Mathematisches Forschungsinstitut Oberwolfach

Report No. 6/2006

The Arithmetic of Fields

Organised by
Wulf-Dieter Geyer (Erlangen)
Moshe Jarden (Tel Aviv)
Florian Pop (Philadelphia)

February 5th – February 11th, 2006

Abstract. This is the report on the Oberwolfach workshop *The Arithmetic of Fields*, held in February 2006. *Field Arithmetic* (MSC 12E30) is a branch of mathematics concerned with studying the inner structure (orderings, valuations, arithmetic, diophantine properties) of fields and their algebraic extensions using Galois theory, algebraic geometry and number theory, partially in connection with model theoretical methods from mathematical logic.

Mathematics Subject Classification (2000): 12E30.

Introduction by the Organisers

The fifth conference with the title **The Arithmetic of Fields**, organized by Wulf-Dieter Geyer (Erlangen), Moshe Jarden (Tel Aviv), and Florian Pop (Philadelphia), was held February 5–11th, 2006. In contrast to the fourth conference held in February 3–9th, 2002, this conference was a "full" one, namely as many participants were invited as the Institute could host. Due to support from the European Union, more young people were invited in the last few weeks prior to the conference, so that the total number of participants reached 54. The participants came from 13 countries: Germany (20), USA (10), Israel (7), France (7), Denmark (2), Austria (1), Brazil (1), Canada (1), Hungary (1), Japan (1), Romania (1), Russia (1), and South Africa (1). Among the participants there were 9 graduate students and 8 young researchers. Six women attended the conference.

The organisers asked four people before the conference to give surveys of one hour on recent progress made by other colleagues in Field Arithmetic.

Tamás Szamuely (Budapest) reported on the solution by János Kollár of a Problem due to Ax from 1968: Every PAC field of characteristic 0 is C_1. The case where the characteristic is positive remains open.

Alexandra Shlapentokh (Greenville) described the progress Bjorn Poonen made on Hilbert's Tenth Problem: There exists a recursive set T_1 of prime numbers of natural density 0 and a set T_2 of prime numbers of natural density 1 such that $T_1 \subseteq T_2$ and for each set S with $T_1 \subseteq S \subseteq T_2$ Hilbert's Tenth Problem for $O_{\mathbb{Q},S}$ has a negative solution. Here $O_{\mathbb{Q},S}$ is the ring of all rational numbers whose denominators are divided only by primes in S. Whether Hilbert's Tenth Problem for $\mathbb{Q}$ has a negative solution is still open.

Alexander Prestel (Konstanz) presented a theorem of Jochen Koenigsmann: If a p-Sylow extension P of a field K is Henselian and P is neither separably closed nor real closed, then K itself is Henselian.

Pierre Dèbes (Lille) surveyed Fried's problem on Modular Towers. He mentioned that the main conjecture is close to completion in the case of 4 branch points (Bayley-Fried). He also reported on a result of Anna Cadoret: The dihedral group has a regular realization over $\mathbb{Q}_{\mathrm{ab}}$ with only inertia groups of order 2.

In addition to these survey talks seventeen participants were invited to report on their own achievements in 45 minutes talks. Altogether, the talks presented the impressive progress made in Field Arithmetic in recent years. The reader may find here extended abstracts of all talks. We hope they will be to the benefit of all of the participants as well as the fans of Field Arithmetic.

The organisers: Wulf-Dieter Geyer, Moshe Jarden, Florian Pop

Workshop: The Arithmetic of Fields

Table of Contents

Abstracts

Diamond theorem for a finitely generated free profinite group

Lior Bary-Soroker

Haran gives, in [Ha2], a general sufficient condition for a closed subgroup of an infinitely generated free profinite group to be free:

Theorem A. *Let m be an infinite cardinal. Let $F = \hat{F}_m$ be the free profinite group of rank m, M_1, M_2 closed normal subgroups of F, and M a closed subgroup of F satisfying $M_1 \cap M_2 \leq M$ and $M_i \not\leq M$ for $i = 1, 2$. Then $M \cong \hat{F}_m$* [FrJ, Thm. 25.4.3].

Problem 25.4.9 of [FrJ] asks for a generalization of Theorem A to the case where m is finite and at least 2. A first step toward the solution of that problem is taken in [Jar]. Proposition 1.3 of [Jar] proves an analog of a theorem of Weissauer for finitely generated profinite groups:

Theorem B. *Let $F = \hat{F}_e$ with $e \geq 2$ an integer, M a closed subgroup of F of an infinite index, N a closed normal subgroup of F contained in M, and M_0 an open subgroup of M which does not contain N. Then $M_0 \cong \hat{F}_\omega$.*

In this talk we explain how, building on Theorems A and B, to settle Problem 25.4.9 of [FrJ], by proving a diamond theorem for free profinite groups of finite rank:

Theorem C. *Let $F = \hat{F}_e$ with $e \geq 2$ an integer, M_1, M_2 closed normal subgroups of F, and M a closed subgroup of F with $(F : M) = \infty$, $M_1 \cap M_2 \leq M$, $M_1 \not\leq M$, and $M_2 \not\leq M$. Then $M \cong \hat{F}_\omega$* [B-S].

The proof of Theorem A (at least in the case $m = \aleph_0$) is reduced to solving a finite embedding problem

$$(\phi\colon F \to G,\ \alpha\colon A\mathrm{wr}_{G_0}G \to G),$$

where G is a finite group, A is a finite nontrivial group, G_0 is a subgroup of G acting on A, and $A\mathrm{wr}_{G_0}G$ is the twisted wreath product. This embedding problem has a solution because every finite embedding problem for $\hat{F}_\omega$ has a solution. The same is true in the case $F = \hat{F}_e$, with e an integer, if $e \geq \mathrm{rank}(A\mathrm{wr}_{G_0}G)$. However, in general, this inequality does not hold.

We observe that $\mathrm{rank}(A\mathrm{wr}_{G_0}G) \leq |G| + \mathrm{rank}(A)$. So, if we replace F by an open subgroup E containing M, then by Nielsen-Schreier $\mathrm{rank}(E)$ increases (linearly depending on $(F : E)$). The main problem is that replacing F by E changes the embedding problem (ϕ, α). In this change the order of G may increase and with it also $|G| + \mathrm{rank}(A)$. We can control the growth of the order of G if there are "many" subgroups between F and M. In this case we say that M is an "abundant subgroup of F".

It may happen that there are not enough closed subgroups between F and one of the subgroups M, MM_1, or MM_2, in which case, the corresponding subgroup is called "sparse". More precisely, a closed subgroup M of a profinite group is called **sparse** if for all $m, n \in \mathbb{N}$ there exists an open subgroup K of F containing M such that $(F : K) \geq m$, and for every proper open subgroup L of K containing M we have $(K : L) \geq n$. In this case, the above proof does not work, so we prove that $M \cong \hat{F}_\omega$ directly or by using either Theorem A or Theorem B.

We also generalize Theorem C to pro-$\mathcal{C}$ groups, where $\mathcal{C}$ is a Melnikov formation [FrJ, Page 343] of finite groups, i.e., $\mathcal{C}$ is closed under taking quotients, normal subgroups, and extensions.

Historically the first diamond theorem was about a sufficient condition for an extension of Hilbertian field to be Hilbertian (See [Ha2]). We also transfer Theorem C to the theory of Hilbertian fields and prove the following result:

Theorem D. *Let K be a PAC field with a finitely generated free absolute Galois group of rank at least 2. Let M_1 and M_2 be Galois extensions of K. Then every infinite extension M of K in M_1M_2 which is contained neither in M_1 nor in M_2 is a Hilbertian field.*

Acknowledgement: The author is grateful to D. Kelmer, E. Paran, and I. Surdin for their help in preparation of this talk.

References

[B-S] Bary-Soroker Lior, Diamond Theorem for a finitely generated Free Profinite Group, Mathematische Annalen, to appear.

