problem has a unique solution).

Patching setups can be found using geometry. For example, let T be a complete discrete valuation ring with uniformizer t, let $\widehat{X}$ be a smooth projective T-curve with closed fibre X. Suppose we are given subsets $U_1, U_2 \subseteq X$ which cover X (these need not be affine), and let U_0 be their intersection. Define $\widehat{R}_i$ to be the t-adic completion of the ring of rational functions on $\widehat{X}$ which are regular on U_i, and let F_i be its fraction field $(i = 0, 1, 2)$. Let moreover F denote the function field of $\widehat{X}$. Then

Theorem 1 ([4], Theorem 4.12). *In the situation above, the base change functor Θ is an equivalence of categories.*

The theorem generalizes to the case of more than two patches, as well as to variants on the geometric setup.

In order to prove that patching can be applied in the above case (and in similar situations), we use a criterion of Harbater which reduces the problem to two conditions.

Proposition 1. *The base change functor Θ is an equivalence of categories if and only if the following two conditions hold:*

- $F = F_1 \cap F_2 \leq F_0$
- *for every $n \in \mathbb{N}$ and every $g \in GL_n(F_0)$ there exist matrices $g_i \in GL_n(F_i)$ for which $g = g_1 g_2$.*

The latter condition turns out to have a natural generalization to rational connected linear algebraic groups (i.e. connected linear algebraic groups which are rational varieties).

2. A Local-Global Principle

Suppose that F, F_i are as in the above geometric setup.

Theorem 2. *Let G be a rational connected linear algebraic group defined over F. Then for every $g \in G(F_0)$ there exist $g_i \in G(F_i)$ for which $g = g_1 g_2$.*

The idea of the proof is the following: By a density argument, we reduce to the case when g is close to the identity $I \in G$. In the case when $G = \mathrm{GL}_n$ (which was considered in [4]), one may obtain the multiplicative decomposition from an additive decomposition using (inductively) that $(I + tA)(I + tB) \equiv I + t(A + B)$ (mod t^2). In the general case, it is a priori not clear that this strategy yields factors that are in $G(F_i)$. However, the rationality assumption may be used to pass back and forth between elements in the group which are close to I and elements in affine space which are close to 0, and an induction similar to the one in the case of GL_n gives the desired factorization.

As an immediate consequence, we obtain a local-global principle for rational points on homogeneous spaces under such groups. Let G be a linear algebraic group over F and let H/F be a G-variety. We say that *G acts transitively on the points of H* if $G(L)$ acts transitively on $H(L)$ for every field extension L/F.

Corollary 1. *Let G be a rational connected linear algebraic group over F and let H be a variety over F such that G acts transitively on the points of H. Then $H(F) \neq \varnothing$ if and only if $H(F_1) \neq \varnothing \neq H(F_2)$.*

The proof is straightforward: Consider $h_i \in H(F_i)$, and view them as elements in $H(F_0)$. Then by the transitivity assumption, $gh_2 = h_1$ for some $g \in G(F_0)$. Using the previous theorem, we may factor g as $g = g_1 g_2$ where $g_i \in G(F_i)$. But then $g_2 h_2 = g_1^{-1} h_1 \in H(F_1) \cap H(F_2) \subseteq H(F)$, using the intersection condition.

In the same way as the patching theorem, this generalizes to the case of several patches etc.

3. Application to u-invariant

The *u-invariant* of a field F is defined as the maximal dimension of anisotropic quadratic forms over F. This invariant and the possible values it can take has been a major object of study in the theory of quadratic forms. For instance, it had long been conjectured but was only proven in 2007 that the u-invariant of $\mathbb{Q}_p(t)$ is 8 [7] for $p \neq 2$. More generally, it is expected that for many fields, the u-invariant should double upon a finitely generated extension of transcendence degree one. Using the above mentioned local global principle, we were able to prove a result about such behaviour for complete discrete valuation fields. Since the u-invariant of $\mathbb{Q}_p$ itself is 4, one can deduce from this a new proof as well as a generalization of the main result of [7]:

Theorem 3 ([7], Theorem 4.6)**.** *Let p be an odd prime and let F be the function field of a curve over a p-adic field. Then $u(F) = 8$.*

The difficult direction is to show that $u(F) \leq 8$. To this end, consider a quadratic form q in 9 variables over F and a sufficiently nice $\mathbb{Z}_p$-model $\widehat{X}$ of F. One can show that q becomes isotropic over certain patches F_i (using that associated residue forms have dimension at least $5 = \lceil 9/2 \rceil$ which exceeds the u-invariant of the residue field), i.e. the quadric hypersurface Q defined by q has points there: $Q(F_i) \neq \varnothing$. But Q is acted upon transitively by the rational group SO_n. Our local-global principle then implies the existence of a point in $Q(F)$, i.e., the isotropy of q over F.

As another concrete application of our results, one finds $u(\mathbb{Q}_p((t))(x)) = 16$.

The local-global principle for isotropy was generalized by J.-L. Colliot-Thélène, R. Parimala, and V. Suresh in [1].

4. Application to the Period-Index Problem

Corollary 1 also yields applications to central simple algebras, concerning the behavior of the relationship of period to index and how that is affected by passing to a finitely generated extension of transcendence degree one.

The *period* $\mathrm{per}(A)$ of a central simple algebra A is the order of its class in the Brauer group, whereas the *index* $\mathrm{ind}(A)$ is the minimal degree of a splitting field for A. It is well known that the period always divides the index, and that both have the same prime factors. Hence for every central simple algebra A, there exists an integer n such that $\mathrm{ind}(A) \mid \mathrm{per}(A)^n$. The *period-index problem* is the question whether there exists a bound on n which depends only on F. Associated to a central simple algebra A is its generalized *Severi-Brauer variety* $\mathrm{SB}(A)$, which is a graded variety with the property that $\mathrm{SB}_r(A)(L) \neq \varnothing$ if and only if $\mathrm{ind}(A_L) \mid r$. Applying our local global principle to the Severi-Brauer variety, which is acted upon transitively by $\mathrm{GL}_1(A)$ (viewed as a linear algebraic group over F), we are able to prove period-index bounds for function fields of curves over complete discrete valuation fields some of which were originally given in [8] and [6]. For example, one obtains that if F is the function field of a p-adic curve and $\mathrm{per}(A)$ is prime to p, then $\mathrm{ind}(A) \mid \mathrm{per}(A)^2$.

References

[1] Jean-Louis Colliot-Thélène, Raman Parimala, and Venapally Suresh, *Patching and Local-Global Principles for Homogeneous Spaces over Function Fields of p-adic Curves*, 2008 manuscript. Available at arXiv:0812.3099

[2] David Harbater, *Patching over Fields (Joint with Julia Hartmann)*, Oberwolfach Report 26 (2007).

[3] Julia Hartmann, *Differential Galois Groups and Patching (Joint with David Harbater)*, Oberwolfach Report 26 (2007).

[4] David Harbater, Julia Hartmann, *Patching over Fields*, 2007 manuscript. To appear in Israel J. Math. Available at arXiv:0710.1392.

[5] David Harbater, Julia Hartmann, and Daniel Krashen, *Applications of Patching to Quadratic Forms and Central Simple Algebras*, 2008 manuscript. To appear in Inventiones Mathematicae. Available at arXiv:0809.4481

[6] Max Lieblich, *Period and index in the Brauer group of an arithmetic surface (with an appendix by Daniel Krashen)*, 2007 manuscript. Available at arXiv:math/0702240v3

[7] Raman Parimala, Venapally Suresh, *The u-invariant of the function fields of p-adic curves*, 2007 manuscript. Available at arXiv:0708.3128.

[8] David Saltman, *Division algebras over p-adic curves*, J. Ramanujan Math. Soc. 12 (1997), no. 1, 25–47.

Elliptic curves with maximal Galois action on their torsion points

David Zywina

Fix a number field k and let E be an elliptic curve over k. For each positive integer m, we denote the group of m-torsion of $E(\overline{k})$ by $E[m]$. The group $E[m]$ is non-canonically isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$ and is equipped with a natural action of the absolute Galois group $G_k := \mathrm{Gal}(\overline{k}/k)$, which may be re-expressed in terms of a Galois representation

$$\rho_{E,m}\colon G_k \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Combining these representation for all m we obtain a single Galois representation

$$\rho_E\colon G_k \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

which encapsulates the Galois action on the torsion points of E.

The main result concerning these representations is the following famous theorem of Serre [3].

Theorem 1 (Serre)**.** *If E/k is a non-CM, then $\rho_E(G_k)$ has finite index in* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Serre's theorem, at least as stated above, is a qualitative result and does not describe how large the image of ρ_E can actually be. In particular, can the Galois representation ρ_E ever be surjective? (in other words, can every possible group automorphism of the torsion points of E arise via a Galois action)

The first example of a surjective ρ_E was given only recently by A. Greicius in his 2007 Ph.D. thesis (see [1]). Define $k = \mathbb{Q}(\alpha)$ where α is a root of x^3+x+1 and define the elliptic curve E by the Weierstrass equation $Y^2+2XY+\alpha Y = X^3 - X$. Greicius shows that indeed $\rho_E(G_k) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

In this talk we shall describe what happens for a "random" elliptic curve over k.

Let $\mathcal{O}_k$ be the ring of integers of k. For each pair $(a,b) \in \mathcal{O}_k^2$, we let $E(a,b)$ be the projective curve defined by the equation $Y^2 = X^3 + aX + b$. If $\Delta_{a,b} := -16(4a^3+27b^2) \neq 0$, then $E(a,b)$ is an elliptic curve over k.

Fix a norm $\|\cdot\|$ on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_k^2 \cong \mathbb{R}^{2[k:\mathbb{Q}]}$. For each real number $x > 0$, define the set

$$B_k(x) = \{(a,b) \in \mathcal{O}_k^2 : \Delta_{a,b} \neq 0,\ \|(a,b)\| \leq x\}.$$

So to each pair $(a,b) \in B_k(x)$, we can associate an elliptic curve $E(a,b)$ over k. The following theorem answers a question of Greicius on the surjectivity of the ρ_E ([1]*§3.4 Problem 3). Let $\mathbb{Q}^{\mathrm{cyc}} \subseteq \overline{k}$ be the cyclotomic extension of $\mathbb{Q}$.

Theorem 2. *Suppose that $k \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ and $k \neq \mathbb{Q}$. Then*

$$\lim_{x\to+\infty} \frac{|\{(a,b) \in B_k(x) : \rho_{E(a,b)}(G_k) = \mathrm{GL}_2(\widehat{\mathbb{Z}})\}|}{|B_k(x)|} = 1.$$

Intuitively, the theorem says that for a randomly chosen pair $(a,b) \in \mathcal{O}_k^2$, the corresponding elliptic curve $E(a,b)$ satisfies $\rho_{E(a,b)}(G_k) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

One can think of this result in terms of the philosophy of the Hilbert irreducibility theorem. Treating a and b as variables, we obtain an elliptic curve $\mathbf{E} = E(a,b)$ over $k(a,b)$ and as before we have a Galois representation $\rho_{\mathbf{E}}\colon G_{k(a,b)} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ which is surjective if $k \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. For each $(a_0,b_0) \in \mathcal{O}_k^2$, there is an inclusion $\rho_{E(a_0,b_0)}(G_k) \subseteq \rho_{\mathbf{E}}(G_{k(a,b)})$ and the theorem says we have equality for most choices of (a_0,b_0).

A similar result holds for $k \neq \mathbb{Q}$ when one takes into account that $\det \circ \rho_E \colon G_k \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character.

However, since $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is profinite we can not apply the Hilbert irreducibility theorem directly (in fact, the above reasoning fails when $k = \mathbb{Q}$!). As first observed by Serre, $\rho_E(G_{\mathbb{Q}})$ is *never* equal to $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ when E is an elliptic curve over $\mathbb{Q}$

(more precisely, he proved that the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})]$ is always even). The obstruction is based on the fact that any quadratic extension of $\mathbb{Q}$ comes from a cyclotomic extension.

N. Jones has proven that, with this constraint in mind, "most" elliptic curves $E/\mathbb{Q}$ have maximal Galois action on their torsion points. (See [2] for details and an explicit version of the theorem).

Theorem 3 (Jones)**.**

$$\lim_{x\to+\infty} \frac{|\{(a,b) \in B_{\mathbb{Q}}(x) : [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] = 2\}|}{|B_{\mathbb{Q}}(x)|} = 1.$$

Idea of proof. Let E be an elliptic curve over a number field $k \neq \mathbb{Q}$ for which $k \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. To prove that $\rho_E(G_k) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ it suffices to verify the following:

- $\rho_{E,\ell}(G_k) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for every prime $\ell \geq 5$,
- $\rho_{E,4}(G_k) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\rho_{E,9}(G_k) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$,
- $\sqrt{\Delta_E} \notin k \cdot \mathbb{Q}^{\mathrm{cyc}}$.

The first condition is the most interesting. Fix a prime $\ell \geq 5$. By considering the Frobenius endomorphism for the reduction of E modulo several primes $\mathfrak{p} \subseteq \mathcal{O}_k$, we can determine which conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ meet $\rho_{E,\ell}(G_k)$. Combining this modulo $\mathfrak{p}$ information together, we use the large sieve to give an asymptotic upper bound for the growth of

$$|\{(a,b) \in B_k(x) : \rho_{E(a,b),\ell}(G_k) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})\}|$$

as a function of x (i.e., *explicit* Hilbert irreducibility). We then use a theorem of Masser and Wüstholz coming from Diophantine approximation to effectively bound the number of ℓ's that must be considered (the bound depends on x).

Combining everything together, one find the following explicit version of the earlier theorem.

Theorem 4. *Let $k \neq \mathbb{Q}$ be a number field such that $k \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. Then*

$$\frac{|\{(a,b) \in B_k(x) : \rho_{E(a,b)}(G_k) \neq \mathrm{GL}_2(\widehat{\mathbb{Z}})\}|}{|B_k(x)|} \ll_{k,\|\cdot\|} \frac{\log x}{\sqrt{x}}.$$

References

[1] Greicius, Aaron, *Elliptic curves with surjective global Galois representation*, Ph.D. thesis, Univeristy of California, Berkeley, 2007.

[2] Jones, Nathan, *Almost all elliptic cuvers are Serre curves*, arXiv:math/0611096v1 [math.NT], 2006.

[3] Serre, Jean-Pierre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), no. 4, 259–331.

Abelian varieties over ample fields

Sebastian Petersen
(joint work with Arno Fehm)

A field F is said to be **ample** provided every smooth algebraic curve C/F satisfies either $C(F) = \emptyset$ or $|C(F)| = \infty$. Ample fields play an important role in modern Galois theory. In a joint project with Arno Fehm abelian varieties over ample fields were studied. In [2] we propose the following

Conjecture. Let F be an ample field which is not algebraic over a finite field. Then every non-zero abelian variety A/F satisfies $\mathrm{rank}(A(F)) = \infty$.

The main result [2] towards this Conjecture is

Theorem A. *Let $p \geq 0$ be the characteristic of F. Then $A(F) \otimes \mathbb{Z}_{(p)}$ is not finitely generated as a $\mathbb{Z}_{(p)}$-module.*

(Here $\mathbb{Z}_{(p)} := (\mathbb{Z} \setminus p\mathbb{Z})^{-1}\mathbb{Z}$ denotes the localization of $\mathbb{Z}$ at the prime ideal (p); the case $p = 0$ is allowed.) In particular $A(F)$ is not finitely generated as a $\mathbb{Z}$-module in the situation of the theorem. Furthermore we see that the conjecture holds true provided $\mathrm{char}(F) = 0$. The proof of Theorem A involves the Mordell-Lang conjecture, which is now a theorem (see [1], [6]), and certain field theoretic results whose proof is based on a trick of Koenigsmann [7].