[FrJ] M. Fried, M. Jarden, Field Arithmetic, Second Edition, revised and enlarged by Moshe Jarden. Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, (2005)

[Ha1] D. Haran, Hilbertian fields under separable algebraic extensions. Inventiones mathematicae **137**, 85–112 (1999)

[Ha2] D. Haran, Free subgroups of free profinite groups. Journal of Group Theory **2**, 307–317 (1999).

[Jar] M. Jarden, A Karrass-Solitar theorem for profinite groups. Journal of Group theory, to appear.

Teichmüller curves and triangle groups

Irene I. Bouw

(joint work with Martin Möller)

Let M_g be the moduli space of curves of genus $g \geq 2$ and let T_g be the Teichmüller space. Write $\Omega T_g \to T_g$ for the total space of the pullback of the Hodge bundle to T_g. We have a natural action of $\mathrm{SL}_2(\mathbb{R})$ on the complement ΩT_g^* of the zero section in ΩT_g. Namely for $A \in \mathrm{SL}_2(\mathbb{R})$ and $(X, \omega) \in \Omega T_g^*$ postcompose the charts with the action of A on $\mathbb{C} \simeq \mathbb{R}^2$. If the image, C, of an $\mathrm{SL}_2(\mathbb{R})$-orbit in M_g is closed, we call C a *Teichmüller curve*.

The fibers of $\Omega T_g \to T_g$ are fixed by the action of $\mathrm{SO}_2(\mathbb{R})$. Therefore a pair (X, ω) as above induces a map

$$\mathbb{H} \simeq \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \to T_g \to M_g.$$

It is known that a pair (X, ω) defines a Teichmüller curve if and only if the stabilizer $\Gamma := \mathrm{Stab}(X, \omega) \subset \mathrm{SL}_2(\mathbb{R})$ of (X, ω) is a lattice. The group Γ is called the *affine group* of a Teichmüller curve C.

It is a natural question to ask which groups Γ may occur as the affine group of a Teichmüller curve. For simplicity, we only consider the image of the affine group in $\mathrm{PSL}_2(\mathbb{R})$. Our main result completely solves this question for the case of triangle groups. Veech ([4]) showed that every Teichmüller curve has at least one cusp. Therefore we only need to consider triangle groups $\Delta(n, m, \infty)$ with $n, m \in \mathbb{Z}_{>1} \cup \{\infty\}$ satisfying $1/n + 1/m < 1$.

Theorem 1. *Let $\Gamma = \Delta(n, m, \infty)$ be a triangle group, as above. Then there exists a Teichmüller curve C with (projective) affine group Γ.*

The theorem, proved in [1], generalizes results of Veech ([4]) and Ward ([5]) who constructed Teichmüller curves whose affine group is $\Delta(2, n, \infty), \Delta(n, n, \infty)$ or $\Delta(3, n, \infty)$. These results are formulated in the language of billiards. McMullen ([2]) showed that there exist Teichmüller curves whose affine group is not a triangle group.

The proof of the theorem relies on a Hodge-theoretical characterization of Teichmüller curves, due to Möller ([3]). I sketch the definition of the family of curves of genus g corresponding to the triangle group $\Delta(n, m, \infty)$ in the special case that n, m are finite and relatively prime. The general case is similar, but somewhat more involved.

Let $N = 2nm$ and consider the family of (projective smooth) curves $\mathcal{Y}$ defined by the Kummer equation

$$y^N = x^{a_1}(x-1)^{a_2}(x-t)^{a_3},$$

where $\{a_1, a_2, a_3, a_4\} = \{nm \pm n \pm m\}$. Here a_4 corresponds to the ramification above ∞. We write $f : \mathcal{Y} \to C \subset \bar{C} := \mathbb{P}^1_t$ for the corresponding family of curves parameterized by t. Let $\mathcal{H} = R^1 f_* \mathbb{C}_{\mathcal{Y}} \otimes_{\mathbb{C}} \mathcal{O}_{\mathbb{C}}$ for the relative de Rham cohomology, and $\mathcal{H}_1$ for the eigenspace of the automorphism $\varphi(x, y) = (x, \zeta_N y)$ with eigenvalue ζ_N. Here $\zeta_N \in \mathbb{C}$ is a primitive Nth root of unity. One can show that $\mathcal{H}_1$ is a rank-2 local system whose projective monodromy group is Γ. Write $S = \{0, 1, \infty\} \subset \bar{C}$ for the set of t for which the fiber $\mathcal{Y}_t$ is singular.

There exists a finite cover $\pi : \bar{D} \to \bar{C}$, exactly branched at S, such that the pullback $\mathcal{Y}_D$ of $\mathcal{Y}$ to $\bar{D}$ has unipotent monodromy. The automorphism group of $\mathcal{Y}_D$ contains a subgroup $G := \mathbb{Z}/N \rtimes (\mathbb{Z}/2 \times \mathbb{Z}/2)$. We choose $H \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ such that the fibers of $\mathcal{X} := \mathcal{Y}_D/H$ have minimal genus. Then $\mathcal{X} \to \bar{D}$ defines a Teichmüller curve.

References

[1] I.I. Bouw and M. Möller, *Teichmüller curves, triangle groups, and Lyapunov invariants*, math.AG/0511738.

[2] C. McMullen, *Billiards and Teichmüller curves on Hilbert modular sufaces*, J. Amer. Math. Soc. 16 (2003), 857–885

[3] Möller, M., *Variations of Hodge structures of Teichmüller curves*, preprint (2004), to appear in J. Amer. Math. Soc.

[4] W. Veech, *Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards*, Invent. Math. 97 (1989), 533–583

[5] C. Ward, *Calculation of Fuchsian groups associated to billiards in a rational triangle*, Ergod. Th. and Dyn. Systems 18 (1998), 1019–1042

$\mathbb{Z}_p$-embeddability of cyclic p-class fields

David Brink

The talk is a report on some results from my Ph.D. thesis (2006).

Denote by $\mathbb{Z}_p$ the additive group of p-adic integers. By a result of Iwasawa, any $\mathbb{Z}_p$-extension of an algebraic number field is unramified outside p. The lower steps of a such extension may very well be unramified also at p. This motivates the following question: *If the p-Hilbert class field of the imaginary quadratic number field K is non-trivial and cyclic over K, is it then embeddable into a $\mathbb{Z}_p$-extension of K?* We have the following result (a criterion in the case $p = 3$ is known):

Theorem 1. *(a) The imaginary quadratic fields K whose 2-class field is non-trivial and embeddable into a $\mathbb{Z}_2$-extension of K are exactly the fields $K = \mathbb{Q}(\sqrt{-l})$ with a prime $l \equiv 5 \pmod 8$, the fields $K = \mathbb{Q}(\sqrt{-2l})$ with a prime $l \equiv 3, 5 \pmod 8$, and the fields $K = \mathbb{Q}(\sqrt{-ll'})$ with two primes $l \equiv 5 \pmod 8$ and $l' \equiv 3 \pmod 8$.*

(b) Assume $p > 3$ and let K be imaginary quadratic. Suppose that K and $K(\zeta)$ have the same non-trivial p-class numbers where ζ is a primitive p'th root of unity. Then the p-Hilbert class field of K is non-trivial cyclic over K and embeddable into a $\mathbb{Z}_p$-extension of K.

When the above theorem does not apply, $\mathbb{Z}_p$-embeddability can be determined by computing the structure of a certain ring class group. For example, it can be shown that the 5-class field of $K = \mathbb{Q}(\sqrt{-166})$ is a $\mathbb{Z}/5$-extension of K which is not $\mathbb{Z}_5$-embeddable (it is not even embeddable into a $\mathbb{Z}/25$-extension of K unramified outside 5) even though it is $\mathbb{Z}/5^n$-embeddable for every $n \in \mathbb{N}$.