There are strong connections with a circle of classical problems on ranks of abelian varieties over infinite algebraic extensions of finitely generated fields. For example, we can use Theorem A in order to strengthen a recent Theorem of Geyer and Jarden [4]. To describe this recall that a **local prime** of a finitely generated field K is an equivalence class $\mathfrak{p}$ of absolute values on K such that the completion $\hat{K}_{\mathfrak{p}}$ is a local field (i.e. a finite extension of $\mathbb{R}$, $\mathbb{Q}_p$ or $\mathbb{F}_p((T))$). If S is a finite set of local primes of K we denote by

$$K_{\mathrm{tot},S} := \bigcap_{\mathfrak{p} \in S} \bigcap_{\eta \in G_K} K_{\mathfrak{p}}^{\eta}$$

the **field of totally S-adic numbers**. For $e \geq 1$ and $\sigma \in G_K^e$ we denote by $K_{\mathrm{sep}}(\sigma)$ the fixed field in the separabel closure K_{sep} of the subgroup $\langle \sigma \rangle \subset G_K$ generated by the components of the vector σ. Finally $K_{\mathrm{sep}}[\sigma]$ stands for the maximal Galois extension of K in $K_{\mathrm{sep}}(\sigma)$. "For almost all" is always meant in the sense of Haar measure on the compact topological group G_K^e.

Theorem B. *Let K be a finitely generated infinite field. Let S be a finite set of local primes of K. Let A/K be a non-zero abelian variety. Then*

$$\mathrm{rank}(A(K_{\mathrm{tot},S} \cap K_{\mathrm{sep}}[\sigma])) = \infty$$

for almost all $\sigma \in G_K^e$.

Geyer and Jarden [4] had shown this by a different method with $K_{\mathrm{sep}}[\sigma]$ instead of $K_{\mathrm{tot},S} \cap K_{\mathrm{sep}}[\sigma]$. Note that in Theorem B there is no restriction on the characteristic of K. Larsen [8] conjectures that $\mathrm{rank}(A(K_{\mathrm{sep}}(\sigma))) = \infty$ for *every* $\sigma \in G_K^e$ and every $e \geq 1$. This conjecture of Larsen is known to be true for $e = 1$ and $\mathrm{char}(K) \neq 2$.

There is also a connection between our conjecture and the following classical

Question. **(Frey and Jarden** [3]**)** Does every non-zero abelian variety $A/\mathbb{Q}$ acquire infinite rank over the maximal abelian extension $\mathbb{Q}_{ab}$ of $\mathbb{Q}$?

It is one of the major questions in field arithmetic whether $\mathbb{Q}_{ab}$ is ample or not. This question is completely open to the speaker's knowledge. The importance of this question can be seen from the following fact: An affirmative answer would imply the Shafarevich conjecture, i.e. that the absolute Galois group of $\mathbb{Q}_{ab}$ is a free profinite group.

Theorem A implies: If $\mathbb{Q}_{ab}$ should be ample, then the answer to the above question of Frey and Jarden is "yes". We briefly report on a related *conditional* result [9] of the speaker that points in the direction that the answer to the question of Frey and Jarden might in fact be "yes" and that Larsen's conjecture might in fact be true.

Theorem C. *Let A be a non-zero abelian variety over a number field K. Assume that either* $\dim(A)$ *is odd and K has a real place or that the conductor ideal of A is not a square.* Assume that the parity conjecture (a subconjecture of the Birch and Swinnerton-Dyer conjecture) holds true for every quadratic twist of A. *Let Ω/K be the maximal abelian extension of exponent* 2*. Let $W(A)$ be the root number of A/K.*

a) *Then* $\mathrm{rank}(A(\Omega)) = \infty$.
b) *If $W(A) = -1$, then* $\mathrm{rank}(A(\Omega \cap K(\sigma))) = \infty$ *for* every $\sigma \in G_K^e$ *and every* $e \geq 1$.
c) *If $W(A) = +1$, then there is an element $\eta \in G_K$ such that* $\mathrm{rank}(A(\Omega \cap K(\sigma))) = \infty$ *for* every $\sigma \in G_K^e$ *which satisfies $\eta \in \langle \sigma \rangle$.*

Finally we mention that we can think of Theorem A as an interesting sufficient condition for non-ampleness. In fact, if a field F of characteristic zero admits an elliptic curve E/F of finite rank, then F is non-ample[1] (even if $E(F)$ is an infinite set). This is useful if one wants to prove non-ampleness (which is a strong finiteness property) for certain infinite algebraic extensions of $\mathbb{Q}$, because Mordell-Weil groups of abelian varieties seem to be much better understood then rational points on arbitrary varieties, and finiteness theorems on abelian varieties usually

[1] A weaker sufficient condition for non-ampleness follows from [5, Lemma 1.23]

give finite generation (or finite rank) of the Mordell-Weil group rather than its finiteness as a set.

For example, consider a number field K, a prime number p and an elliptic curve E/K with good ordinary reduction in the primes above p. A deep theorem of Mazur in Iwasawa theory[2] implies: If $E(K)$ is finite and the Tate-Shafarevich group of E/K is finite, then $E(F)$ is of finite rank for every $\mathbb{Z}_p$-extension F/K. Thus, by Theorem A, every $\mathbb{Z}_p$-extension of K is non-ample, provided such an elliptic curve exists over K. It is an open problem, however, whether every number field K admits an elliptic curve E/K with $\mathrm{rank}(E(K)) = 0$.

One can use Theorem A to see that very deep theorems of Rohrlich and Kato in Iwasawa theory imply the following statement: For every finite set S of primes, the maximal abelian extension of $\mathbb{Q}$ unramified outside S is non-ample.

References

[1] Gerd Faltings. The general case of S. Lang's conjecture. In *Barsotti symposium in algebraic geometry*, Perspectives in Mathematics, vol. 15, pages 175–182. Academic Press, 1994.

[2] Arno Fehm and Sebastian Petersen. On the rank of abelian varieties over ample fields. To appear in *International Journal of Number Theory*

[3] Gerhard Frey and Moshe Jarden. Approximation theory and the rank of abelian varieties over large algebraic fields. *Proceedings of the London Mathematical Society*, 28:112–128, 1974.

[4] Wulf-Dieter Geyer and Moshe Jarden. The rank of abelian varieties over large algebraic fields. *Archiv der Mathematik*, 86(3):211–216, 2006.

[5] Ralph Greenberg. Introduction to Iwasawa theory for elliptic curves. *IAS Park City Mathematics Series*, 9: 407–464, 2001.

[6] Ehud Hrushovski. The Mordell-Lang conjecture for function fields. *Journal of the AMS*, 9(3):667–690, 1996.

[7] Jochen Koenigsmann. Defining transcendentals in function fields. *Journal of Symbolic Logic*, 67(3):947–956, 2002.

[8] Michael Larsen. Rank of elliptic curves over almost separably closed fields. *Bulletin of the London Mathematical Society*, 35(6):817–820, 2003.

[9] Sebastian Petersen. Root numbers and the rank of abelian varieties. Paper submitted

Principe local global pour les espaces homogènes sur les corps de fonctions de courbes p-adiques

Jean-Louis Colliot-Thélène

J'ai exposé une partie de l'article [1], écrit en collaboration avec R. Parimala et V. Suresh.

Soit A un anneau de valuation discrète de rang 1, complet, de corps des fractions K et de corps résiduel k. Soit F un corps de fonctions d'une variable sur K. A toute valuation discrète v de rang 1 sur F, non nécessairement triviale sur K,

[2] Thanks to Mirela Ciperiani for a clarifying discussion on this issue!

associons le complété F_v de F. Soit Y une F-variété qui est un espace homogène d'un F-groupe linéaire connexe G .

Question (ouverte) : si la F-variété Y a des points dans tous les F_v, a -t-elle un point dans F ?

On montre qu'il en est ainsi dans les deux cas suivants :

(1) La variété Y est une quadrique lisse de dimension au moins 1, et la caractéristique de k n'est pas 2.

(2) Le F-groupe G est extension de A à F d'un groupe réductif (connexe) sur A, la F-variété sous-jacente à $G \times_A F$ est F-rationnelle, et Y est un espace principal homogène de G.

De récents théorèmes de recollement de Harbater, Hartmann et Krashen ([2, 3]) jouent un rôle fondamental dans les démonstrations. L'hypothèse de F-rationalité de la variété sous-jacente au groupe connexe G_F est essentielle dans leurs démonstrations, mais on ne sait pas si elle est nécessaire pour leurs énoncés.

Voici un corollaire de l'énoncé (2) :

(3) Le groupe de Brauer de F s'injecte dans le produit des groupes de Brauer des complétés F_v.

Supposons maintenant que le corps k est fini, c'est-à-dire que le corps K est un corps p-adique. Dans ce cas, l'énoncé (3) est essentiellement équivalent à des théorèmes de Lichtenbaum (et Tate) et de Grothendieck. L'énoncé (1) quant à lui a alors pour conséquence le résultat suivant.

(4) Pour K p-adique avec $p \neq 2$, toute forme quadratique sur F en au moins 9 variables a un zéro.

On reconnaît là un théorème de Parimala et Suresh [4], dont une démonstration radicalement nouvelle est donnée par Harbater, Hartmann et Krashen dans [3]. Ces derniers obtiennent d'ailleurs des généralisations de l'énoncé (4) pour d'autres corps résiduels k que les corps finis.

Bibliographie

[1] J.-L. Colliot-Thélène, R. Parimala et V. Suresh, *Patching and local-global principles for homogeneous spaces over function fields of p-adic curves*, prépublication, décembre 2008.

[2] D. Harbater et J. Hartmann, *Patching over Fields*, arXiv:0710.1392v3 [math. AG] September 27, 2008, à paraître dans Israel Journal of Mathematics.

[3] D. Harbater, J. Hartmann et D. Krashen, *Applications of patching to quadratic forms and central simple algebras*, arXiv:0809.4481v1 [math.RA] September 25, 2008.

[4] R. Parimala et V. Suresh, *The u-invariant of the function fields of p-adic curves*, arXiv:0708.3128v1 [math NT] August 23, 2007.

Solvable points on genus one curves

Ambrus Pál

We say that a finite extension $L|K$ of fields is solvable if the automorphism group $\mathrm{Aut}(N|K)$ is solvable, where the extension $N|K$ is the normal closure of $L|K$. Let F be a function field of transcendence degree one defined over a finite field of characteristic p and let C be a smooth, geometrically connected, projective curve of genus 1 defined over F. We are interested in proving the following

Claim. *There is a finite solvable extension $K|F$ such that C has a K-rational point.*

By passing to a finite solvable extension of F, if it is necessary, we may reduce to the case when the following properties hold:

(1) the curve C has a F_x-rational point for every place x of F where F_x denotes the completion of F with respect to x,
(2) the order of the class $[C] \in H^1(F, \mathrm{Jac}(C))$ defined by C as a homogeneous space over $\mathrm{Jac}(C)$ has prime order l,
(3) we have $l \neq p$,
(4) the elliptic curve $E = \mathrm{Jac}(C)$ has split multiplicative reduction at every place of bad reduction,
(5) we have $j(E) \notin \overline{\mathbb{F}}_p$,
(6) the image of the absolute Galois group $\mathrm{Gal}(\overline{F}|F)$ in $\mathrm{Aut}(E[l](\overline{F}))$ is not solvable.

Under these assumptions it is natural to follow the strategy of [1] which studies a similar situation over the rational number field. Here we give a very rough sketch of the basic idea. Let us recall that the Kummer exact sequence

$$0 \to E[l] \to E \to E \to 0$$

furnishes a commutative diagram:

$$\begin{tikzcd}
H^1(F, E[l]) \arrow[r] \arrow[d] \arrow[dr, "\phi_x"] & H^1(F, E)[l] \arrow[d] \\
H^1(F_x, E[l]) \arrow[r] & H^1(F_x, E)[l]
\end{tikzcd}$$

for every place x of F. The Selmer group of E is defined as:

$$H^1_{Sel}(F, E[l]) = \bigcap_{x \in |F|} Ker(\phi_x)$$

where $|F|$ denotes the set of places of F. For every finite set $Q \subset |F|$ let $H^1_{Sel,Q}(F, E[l])$ denote the subgroup of $H^1(F, E[l])$ which we get by requiring the Selmer condition for every place $x \notin Q$. Let $K|F$ be a finite solvable Galois extension. Then the cohomological exact sequence associated to the Kummer exact sequence of E over K furnishes an injection:

$$\delta : (E(K)/lE(K))^{\mathrm{Gal}(K|F)} \to H^1(K, E[l])^{\mathrm{Gal}(K|F)}.$$

By property (6) the restriction map res: $H^1(F, E[l]) \to H^1(K, E[l])^{\mathrm{Gal}(K|F)}$ is an isomorphism, hence we have an injective map:

$$i = \mathrm{res}^{-1} \circ \delta : (E(K)/lE(K))^{\mathrm{Gal}(K|F)} \to H^1(F, E[l]).$$

Then $\mathrm{Im}(i)$ lies in $H^1_{Sel,Q}(F, E[l])$ for a finite set $Q \subset |F|$ which can be computed explicitly in terms of E and $K|F$. At first approximation the strategy of Ciperiani and Wiles is to choose $K|F$ and Q so carefully such that

(i) the finite group $H^1_{Sel,Q}(F, E[l])$ is computable,

(ii) there are elements in $(E(K)/lE(K))^{\mathrm{Gal}(K|F)}$ which generate a group which is at least as large as $H^1_{Sel,Q}(F, E[l])$.

Because there is a class in $H^1_{Sel}(F, E[l])$ which maps to $[C]$ by property (2) and $H^1_{Sel,Q}(F, E[l])$ obviously contains $H^1_{Sel}(F, E[l])$ this is sufficient to conclude the claim above. In theory it is possible to compute groups like $H^1_{Sel,Q}(F, E[l])$ because of the Grothendieck-Verdier trace formula. Part (ii) lies deeper. By assumption (5) there is a place ∞ of F where E has split multiplicative reduction. Hence there is a modular parameterisation $\pi_E : X_0(\mathfrak{n}) \to E$ where $X_0(\mathfrak{n})$ is the smooth compacification the Drinfeld modular curve classifying Drinfeld A-modules of rank 2 of generic characteristic with Hecke $\mathfrak{n}$-level structure, where $\mathfrak{n} + \infty$ is the conductor of E, and $A \subset F$ is the Dedekind domain of elements of F having a pole only at ∞. Good candidates for elements in (ii) are supplied by Kolyvagin classes associated to CM-points on E furnished by the modular parametrisation π_E. My main result is a sufficiently general Gross-Zagier formula for such CM points to carry this program out.

References

[1] M. Ciperiani and A. Wiles, *Solvable points on genus one curves*, Duke Math. **142** (2008), 381–464.

Infinite index normal subgroups of the fundamental group of a curve in characteristic p

Katherine F. Stevenson

(joint work with Amilcar Pacheco, Pavel Zalesskii)

1. Introduction

Let k be an algebraically closed field of countable rank and characteristic $p > 0$. Let C be a smooth affine k-curve. We want to understand the profinite group structure of infinite index normal subgroups N of $\pi_1(C)$. For example, under what conditions is such an N free, and when it is not free, how “far from free” is it? Since k is countable, we know that $\pi_1(C)$, and hence N, is a profinite group of countable rank. Thus N is free if and only if every finite embedding problem (FEP) has a proper solution, and one approach to measuring of how close N is to being free N is to determine which FEPs for N have a proper solution. In this summary, we discuss the main result in [2] which uses results of Melnikov to measure how close N is to being free when $\pi_1(C)/N$ has a Sylow p-subgroup which is infinitely generated. Roughly speaking, this result shows that the majority of the infinite index normal subgroup structure of $\pi_1(C)$ agrees with that of a free profinite group of countable rank. Specifically we prove the following theorem.