Consider an imaginary quadratic number field K and a prime p. K has a unique $\mathbb{Z}_p$-extension which is prodihedral over $\mathbb{Q}$. We call it the *anti-cyclotomic* p-extension of K. We give laws for the decomposition of primes q in the anti-cyclotomic extension. These laws involve representation of some power q^h by certain quadratic forms. Using Gauss' theory of composition of forms, we show that it suffices instead to represent q by some form. The whole story becomes particularly simple when each genus of forms the same discriminant as K consists

of a single class. This happens for 65 discriminants closely connected to Euler's *numeri idonei* or *convenient numbers.* As an application, we show that the splitting field of $f = X^5 + 5X^2 + 3$ is the first step of the anti-cyclotomic 5-extension of $K = \mathbb{Q}(\sqrt{-15})$, and that f splits into linear factors modulo a prime number $q \neq 3, 5$ if and only if q is of the form $x^2 + 5xy + 100y^2$ or $3x^2 + 15xy + 50y^2$.

As a final example, we use prime decomposition in the anti-cyclotomic 2-extensions of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$ to show:

Theorem 2. *Put $K = \mathbb{Q}(\sqrt{-l})$ and $K' = \mathbb{Q}(\sqrt{-2l})$ with a prime $l \equiv 1$ (mod 8). Let h and h' be the class numbers of K and K', respectively. (It is then known that h and h' are both divisible by 4). Now $8 \mid h \Leftrightarrow 8 \mid h'$ for $l \equiv 1$ (mod 16), and $8 \mid h \Leftrightarrow 8 \nmid h'$ for $l \equiv 9$ (mod 16).*

Descent theory for covers and rational points on Hurwitz spaces

Anna Cadoret

Convention: We always denote by k a field of characteristic 0 and assume a compatible system of primitive roots of unity $(\zeta_n)_{n\geq 1}$ ($\zeta_{mn}^m = \zeta_n$, $m, n \geq 1$) is given in a fixed algebraic closure $\overline{k}$ of k.

Given a finite group G and an r-tuple $\mathbf{C}$ of non trivial conjugacy classes of G, let $H(\mathbf{C})(k)$ denote the set of all G-covers of the projective line defined over k, with group G and inertia canonical invariant $\mathbf{C}$. The set $H(\mathbf{C})(k)$ can be equipped with two structures of groupoids:

- The *G-structure*, where an isomorphism between $(f_1 : X_1 \to \mathbb{P}^1_k, \alpha_1)$ and $(f_2 : X_2 \to \mathbb{P}^1_k, \alpha_2)$ is a k-isomorphism $u : X_1 \tilde{\to} X_2$ such that $f_2 \circ u = f_1$ and $\alpha_1(g_1) = \alpha_2(ug_1u^{-1})$, $g_1 \in \mathrm{Aut}(f_1)$.
- The *G/PGL_2-structure*, where an isomorphism between $(f_1 : X_1 \to \mathbb{P}^1_k, \alpha_1)$ and $(f_2 : X_2 \to \mathbb{P}^1_k, \alpha_2)$ is a pair (u, v) with $v \in \mathrm{PGL}_2(k)$ and u a G-cover isomorphism between $(v \circ f_1, \alpha_1)$ and (f_2, α_2).

The groupoid of G-covers admits a coarse moduli space - called *Hurwitz space* $\Psi : \mathcal{H}(\mathbf{C}) \to \mathcal{U}_r$ which is a finite etale cover of the configuration space $\mathcal{U}_r$ of order r subsets of the projective line and is defined over an explicitly computable cyclotomic number field $\mathbb{Q}_{\mathbf{C}}$. The action of PGL_2 over $H(\mathbf{C})$ modulo G-isomorphism produces an algebraic action of the affine reductive $\mathbb{Q}_{\mathbf{C}}$-group PGL_2 on the affine $\mathbb{Q}_{\mathbf{C}}$-varieties $\mathcal{H}(\mathbf{C})$ and $\mathcal{U}_r$ for which the ramification divisor map Ψ is invariant. Hence, via geometric invariant theory, the quotient spaces exist in the category of affine $\mathbb{Q}_{\mathbf{C}}$-varieties

$$\begin{array}{ccc} \mathcal{H}(\mathbf{C}) & \xrightarrow{\Pi} & \mathcal{H}^{rd}(\mathbf{C}) \\ \Big\downarrow{\scriptstyle \Psi} & & \Big\downarrow{\scriptstyle \Psi^{rd}} \\ \mathcal{U}_r & \xrightarrow{\Pi_r} & \mathcal{J}_r \end{array}$$

and the *reduced Hurwitz space* $\mathcal{H}^{rd}(\mathbf{C})$ is the coarse moduli spaces for $\mathrm{G}/\mathrm{PGL}_2$-covers.

When $r = 4$, reduced Hurwitz spaces are curves. *Via* topology, one can compute their geometrically irreducible components and for each such component O^{rd} the ramification data of the normalized cover $\overline{O}^{rd} \to \mathbb{P}^1$. Thus, according to Riemann-Roch theorem, this provides an effective method to find geometrically irreducible components defined and birational to $\mathbb{P}^1$ over $\mathbb{Q}_{\mathbf{C}}$. However, in view of the regular inverse Galois problem, the significant Hurwitz space is not the reduced one but the non-reduced one. This motivates:

Problem: Given $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$, find an optimal upper bound for

$$m_k(\mathbf{p}^{rd}) := \min\{[k(\mathbf{p}) : k]\}_{\mathbf{p} \in \Pi^{-1}(\mathbf{p}^{rd})}$$

Reformulating this problem in moduli terms led me to construct a cohomological obstruction, that is a cohomological object $I_k(\mathbf{p}^{rd}) \subset \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ such that $\mathrm{Res}^{\Gamma_{k_0}}_{\Gamma_k}(I_k(\mathbf{p}^{rd}))$ contains the trivial cohomology class if and only if $\Pi^{-1}(\mathbf{p}^{rd})$ contains a k_0-rational point. The construction of $I_k(\mathbf{p}^{rd})$ rests on the following classification result for finite subgroups of $\mathrm{PGL}_2(\overline{k})$.

Theorem: $\mathrm{PGL}_2(\overline{k})$ contains a Γ_k-invariant copy of C_n, $n \geq 1$, D_{2n}, $n \geq 3$, V_4, $\mathcal{A}_4$, $\mathcal{S}_4$, $\mathcal{A}_5$ and any finite subgroup of $\mathrm{PGL}_2(\overline{k})$ is conjugate to one of these groups.

To any G-cover f defined over $\overline{k}$, associate the *base group* of f that is the stabilizer E_f of the G-isomorphism class of f in $\mathrm{PGL}_2(\overline{k})$. Provided $r \geq 3$, which we will always assume in the following, E_f is finite. Hence it is conjugate to one of the Γ_k-invariant subgroups of the above theorem, which we denote by E_f^0 and call the *normalized base group* of f. A *normalized representative* f^0 of f is a G-cover $\mathrm{G}/\mathrm{PGL}_2$-isomorphic to f such that $E_{f^0} = E_f^0$. Now, assume that f has field of moduli k as $\mathrm{G}/\mathrm{PGL}_2$-cover and pick a normalized representative f^0 of f. Then, for any $\sigma \in \Gamma_k$ there exists a $\mathrm{G}/\mathrm{PGL}_2$-isomorphism (u_σ, v_σ) between ${f^0}^\sigma$ and f^0. Furthermore, the fact E_f^0 is Γ_k-invariant forces v_σ to lie in the normalizer N_f^0 of E_f^0 in $\mathrm{PGL}_2(\overline{k})$. Denote by Q_f^0 the resulting quotient (non-abelian) Γ_k-module N_f^0/E_f^0 then

Lemma: The map $\overline{c}_{f^0}$: $\begin{array}{ccc} \Gamma_k & \to & Q_f^0 \\ \sigma & \to & v_\sigma E_f^0 \end{array}$ is a well-defined 1-cocycle. Furthermore the corresponding cohomological class $[\overline{c}_f] \in \mathrm{H}^1(k, Q_f^0)$ is independent of the choice of the normalized representative f^0.

The cohomology class $\mathrm{Res}^{\Gamma_{k_0}}_{\Gamma_k}([\overline{c}_f])$ is trivial if and only if there is a normalized representative f^0 of f with field of moduli k_0 as G-cover. However, there is no reason why normalized representative should behave better than other representatives with respect to the field of moduli problem. Hence, the "good" cohomological

object is the *cohomological obstruction of f over k* defined by

$$I_k(f) := i(p^{-1}(\tilde{I}_k(f))) \subset \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$$

where, p and i are the natural map induced by functoriality

$$\mathrm{H}^1(k, N_f^0) \xrightarrow{i} \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k})) \quad \text{and} \quad \mathrm{H}^1(k, N_f^0) \xrightarrow{p} \mathrm{H}^1(k, Q_f^0).$$

Now, the lifting problem amounts to studying the vanishing of $I_k(f)$, that is – essentially – to non-abelian Galois cohomology computations.

1- Fields of cohomological dimension ≤ 1:

1-1 If $\mathrm{cd}_2(k) \leq 1$ then the natural map $\mathcal{H}(\mathbf{C})(k) \to \mathcal{H}^{rd}(\mathbf{C})(k)$ is surjective. If, furthermore, $\mathrm{cd}(k) \leq 1$ then the natural map $H(\mathbf{C})(k) \to \mathcal{H}^{rd}(\mathbf{C})(k)$ is surjective (or, in other words, any G-cover with field of moduli k as $\mathrm{G}/\mathrm{PGL}_2$-cover is defined over k) [1].

1-2 Using that a number field is an intersection of field of cohomological dimension ≤ 1, one gets in particular that $\mathbb{Q}_{\mathbf{C}}(\mathbf{p}^{rd}) = \bigcap_{\mathbf{p} \in \Pi^{-1}(\mathbf{p}^{rd})} \mathbb{Q}_{\mathbf{C}}(\mathbf{p})$, for any $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(\overline{\mathbb{Q}})$.

2- p-adic fields:

2-1 Let $k/\mathbb{Q}_p$ be a p-adic field. As Γ_k is finitely generated, $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ is finite and, in particular, there exists an integer $d(k) \geq 1$ depending only on k such that $m_k(\mathbf{p}^{rd}) \leq d(k)$, for any $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$.

2-2 Using that, for a number field $k/\mathbb{Q}$, $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ satisfies the Hasse principle and that when f has trivial base group $|I_k(f)| = 1$, one obtains a restricted Hasse principle. For any $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponding to a G-cover with trivial base group, $\Pi^{-1}(\mathbf{p}^{rd})$ contains a k-rational point if and only if it contains a $\widehat{k^v}$-rational point for each place v of k.

3- The general case: Here, things depend widely on whether the base group is trivial or not.

3-1 Let $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponding to a G-cover with

(i) base group $\mathcal{S}_4$, $\mathcal{A}_5$, D_{2n}, $n \geq 3$ odd (resp. C_n, $n \geq 2$,D_{2n}, $n \geq 3$, $\mathcal{A}_4$, resp. V_4) then $m_k(\mathbf{p}^{rd}) = 1$ (resp. $m_k(\mathbf{p}^{rd}) \leq 2$, resp. $m_k(\mathbf{p}^{rd}) \leq 6$).

(ii) trivial base group then $m_k(\mathbf{p}^{rd}) \leq r!c(r)$, where $c(r)$ denotes the maximal order of a stabilizer of an order r subset of the projective line.

[1] The difficult part of this statement is to ensure that $I_k(f) \neq \emptyset$. This is where the condition $\mathrm{cd}_2(k) \leq 1$ is necessary.

3-2 One can also prove that for any projective system of k-rational points $(\mathbf{p}_n^{rd})_{n\geq 0} \in \varprojlim \mathcal{H}^{rd}(\mathbf{C}_n)(k)$ there exists a finite field extension k_0/k (depending on $(\mathbf{p}_n^{rd})_{n\geq 0}$) such that $(\mathbf{p}_n^{rd})_{n\geq 0}$ can be lifted to a projective system $(\mathbf{p}_n)_{n\geq 0} \in \varprojlim \mathcal{H}(\mathbf{C}_n)(k_0)$.

3-3 (Application to hyperelliptic curves). A ramification divisor version of **3-1** (where stabilizers play the part base groups) yields the following result for hyperelliptic curves. Given an integer $g \geq 2$, there exists an integer $d(g) \geq 1$ such that any genus g hyperelliptic curve X can be defined over a degree $\leq d(g)$ extension of its field of moduli. Furthermore, if $\mathrm{Aut}(X)/ < i >$ is non-cyclic then X is defined over its field of moduli and if $\mathrm{Aut}(X)/ < i >$ is cyclic non trivial then X is defined over a quadratic extension of its field of moduli (where i denotes the hyperelliptic involution).

3-4 When $r = 4$ and k is a number field, the natural map $\Pi_4 : \mathcal{U}_4(k) \to \mathcal{J}_4(k)$ is always surjective because any elliptic curve is defined over its field of moduli. As a result, for any $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponding to a G-cover with ramification divisor $\mathbf{t}$ and normalized base group E, if $j(\mathbf{t}) = 1$ and $E = C_4, D_8$ or if $j(\mathbf{t}) \neq 0, 1$ and $E = V_4$ then $m_k(\mathbf{p}^{rd}) = 1$.

Combining this with the fact that one can read the base group out of the Nielsen class in a purely group theoretical way (regarding the stabilizer of a ramification divisor as a subgroup of the mapping class-group, which allows to identify it with a subgroup of the Hurwitz braid group acting on the Nielsen class) provides group-theoretical effective new rigidity and genus 0 criteria to realize regularly finite groups over $\mathbb{Q}$.

Examples:

- The alternating group $\mathcal{A}_7$ with inertia canonical invariant $(5A, 5A, 5A, 5A)$ over $\mathbb{Q}$ (rigidity).
- The projective special linear group $L_2(19)$ with inertia canonical invariant $(3A, 3A, 3A, 3A)$ over $\mathbb{Q}$ (genus 0).

References

[C05] A. Cadoret, *Lifting results for rational points on Hurwitz moduli spaces*, preprint 2005, available at http://www.math.jussieu.fr/ cadoret.

[CT05] A. Cadoret and A. Tamagawa, *Stratification of Hurwitz spaces by the base invariant*, in preparation.

Galois theory and the arithmetic of hyperbolic 3-manifolds

Ted Chinburg

1. Introduction

This talk was motivated by an analogy appearing in a paper of Sunada [5] between prime closed geodesics P on a compact Riemannian manifold M of negative curvature and non-zero prime ideals $\mathcal{P}$ of the ring of integers $\mathcal{O}_K$ of a number field K. In this analogy, the quantity $N(P) = e^{\text{length}(P)}$ corresponds to the norm $N(\mathcal{P}) = [\mathcal{O}_K : \mathcal{P}]$. One can define zeta functions

$$\zeta_M(s) = \prod_P (1 - N(P)^{-s})^{-1} \quad \text{and} \quad \zeta_K(s) = \prod_{\mathcal{P}} (1 - N(\mathcal{P})^{-s})^{-1}$$

for s having sufficiently large real part, where the products are over all the free homotopy classes of prime closed geodesics P on M in the first case, and over all (non-zero) prime ideals $\mathcal{P}$ of $\mathcal{O}_K$ in the second case.

A method of Perlis [4] constructs non-isomorphic number fields K and K' such that $\zeta_K(s) = \zeta_{K'}(s)$. Sunada observed that the same method leads to examples of non-isometric manifolds M and M' such that $\zeta_M(s) = \zeta_{M'}(s)$. (Examples in which M and M' are hyperbolic surfaces had been constructed earlier by Vigneras [6], following earlier examples of Milnor [3] involving flat tori.) However, the methods of Perlis, Sunada and Vigneras always lead to M and M' which are commensurable, in the sense that they have isometric finite unramified covers. This leads to the following question, which has been of some interest to differential geometers:

Question 1. *If M and M' are compact Riemannian manifolds of negative curvature, and $\zeta_M(s) = \zeta_{M'}(s)$, must M and M' be commensurable?*

In case M and M' are locally symmetric, their zeta functions both determine and are determined by the spectrum of their Laplacian operators. So one could paraphrase this question in this case as being whether one can hear the shape of a commensurability class.

This talk was about the following results, which are a joint work with Emily Hamilton, Darren Long and Alan Reid.