Theorem 1. *Let $\pi_1(C)$ be the algebraic fundamental group of a smooth connected affine curve C defined over an algebraically closed field k of characteristic $p > 0$ of countable cardinality. Let N be a normal (resp. characteristic) subgroup of $\pi_1(C)$ such that a Sylow p-subgroup M_p of the quotient group $M = \pi_1(C)/N$ is infinitely generated. Then N is isomorphic to a normal (resp. characteristic) subgroup of a free profinite group of countable rank.*

This gives an almost complete description of such subgroups if one takes into account the known structure of the normal subgroups of a free profinite group (*cf.* [3, chapter 8]). For example one deduces immediately from Theorem 1 the following result.

Corollary 1. *Every proper open subgroup of N is a free profinite group of countable rank.*

As mentioned above, proving the above theorem required finding solutions to finite embedding problems for N. A finite embedding problem $\mathcal{E} = (\alpha, \psi)$ for N consists of the following data:

(1)
$$\begin{tikzcd} & N \arrow[d, "\psi", two heads] \\ \Gamma \arrow[r, "\alpha", two heads] & G \end{tikzcd}$$

A *proper solution* is a surjection $\lambda : N \to \Gamma$ such that $\psi = \alpha \circ \lambda$. Let X be the smooth projective completion of C, and let $S = X - C$. Let $k(C)$ be the function field of C over k and let $k(C)_{ur,S}$ be the maximal Galois extension of $k(C)$ unramified outside of S. Then $Gal(k(C)_{ur,S}/k(C)) = \pi_1(C)$. The map $\psi : N \to G$ corresponds to a G Galois extension of the subfield $k(C)^N_{ur,S}$ of $k(C)_{ur,S}$ fixed by N. Since G is finite, this extension descends to a G Galois extension of a finite extension $K/k(C)$ where $K \subset L$. On the level of groups, this means that there exists an open subgroup N' of Π containing N and an embedding problem $\mathcal{E}' = (\alpha, \psi')$

(2)
$$\begin{tikzcd} & N \arrow[r, hook] \arrow[d, "\psi"', two heads] & N' \arrow[dl, "\psi'", two heads] \\ \Gamma \arrow[r, "\alpha"', two heads] & G & \end{tikzcd}$$

such that $\mathcal{E}'$ induces $\mathcal{E}$ by restriction. As N' is open in $\pi_1(C)$, we have that $N' = \pi_1(U')$ for some finite étale cover U' of C. Our technique to solve embedding problems for N is to find for each $\mathcal{E}$ a U' over C with a proper solution λ' :

$\pi_1(U') \to \Gamma$

(3)
$$\begin{tikzcd}
& N \arrow[r, hook] \arrow[dl, "\lambda'|_N"'] \arrow[d] & \pi_1(U') \arrow[dll] \arrow[dl, "\psi'"] \\
\Gamma \arrow[r, two heads, "\alpha"'] & G &
\end{tikzcd}$$

such that the following hold:

(1) $\psi'|_N = \psi$ and

(2) $\lambda'|_N$ is surjective.

Before sketching the proof Theorem 1, we give an example of an infinite index normal subgroup N of $\pi_1(C)$ where the strategy above can be used to solve all embedding problems.

Corollary 2. *The commutator subgroup of $\pi_1(C)$ is a free profinite group of countable rank.*

This result was originally proven by Kumar in [1]. In [2] we prove that it also follows as a corollary of the Theorem 1. In addition we show in [2, Example 5.9] that Theorem 1 addresses situations which are not covered in [1].

2. Main Theorem: sketch of proof

We want to show that if N be a normal subgroup of $\pi_1(C)$ such that a Sylow p-subgroup M_p of the quotient group $M = \pi_1(C)/N$ is infinitely generated, then N is isomorphic to a normal subgroup of a free profinite group of countable rank. To do so we use the descent described above and results of Melnikov to reduce the problem to one of solving finite embedding problems for covers of C in such a way that the solutions satisfy conditions (1) and (2) above.

For a profinite group F and a finite simple group S, let $M_S(F)$ be the kernel of the maximal surjection of F onto a direct product of copies of S and let $M(F)$ be the intersection of all maximal normal subgroups of F. In the case that the profinite group F is countably generated, we say that F is *homogeneous* if every finite embedding problem

(4)
$$\begin{tikzcd}
& N \arrow[d] \\
\Gamma \arrow[r, two heads, "\alpha"] & G,
\end{tikzcd}$$

for which $\ker(\alpha)$ is minimal normal and is contained in $M(\Gamma)$, has a proper solution. Continuing in the case that F is countably generated, F is free if and only if it is homogeneous and $F/M_S(F)$ is infinite for all finite simple groups S ([3, Melnikov, chapter 8]). Roughly speaking, the second condition requires that there are "a lot" of S covers for every finite simple group.

In [2], the goal is not to prove that N is free, but just to show that N is isomorphic to a normal subgroup of a free group. Melnikov's results ([3, chapter 8]) tell us that in this case it suffices to show that N is homogeneous and $N/\left(M_{\mathbb{Z}/\ell\mathbb{Z}}(N)\right)$

is infinite or trivial for all primes ℓ. To show the latter condition, we use facts about the p part and the prime to p part of the fundamental groups of affine curves in characteristic p. To show that N is homogeneous we prove the following result using patching arguments and translating properties about the Sylow p-subgroup of N into properties of covers of C.

Proposition 1. *Let k be an algebraically closed field of countable rank and let D be an affine k curve. Let $\Pi = \pi_1(D)$ and suppose that N is a normal closed subgroup of $\pi_1(D)$ such that Π/N has a Sylow p-subgroup M_p is infinitely generated. Let*

$$\mathcal{E}_D = (\mu_D\colon \pi_1(D) \to G, \alpha\colon \Gamma \to G)$$

be an FSEP for $\pi_1(D)$. Then there exists a finite Galois cover $T \to D$ with $N \leq \pi_1(T)$; an embedding problem

$$\mathcal{E}_T = (\mu_T\colon \pi_1(T) \to G, \alpha\colon \Gamma \to G)$$

inducing $\mathcal{E}_D$; and a proper solution $\lambda_T : \pi_1(T) \to \Gamma$.

It should be noted here that as $\pi_1(C)$ is projective, it follows that N is also projective. The projectivity of N is used in [2] to solve the embedding problem for T by first solving an induced finite split embedding problem (FSEP) for $\pi_1(T)$. Then, using the injectivity of the set of solutions to the induced FSEP problem to the set of solutions to the original FEP, one obtains a solution for the original FEP.

References

[1] M. Kumar, *Fundamental groups in positive characteristic*, preprint arxiv, 2006.

[2] A. Pacheco, K. Stevenson, P. Zalesskii, *Normal subgroups of the algebraic fundamental group of affine curves in positive characteristic*, Math. Annalen, **343** (2009) Issue 2, 463-486.

[3] L. Ribes, P. Zalesskii, *Profinite groups*, Springer-Verlag, 2000.

The Brauer-Manin obstruction for curves over function fields

José Felipe Voloch

(joint work with Bjorn Poonen)

Let K be a number field or a function field in one variable over a finite field. For each nontrivial valuation v of K, let K_v be the completion of K at v, equipped with the v-adic topology. Define the ring of adèles $\mathbf{A}$ as the restricted direct product $\prod_v (K_v, \mathcal{O}_v)$ of the K_v with respect to their valuation sub-rings $\mathcal{O}_v$. Then $\mathbf{A}$ is a topological ring, in which $\prod_v \mathcal{O}_v$ is open and has the product topology.

If A is an abelian variety over K, then $A(K)$ embeds diagonally into $A(\mathbf{A}) \simeq \prod_v A(K_v)$. Define the adelic topology on $A(K)$ as the topology induced from $A(\mathbf{A})$. Let $\overline{A(K)}$ be the closure of $A(K)$ in $A(\mathbf{A})$. Similarly for X, a closed K-subscheme of A. Call such an X coset-free if $X_{\overline{K}}$ does not contain a translate of a positive-dimensional subvariety of $A_{\overline{K}}$. Although the primary interest here in on curves embedded in their Jacobians, it is useful to the state the following conjecture (first stated for curves by Scharaschkin) in greater generality:

Conjecture 1. *For any closed K-subscheme X of any A, we have $\overline{X(K)} = X(\mathbf{A}) \cap \overline{A(K)}$, where $\overline{X(K)}$ is the closure of $X(K)$ in $X(\mathbf{A})$.*

If X is coset-free and, in the function field case, if $A_{\overline{K}}$ has no nonzero isotrivial quotient, then $X(K)$ is finite, by Mordell-Lang, so $\overline{X(K)} = X(K)$. Conjecture 1 has been proved under mild hypotheses in the function field case in [1], the precise result is as follows:

Theorem 1. *Suppose that K has characteristic $p > 0$, that $A_{\overline{K}}$ has no nonzero isotrivial quotient, and that $A(K^s)[p^\infty]$ is finite. Suppose that X is coset-free. Then $X(K) = X(\mathbf{A}) \cap \overline{A(K)}$.*

It is known that in the "general case" in which A is ordinary and the Kodaira-Spencer class of A/K has maximal rank, we have $A(K^s)[p^\infty] = 0$.

The intersection $X(\mathbf{A}) \cap \overline{A(K)} \subset A(\mathbf{A})$ is closely related to the Brauer-Manin set $X(\mathbf{A})^{\mathrm{Br}}$ of adelic points pairing trivially with every element of the Brauer group of X. For curves over number fields, V. Scharaschkin and A. Skorobogatov independently raised the question of whether the Brauer-Manin obstruction is the only obstruction to the Hasse principle, and proved that this is so when the Jacobian has finite Mordell-Weil group and finite Shafarevich-Tate group. The connection with the adelic intersection is stated explicitly in [2] where Conjecture 1 is stated for curves over number fields embedded in their Jacobians. This special case of Conjecture 1 will be referred to as Scharaschkin's conjecture in what follows. See also [3, 4].

The strategy of the proof of Theorem 1 is as follows. First a souped-up version of a proof of the Mordell conjecture is used to prove that there exists a finite K-subscheme Z of X such that $X(\mathbf{A}) \cap \overline{A(K)} \subseteq Z(\mathbf{A})$. This is proved locally at every place, showing that the intersection of the closure of $A(K)$ in the v-adic topology with X is contained in Z. This allows the reduction of Conjecture 1 to the zero-dimensional case, which is then treated separately.

Conjecture 1 in the zero-dimensional case has been proved in the number field case by Stoll in [4].

Under conjecture 1 one has an algorithm to verify if $X(K)$ is empty, using the so-called Mordell-Weil sieve, which coupled with a search for points provides an algorithm to decide whether $X(K)$ is empty or not.

References

[1] Poonen, Bjorn; Voloch, José Felipe, *The Brauer-Manin obstruction for subvarieties of abelian varieties over function fields*, 2007, preprint. To appear in Annals of Math. http://www.ma.utexas.edu/users/voloch/Preprints/brauer.pdf

[2] Scharaschkin, Victor, *Local-global problems and the Brauer-Manin obstruction*, 1999, Ph.D. thesis, University of Michigan.

[3] Skorobogatov, Alexei, *Torsors and rational points*, Cambridge Tracts in Mathematics, 144, Cambridge University Press, Cambridge, 2001.

[4] Stoll, Michael, *Finite descent and rational points on curves*, Algebra Number Theory 1 (2007), no. 4, 349–391.

Katz-Gabber covers with extra automorphisms

Ted Chinburg

(joint work with Frauke Bleher, Bjorn Poonen, Florian Pop and Peter Symonds)

Let k be an algebraically closed field of characteristic $p > 0$. Suppose that $\phi : G \to \mathrm{Aut}_k(k[[t]])$ is an embedding of a finite group G into the group of continuous k-automorphisms of the power series ring $k[[t]]$. Associated to ϕ there is a faithful action of G on a smooth projective curve X over k having the following properties [2, Thm. 1.4.1]. The quotient X/G is isomorphic to $\mathbb{P}^1_k$. There are two points $\{0, \infty\}$ on $X/G = \mathbb{P}^1_k$ such that the morphism $\pi : X \to X/G$ is totally ramified over ∞, at most tamely ramified over 0 and unramified off of $\{0, \infty\}$. Finally, if x is the unique point of X over ∞, there is a G-equivariant continuous isomorphism between $k[[t]]$ and the completion $\hat{O}_{X,x}$ of the local ring of x on X. The G-curve X is uniquely determined by ϕ up to G-isomorphism.

We will call $\pi : X \to X/G$ a Katz-Gabber G-cover. We will say that X has extra automorphisms if there is a finite subgroup $H \subset \mathrm{Aut}_k(X)$ which properly contains G. The following result is joint with F. Bleher and P. Symonds.

Theorem 1. *Suppose $\pi : X \to X/G$ is a Katz-Gabber G-cover, p divides the order of G and that H is a finite subgroup of $\mathrm{Aut}_k(X)$ which properly contains G. Then one of the following alternatives occurs:*

1. *$X \to X/H$ is a Katz-Gabber H-cover;*
2. *$X = \mathbb{P}^1_k$, and $G \subset H \subset \mathrm{Aut}_k(\mathbb{P}^1_k) = \mathrm{PGL}_2(k)$, with G contained in the image in $\mathrm{PGL}_2(k)$ of a Borel subgroup of $\mathrm{GL}_2(k)$;*
3. *$p = 2$ or 3, X is an elliptic curve, and after conjugation by an automorphism of X, G fixes the identity element $\underline{0}$ of the group $X(k)$. Thus G is a subgroup of $A = \mathrm{Aut}(X, \{\underline{0}\})$, and $\#A|24$. One has $G \subset H \subset \mathrm{Aut}_k(X)$, where $\mathrm{Aut}_k(X)$ is the semi-direct product of A with the normal subgroup of translations by elements of $X(k)$.*

If $p^2|\#G$ then either option (1) or (3) holds, and if (3) holds then $p = 2$ and X is the supersingular elliptic curve with j-invariant $j(X) = 0$.

The strategy of the proof is to consider the inertia group $H_x \supset G$ in H of the unique point x of X which is fixed by all of G. Let $Z \to Z/H_x$ be the Katz-Gabber H_x-cover which is associated to the action of H_x on $\hat{\mathcal{O}}_{X,x} = k[[t]]$. One can show that option (1) of the theorem occurs if $H_x = H$ and if $Z \to Z/G$ is a Katz-Gabber G-cover. For then $X \to X/G$ must be isomorphic to $Z \to Z/G$, and $G \subset H_x = H$ shows $X \to X/G$ can be embedded in the Katz-Gabber H-cover $Z \to Z/H$. One uses the Hurwitz formula for the covers $X \to X/G$, $X \to X/H_x$, $X \to X/H$, $Z \to Z/G$ and $Z \to Z/H_x$ to show that if $H_x \neq H$ or $Z \to Z/G$ is not Katz-Gabber, then options (2) or (3) must hold. The final statement concerning the case in which $p^2|\#G$ follows from the fact $\mathrm{Aut}(\mathbb{P}^1_k)$ has no elements of order p^2 and the only automorphisms of an elliptic curve X which fix the origin and have order p^2 arise from letting $p = 2$ and $j(X) = 0$.

One application of Theorem 1 concerns explicit formulas

$$\sigma(t) = \sum_{i=1}^{\infty} a_i t^i \tag{1}$$

which define continuous automorphisms σ of $k[[t]]$ of order p^n. As remarked above, if $n \geq 2$, there are no formulas of this kind for which $\sigma(t)$ is a rational function in $k(t)$. For all $n \geq 1$, Lubin [3], Green [1] and others have shown how to use formal groups and local class field theory to recursively define a_i in (1) for which the associated automorphism σ of $k[[t]]$ has order p^n. One would still like to find particularly explicit formulas for $\sigma(t)$ as a power series in t. One approach is to consider automorphisms with the following property.