Theorem 1. (CHLR [1]) *If M and M' are arithmetic hyperbolic 3-manifolds and $\zeta_M(s) = \zeta_{M'}(s)$ then M and M' are commensurable.*

The proof hinges on the following result in Galois theory:

Theorem 2. (CHLR [1]) *Suppose F and F' are two number fields each having exactly one complex place and the same normal closure N over $\mathbb{Q}$. Then either F' is isomorphic to F or to a quadratic extension of a totally real subfield F^+ of F such that $[F : F^+] = 2$.*

It is possible that F' and F are not isomorphic. For each $n > 2$ such that $n \equiv 2 \bmod 4$, there is an example in which $\text{Gal}(N/\mathbb{Q})$ is a semidirect product of the symmetric group $S_{n/2}$ with $(\mathbb{Z}/2)^{n/2}$, where $S_{n/2}$ acts on $(\mathbb{Z}/2)^{n/2}$ by permuting

the factors. Thus far, all of the examples we have constructed in which F and F' are not isomorphic have the property that $\zeta_F(s) \neq \zeta_{F'}(s)$; it would be interesting to see whether this must always be true.

Concerning arithmetic counterparts of Question 1, one could consider replacing M and M' by smooth projective varieties X and X' over $\mathbb{Q}$. Let $\zeta_X^{HW}(s)$ be the Hasse-Weil zeta function of X. One could ask:

Question 2. (CHLR [1]) *If $\zeta_X^{HW}(s) = \zeta_{X'}^{HW}(s)$, must X and X' have a common finite branched cover?*

For example, if X and X' are abelian varieties, it is a consequence of Falting's Theorem ([2, Cor. 2]) that $\zeta_X^{HW}(s) = \zeta_{X'}^{HW}(s)$ implies X and X' are isogenous.

2. Proofs

The proof of Theorem 2 involves analyzing the subgroups H of $G = \mathrm{Gal}(N/\mathbb{Q})$ which contain no non-trivial normal subgroup of G and for which N^H has exactly one complex place. Let $\pi : G \to S_n$ be the permutation representation resulting from letting G act on the $n = [F : \mathbb{Q}]$ embeddings of F into $\mathbb{C}$. Define the conjugation graph $\mathcal{C}(H)$ to have vertices $\{1, 2, \ldots, n\}$ and an edge between i and j if and only if the transposition $(i, j) \in S_n$ is a complex conjugation in $\pi(H)$. We show that there is an integer k such that either

i. $k > 2$ and $\mathcal{C}(H)$ is the disjoint union of $\frac{n}{k} - 1$ complete graphs on k vertices with a complete graph on $k - 1$ vertices, or
ii. $k = 2$ and $\mathcal{C}(H)$ is the disjoint union of either $\frac{n}{2}$ or $\frac{n}{2} - 1$ complete graphs on 2 vertices.

Using this description of $\mathcal{C}(H)$ we can limit the possibilities for H up to conjugacy, leading to Theorem 2. For example, in case (i), one shows that H equals the stabilizer of the one vertex of $\mathcal{C}(G)$ which is not joined by an edge of $\mathcal{C}(H)$ to another vertex.

The proof of Theorem 1 reduces to showing the following statement concerning quaternion algebras B over a number field F such that F has exactly one complex place and B ramifies over all the real places of F. One needs to show that F and B are determined up to isomorphism by the set S of square absolute values $|\lambda|^2 \in \mathbb{C}$ of eigenvalues λ of matrices which are the images of elements of B under an embedding $B \to \mathrm{Mat}_2(\mathbb{C})$.

The key step is to show F is determined by S. The field N in Theorem 2 is the intersection of the Galois closures over $\mathbb{Q}$ of the fields $\mathbb{Q}(|\lambda|^2)$ associated to $|\lambda|^2 \in S$, so N is determined by S. In the first case of Theorem 2, F is determined up to isomorphism by N. When one has the second case of Theorem 2, one needs some further arguments, taking advantage of more information than N. In this second case, one shows there is a $|\lambda|^2 \in S$ such that the Galois closure L of $\mathbb{Q}(|\lambda|^2)$ over F^+ is a dihedral extension of F^+ of degree 8. Then F turns out to L^J when J is the unique non-cyclic order 4 subgroup of $\mathrm{Gal}(L/F^+)$ which does not contain $\mathrm{Gal}(L/\mathbb{Q}(|\lambda|^2))$.

References

[1] T. Chinburg, E. Hamilton, D. Long and A. Reid, Arithmetic and iso-length spectral implies commensurability, in preparation (2006).
[2] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), no. 3, 349–366. Erratum: Invent. Math. 75 (1984), no. 2, 381.
[3] J. Milnor, Eigenvalues of the Laplace operator on certain manifolds. Proc. Nat. Acad. Sci. U.S.A. 51 (1964), 542.
[4] R. Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory 9 (1977), 342–360.
[5] T. Sunada, Riemannian Coverings and Isospectral Manifolds, Ann. of Math, (2), 121 (1985), no. 1, 169–186.
[6] M. F. Vigneras, Variétés riemanniennes isospectrales et non isométriques. Ann. of Math. (2) 112 (1980), no. 1, 21–32.

On Fried's modular towers

Pierre Dèbes

Modular towers have been introduced by Michael Fried [Fr1]. They are towers $\underline{\mathcal{H}}(p, G, \underline{C}) : (\mathcal{H}_{n+1} \to \mathcal{H}_n)_{n\geq 0}$ of Hurwitz spaces. Levels $\mathcal{H}_n$ $(n \geq 0)$ correspond to some characteristic quotients $\widetilde{G}_n$ (given by some universal construction) of the p-universal Frattini cover ${}_p\widetilde{G}$ of a fixed finite group G; p is a prime divisor of $|G|$ such that G is p-perfect, *i.e.*, generated by its elements of prime-to-p order; $\underline{C}$ is at each level the unique lift of some given tuple of conjugacy classes of prime-to-p order of $G_0 = G$; $\mathcal{H}_n = \mathcal{H}_n(\widetilde{G}_n, \underline{C})$ is then the Hurwitz moduli space of G-covers of $\mathbf{P}^1$ with group $\widetilde{G}_n$ and ramification type $\underline{C}$ and the map $\mathcal{H}_{n+1} \to \mathcal{H}_n$ is induced by the natural surjection $\widetilde{G}_{n+1} \to \widetilde{G}_n$. There is an abelianized variant $\underline{\mathcal{H}}(p, G, \underline{C})^{\mathrm{ab}}$ (introduced in [Ca]) for which the groups $\widetilde{G}_n$ are replaced by some abelian quotients $\overline{G}_n$ obtained by abelianizing the kernel of the natural projection ${}_p\widetilde{G} \to G$, and there are reduced variants of these towers for which covers are considered modulo the action of PGL_2 on the base space $\mathbf{P}^1$.

The following conjecture is a main goal of the modular tower program.

Main Conjecture on Modular Towers: *For every number field k, there are no k-rational points on suitably high levels of the reduced abelianized modular tower (and consequently of any other variant of modular tower).*

The tower of modular curves $X^1(p^n)$ $(n > 0)$ is the original example: the group G is then the dihedral group D_p given with its involution conjugacy class repeated 4 times. In this case the conjecture is a classical result on modular curves, or in other words, on torsion of elliptic curves.

The Main Conjecture has significant implications for the Regular Inverse Galois Problem.

Theorem (Fried-Kopeliovich [FrKo], Cadoret [Ca])**:** *Given $r_0 \geq 3$, suppose each characteristic quotient $\widetilde{G}_n$ (resp. each $\overline{G}_n$) can be regularly realized over $\mathbf{Q}(T)$ with no more than r_o branch points. Then there exist $r \leq r_0$ and an r-tuple*

$\underline{C}$ of conjugacy classes of prime-to-p order of G such that each $\widetilde{G}_n$ (resp. each $\overline{G}_n$) can be regularly realized over $\mathbf{Q}(T)$ with ramification type $\underline{C}$, or, in other words, such that the modular tower $\underline{\mathcal{H}}(p, G, \underline{C})$ (resp. the abelianized modular tower $\underline{\mathcal{H}}(p, G, \underline{C})^{\mathrm{ab}}$) has $\mathbf{Q}$-rational points at every level. As a consequence, under the Main Conjecture, only finitely many groups $\overline{G}_n$ can be regularly realized over $\mathbf{Q}(T)$.

Genralizing the orginal dihedral example, a bridge has been established between the non abelian Galois world of Modular Towers and the arithmetic of Abelian Varieties: rational points on modular towers are connected to torsion points on abelian varieties. In particular, it was proved by A. Cadoret that the

Strong Torsion Conjecture: *Given $g, d \geq 1$, there exists $n(d, g) \geq 1$ such that there is no abelian variety of dimension $\leq g$ defined over a number field of degree $\leq d$ and carrying a k-rational torsion point of order $n \geq n(d, g)$.*

implies the Main Conjecture on modular towers. Using the same connection, one can also prove a first stage of the Main Conjecture:

Theorem 1 (Bayley-Fried[BaFr], Cadoret [Ca], Kimura[Ki]) *Given any number field k, there is no projective system of k-rational points on the reduced abelianized modular tower.*

This result was recently improved:

Theorem 2 (Cadoret [Ca]) *Let k be a number field, F a function field of one variable over k and $\widetilde{G}$ a profinite extension of a finite group by a free pro-p group with at least a $\mathbf{Z}_p$ quotient. Then there is no regular realisation of $\widetilde{G}$ over F.*

The link with abelian varieties goes both ways. Using results of Flynn on existence of $\mathbf{Q}$-rational points of arbitrarily large order on jacobians of hyperelliptic curves, A. Cadoret proved the following statement:

Theorem 3 (Cadoret [Ca]) *For every integer $n \geq 2$, the dihedral group D_n can be regularly realized over $\mathbf{Q}^{\mathrm{ab}}$ with only inertia groups of order 2.*

There is a significant special case of the general program which seems close to completion: the case of 4 branch points covers. Levels of reduced modular towers then are curves and due to Faltings' theorem we have this conclusion:

Proposition (Bayley-Fried [BaFr])**:** *The Main Conjecture for modular towers holds for $r = 4$ provided that the genus gets ≥ 2 in every Projective System of irreducible Components in the modular tower.*

However checking that the genus grows along a modular tower is extremely difficult. The genus is given by the Riemann-Hurwits formula but the group action involved — a braid action — is quite intricate. One should control the growth of

the ramification indices, notably at points above ∞ — the cusps — on the tower. There are both a profinite group-theoretic aspect and a geometric aspect and one should understand the interaction. This part of the theory has been M. Fried's current work [Fr2].

Over ℓ-adic fields, the situation is interestingly quite the opposite.

Theorem 4 (Dèbes-Deschamps [DeDes] & Dèbes-Emsalem [DeEm]) *Assume* $\underline{C}$ *is* $\mathbf{Q}$*-rational and of Harbater-Mumford (HM) type:* $\underline{C} = \{C_1, C_1^{-1}, \dots, C_s, C_s^{-1}\}$.

Let k *be a henselian field of characteristic* 0*, of residue characteristic* $\ell \geq 0$ *and containing all* N*th roots of* 1 *with* $N = \text{l.c.m.}(\text{ord}(C_1), \dots, \text{ord}(C_s))$.

(a) *There exist projective systems of* k*-rational points on the modular tower.*

(b) *If in addition* $\underline{C}$ *is "HM-g-complete", such projective systems can be found on a HM Projective System of Components defined over* $\mathbf{Q}$.

For ample fields however, the analog of statement (a) is unclear.

The Modular Tower program is still at a growing stage. It has revealed some deep diophantine obstructions to the Regular Inverse Galois Problem but has also provided some tools to understand them.

References

[BaFr] P. Bailey and M. Fried, *Hurwitz monodromy, spin separation and higher levels of a modular tower*, Proceedings of the Von Neumann Symposium on Arithmetic Fundamental Groups and Noncommutative Algebra (MSRI 1999), Proceedings of Symposia in Pure Mathematics,**7**0, AMS, ed. by M. Fried and Y. Ihara, (2002), 70–220.

[Ca] A. Cadoret, *Modular towers and torsion on abelian varieties*, preprint.

[De] P. Dèbes, *An introduction to the modular tower program*, in *Groupes de Galois arithmétiques et différentiels* (Luminy 2004; eds. D. Bertrand and P. Dèbes), *Séminaires et Congrès*, **13**, SMF, (to appear).

[DeDes] P. Dèbes and B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, J. für die reine und angew. Math., **5**74, (2004), 197–218.

[DeEm] P. Dèbes and M. Emsalem, *Harbater-Mumford Components and Hurwitz Towers*, J. Math. Inst. Jussieu, (to appear).

[Fr1] M. Fried, *Introduction to modular towers*, in *Recent Developments in the Inverse Galois Problem*, Contemporary Math., **1**86, (1995), 111–171.

[Fr2] M. Fried, *The Main Conjecture of modular towers and its higher rank generalization*, in *Groupes de Galois arithmétiques et différentiels* (Luminy 2004; eds. D. Bertrand and P. Dèbes), *Séminaires et Congrès*, **13**, SMF, (to appear).

[FrKo] M. Fried and Y. Kopeliovich, *Applying modular towers to the inverse Galois problem*, in textit Geometric Galois Action, London Math. Soc. Lecture Note Series **2**43, L. Schneps and P. Lochak ed., Cambridge University Press, (1997), 151–175.

[Ki] K. Kimura, *Modular towers for finite groups that may not be centerfree*, Master Thesis (Kyoto Univ. March 2004), english translation as of 09/05.

Geometric Galois representations and the inverse Galois problem

Michael Dettweiler

The convolution

$$f * g\,(y) := \int f(x)g(y-x)dx$$

of sufficiently integrable functions plays an important role in many areas of mathematics and physics.

Suppose that the functions f and g are solutions of meromorphic connections on the complex affine line $\mathbb{A}^1$. Then f and g can be viewed as sections of the solution sheaves of these connections. The comparison theorem between singular cohomology and de Rham cohomology shows that the integral

$$\int_\gamma f(x)g(y_0-x)dx, \quad \text{where} \quad y_0 \in \mathbb{A}^1\,,$$

can be seen as a cohomology class in the sheaf cohomology on $\mathbb{A}^1$. This suggests the following generalization from the convolution of functions to the convolution of sheaves V_1, V_2 on $\mathbb{A}^1$:

$$V_1 *_{\text{aff}} V_2 := R^1\text{pr}_{2*}(V_1 \circ V_2)\,.$$

Here, $\text{pr}_2 : \mathbb{A}^2 \to \mathbb{A}^1$ denotes the second projection of $\mathbb{A}^2 = \mathbb{A}^1_x \times \mathbb{A}^1_y$, $R^1\text{pr}_{2*}$ is the first higher direct image of the functor pr_{2*}, and

$$V_1 \circ V_2 := \text{pr}_1^*(V_1) \otimes \text{d}^*(V_2)\,,$$

where $\text{pr}_1 : \mathbb{A}^2 \to \mathbb{A}^1$ is the first projection and $\text{d} : \mathbb{A}^2 \to \mathbb{A}^1$ is the difference map $(x, y) \mapsto y - x$.

Let us assume that V_1 and V_2 are sheaves on $\mathbb{A}^1$ which are pushforwards of local systems on open subsets of $\mathbb{A}^1$. Such sheaves naturally arise as the sheaves of solutions of connections on $\mathbb{A}^1$. Then the "affine" convolution $V_1 *_{\text{aff}} V_2$ contains a canonical subsheaf

$$\text{im}\left(R^1\text{pr}_{2!}(V_1 \circ V_2) \;\longrightarrow\; R^1\text{pr}_{2*}(V_1 \circ V_2)\right)\,,$$

where $R^1\text{pr}_{2!}$ denotes the first higher direct image with compact supports. The latter sheaf is canonically isomorphic to $R^1\overline{\text{pr}}_{2*}(j_*(V_1 \circ V_2))$, where $j : \mathbb{A}^2 \to \mathbb{P}2^1 \times \mathbb{A}^1$ denotes the natural inclusion and $\overline{\text{pr}}_{2*} : \mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ is the second projection. We set

$$V_1 * V_2 := R^1\overline{\text{pr}}_{2*}(j_*(V_1 \circ V_2))\,. \tag{0.1}$$

Following Katz (*Rigid Local systems*, Ann. Math. Studies 139 (1996)), we call the sheaf $V_1 * V_2$ the *middle convolution* of V_1 and V_2. (In loc. cit., Katz gives a similar construction in a more general category of complexes of sheaves.) The term *middle* indicates the fact that there is a natural interpretation of $V_1 * V_2$ as a middle direct image, i.e., one obtains the middle convolution by taking the image

of the cohomology with compact supports in the cohomology.