Definition 1. An automorphism σ of $k[[t]]$ is *almost rational* if there is a rational function $\alpha \in k(t) \cap tk[[t]]$ for

$$X^p - X = \alpha. \tag{2}$$

is irreducible over $k(t)$ and the following is true. Let

$$\beta = -\sum_{i=0}^{\infty} \alpha^{p^i} \tag{3}$$

be the unique non-unit root in $k[[t]]$ of (2). Then $\sigma(t) = F(t, \beta)$ for some rational function $F(u, v) \in k(u, v)$ in two commuting indeterminates u and v. In this case we will say σ is almost rational with respect to β.

More colloquially, requiring that σ be almost rational amounts to asking that $\sigma(t)$ be constructible via a rational function of t and the root of just one degree p Artin-Schreier equation. When $n \geq 2$, one would expect such σ to be "simpler" than the generic case, since n successive Artin-Schreier equations of degree p are required to describe a cyclic extension of degree p^n. The expression for β in (3) leads to an explicit formula for $\sigma(t) = F(t, \beta)$, as in the following example which was found with Peter Symonds.

Example 1. Let $p = 2$ and $n = 2$. There is an automorphism σ_0 of $k[[t]]$ of order $p^n = 4$ defined by

$$\begin{aligned} \sigma_0(t) &= t + t^2 + \sum_{j=0}^{\infty} \sum_{\ell=0}^{2^j - 1} t^{6 \cdot 2^j + 2\ell} \\ &= t + t^2 + (t^6) + (t^{12} + t^{14}) + (t^{24} + t^{26} + t^{28} + t^{30}) + \cdots \end{aligned}$$

This σ_0 is almost rational because

$$\sigma_0(t) = \frac{t}{1+t} + \frac{\beta_0}{(1+t)^2} \quad \text{when} \quad \beta_0 = -\sum_{i=0}^{\infty} (t^3 + t^4)^{2^i}$$

is a root of the Artin-Schreier equation

$$X^2 - X = t^3 + t^4 = \alpha$$

During the conference, conversations with B. Poonen and F. Pop led to improvements of a partial classification of almost rational automorphisms of p-power order. This eventualy led to the following result, which is joint with Bleher, Poonen, Pop and Symonds.

Theorem 2. *Suppose $n \geq 2$ and that σ is an almost rational automorphism of $k[[t]]$ of order p^n with respect to β. Suppose further that for all integers j, σ^j is also almost rational with respect to the same β. Then $p^n = 4$ and σ is conjugate in $\mathrm{Aut}(k[[t]])$ to the automorphism σ_0 described in Example 1.*

The first step in the proof is to observe that since σ^j is almost rational with respect to β for all j, and $\sigma(t)$ does not lie in $k(t)$, the field

$$k(t,\beta) = k(t,\sigma(t)) = k(t,\sigma(t),\ldots,\sigma^{p^n-1}(t))$$

is an Artin-Schreier extension of $k(t)$ of degree p having an faithful action of the cyclic group G of order p^n generated by σ Let X be a smooth projective curve of k having function field $k(t,\beta)$. Let $\Gamma = \mathrm{Gal}(k(t,\beta)/k(t))$, so that Γ is cyclic of order p. Then Γ acts on X, and $X/\Gamma = Y$ is isomorphic to $\mathbb{P}^1_k$ since $k(X)^\Gamma = k(t,\beta)^\Gamma = k(t)$. Let $x \in X$ be the closed point of X determined by the embedding $k(t,\beta) \subset k[[t]]$ Then x is fixed by G since $\sigma^j(t) \in k[[t]]$ for all j. The point y of $Y = \mathbb{P}^1_k$ under x is the one determined by $t = 0$, and y splits in X since $\hat{O}_{X,x} = k[[t]] = \hat{O}_{Y,y}$. We thus have a diagram of curves

$$\begin{tikzcd}
& X \arrow[dl, "\pi"'] \arrow[dr, "\gamma"] & \\
X/G & & Y = X/\Gamma = \mathbb{P}^1_k
\end{tikzcd}$$

with G (resp. Γ) fixing (resp. not fixing) $x \in X$. If G normalizes Γ in $\mathrm{Aut}_k(X)$, we could get a faithful action of $G \cong \mathbb{Z}/p^n$ on $Y = \mathbb{P}^1_k$, which does not exist since $n > 1$. So G does not normalize Γ, and by considering a conjugate of Γ by a generator of G we arrive at another map $\gamma' : X \to \mathbb{P}^1_k$. The product map $\gamma \times \gamma' : X \to \mathbb{P}^1_k \times \mathbb{P}^1_k$ has image X' a (possibly singular) curve of bidegree (p,p) which must be birational to X. Using the adjunction formula on $\mathbb{P}^1_k \times \mathbb{P}^1_k$ now leads to a bound on the genus of X in terms of p. This bound together with the Hurwitz formula for $X \to X/G$ shows that $X \to X/G$ must in fact be a Katz-Gabber G-cover. This cover has extra automorphisms arising from the action of Γ. The classification of such covers in Theorem 1 leads to Theorem 2.

As a final comment, it remains open to classify all almost rational σ of order $p^n > p$ when we make no further condition on σ^j for $j \neq 1$.

References

[1] B. Green, *Realizing deformations of curves using Lubin-Tate formal groups*, Israel J. Math. **139** (2004), 139–148.

[2] N. Katz, Local-to-global extensions of representations of fundamental groups. Ann. Inst. Fourier, Grenoble **36** (1986), 69-106.

[3] J. Lubin, *Torsion elements in the Nottingham group*, preprint, Dec. 2008.

The descending q-central sequence of an absolute Galois group

Ido Efrat

The talk was based on a joint work with Ján Mináč and Sunil Chebolu [5], [3]. We obtain new restrictions on the group-theoretic structure of the absolute Galois group of a field related to its descending q-central sequence and its mod-q cohomology.

Specifically, let p be a prime number and let $q = p^s$. The descending q-central sequence $G^{(i)}$, $i = 1, 2, 3, \ldots$ of a profinite group G is defined inductively by $G^{(1)} = G$, $G^{(i+1)} = (G^{(i)})^q[G^{(i)}, G]$. Let $H^*(G) = H^*(G, \mathbb{Z}/q)$ be the profinite cohomology (graded) ring relative to the trivial action of G on $\mathbb{Z}/q$ and with the cup product. Also let $H^*(G)_{\mathrm{dec}}$ be the decomposable part of $H^*(G)$, i.e., its subring generated by $H^1(G)$.

Now consider a field F which contains a root of unity of order q. Let $G_F = \mathrm{Gal}(F_{\mathrm{sep}}/F)$ be its absolute Galois group and let $F^{(i)}$ be the fixed field of $G_F^{(i)}$ in F_{sep}. Thus we have a tower of Galois extensions $F = F^{(1)} \subseteq F^{(2)} \subseteq F^{(3)} \subseteq \cdots \subseteq F_{\mathrm{sep}}$ of F.

Theorem A. The Galois cohomology ring $H^*(G_F)$ is determined by $\mathrm{Gal}(F^{(3)}/F)$. Namely, $\mathrm{inf}\colon H^*(\mathrm{Gal}(F^{(3)}/F))_{\mathrm{dec}} \to H^*(G_F)$ is an isomorphism.

One has the following partial converse of Theorem A:

Theorem B. $\mathrm{Gal}(F^{(3)}/F)$ is determined by $H^r(G_F)$, $r = 1, 2$, the cup product $\cup\colon H^1(G_F) \times H^1(G_F) \to H^2(G_F)$, and the Bockstein map $\beta\colon H^1(G_F) \to H^2(G_F)$.

Recall that β is the connecting homomorphism corresponding to the short exact sequence of trivial G_F-modules

$$0 \to \mathbb{Z}/q \to \mathbb{Z}/q^2 \to \mathbb{Z}/q \to 0.$$

See [1]*Th. 3.14 for the case $q = 2$.

The arithmetical significance of Theorem A lies in the fact that $H^*(G_F)$ is known to encode considerable arithmetical information about the field F. Therefore this arithmetical information is already encoded in the Galois group $\mathrm{Gal}(F^{(3)}/F)$. For instance, when $q = 2$, $H^*(G_F)$ (together with the Kummer element $(-1)_F$ of -1) explicitly determine the ordered structure of F and its Witt ring. In fact, in [6] and [7] it was shown that this "real arithmetical" structure can be read off from the structure of $\mathrm{Gal}(F^{(3)}/F)$. Likewise, for $q = p$ an arbitrary prime, one can recover the main valuation-theoretic structure of F from $H^r(G_F)$, $r = 1, 2$, and $(-1)_F$ (see [4]*Ch. 26). In this respect, Theorem A is also related to works by Bogomolov, Tschinkel [2] and Pop, which show that for certain classes of fields F, the field is determined by the structure of the Galois group $G_F/[G_F, [G_F, G_F]]$ only.

Next we note that the field $F^{(2)}$ is the compositum of all $\mathbb{Z}/q$-extensions of F. We have the following analogous description of $F^{(3)}$ when $q = p$. Here M_{p^3} denotes the unique non-abelian group of order p^3 and exponent p^2.

Theorem C. When $q = p \neq 2$ the field $F^{(3)}$ is the compositum of all Galois $\mathbb{Z}/p^2\mathbb{Z}$- and M_{p^3}-extensions of F.

Equivalently, $G_F^{(3)}$ is the intersection of all open normal subgroups N of G_F such that G_F/N is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or to M_{p^3}.

In the complementary case $q = 2$, it was earlier shown by Villegas [8] (implicitly) and by Mináč and Spira [7] that $F^{(3)}$ is the compositum of all Galois $\mathbb{Z}/2\mathbb{Z}$-, $\mathbb{Z}/4\mathbb{Z}$-, and $D_4 = M_8$-extensions of F.

The proof of Theorem A is based on the bijectivity of the norm residue homomorphism $K_*^M(F)/qK_*^M(F) \xrightarrow{\sim} H^*(G_F)$ (Voevodsky, Rost, Weibel). This isomorphism implies that $H^*(G_F)$ is decomposable, as well as quadratic (i.e., relations originate in the degree 2 component). Theorem B (resp., C) is based on the surjectivity (resp., injectivity) of the norm residue homomorphism in degree 2 (the Merkurjev–Suslin theorem).

We showed that the conditions imposed in Theorems A and C on $G = G_F$ are of a genuine Galois-theoretic nature. That is, there are examples of profinite groups G (even torsion-free ones) for which these conditions fail. In particular, these examples are not absolute Galois groups of fields. We gave the following torsion-free examples (with $q = p$):

(i) $G = S/[S, [S, S]]$, where S is a free pro-p group on $2 \leq n < \infty$ generators;

(ii) $G = \mathbb{Z}_p^{p^k} \rtimes \mathbb{Z}_p$, where a generator of $\mathbb{Z}_p$ acts on $\mathbb{Z}_p^{p^k}$ by permuting the coordinates cyclically (after projection to $\mathbb{Z}/p^k$).

(iii) $G = S/R[S, [S, S]]$, where S is a free pro-p group on $n > p^2$ generators $\sigma_1, \ldots, \sigma_n$, and R is the normal closed subgroup of S generated by all relations $[\sigma_1, \sigma_2][\sigma_i, \sigma_j]^{-1}$, $i < j$.

We showed that in examples (i) and (ii) the assertion of Theorem A fails, whereas for example (iii) the assertion of Theorem C fails.

References

[1] Adem, Alejandro, Dikran B. Karagueuzian, and Ján Mináč , *On the cohomology of Galois groups determined by Witt rings*, Adv. Math. 148 (1999), 105–160.

[2] Bogomolov, F. A. and Yuri Tschinkel, *Commuting elements in Galois groups of function fields.* In "Motives, Polylogarithms and Hodge theory", F. Bogomolov, L. Katzarkov, eds., International Press, 2002, 75–120.

[3] S.K. Chebolu, Ido Efrat, and Ján Mináč, *Quotients of absolute Galois groups and cohomology*, in preparation.

[4] Efrat, Ido, *Valuations, Orderings, and Milnor K-theory*, Mathematical Surveys and Monographs 124. American Mathematical Society, Providence, RI, 2006.

[5] Efrat, Ido and Ján Mináč, *On the descending central sequence of absolute Galois groups*, 2007, http://arxiv.org/abs/0809.2166.

[6] Mináč, Ján and Michel Spira, *Formally real fields, Pythagorean fields, C-fields and W-groups*, Math. Z. 205 (1990), 519–530.

[7] Mináč, Ján and Michel Spira, *Witt rings and Galois groups*, Ann. of Math. 144 (1996), no. 2, 35–60.

[8] Villegas, Fernando Rodriguez, *Relations between quadratic forms and certain Galois extensions*, Ohio State University, 1988, http://www.math.utexas.edu/users/villegas/osu.pdf,

Galois analogue of functional equations of polylogarithms

Hiroaki Nakamura
(joint work with Zdzisław Wojtkowiak)

Complex polylogarithm functions $Li_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}$ $(k = 1, 2, ...)$, analytically continued to multi-valued functions on $\mathbb{C} \setminus \{0, 1\}$, have been known to satisfy a number of functional equations (as well as special value formulas) as found in Lewin's book [1]. In this talk, we introduced their ℓ-adic analogues as functions

$$\tilde{\chi}_k^z : G_K = Gal(\bar{K}/K) \to \mathbb{Z}_\ell \quad (k = 1, 2, ...),$$

where K is a subfield of $\mathbb{C}$ and z is a point of $\mathbf{P}^1(K) - \{0, 1, \infty\}$ (or a K-rational tangential basepoint) with given a specific path from $\overrightarrow{01}$ to z, defined by Kummer properties along towers of certain arithmetic sequences. These functions — the ℓ-adic polylogarithmic characters introduced in [2] — generalize what are called the Soulé characters corresponding to the special case $z = \overrightarrow{10}$. We also discussed equivalence of tests by Zagier [6] and Wojtkowiak [4,5] for a functional equation to arise from a finite family of morphisms of algebraic varieties $f_i : X \to \mathbf{P}^1 - \{0, 1, \infty\}$ and integers $n_i \in \mathbb{Z}$ $(i = 1, ..., m)$. Finally, supposing Wojtkowiak's condition, we showed how a functional equation over G_K with explicit lower degree terms can be derived from the images of an "ℓ-adic associator" by f_i's which have ℓ-adic polylogarithms in their Lie expansion coefficients.

References

[1] L.Lewin, *Polylogarithms and associated functions*, North Holland, 1981.

[2] H.Nakamura, Z.Wojtkowiak, *On explicit formulae for l-adic polylogarithms*, Proc. Symp. Pure Math. (AMS) **70** (2002) 285–294.

[3] H.Nakamura, Z.Wojtkowiak, *Tensor and homotopy criterions for functional equations of ℓ-adic and classical iterated integrals*, Preprint, January 2009.

[4] Z.Wojtkowiak, *The basic structure of polylogarithmic functional equations*, in "Structural Properties of Polylogarithms", L.Lewin (ed.), Mathematical Surveys and Monographs (AMS), **37** (1991), 205–231.

[5] Z.Wojtkowiak, *On ℓ-adic iterated integrals, II – Functional equations and ℓ-adic polylogarithms*, Nagoya Math. J., **177** (2005), 117–153.

[6] D.Zagier, *Polylogarithms, Dedekind zeta functions and the algebraic K-theory of Fields*, in "Arithmetic Algebraic Geometry", G. van der Geer et.al.(eds.), Progress in Math., Birkhäuser, **89**, (1991) 391–430.

Grothendieck's Section Conjecture and zero-cycles on varieties

Tamás Szamuely
(joint work with David Harari)

This report can be regarded as a follow-up to the one by Jakob Stix.

We are concerned with Grothendieck's Section Conjecture (stated in a 1983 letter to Faltings [2]). Let X be a smooth proper geometrically integral curve of genus ≥ 2 defined over a number field k. Consider the exact sequence of profinite groups

$$1 \to \pi_1(\overline{X}, \bar{x}) \to \pi_1(X, \bar{x}) \to \mathrm{Gal}(\overline{k}|k) \to 1, \tag{1}$$

where $\pi_1(X, \bar{x})$ denotes the étale fundamental group of X, and $\overline{X}$ stands for the base change $X \times_k \overline{k}$.

Each k-rational point Spec $k \to X$ determines a section of the structure map $X \to$ Spec k. As the étale fundamental group is functorial for morphisms of pointed schemes, taking the induced map on fundamental groups defines a map

$$X(k) \to \{\text{continuous sections of } \pi_1(X, \bar{x}) \to \mathrm{Gal}(\overline{k}|k)\}/\sim,$$

where two sections are equivalent under the relation $\sim$ if they are conjugate under the action of $\pi_1(\overline{X}, \bar{x})$.

The Section Conjecture predicts that the above map is a bijection. As already explained in the lecture by Stix, an argument going back to Tamagawa which uses the theorem of Faltings (see [4], Lemma 1.7) implies that the conjecture is equivalent to the following a priori weaker statement:

Conjecture 1. *A smooth projective curve X of genus at least 2 over a number field k has a k-rational point if and only if the map $\pi_1(X, \bar{x}) \to \mathrm{Gal}(\overline{k}|k)$ has a continuous section.*

Until the recent work of Stix [6] there seems to have been no examples where the statement of Conjecture 1 holds in a nonobvious way, i.e. where $X(k) = \emptyset$ and $\pi_1(X, \bar{x}) \to \mathrm{Gal}(\overline{k}|k)$ has no continuous section. This may be because, as we shall see below, verifying that sections do *not* exist is by no means straightforward. In the examples of Stix there is a local obstruction to the existence of a section. With David Harari we have produced examples where X has points everywhere locally, so there is no such local obstruction. More precisely, we have shown in [3]:

Theorem 1. *Let X be a smooth projective curve over $\mathbf{Q}$ whose Jacobian is isogenous over $\mathbf{Q}$ to a product of elliptic curves each of which has finite Tate-Shafarevich group and infinitely many $\mathbf{Q}$-points. Assume moreover that X has points everywhere locally but no $\mathbf{Q}$-rational divisor class of degree 1. Then (1) has sections everywhere locally but not globally.*

In an appendix to our paper Victor Flynn gives numerical examples of curves of genus 2 satisying the assumptions of our theorem. In particular, he shows that a smooth proper model of the affine curve of equation $y^2 = 2(x^2+7)(x^2+14)(x^2-11)$ X has points everywhere locally but no $\mathbf{Q}$-rational divisor class of degree 1. Its Jacobian is isogenous over $\mathbf{Q}$ to the product of two elliptic curves of analytic rank 1. By work of Kolyvagin [5] they therefore have a rank 1 Mordell–Weil group and finite Tate-Shafarevich group.

Theorem 1 results from a more general investigation of splittings of the abelianized version of exact sequence (1). By the latter we mean the short exact sequence

$$1 \to \pi_1^{\mathrm{ab}}(\overline{X}) \to \Pi^{\mathrm{ab}}(X) \to \mathrm{Gal}(\overline{k}|k) \to 1 \tag{2}$$

obtained from (1) by pushout via the natural surjection $\pi_1(\overline{X}, \bar{x}) \to \pi_1^{\mathrm{ab}}(\overline{X})$, where $\pi_1^{\mathrm{ab}}(\overline{X})$ is the maximal abelian profinite quotient of $\pi_1(\overline{X}, \bar{x})$. Of course, if (1) has a continuous section, then so does (2).

To state our main general result concerning this exact sequence, denote by J the Jacobian of X. It is an abelian variety over k whose k-points correspond to the degree zero part in the Picard group $\operatorname{Pic} X$. The degree 1 part corresponds to a k-torsor over J that we denote by J^1.

Theorem 2. *Let X be a smooth projective geometrically integral curve over an arbitrary perfect field k. The map $\Pi^{\mathrm{ab}} \to \mathrm{Gal}(\overline{k}|k)$ has a continuous section if and only if the class of J^1 lies in the maximal divisible subgroup of the group $H^1(k, J)$ of isomorphism classes of torsors under J.*

Recall that the maximal divisible subgroup of an abelian group does not necessarily coincide with the subgroup of divisible elements.

Remark. Theorem 2 generalizes to arbitrary dimension: in the general case the role of J is played by the Albanese variety Alb_X of X, and one has to make yet another pushout of exact sequence (2), by the morphism $\pi_1^{\mathrm{ab}}(\overline{X}) \to T(\mathrm{Alb}_X(\overline{k}))$, where T denotes the full Tate module. For varieties with torsion-free Néron-Severi group (e.g. curves or abelian varieties) this map is an isomorphism.

Assume now again that k is a number field, and assume moreover that X has points everywhere locally. The class of the torsor J^1 then lies in the Tate-Shafarevich group $\text{Ш}(J) \subset H^1(k, J)$. We therefore run into the following well-known question:

Question. *Can a nonzero element of* $\text{Ш}(J)$ *lie in the maximal divisible group of* $H^1(k, J)$*?*

The answer to this question is not known at present. To our knowledge, the only person to study it was M. I. Bashmakov more than 30 years ago. He did not decide the issue either way, but an adaptation of his arguments shows that under the assumptions of Theorem 1 the answer is no. This is how the theorem is proven.

References

[1] M. I. Bashmakov, Cohomology of Abelian varieties over a number field (Russian), *Uspehi Mat. Nauk* 27 (1972), 25–66.

[2] A. Grothendieck, Brief an G. Faltings, reprinted in P. Lochak, L. Schneps (eds.) *Geometric Galois actions I*, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge University Press, Cambridge, 1997, pp. 49–58; English translation *ibid.*, pp. 285–293.

[3] D. Harari, T. Szamuely, Galois sections for abelianized fundamental groups, *Math. Ann.*, 2009, DOI: 10.1007/s00208-008-0327-z.

[4] J. Koenigsmann, On the section conjecture in anabelian geometry, *J. reine angew. Math.* 588 (2005), 221–235.

[5] V. A. Kolyvagin, Euler Systems. in P. Cartier et al. (eds.) *The Grothendieck Festschrift*, volume II, Progress in Mathematics, vol. 87, Birkhäuser, Boston, 1990, 435–483.

[6] J. Stix, On the period-index problem in light of the section conjecture, preprint `arXiv:0802.4125`.

A Chebotarev Density Theorem for Function Fields

Armin Holschbach

Let $f : Y \to X$ be a finite branched Galois cover of normal varieties over a field k, and let $G = \mathrm{Gal}(X/Y)$ denote its Galois group.

The Serre-Chebotarev density theorem considers the case where k is a finite field. It defines a Dirichlet density on the set of closed points of X and describes the asymptotic decomposition behavior of these points in the cover $Y \to X$ ([4, Theorem 7]).

Instead of looking at closed points, we will consider points of codimension one on X and describe "how many" of those have a given decomposition behavior:

To any codimension 1 point $x \in X$ (or the corresponding Weil prime divisor), we associate a *decomposition type* by taking the conjugacy class of the decomposition group of any point y on Y mapping to x. This notion does not depend on the choice of the point y. If the decomposition type of x is trivial, we say x *splits completely* in Y. In the following we restrict ourselves to Weil prime divisors that stay prime after finite base extensions, i.e. geometrically integral divisors.

1. Density Results for Divisors

Assume k is perfect and X, Y are projective and geometrically integral over k. Moreover, assume $d := \dim X \geq 2$ and $\operatorname{char} k = 0$ if $d > 3$.

We fix a very ample divisor D on X and consider the linear systems $|mD|$ for $m \in \mathbf{N}$. Every such $|mD|$ can be considered as the set of closed points of a projective space, and we will indeed identify $|mD|$ with the corresponding projective space over k.

Theorem 1. *For any $m \in \mathbf{N}$, the geometrically integral divisors in the linear system $|mD|$ form an open subvariety $\mathcal{P}_{mD}$. For any conjugacy class $\mathcal{C}$ of a subgroup H of G, there is a locally closed subvariety $\mathcal{D}^{\mathcal{C}}_{mD}$ consisting of those divisors in $\mathcal{P}_{mD}$ of decomposition type $\mathcal{C}$, and*

$$\limsup_{m\to\infty} \frac{\dim \mathcal{D}^{\mathcal{C}}_{mD}}{\dim \mathcal{P}_{mD}} = \frac{1}{[G:H]^{d-1}}.$$

Moreover, this limit inferior becomes a limit if D (or any linearly equivalent prime divisor) splits completely in Y.

In particular, for every subgroup H of G there are infinitely many Weil prime divisors on Y with decomposition group H. Furthermore, for fixed X, one can deduce that a finite branched Galois cover $f : Y \to X$ is completely described by the set of Weil prime divisors that split completely.

One side note: The more precise description of $\mathcal{P}_{mD}$ is that for *every* field extension $k'|k$, $\mathcal{P}_{mD}(k')$ consists exactly of those effective divisors on $X' := X \times_{\operatorname{Spec} k} \operatorname{Spec} k'$ which are linearly equivalent to the base change D' of D to X'. Similarly, one describes $\mathcal{D}^{\mathcal{C}}_{mD}$. This way, the scheme structures and hence dimensions of $\mathcal{P}_{mD}$ and $\mathcal{D}^{\mathcal{C}}_{mD}$ are indeed uniquely defined.

2. Special Case: $k = \mathbf{F}_q$

In the case where k is a finite field, the sets $\mathcal{P}_{mD}(k)$, $\mathcal{D}_{mD}(k)$ are finite, and we can actually *count* divisors:

Theorem 2. *Under the assumptions from above, let k be a finite field. Then*

$$\limsup_{m\to\infty} \frac{\log \#\mathcal{D}^{\mathcal{C}}_{mD}(k)}{\log \#\mathcal{P}_{mD}(k)} = \frac{1}{[G:H]^{d-1}}.$$

Both theorems are proven in a similar manner using considerations on the behavior of volumes of divisors under pullback and push-forward. The only major difference of the two proofs is that the first one uses the classical Bertini theorem whereas the second one use Poonen's Bertini theorem over finite fields ([2]).

3. Connection with a Result of F.K. Schmidt

The above-mentioned statements can also be reinterpreted as giving effective versions of (a special case of) a result of F.K. Schmidt ([3]):

Theorem 3 (F.K. Schmidt)**.** *Suppose Ω is a Hilbertian field, and $K|\Omega$ is a separably generated function field in one variable. Let $L|K$ be a finite Galois extension. Then for any subgroup H of $\mathrm{Gal}(L|K)$, there are infinitely many valuations on L which are constant on Ω and have decomposition group H.*

An important case of Hilbertian fields are function fields. For these fields, our theorem can be used to describe more explicitly "how often" a particular subgroup H actually occurs as a decomposition group, at least under some mild additional assumptions:

Assume Ω itself is a function field in one variable over a perfect field k, i.e. L and K are both function fields in two variables over k; and assume k is relatively algebraically closed in L. Then we can choose a normal projective model X/k for $K|k$ and take its normalization Y in L to get a finite branched Galois cover $f : Y \to X$ of two-dimensional, normal, geometrically integral projective k-varieties. F.K. Schmidt's theorem follows from ours by identifying Weil prime divisors on Y with the corresponding valuations.

References

[1] A. Holschbach, *A Chebotarev-like Density Theorem in Algebraic Geometry*, Ph.D. Thesis, University of Pennsylvania (2008).

[2] B. Poonen, *Bertini Theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127.

[3] F.K. Schmidt, *Über die Kennzeichnung algebraischer Funktionenkörper durch ihren Regularitätsbereich*, J. Reine Angew. Math. **171** (1934), 162–169.

[4] J.-P. Serre, *Zeta and L functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), 82–92. Harper & Row, New York, 1965.

Obstructions to rational points

Bjorn Poonen

1. Introduction

Let k be a global field. For each place v, let k_v be the completion of k at v. Let $\mathbb{A}$ be the adele ring of k. Let X be a nice k-variety: by nice, we mean smooth, projective, and geometrically integral. We want to decide whether $X(k)$ is empty. Since $X(k)$ embeds diagonally in $X(\mathbb{A})$, if $X(\mathbb{A})$ is empty, then $X(k)$ is empty.

But the converse (known as the local-global principle) need not hold. Using cohomology, one can define various subsets of $X(\mathbb{A})$ in which the k-rational points are constrained to lie. Our goal is to describe the inclusion relations between these subsets and to determine whether their nonemptiness implies the nonemptiness of $X(k)$. One has, for example, $X(\mathbb{A})^{\mathrm{Br}}$ defined using elements of the Brauer group $\operatorname{Br} X$, and the descent subset $X(\mathbb{A})^{\mathrm{descent}}$ defined using torsors of affine algebraic groups; we describe these in more detail below. These fit into a chain

$$X(k) \subseteq X(\mathbb{A})^{\mathrm{descent}} \subseteq X(\mathbb{A})^{\mathrm{Br}} \subseteq X(\mathbb{A}).$$

The first examples where $X(\mathbb{A}) \neq \emptyset$ and $X(k) = \emptyset$ were given in the 1940s [6],[9]. In 1999, Skorobogatov [10] constructed a variety for which one could prove $X(\mathbb{A})^{\mathrm{Br}} \neq \emptyset$ and $X(k) = \emptyset$. Today we explain our 2008 work [8], which, together with subsequent work of Demarche [3], yields an example with $X(\mathbb{A})^{\mathrm{descent}} \neq \emptyset$ and $X(k) = \emptyset$.

2. Brauer-Manin obstruction

The Brauer-Manin obstruction was discovered by Manin [7]. Let $\operatorname{Br} X$ be the cohomological Brauer group $H^2_{\mathrm{et}}(X, \mathbb{G}_m)$. There is an evaluation pairing

$$\operatorname{Br} X \times X(\mathbb{A}) \to \mathbb{Q}/\mathbb{Z},$$

and $X(\mathbb{A})^{\mathrm{Br}}$ is defined as the set of elements of $X(\mathbb{A})$ that pair with every element of $\operatorname{Br} X$ to give 0. The reciprocity law for $\operatorname{Br} k$ implies $X(k) \subseteq X(\mathbb{A})^{\mathrm{Br}}$. For a more detailed exposition, see [11, §5.2].

3. Descent obstruction

Let G be an algebraic group (smooth group scheme of finite type over k) and assume that G is affine. A trivial X-torsor under G is the X-scheme $X \times G$ with the right action of G given by right translation on the second factor. An X-torsor under G is an X-scheme $Y \xrightarrow{f} X$ equipped with a right action of G such that it becomes a trivial torsor after some étale surjective base extension. There is a bijection

$$\frac{\{X\text{-torsors under } G\}}{\text{isomorphism}} \leftrightarrow H^1(X, G),$$

where the right side should be interpreted as a nonabelian Čech cohomology set for the étale topology.

Fix a torsor $Y \xrightarrow{f} X$ under G. Then there is a map

$$\begin{aligned} X(k) &\to H^1(k,G) \\ x &\mapsto \text{ class of } f^{-1}(x). \end{aligned}$$

For each $[\sigma] \in H^1(k,G)$, where σ denotes a 1-cocycle, we may twist by σ to obtain a new torsor $Y^\sigma \xrightarrow{f^\sigma} X$ under a twisted form G^σ of G. This twisted torsor is defined so that

$$\{x \in X(k) : \text{ class of } f^{-1}(x) = [\sigma]\} = f^\sigma(Y^\sigma(k)).$$

Taking the disjoint union over all $[\sigma] \in H^1(k,G)$ yields

$$\begin{aligned} X(k) &= \coprod_{[\sigma]\in H^1(k,G)} f^\sigma(Y^\sigma(k)) \\ &\subseteq \bigcup_{[\sigma]\in H^1(k,G)} f^\sigma(Y^\sigma(\mathbb{A})). \end{aligned}$$

Imposing these restrictions on $X(k)$ coming from all torsors under all G leads one to define

$$X(\mathbb{A})^{\text{descent}} := \bigcap_{\substack{G \text{ affine} \\ Y \xrightarrow{f} X \text{ under } G}} \bigcup_{[\sigma]\in H^1(k,G)} f^\sigma(Y^\sigma(\mathbb{A})).$$

This theory is due to Colliot-Thélène and Sansuc [1],[2], and was generalized to the nonabelian case by Harari and Skorobogatov in [5]. For a more detailed exposition, see [11, §5.3].