The formulation of the convolution in terms of sheaf cohomology has the advantage that this construction works similarly also in different categories, e.g., in the category of étale local systems. The latter category corresponds to the category of Galois representations of étale fundamental groups (this yields the connection of the middle convolution to the inverse Galois problem).

The relevance of the middle convolution for the inverse Galois problem was first noticed by S. Reiter and the speaker of the talk (*An algorithm of Katz and its application to the inverse Galois problem*, J. Symb. Comb. 30 (2000)). Also, it turned out that most of the older results on Galois realizations of classical groups (including the famous results of Belyi) can easily be derived using the middle convolution. A similar approach is given by Völklein's *braid companion functor* (*The braid group and linear rigidity*, Geom. Dedicata 84 (2001)).

Although the middle convolution is, up to date, the strongest tool to realize classical groups regularly as Galois groups over $\mathbb{Q}(t)$, the existing methods have some limitations: Most of the time only the topological information is available and it is not possible to obtain more precise information (like the determination of Frobenius elements acting on specializations). Also, in many cases the existing methods fail to produce simple groups like the projective special linear groups $\mathrm{PSL}_n(\mathbb{F}_q)$ as Galois groups over $\mathbb{Q}(t)$. The problem is that if the index of $\mathrm{PSL}_n(\mathbb{F}_q)$ in $\mathrm{PGL}_n(\mathbb{F}_q)$ is > 1, then it is usually impossible to bound the arithmetic part of the underlying Galois representations.

Based on methods of Katz and on previous work of S. Wewers (*Variation of local systems and parabolic cohmology*, to appear in Israel J. Math.) and the speaker, in the Habilitation Thesis of the speaker (*Galois realizations of classical groups and the middle convolution,* Heidelberg (2005)), there is given a geometric approach to the middle convolution in order to overcome the above mentioned limitations of the existing methods. This approach gives a geometric (motivic) interpretation of ℓ-adic sheaves which are obtained via the middle convolution process, by considering higher direct images of fibre products of Galois covering maps of the punctured Riemann sphere.

Using this approach, one obtains valuable information on the occurring determinants, leading to new Galois realizations of special linear groups. Moreover, computation of Frobenius elements for many of the known Galois realizations of classical groups is now possible. Together with a deep theorem of Henniart on the algebraicity of one-dimensional compatible systems and the theory of Hecke characters, one obtains the following result:

Theorem I. *Let F_1, F_2, F_3, G be irreducible and non-trivial E_λ-valued étale local systems on punctured affine lines over $\mathbb{Q}$ having finite monodromy. Let*

$$V = ((F_1 * F_2) \otimes G) * F_3 \,,$$

and let $\rho_V : \pi_1^{\mathrm{geo}}(S) \rtimes G_{\mathbb{Q}} \to \mathrm{GL}(V)$ be the Galois representation associated to V. Assume that the geometric monodromy is irreducible and infinite. Then the determinant of ρ_V is of the form

$$\det(\rho_V) = \det(\rho_V)|_{\pi_1^{\mathrm{geo}}(S)} \otimes \chi_\ell^m \otimes \epsilon \,.$$

Here, $\chi_\ell : G_{\mathbb{Q}} \to \mathbb{Q}_\ell$ denotes the ℓ-adic cyclotomic character, m is an integer, and $\epsilon : G_{\mathbb{Q}} \to E^\times$ is a finite character.

The description of the determinant in Thm. I is crucial for the next result:

Theorem II. *Let $\mathbb{F}_q$ be the finite field of order $q = \ell^k$, where $k \in \mathbb{N}$. Then the special linear group $\mathrm{SL}_{2n+1}(\mathbb{F}_q)$ occurs regularly as Galois group over $\mathbb{Q}(t)$ if*

$$q \equiv 5 \mod 8 \quad \textit{and} \quad n > 6 + 2\varphi((q-1)/4)$$

(φ denoting Euler's φ-function).

Thm. II implies that, under the conditions of the theorem, the simple group $\mathrm{PSL}_{2n+1}(\mathbb{F}_q)$ occurs regularly as Galois group over $\mathbb{Q}(t)$. The latter result is the first result on regular Galois realizations of the groups $\mathrm{PSL}_n(\mathbb{F}_q)$ over $\mathbb{Q}(t)$, where

$$(n, q-1) = [\mathrm{PGL}_n(\mathbb{F}_q) : \mathrm{PSL}_n(\mathbb{F}_q)] > 2 \,.$$

The idea of the proof of Thm. II is the following: By our assumptions, the finite field $\mathbb{F}_q$ is generated over its prime field $\mathbb{F}_\ell$ by an element of odd order m. Let

$$E := \mathbb{Q}(\zeta_m + \zeta_m^{-1}, i) \,,$$

where $m = (q-1)/4$, where ζ_m denotes a primitive m-th root of unity, and where i is a primitive fourth root of unity. Let λ be a prime of E lying over ℓ. One considers E_λ-valued étale local systems F_1, F_2, F_3, G associated to Galois representations with values in the dihedral group of order $2m$ and to Galois representations with values in cyclic groups of order 2 and 4. Then one forms their convolution

$$V = ((F_1 * F_2) \otimes G) * F_3 \in \mathrm{LS}^{\text{ét}}_{E_\lambda}(S) \,.$$

Let $\rho_V : \pi_1^{\text{ét}}(S) \to \mathrm{GL}(V)$ be the Galois representation associated to V and let O_λ be the valuation ring of E_λ. Using analytification and reduction modulo λ, one can show that the image of the geometric fundamental group under ρ_V is, up to scaling, isomorphic to $\mathrm{SL}_{2n+1}(O_\lambda)$. Here, n depends on m, enforcing the condition $n > 6+2\varphi(m)$. Since m is odd, the only roots of unity which are contained in E are fourth roots of unity. It then follows from Thm. I that the occurring determinants which arise from $G_{\mathbb{Q}} \leq \pi_1^{\text{ét}}(S)$ are, up to a twist with the cyclotomic character, contained in the group of fourth roots of unity. Thus by a twist with a suitable finite character of order four, one can assume that the image of the whole étale

fundamental group $\pi_1^{\text{ét}}(S)$ is equal to $\mathrm{SL}_{2n+1}(O_\lambda)$. The result then follows from reduction modulo λ and from the interpretation of $\pi_1^{\text{ét}}(S)$ as a factor of $G_{\mathbb{Q}(t)}$.

A generalization of Marshall's equivalence relation

Ido Efrat

Let p be a prime number, let F be a field of characteristic $\neq p$, and let $G_F(p) = \mathrm{Gal}(F(p)/F)$ be its maximal pro-p Galois group. One of the rare cases where the group-theoretic structure of $G_F(p)$ is completely understood is when $p = 2$, F is Pythagorean, and $G_F(2)$ is finitely generated as a pro-2 group (recall that F is *Pythagorean* if every sum of squares in F is already a square). This is by striking results of B. Jacob [4], which are based on a decomposition theory for the so-called "spaces of orderings", due to M. Marshall [5].

Specifically, let X_F be the set of orderings on F, i.e., all additively closed subgroups of $F^\times$ of index 2. Call $P_1, P_2 \in X_F$ *Marshall–equivalent* if $P_1 = P_2$, or there exist $P_3, P_4 \in X_F$ such that P_1, P_2, P_3, P_4 are distinct, and the intersection of any three of them equals the intersection of all four; as shown in [5] this is indeed an equivalence relation on X_F.