4. Variants and comparisons

Let $X(\mathbb{A})^{\text{PGL}}$ be defined the same way as $X(\mathbb{A})^{\text{descent}}$, but where we intersect only over torsors under groups of the form PGL_n for all $n \geq 1$. Then

$$X(\mathbb{A})^{\text{descent}} \subseteq X(\mathbb{A})^{\text{PGL}} = X(\mathbb{A})^{\text{Br}},$$

where the equality follows from the equivalence of the cohomological Brauer group and Azumaya Brauer group proved by Gabber and reproved by de Jong. Harari [4] proved the stronger equality $X(\mathbb{A})^{\text{connected}} = X(\mathbb{A})^{\text{Br}}$, where $X(\mathbb{A})^{\text{connected}}$ is defined the same way as $X(\mathbb{A})^{\text{descent}}$, but using only *connected* affine algebraic groups.

An arbitrary affine algebraic group is an extension of a finite étale group by a connected affine algebraic group, so in light of Harari's result it is natural to ask whether $X(\mathbb{A})^{\text{descent}}$ equals the combination subset

$$X(\mathbb{A})^{\text{et,Br}} := \bigcap_{\substack{\text{finite étale } G \\ Y \xrightarrow{f} X \text{ under } G}} \bigcup_{[\sigma]\in H^1(k,G)} f^\sigma(Y^\sigma(\mathbb{A})^{\text{Br}}).$$

A positive answer follows from the sequence of inclusions:

$$\begin{aligned} X(k) \quad &\subseteq X(\mathbb{A})^{\text{descent}} &&\overset{1}{\subseteq} X(\mathbb{A})^{\text{et,descent}} &&\overset{2}{\subseteq} X(\mathbb{A})^{\text{et,Br}} \\ &\overset{3}{\subseteq} X(\mathbb{A})^{\text{descent}} &&\overset{4}{\subseteq} X(\mathbb{A})^{\text{Br}} &&\subseteq X(\mathbb{A}). \end{aligned}$$

Inclusion 4 was explained above, and inclusion 2 follows formally from it. Inclusion 3 (perhaps the most difficult part) was proved by Demarche [3], building on work of Borovoi and Harari. Then inclusion 1 was proved by Skorobogatov [12], building on work of Stoll [13].

5. Insufficiency of the obstructions

Skorobogatov [10] gave an example proving that the Brauer-Manin obstruction is insufficient to decide whether $X(k)$ is empty: his example has $X(\mathbb{A})^{\mathrm{Br}} \neq \emptyset$ but $X(\mathbb{A})^{\mathrm{et,Br}} = \emptyset$. We strengthen this by constructing a variety such that *none* of the obstructions defined so far are sufficient. Assume $\mathrm{char} k \neq 2$ from now on.

Theorem 1 ([8])**.** *There exists a nice k-variety X such that $X(\mathbb{A})^{\mathrm{et,Br}} \neq \emptyset$ but $X(k) = \emptyset$.*

This result follows easily from the following:

Theorem 2 ([8])**.** *Let C be a nice curve with $C(k) = \{P\}$. Then there exists a nice 3-dimensional variety $X \xrightarrow{\beta} C$ such that*

(1) *The fiber $X_P := \beta^{-1}(P)$ violates the local-global principle.*
(2) *The category of finite étale covers of C is equivalent to the analogous category for X.*
(3) *For all finite étale covers $C' \to C$, the map $\mathrm{Br}\, C' \to \mathrm{Br}\, X \times_C C'$ is an isomorphism.*

The proof involves choosing X_P to be a known Châtelet surface violating the Hasse principle, and fitting it into a family $X \to C$ of Châtelet surfaces. In fact, X is chosen as a conic bundle over $C \times \mathbb{P}^1$ that degenerates over a nice curve in $C \times \mathbb{P}^1$. For more details, see [8].

References

[1] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles*, in *Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979*, Sijthoff & Noordhoff, Alphen aan den Rijn (1980), 223–237.

[2] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles. II*, Duke Math. J. **54** (1987), 375–492.

[3] C. Demarche, *Obstruction de descente et obstruction de Brauer-Manin*, preprint, October 21, 2008, to appear in Algebra & Number Theory.

[4] D. Harari, *Groupes algébriques et points rationnels*, Math. Ann. **322** (2002), 811–826.

[5] D. Harari and A. Skorobogatov, *Non-abelian cohomology and rational points*, Compositio Math. **130** (2002), 241–273.

[6] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppsala (1940).

[7] Yu. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, in *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, 401–411, Gauthier-Villars, Paris (1971).

[8] B. Poonen, *Insufficiency of the Brauer-Manin obstruction applied to étale covers*, preprint, June 4, 2008.

[9] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18.

[10] A. Skorobogatov, *Beyond the Manin obstruction*, Invent. Math. **135** (1999), 399–424.

[11] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics **144**, Cambridge University Press (2001).

[12] A. Skorobogatov, *Descent obstruction is equivalent to étale Brauer-Manin obstruction*, preprint (2008).

[13] M. Stoll, *Finite descent obstructions and rational points on curves*, Algebra & Number Theory **1** (2007), 349–391.

Difference fields and descent in algebraic dynamics

Zoé Chatzidakis
(joint work with Ehud Hrushovski)

1. Preliminaries

Definition 1. A *difference field* is a field K with a distinguished endomorphism σ. (Then σ will of course be injective, but not necessarily surjective.) If $\sigma(K) = K$ then K is a *reflexive* difference field.

Any difference field has a reflexive closure, which is unique up to K-isomorphism. Difference fields are naturally structures in the language $\{+, -, \cdot, 0, 1, \sigma\}$. I have a tendency to work with automorphisms.

1. The study of difference algebra was started by Ritt in the 30's, in parallel with differential algebra. Extensive work was done by Richard Cohn, and you can find most of the algebraic results I cite in his book [4].

2. Examples
1. $\mathbb{C}(t)$, where $\sigma|_{\mathbb{C}} = id$, $\sigma(t) = t + 1$. This example is where difference fields acquired their names, from difference equations:

$$y(t+1) - y(t) = g(t)$$

2. $\mathbb{C}(t)$, where $\sigma|_{\mathbb{C}} = id$, $\sigma(t) = qt$, where $0 \neq q \in \mathbb{C}$, q not a root of unity (q-difference equations).
3. K a field of characteristic $p > 0$, $q = p^n$, and $\sigma_q = \text{Frob}^n : x \mapsto x^q$. Note that if K is not perfect, then σ_q is not onto. Note also that each σ_q is definable in the (pure) field K.

3. Difference polynomials, difference equations, σ-topology, etc. Given a difference field K, a *difference polynomial*, or σ-polynomial, $f(X_1, \dots, X_n)$ over K, is simply a polynomial over K in the variables $X_1, \dots, X_n, \sigma(X_1), \dots, \sigma(X_n)$, $\sigma^2(X_1), \dots, \sigma^i(X_j) \dots$.

A *difference equation*, or *σ-equation* is then just an equation $f(X_1, \dots, X_n)$ where f is a difference polynomial. The zero-sets of difference polynomials in a difference field K are called σ-closed - this defines a topology on K^n, analogous to the Zariski topology, and called the σ-topology; and the topology is Noetherian.

Definition 2. An *existentially closed difference field* (e.c.) is an inversive difference field (K, σ) such that every finite system of difference equations with coefficients in K which has a solution in some inversive difference field extending K, has a solution in K.

E.c. difference fields were sometimes called *generic difference fields*. They form an elementary class, whose theory (= system of axioms) is called ACFA. It is convenient to work inside a "large" e.c. difference field $(\mathcal{U}, \sigma)$, where by large I mean playing the role of a universal model, e.g. for some large cardinal κ, every system of $\leq \kappa$ σ-equations (with parameters) which has a solution in some extension of $\mathcal{U}$ already has a solution in $\mathcal{U}$.

4. Some more results. While derivations extend uniquely from a field to the algebraic closure, this is not the case with endomorphisms or automorphisms: the endomorphism σ of a field K can have several non-isomorphic extensions to the algebraic closure K^{alg} of K. This makes their study sometimes challenging, and is at the source of the differences in behaviour - eg, failure of quantifier elimination. In particular, observe that some choice has to be made: the isomorphism type of the algebraic closure of the prime field is an invariant of $(\mathcal{U}, \sigma)$ It turns out that the completions of ACFA are obtained by describing this isomorphism type, and this implies (with the same proofs as for pseudo-finite fields) that the theory ACFA is decidable. In fact, many proofs for e.c. difference fields are very similar to those given for pseudo-finite fields. Hrushovski shows in [5] that non-principal ultraproducts of the difference fields K_q of example 3 are e.c.: in other words, the automorphism σ of $\mathcal{U}$ can be thought of as a *non-standard Frobenius*.

2. Algebraic dynamics, the main result

5. By an *algebraic dynamics* over a field K, I mean an algebraic variety V (preferably irreducible), together with a dominant rational map $\phi : V \to V$, both defined over K. If L is an overfield of K, then the system (V, ϕ) can naturally be viewed as an algebraic dynamics over L, and I won't distinguish between the two. A *morphism* from (V, ϕ) to (W, ψ) is a dominant rational map $h : V \to W$ such that $h\phi = \psi h$.

To such a (V, ϕ) corresponds a difference field in the following way. Write $K(V) = K(a)$ (i.e., a a generic of V), define σ to be the identity on K, and $\sigma(a) = \phi(a)$. Then if h and W are as above, $h(a) = b$ will satisfy $\psi(y) = y \wedge y \in W$. For more details, see [2].

Theorem 1. *Let $K_1 \subseteq K_2$ be fields (algebraically closed; or K_2/K_1 regular), and let (V_i, ϕ_i) be algebraic dynamics defined over K_i, $i = 1, 2$. Assume that (V_1, ϕ_1) dominates (V_2, ϕ_2), with* $\dim(V_2) > 0$. *Then (V_2, ϕ_2) dominates an algebraic dynamics (V_3, ϕ_3) defined over K_1, and with* $\dim(V_3) > 0$.

6. Remarks. The hypotheses of this theorem do arise in nature, in fact in a result of M. Baker [1]. Assume that $K_2 = K_1(t)$, $V_2 = \mathbb{P}^n$, fix some d, and let S_d be the set of points of $\mathbb{P}^n(K_2)$ which are represented by polynomials of degree

$\leq d$. Then S_d is naturally the image of the K_1-rational points of some algebraic set defined over K_1. The existence of *sufficiently* many arbitrarily long sequences of points P_i with $\phi(P_i) = P_{i+1}$ and which lie in S_d, will then imply the existence of a difference variety (V_1, ϕ_1) defined over K_1, and which dominates (V_2, ϕ_2^m) for some m. In Baker's result, he takes for K_2 a function field in 1 variable, $n = 1$, and ϕ_2 of degree > 1; his assumptions on the set of canonical height 0 then imply that for some d, S_d contains arbitrarily long sequences as above, and allows one to be in the situation of the theorem.

One of the tools used in the proof is the following

Theorem 2. *Let K be a difference field, and L a finitely generated difference field extension of K, of finite transcendence degree. Then there are difference fields $L_0 = K \subset L_1 \subset \cdots \subset L_m = L$ such that for every i, the extension L_{i+1}/L_i is either*

- *algebraic, or*
- *qf-internal to a fixed field* Fix(τ)*, or*
- *one-based.*

7. Comments. There are two important notions appearing in this result, the one of *qf-internal to a field*, and the one of *one-based*, and I will define them below. This result is often referred to as the *dichotomy theorem*. It was first proved in a weaker form (the L_i's were contained in L^{alg}, not necessarily in L).

If $\tau = \sigma^n \text{Frob}^m$, then we know that $\text{Fix}(\tau) = \{a \in \mathcal{U} \mid \tau(a) = a\}$ is a (pseudo-finite) field. We say that M/K is *qf-internal to* Fix(τ), if for some difference field N containing K and which is linearly disjoint from M over K, we have $M \subset N\text{Fix}(\tau)$. We say that M/K is *one-based* if whenever $M_1, \ldots, M_r$ are K-isomorphic copies of M (within $\mathcal{U}$), and $N = \sigma(N)^{alg}$ contains K, $C = (M_1 \cdots M_r)^{alg} \cap N$, then $(M_1 \cdots M_r)^{alg}$ and N are free over C. A definable set S is *one-based* if whenever $a_1, \ldots, a_r \in S$, K is a difference field containing the parameters needed to define S, M is the algebraic closure of the difference field generated by $a_1, \ldots, a_r$ over K and $N = \sigma(N)^{alg}$ is a difference field, then M and N are linearly disjoint over their intersection. A one-based subgroup B of an algebraic group G has the following property: if $X \subset B^n$ is irreducible σ-closed, then X is a coset of a σ-closed subgroup of B^n.

8. Very rough sketch of the proof of Theorem 1. Let a_1 be a generic of V_{1K_2} over K_2, define σ to be the identity on K_2, and $\sigma(a_1) = \phi_1(a_1)$. If $h : (V_1, \phi_1) \to (V_2, \phi_2)$ is a dominant map, then $a_2 = h(a_1)$ satisfies $\sigma(x) = \phi_2(x)$. We need to find some $a_3 \in K_2(a_2)$, such that $a_3 \notin K_2^{alg}$, and $K_1(a_3)$ is linearly disjoint from K_2 over K_1. In fact we will find such an a_3 inside the perfect hull of $K_1(a_1)$.

Using 2, the proof of Theorem 1 splits into two cases: whether the extension $K_2(a_2)/K_2$ has an analysis in which no extension is qf-internal to Fix(σ), or whether it is qf-internal to Fix(σ).

In the first case, using model-theoretic techniques telling us things about fields of definition of σ-algebraic loci, we obtain that in fact (V_2, ϕ_2) completely descends to K_1: there is (V_3, ϕ_3) defined over K_1, $h' : (V_2, \phi_2) \to (V_3, \phi_3)$ which is bijective (and an isomorphism in characteristic 0, or if K_1 is perfect and $\dim(V_2) = 1$). This first case allows us to retrieve Baker's result, and appears in [3].

In the case where $K_2(a_2)/K_2$ is qf-internal, we must assume that K_2 and K_1 are algebraically closed. We develop some *definable Galois theory*, and show in a first step that (V_2, ϕ_2) is isomorphic to (A, t_a) where A is some commutative algebraic group, and t_a is translation by some element $a \in A(K_2)$. We may assume that A is simple, i.e., equals $\mathbb{G}_a$, $\mathbb{G}_m$ or a simple Abelian variety. After more manipulations, we obtain the result. The proof is particularly easy when $A = \mathbb{G}_a$: if $a = 0$, there is nothing to do, $(V_2, \phi_2) \simeq (\mathbb{G}_a, id)$; if $a \neq 0$, then putting $y = xa^{-1}$, the equation $\sigma(x) = x + a$ becomes $\sigma(y) = y + 1$. This part is still being written.

References

[1] M. Baker, *A Finiteness Theorem for Canonical Heights Attached to Rational Maps over Function Fields*, to appear in J. Reine Angew. Math. Available on arxiv.

[2] Z. Chatzidakis, E. Hrushovski, *Difference fields and descent in algebraic dynamics, I* Journal of the IMJ, 7 (2008) No 4, 653 – 686.

[3] Z. Chatzidakis, E. Hrushovski, D*ifference fields and descent in algebraic dynamics, II* Journal of the IMJ, 7 (2008) No 4, 687 – 704.

[4] R.M. Cohn, *Difference algebra*, Tracts in Mathematics 17, Interscience Pub. 1965.

[5] E. Hrushovski, *The first-order theory of the Frobenius*, preprint, available on `arxiv`.

[6] E. Hrushovski, *The Manin-Mumford conjecture and the model theory of difference fields*, Ann. Pure Appl. Logic 112 (2001), no. 1, 43–115.

Twisting and reducing covers over big fields

Pierre Dèbes
(joint work with Nour Ghazi)

The general goal is to understand the specializations of Galois covers. More specifically consider a (branched) cover $f : X \to B$ (over some base), that is: B is a smooth projective geometrically irreducible variety, X a normal and geometrically irreducible variety and f a finite, flat and generically unramified morphism. Over some field K, a cover equivalently corresponds, *via* the function field functor, to a separable extension $K(X)/K(B)$, regular over K. If t_0 is an unramified K-rational point on B, the *specialization* of f at t_0 is the residue field of the Galois closure $\widehat{f} : \widehat{X} \to B$ at some point of $\widehat{X}$ above t_0. We denote it by $K(X)_{t_0}/K$; it is well-defined up to K-isomorphism of K^{S} (the separable closure of K).

Assume $f : X \to B$ is Galois over K, *i.e.* is a K-G-cover, of group G. The general problem we address is whether a given Galois extension E/K of group $H \subset G$ is a specialization $K(X)_{t_0}/K$ of f at some point unramified $t_0 \in B(K)$.

This problem reformulates as follows using (étale) fundamental groups. Denote by D the branch divisor of f and consider the following diagram where the horizontal line is the classical fundamental group exact sequence, where s_{t_0} is the section associated with the K-rational point $t_0 \in B \setminus D$ (defined up to conjugation by some element in $\pi_1(B \setminus D)_{K^{\mathrm{S}}}$), where $\Phi : \pi_1(B \setminus D)_K \to G$ is an epimorphism (corresponding to the cover $f : X \to B$), where $\varphi : \mathrm{G}_K \to G$ is a morphism such that $\varphi(\mathrm{G}_K) = H$ (corresponding to the extension E/K) and where $\gamma : G \to S_d$ (resp. $\delta : G \to S_d$) is the left-regular representation (resp. the right-regular representation) of G in S_d (with $d = |G|$).

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(B \setminus D)_{K^{\mathrm{S}}} \arrow[r] & \pi_1(B \setminus D)_K \arrow[r, "r"] \arrow[d, "\Phi"'] & \mathrm{G}_K \arrow[r] \arrow[d, "\varphi"] \arrow[l, bend right, "s_{t_0}"'] & 1 \\
 & & G \arrow[d, "\gamma"'] & G \arrow[d, "\delta"] & \\
 & & S_d & S_d &
\end{tikzcd}$$

The question is whether φ and Φs_{t_0} are conjugate in G for some $t_0 \in B(K) \setminus D$.

The formula $\widetilde{\phi}^{\varphi} = \gamma\phi \times \delta\varphi^* r$, where "×" is the product in S_d and φ^* is the anti-morphism defined by $\varphi^*(g) = \varphi(g)^{-1}$, yields a morphism $\widetilde{\phi}^{\varphi} : \pi_1(B \setminus D)_K \to S_d$, which equals ϕ on $\pi_1(B \setminus D)_{K^{\mathrm{S}}}$. This "twisted" morphism corresponds to a "twisted" cover $\widetilde{f}^{\varphi} : \widetilde{X}^{\varphi} \to B$, which is a K-model (as mere cover) of the K^{S}-cover obtained from f by scalar extension to K^{S}. A main property of the twisted cover is the following:
(*) *For every $t_1 \in B(K) \setminus D$, there exists $x_1 \in \widetilde{X}^{\varphi}(K)$ such that $\widetilde{f}^{\varphi}(x_1) = t_1$ if and only if the specialization $K(X)_{t_1}/K$ of f at t_1 is the extension E/K.*

This result which was proved in [2] and which is a fundamental group variant of the so-called field crossing argument reduces the problem to finding K-rational points on the twisted variety $\widetilde{X}^{\varphi}$.

Assume now that K is the quotient field of some integral domain A, noetherian and integrally closed, given with some maximal ideal $\mathfrak{m}$ and that B is given with a model $\mathcal{B}$ over A with good reduction (that is: the special fiber of $\mathcal{B}$ has the same properties initially requested for B). Denote the residue field $A/\mathfrak{m}$ by κ.

Consider the morphism $\mathcal{F} : \mathcal{X} \to \mathcal{B}$ (resp. the morphism $\widetilde{\mathcal{F}}^{\varphi} : \mathcal{X}^{\varphi} \to \mathcal{B}$) obtained by normalizing $\mathcal{B}$ in $K(X)$ (resp. by normalizing $\mathcal{B}$ in $K(\widetilde{X}^{\varphi})$).

The following assumptions on $\mathcal{F}$ guarantee that $\mathcal{F} : \mathcal{X} \to \mathcal{B}$ has good reduction (that is: the special fiber $\mathcal{F}^{\equiv} : \mathcal{X}^{\equiv} \to \mathcal{B}^{\equiv}$ is finite, flat, generically unramified and $\mathcal{X}^{\equiv}$ is geometrically irreducible):

(a) *$\mathcal{F}$ has geometric good reduction, that is: the cover obtained from $\mathcal{F}$ by extending the scalars from the ring A to its integral closure in $\overline{K}$ has good reduction.*

(b) *the ideal $\mathfrak{m}$ in unramified in $\mathcal{F}$ (i.e. there is no vertical ramification).*

Assume (a) and (b) hold. As f and $\widetilde{f}^{\varphi}$ coincide over $\overline{K}$, condition (a) automatically holds for $\widetilde{\mathcal{F}}^{\varphi}$ as well. Furthermore condition (b) also holds for $\widetilde{\mathcal{F}}^{\varphi}$ if we assume in addition that

(c) *the ideal $\mathfrak{m}$ in unramified in the extension E/K.*

Consequently, under (a), (b) and (c), $\widetilde{\mathcal{F}}^{\varphi} : \mathcal{X}^{\varphi} \to \mathcal{B}$ has good reduction.

Assume next that $(A,\mathfrak{m})$ has the henselian property and that κ is "big enough" in the following sense. Let $(\mathcal{F}^{\equiv})_{\overline{\kappa}} : (\mathcal{X}^{\equiv})_{\overline{\kappa}} \to (\mathcal{B}^{\equiv})_{\overline{\kappa}}$ be the geometric special fiber of $\mathcal{F} : \mathcal{X} \to \mathcal{B}$. For κ to be big enough, we require that

(d) *any κ-model of $(\mathcal{F}^{\equiv})_{\overline{\kappa}}$ has unramified κ-rational points on its covering space.*

In particular this should hold for the κ-model $(\widetilde{\mathcal{F}}^{\varphi})^{\equiv}$. PAC fields and finite fields $\mathbb{F}_q$ with $q \gg 1$ are basic examples of big enough fields.

Combined with the henselian property, the big enough assumption makes it possible to lift unramified κ-rational points from the κ-variety $(\widetilde{\mathcal{X}}^{\varphi})^{\equiv}$ to K-rational points on the K-variety $\widetilde{X}^{\varphi}$. We have proved the following.

Theorem *Let $(A,\mathfrak{m})$ be a henselian ring as above, K be the quotient field, κ be the residue field. Let $f : X \to B$ be a K-G-cover with group G and E/K be a Galois extension of group $H \subset G$. Assume that B is given with a A-model $\mathcal{B}$ with good reduction, that assumptions* (a), (b), (c) *above hold and that κ is big enough in the sense of* (d) *above. Then the extension E/K is a specialization of f at some unramified point $t \in B(K)$.*

We will illustrate this result in two special situations.

Situation 1: PAC fields
Assume that the field K itself is PAC. No reduction process is then needed (or it corresponds to the trivial case $A = K$ and $\mathfrak{m} = 0$). We obtain this statement which appeared in [2] and is also noted in [5].

Corollary 1 *Let K be a PAC field, $f : X \to B$ be a K-G-cover with group G and E/K be a Galois extension of group $H \subset G$. Then E/K is a specialization of f at infinitely many points $t \in B(K)$.*

In his thesis [1], Bary-Soroker develops a similar approach and obtains related results. For example, he proves this weak version of Hilbert's irreducibility theorem for "PAC-extensions". Recall a field M is PAC if every geometrically irreducible variety V of positive dimension r and defined over M has M-rational points. For a field extension M/K to be PAC, it is further required that if a separable dominant morphism $\nu : V \to \mathbb{A}^r$ defined over M is also given, then some M-rational points exist on V that map to K-rational points on $\mathbb{A}^r$.

Theorem (Bary-Soroker) *Let K be a field and $f(T,Y) \in K(T)[Y]$ be an irreducible polynomial of degree d in Y with Galois group S_d over $\overline{K}(T)$. Assume that there exists a PAC extension M/K and a separable extension N/M of degree d. Then there exist infinitely many $t \in K$ such that $f(t,Y)$ is irreducible in $K[Y]$.*

Situation 2: local fields
Let G be a finite group, Q be a number field, S be a finite set of finite places of Q and $\mathbf{E} = (E_v/Q_v)_{v\in S}$ be a collection of Galois extensions of group $H_v \subset G$ ($v \in S$). In this context, there is the following classical result.

Theorem (Grunwald-Wang, Neukirch) *If G is solvable of odd order, then there exists a Galois extension E/Q of group G such that $EQ_v/Q_v \simeq E_v/Q_v$ ($v \in S$).*

Given a Q-G-cover $f : X \to B$, consider the subset $H_{f,\mathbf{E}} \in B(Q)$ of all t such that the specialization $Q(X)_t/Q$ at t is an extension as in the Grunwald theorem. Corollary 2 below follows from our theorem. It refines some results of Fried [4], Colliot-Thélène (see [6, §3.5]) and Ekhedal [3].

Corollary 2 *Assume that for each $v \in S$*
(a) *f has good reduction at v,*
(b) *E_v/Q_v is unramified,*
(c) *the residue field of v is big enough.*
Then there exist a finite set T of finite places of Q such that $S \cap T = \emptyset$ and non-empty open subsets $U_v \subset B(Q_v)$ ($v \in S \cup T$) such that $H_{f,\mathbf{E}} \supset B(Q) \cap \prod_{v \in S \cup T} U_v$. If in addition B has the weak approximation property, then $H_{f,\mathbf{E}} \neq \emptyset$.

References

[1] L. Bary-Soroker, *Pseudo Algebraically Closed Extensions*, PhD thesis, Tel Aviv University, (2009).

[2] P. Dèbes, *Galois covers with prescribed fibers: the Beckmann-Black problem*, Ann. Scuola Norm. Sup. Pisa, Cl. Sci. (4), **28** (1999), 273–286.

[3] T. Ekedahl, *An effective version of Hilbert's irreducibility theorem*, Sém. Théorie des Nombres de Paris 1988/89, Birkhäuser, (1990), 241–248.

[4] M. Fried, "On Hilbert's irreducibility theorem", J. Number Theory, **6**, (1974), 211–231.

[5] D. Haran, M. Jarden, *Regular Lifting of Covers over Ample Fields*, Albanian Journal of Mathematics **1** (2007), 215224.

[6] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett Publ., Boston, (1992).

Ramification of Primes in Fields of Moduli

Andrew Obus

1. Overview

This talk investigates a connection between number theory and topology. One knows, as a consequence of Serre's GAGA principle, that any finite topological branched cover of the 2-sphere can be cut out as the zero locus of polynomial equations with complex coefficients in projective space. We can then ask the following question: Given only topological information about the branched cover, what can we say about the field extension of $\mathbb{Q}$ generated by the coefficients of the defining equations? This field is called a *field of definition* of the cover.

Since the proof of GAGA is non-constructive, the answer to this question is not obvious. It motivates our study of the *field of moduli* of covers (§1.1). In particular, we aim to understand the ramification of primes in the field of moduli. To this end, my main result (Theorem 3) generalizes work of Beckmann and Wewers. For further motivation, if desired, see §1.2.

1.1. **Fields of Moduli.** Let X be the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$, and suppose $f : Y \to X$ is a finite branched cover of Riemann surfaces. By GAGA, Y is isomorphic to a projective algebraic variety, and we can take f to be an algebraic, regular map. Assume that the branch points of f can be taken to lie in $\overline{\mathbb{Q}} \cup \{\infty\}$. This is the case, for instance, whenever we have a *three-point cover*, i.e., f is branched at exactly three points, as the branch points can be mapped to 0, 1, and ∞ via an algebraic automorphism of X. Then, by a theorem of Grothendieck, the polynomial equations of the cover f themselves can be defined over $\overline{\mathbb{Q}}$ (in fact, even over some number field).

Let $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then σ acts on the set of all finite branched covers of X by acting on the coefficients of the polynomial equations defining each cover. Say f is a *G-Galois cover*, i.e., we choose an isomorphism $\mathrm{Aut}(Y/X) \cong G$ and $\deg(f) = |G|$. Let $\Gamma^{in} \subset G_{\mathbb{Q}}$ be the subgroup consisting of those σ which preserve the isomorphism class of f as well as the G-action. Then the fixed field of $\overline{\mathbb{Q}}$ under the action of Γ^{in} is known as the *field of moduli* of f (as a G-cover). It is the intersection of all the fields of definition of f as a G-cover, see [3].

1.2. **The Fundamental Exact Sequence.** Let C be the projective line minus $\{0, 1, \infty\}$ defined over $\mathbb{Q}$. Let $C_{\overline{\mathbb{Q}}}$ be the base change of C to $\overline{\mathbb{Q}}$. We then have the following so-called *fundamental exact sequence* of groups:

$$1 \to \pi_1(C_{\overline{\mathbb{Q}}}) \to \pi_1(C) \to G_{\mathbb{Q}} \to 1. \tag{1}$$

Here π_1 is the *étale fundamental group* functor, which classifies automorphisms of the pro-universal cover (i.e., the projective limit of all unramified finite covers). By GAGA and the Lefschetz principle, $\pi_1(C_{\overline{\mathbb{Q}}})$ is the profinite completion of the standard fundamental group of C viewed as a complex curve, i.e., the free profinite group on two generators $\hat{F}_2$. Thus $\pi_1(C)$ encodes both topological information about C and arithmetic information about $\mathbb{Q}$. The fundamental exact sequence splits, and we obtain an outer action of $G_{\mathbb{Q}}$ on $\pi_1(C_{\overline{\mathbb{Q}}})$.

The relation between the fundamental exact sequence and the field of moduli is as follows: Let $f : Y \to X = \mathbb{P}^1$ be a G-Galois cover branched at three points, thus defined over $\overline{\mathbb{Q}}$. Then the choice of f is equivalent to a choice of a normal subgroup $N \subset \pi_1(C_{\overline{\mathbb{Q}}})$ such that $\pi_1(C_{\overline{\mathbb{Q}}})/N \cong G$. The group Γ^{in} from §1.1 is the maximal subgroup of $G_{\mathbb{Q}}$ whose outer action preserves N and descends to an inner action on $\pi_1(C_{\overline{\mathbb{Q}}})/N$.

Milne has called the group $\pi_1(C)$, the middle term of the exact sequence (1), “the most interesting object in mathematics” ([4, p. 30]). Understanding (1) fully is a monumental task, and would yield, among other things, a description of $G_{\mathbb{Q}}$. My work involves trying to better understand the outer action of $G_{\mathbb{Q}}$ on $\pi_1(C_{\overline{\mathbb{Q}}}) \cong \hat{F}_2$ arising from (1), by investigating the field of moduli of various finite covers.

Remark. It might seem like considering only the case of three-point covers of $\mathbb{P}^1$ is very restrictive, and indeed, the framework of this section is valid for more general branched covers of curves. However, according to Belyi's theorem ([2, Theorem

4]), any curve defined over $\overline{\mathbb{Q}}$ has a map to $\mathbb{P}^1$ with exactly three branch points. So while the case of three-point covers does not include all covers of curves, it includes *some* cover $f : Y \to X$ for each curve Y defined over $\overline{\mathbb{Q}}$.

2. Results

The relationship between branched covers and fields of moduli is rather mysterious. One of the first major results in this direction is due to Beckmann, and was generalized by Wewers:

Theorem 1 ([1]). *Let $f : Y \to X$ be a three-point G-Galois cover of the Riemann sphere. If $p \nmid |G|$, then p is unramified in the field of moduli of f.*

Theorem 2 ([5]). *Let $f : Y \to X$ be a three-point G-Galois cover of the Riemann sphere. If $p^2 \nmid |G|$, then p is tamely ramified in the field of moduli of f.*

To state my main theorem, which is a further generalization, we will need some group theory. Call a finite group G *p-solvable* if its simple composition factors with order divisible by p are all isomorphic to $\mathbb{Z}/p$. Note that any solvable group is p-solvable. If $H \subset G$, write $N_G(H)$ for the normalizer of H in G and $Z_G(H)$ for the centralizer of H in G. Lastly, let μ_{p^n} be the set of p^nth roots of unity.

The main result of my talk is:

Theorem 3 (Obus, thesis). *Let $f : Y \to X$ be a three-point G-Galois cover of the Riemann sphere, and suppose that a p-Sylow group $P \subset G$ is cyclic of order p^n. Let $K/\mathbb{Q}$ be the field of moduli of f. Let $m = |N_G(P)/Z_G(P)|$. Then the nth higher ramification groups for the upper numbering of $K/\mathbb{Q}$ vanish in either of the following cases:*

: *(i) G is p-solvable.*

: *(ii) $m = 2$, provided that $p \neq 3$ and at least one of the three branch points has prime-to-p branching index.*

Remark. Note that Beckmann's and Wewers's theorems cover the cases $n = 0, 1$.

Remark. The author fully expects theorem 3 to hold in the case $m = 2$, even without either of the assumptions $p = 3$ or one branch point having prime-to-p branching index. However, at the moment there is a gap in the argument.

Now, one can show that if G has a cyclic p-Sylow and is not p-solvable, it must have a simple composition factor with order divisible by p^n. There are "not too many" simple groups with cyclic p-Sylow subgroups of order greater than p. Indeed, there are no sporadic groups or alternating groups. Furthermore, many of the examples that do exist satisfy $m = 2$ (e.g., $PSL_2(q)$, where p^n divides $q^2 - 1$). This shows that the groups covered in the theorem really do represent a large portion of the finite groups with cyclic p-Sylow subgroup.

References

[1] Beckmann, Sybilla. "Ramified Primes in the Field of Moduli of Branched Coverings of Curves," J. Algebra 125 (1989), 236–255.

[2] Belyi, G. V. "Galois Extensions of a Maximal Cyclotomic Field," Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), 267–276.

[3] Coombes, Kevin; Harbater, David. "Hurwitz Families and Arithmetic Galois Groups," Duke Math. J., 52 (1985), 821–839.

[4] Milne, James S. "Lectures on Étale Cohomology," v. 2.10 (2008). Available at www.jmilne.org/math/index.html.

[5] Wewers, Stefan. "Three Point Covers with Bad Reduction," J. Amer. Math. Soc. 16 (2003), 991–1032.

Virtually free pro-p groups

Pavel Zaleskii
(joint work with Wolfgang Herfort)

Let p be a prime number, and G a pro-p group containing an open free pro-p subgroup F. If G is torsion free, then, according to the celebrated theorem of Serre in [14], G itself is free pro-p.

The main objective of the paper is to give a description of virtually free pro-p groups without the assumption of torsion freeness.

Theorem 1. *Let G be a finitely generated pro-p group with an open free pro-p subgroup F. Then G is the fundamental pro-p group of a finite graph of finite p-groups of order bounded by $|G : F|$.*

This theorem is the pro-p analogue of the description of finitely generated virtually free discrete groups proved by Karrass, Pietrovski and Solitar [9]. In the characterization of discrete virtually free groups Stallings' theory of ends played a crucial role. In fact the proof of the theorem of Karrass-Pietrovski and Solitar uses the celebrated theorem of Stallings in [15], according to which every virtually free group splits as an amalgamated free product / HNN-extension over a finite group. We prove a pro-p analogue of Stallings' Theorem and Theorem 1 using purely combinatorial pro-p group methods combined with results on p-adic representations of finite p-groups.

Theorem 2. *Let G be a finitely generated virtually free pro-p group. Then G is either a non-trivial amalgamated free pro-p product with finite amalgamating subgroup or it is a non-trivial HNN-extension with finite associated subgroups.*

As a consequence of Theorem 1 we obtain that a finitely generated virtually free pro-p group is the pro-p completion of a virtually free discrete group. However, the discrete result is not used (and cannot be used) in the proof.

Note that the assumption of finite generation in Theorem 1 is essential: there is an example of a split extension $H = F \rtimes D_4$ of a free pro-2 group F of countable rank which can not be represented as the fundamental pro-2 group of a profinite graph of finite 2-groups.

The line of proof is as follows. We use a pro-p HNN-extension to embed a finitely generated virtually free pro-p group G in a split extension $E = F \rtimes K$

of a free pro-p group F and a finite p-group K with unique maximal finite subgroups up to conjugation. Then we use a deep result of A. Weiss on integral p-adic representations [16] to prove that the K-module $M = F/[F, F]$ is permutational. After this we prove the following theorem showing that the basis of M lifts to a K-invariant basis of F.

Theorem 3. *Let E be a semidirect product $E = F \rtimes K$ of a free pro-p group F of finite rank and a finite p-group K. Then the K-module $M = F/[F, F]$ is permutational if and only if F posesses a K-invariant basis.*

This theorem gives an HNN-extension structure on E with finite base group. In particular, E and, therefore, G acts on a pro-p tree with finite vertex stabilizers. Using this, the machinery of the theory of profinite groups acting on trees [20, 18, 19], and, as an induction basis, a result due to C. Scheiderer for finitely generated free pro-p by C_p groups [13], we prove Theorems 1 and 2.

Basic material on profinite groups can be found in [17, 11]. For profinite graphs we shall employ (standard) notations as found in [11] or [12]. Below we include references that have been relevant during proofs in a detailled version [7].

Acknowledgement

The authors are grateful to the organizers for having invited us to the meeting and given us the opportunity to report on our progress.

References

[1] W. Dicks, Groups, Trees and Projective Modules, Springer 1980.

[2] A. Heller and I. Reiner, Representations of cyclic groups in rings of integers. I, Ann. of Math. (2) **76** 1962 73–92

[3] W. Herfort, P.A. Zalesskii and L. Ribes, p - Extensions of free pro-p groups, Forum Math. **11** (1998), 49–61.

[4] W. Herfort and P.A. Zalesskii, Cyclic Extensions of free pro-p groups, Journal of Algebra, **216** (1999) 511–547.

[5] W. Herfort and P.A. Zalesskii, Virtually free pro-p groups whose torsion elements have finite centralizers, Bulletin of the London Math. Soc. **40**6 (2008) 929–936.

[6] W. Herfort and P.A. Zalesskii, Profinite HNN-constructions, J. of Group Theory, **10** (2007), 6; S. 799–809.

[7] W. Herfort and P.A. Zalesskii, Virtually free pro-p groups, manuscript (2007) (submitted)

[8] W. Herfort and P.A. Zalesskii, Subgroups of fundamental pro-p groups of finite graphs of groups, Preprint (2007)

[9] A. Karrass, A. Pietrovski and D. Solitar, Finite and infinite cyclic extensions of free groups, J.Australian Math.Soc. **16** (1973) 458–466.

[10] O.V. Mel'nikov, Subgroups and Homology of Free Products of Profinite Groups, Math. USSR Izvestiya, **34**, 1, (1990), 97-119.

[11] L. Ribes and P.A. Zalesskii, Profinite Groups, Springer 2000.

[12] L. Ribes and P.A. Zalesskii, Pro-p Trees and Applications, (2000), Chapter, Ser. Progress in Mathematics, Birkhäuser Boston (2000), Ed. A. Shalev, D. Segal.

[13] C. Scheiderer, The structure of some virtually free pro-p groups, Proc. Amer. Math. Soc. **127** (1999) 695-700.

[14] J.-P. Serre, Sur la dimension cohomologique des groupes profinis, Topology **3**, (1965) 413-420.

[15] J.R. Stallings, On torsion-free groups with infinitely many ends, Ann. of Math. II. Ser. **88** (1968) 312-334.

[16] A. Weiss, Rigidity of p-adic p-torsion, Ann. of Math. (2) **127** (1988) 317–332.

[17] J.S. Wilson, Profinite Groups, London Math.Soc. Monographs (Clarendon Press, Oxford, 1998)

[18] P.A. Zalesskii, A geometric characterization of free formations of profinite groups, Sib. Math. J. **30**, No.2, 227-235 (1989), (translation from Sib. Mat. Zh. **30**, No.2(174), 73-84 (1989))

[19] P.A. Zalesskii and O.V. Mel'nikov, Fundamental Groups of Graphs of Profinite Groups, Algebra i Analiz **1** (1989); translated in: Leningrad Math. J. **1** (1990), 921-940.

[20] P.A. Zalesskii and O.V. Mel'nikov, Subgroups of profinite groups acting on trees, Math. USSR Sbornik **63** (1989) 405-424.

[21] P.A. Zalesskii, Virtually projective groups, J. für die Reine und Angewandte Mathematik (Crelle's Journal) **572** (2004) 97-110.

[22] P.A. Zalesskii, Open Subgroups of Free Profinite Products, Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989), 473–491, Contemp. Math., **131**, Part 1, Amer. Math. Soc., Providence, RI, 1992.

Reporter: Andrew Obus

Participants

Lior Bary-Soroker
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
P.O.Box 39040
Ramat Aviv, Tel Aviv 69978
ISRAEL

Alp Bassa
EPFL
SB IACS (Batiment MA)
Station 8
CH-1015 Lausanne

Prof. Dr. Irene Bouw
Institut f. Reine Mathematik
Universität Ulm
Helmholtzstr. 18
89081 Ulm

Prof. Dr. Zoe Chatzidakis
U.F.R. de Mathematiques
Case 7012
Universite Paris 7
F-75205 Paris Cedex 13

Prof. Dr. Ted C. Chinburg
Department of Mathematics
University of Pennsylvania
Philadelphia , PA 19104-6395
USA

Prof. Dr. Mirela Ciperiani
Dept. of Mathematics
Barnard College
Columbia University
New York , NY 10027
USA

Prof. Dr. Jean-Louis Colliot-Thelene
Laboratoire de Mathematiques
Universite Paris Sud (Paris XI)
Batiment 425
F-91405 Orsay Cedex

Prof. Dr. Pierre Debes
UFR de Mathematiques
Universite Lille I
F-59655 Villeneuve d'Ascq. Cedex

Luca Demangos
Mathematiques
UMR 8524 CNRS
Universite de Lille 1
F-59655 Villeneuve d'Ascq.

Dr. Michael Dettweiler
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Dr. Frederic A.B. Edoukou
Institut de Mathematiques
de Luminy
Case 907
163 Avenue de Luminy
F-13288 Marseille Cedex 9

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

Arno Fehm
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

Prof. Dr. Gerhard Frey
Fachbereich Mathematik
Universität Duisburg-Essen
45117 Essen

Prof. Dr. Wulf-Dieter Geyer
Department Mathematik
Universität Erlangen-Nürnberg
Bismarckstr. 1 1/2
91054 Erlangen

Prof. Dr. Barry William Green
Department of Mathematics
University of Stellenbosch
7600 Stellenbosch
SOUTH AFRICA

Linda Gruendken
Department of Mathematics
University of Pennsylvania
Philadelphia , PA 19104-6395
USA

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

Prof. Dr. David Harbater
Department of Mathematics
University of Pennsylvania
Philadelphia , PA 19104-6395
USA

Dr. Julia Hartmann
Lehrstuhl A für Mathematik
RWTH Aachen
Templergraben 55
52062 Aachen

Prof. Dr. Wolfgang Herfort
Institut für Analysis und
Scientific Computing
Technische Universität Wien
Wiedner Hauptstr. 8 - 10
A-1040 Wien

Armin Holschbach
Fakultät für Mathematik
Universität Regensburg
Universitätsstr. 31
93053 Regensburg

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

Prof. Dr. Ernst Kani
Dept. of Mathematics & Statistics
Queen's University
Jeffery Hall
Kingston, Ontario K7L 3N6
CANADA

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

Prof. Dr. B. Heinrich Matzat
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Prof. Dr. Laurent Moret-Bailly
U. F. R. Mathematiques
I. R. M. A. R.
Universite de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex

Prof. Dr. Peter Müller
Mathematisches Institut
Universität Würzburg
Am Hubland
97074 Würzburg

Prof. Dr. Hiroaki Nakamura
Dept. of Mathematics
Faculty of Science
Okayama University
3-1-1 Tsushima-naka
Okayama 700-8530
JAPAN

Andrew S. Obus
Department of Mathematics
University of Pennsylvania
Philadelphia , PA 19104-6395
USA

Prof. Dr. Ambrus Pal
Imperial College
Department of Mathematics
Huxley Building
180 Queen's Gate
GB-London SW7 2AZ

Elad Paran
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
P.O.Box 39040
Ramat Aviv, Tel Aviv 69978
ISRAEL

Dr. Sebastian Petersen
Institut für Theoretische
Informatik und Mathematik
Universität der Bundeswehr
85577 Neubiberg

Pietro Ploner
Dipartimento di Matematica
Universita di Roma "La Sapienza"
Citta Universitaria
I-00100 Roma

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

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

Prof. Dr. Alexander Prestel
Fachbereich Mathematik u. Statistik
Universität Konstanz
Universitätsstr. 10
78457 Konstanz

Dr. Aharon Razon
c/o Moshe Jarden
School of Mathematics
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

Prof. Dr. Luis Ribes
School of Mathematics & Statistics
Carleton University
1125 Colonel By Drive
Ottawa , Ont. K1S 5B6
CANADA

Prof. Dr. Dr.h.c. Peter Roquette
Jaspers-Str.2, Apt. 345
69126 Heidelberg

Prof. Dr. Claus Scheiderer
Fakultät für Mathematik
Universität Konstanz
78457 Konstanz

Tomer Schlank
Institute of Mathematics
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

Dr. Leila Schneps
Institut de Mathematiques
Analyse Algebrique
Universite Pierre et Marie Curie
4, place Jussieu, Case 247
F-75252 Paris Cedex 5

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

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

Dr. Tamas Szamuely
Alfred Renyi Institute of
Mathematics
Hungarian Academy of Sciences
P.O.Box 127
H-1364 Budapest

Prof. Dr. Jose Felipe Voloch
Department of Mathematics
The University of Texas at Austin
1 University Station C1200
Austin , TX 78712-1082
USA

Prof. Dr. Stefan Wewers
Institut für Algebra, Zahlentheorie
und Diskrete Mathematik
Leibniz Universität Hannover
Welfengarten 1
30167 Hannover

Kirsten Wickelgren
Department of Mathematics
Stanford University
Stanford , CA 94305-2125
USA

Prof. Dr. Pavel Alexandr. Zalesski
Departamento de Matematica
Instituto de Ciencias Exatas
Universidade de Brasilia
Campus Universitario-Asa Norte
Brasilia DF 70910-900
BRAZIL

David Zywina
Department of Mathematics
University of Pennsylvania
Philadelphia , PA 19104-6395
USA