For F Pythagorean and for a Marshall-equivalence class C in X_F one associates a *closure* $F \subseteq \hat{F} \subseteq F(2)$ as follows: When C consists of a single ordering P we take $\hat{F}$ to be a Euclidean closure of F at P, i.e., a relative real closure of (F, P) inside $F(2)$. When $1 < |C| < \infty$ there exists a valuation v on F with non-2-divisible value group, such that C consists of all orderings containing the 1-units of v. We then take $\hat{F}$ to be a decomposition field of v inside $F(2)$. When $|C| = \infty$ one takes $\hat{F}$ to be an intersection of a (well-chosen) collection of decomposition fields of such valuations corresponding to subsets of C (see [1]).

The Jacob–Marshall theory shows that for F Pythagorean with $G_F(2)$ finitely generated, the partition of X_F into equivalence classes corresponds to a free pro-2 product decomposition of $G_F(2)$ as follows (see [1] for a generalization to the infinite rank case):

(1) if $\hat{F}$ is a closure of F at an equivalence class C, then $G_{\hat{F}}(2)$ cannot be decomposed as a free pro-2 product in a nontrivial way;
(2) there exist closures $\hat{F}_1, \ldots, \hat{F}_n$ of F at the distinct equivalence classes of X_F such that $G_F(2) = G_{\hat{F}_1}(2) *_2 \cdots *_2 G_{\hat{F}_n}(2)$;
(3) if $H_1, \ldots, H_n$ are closed subgroups of $G_F(2)$ with $G_F(2) = H_1 *_2 \cdots *_2 H_n$, then each H_i is generated by subgroups of the form $G_{\hat{F}}(2)$, where $\hat{F}$ is a closure of F at some equivalence class;
(4) if C is a Marshall-equivalence class in X_F with closure $\hat{F}$, then C is the image of the restriction map $X_{\hat{F}} \to X_F$, $\hat{P} \mapsto F \cap \hat{P}$.

Now the structure of the free pro-2 factors in (2) is known; namely, when $|C_i| = 1$, $G_{\hat{F}_i}(2) \cong \mathbb{Z}/2$. When $|C_i| > 1$, the valuation yielding $\hat{F}_i$ has a real Pythagorean residue field $\bar{F}_i$. By the Galois theory of valued fields, $G_{\hat{F}_i}(2) \cong \mathbb{Z}_2^m \rtimes G_{\bar{F}_i}(2)$

where $m = \dim_{\mathbb{F}_2}(v(F^\times)/2v(F^\times))$ and where the action of $G_{\bar{F}_i}(2)$ on $\mathbb{Z}_2^m$ is given by multiplication by the cyclotomic character. Since $G_{\bar{F}_i}(2)$ is generated by fewer elements than $G_{\hat{F}_i}(2)$, we inductively obtain in this way a complete *group-theoretic* description of $G_F(2)$

In our talk we explained how to generalize this theory from the case of orderings on Pythagorean fields to the case of arbitrary subgroups of $F^\times$ of index p, where F is an arbitrary field of characteristic $\neq p$ containing the pth roots of unity. Our generalized equivalence relation is defined by valuation-theoretic means. In this generalized set-up, (1), (3) and (4) extend to free pro-p decompositions of $G_F(p)$. Further, one can handle the infinite rank case by "iterated" decomposition fields, as above. The expected generalization of (2) turns out to be equivalent to the arithmetic pro-p version of the *"Elementary Type Conjecture"* (see [2], Question 4.8). This conjecture says that if $G_F(p)$ is finitely generated then it is a free pro-p product of subgroups which are isomorphic to $\mathbb{Z}_p$, $\mathbb{Z}/2$ (when $p = 2$), or are decomposition groups of valuations with nontrivial inertia group. Various variants of this conjecture were studied in numerous works over the past 25 years, and it is known to hold, e.g., for global fields, fields of transcendence degree ≤ 1 over a local field, and fields of transcendence degree ≤ 1 over a PAC field. It implies a group-theoretic description of the finitely-generated groups $G_F(p)$ for fields F containing a pth root of unity, similarly to the Pythagorean case discussed above.

These results will appear in [3]

References

[1] I. Efrat, *Free product decompositions of Galois groups over Pythagorean fields*, Comm. Algebra **21** (1993), 4495–4511.

[2] I. Efrat, *Pro-p Galois groups of algebraic extensions of* $\mathbb{Q}$, J. Number Theory **64** (1997), 84–99.

[3] I. Efrat, *A generalization of Marshall's equivalence relation*, Trans. Amer. Math. Soc. **358** (2006), 2561–2577.

[4] B. Jacob, *On the structure of Pythagorean fields*, J. Algebra **68** (1981), 247–267.

[5] M. Marshall, *Abstract Witt Rings*, Queen's Papers in Pure and Applied Mathematics **57**, Queen's University, Kingston, 1980.

Continuity of roots over valued fields

Yuri Ershov

Let F be a field, R be an henselian valuation ring over F, $\bar{R}$ be the extension of R given by the algebraic closure $\bar{F}$ of F, v be the valuation of $\bar{F}$ defined by $\bar{R}$.

Basic Proposition (BP). *Let $f \in F[x]$ be a monic polynomial, $a \in F$ and let $\alpha \in \bar{F}$ be a zero of f nearest to a, i.e.*

$$v(a-\alpha) = \max\{v(a-\alpha') \mid f(\alpha') = 0, \alpha' \in \bar{F}\}.$$

Then the following is true:

a) *The inequalities $vf(a) \leq v(a-\alpha)+vf'(a)$, $vf(a) \leq v(a-\alpha)+vf'(\alpha)$ hold;*

b) *if α is unique, i.e. $f'(\alpha) \neq 0$ and $v(a-\alpha) > v(a-\alpha')$ for all $\alpha' \neq \alpha$, $f(\alpha') = 0$, then $\alpha \in F$ and $vf(a) = v(a-\alpha) + vf'(a)$, $vf'(a) = vf'(\alpha)$.*

If $f(x) = \prod_{i<n}(x-\alpha_i)$, put $\sigma_{f,\alpha_i} := vf'(\alpha_i) + \max\{v(\alpha_i - \alpha_j) \mid i \neq j\}$.

Corollary. *Let $a \in F$ and $\alpha \in \bar{F}$ as in BP; if $vf(a) > \sigma_{f,\alpha}$ then case b) of BP holds and $v(a-\alpha) = vf(a) - vf'(a) > v(\alpha - \alpha')$ for any $\alpha' \neq \alpha$, $f(\alpha') = 0$.*

Put $\sigma_f := \max\{\sigma_{f,\alpha_i} \mid i < n\}$, $\kappa_f := \max\{v(\alpha_i - \alpha_j) \mid i < j < n\}$ and $\Delta_f := \max\{vf'(\alpha_i) \mid i < n\}$.

Then $\sigma_{f,\alpha_i} \leq \sigma_f \leq \kappa_f + \Delta_f \leq v\delta_f$, where δ_f is the discriminant of f.

Theorem 1. *Let $f \in F[x]$ be a monic separable polynomial and $a \in F$ be such that $vf(a) > \sigma_f$. Then there is a root α of f in F such that $v(a-\alpha) = vf(a) - vf'(a) > v(a-\alpha')$ for any $\alpha' \neq \alpha$, $f(\alpha') = 0$.*

Proof. Take α as in BP, then use the corollary.

Theorem 2. *Let $f, g \in R[x]$ be monic polynomials, $n = \deg f = \deg g$, f separable and $v(f-g) > \delta = \varepsilon + \Delta_f$, $\varepsilon \geq \sigma_f$. Then g is separable, $\sigma_g = \sigma_f$, $\Delta_g = \Delta_f$, and if $\alpha_0, \ldots, \alpha_{n-1}$ are all roots of f then it is possible to enumerate the roots $\beta_0, \ldots, \beta_{n-1}$ of g in such a way that $v(\alpha_i - \beta_i) > \varepsilon$.*

Pseudo-$\mathcal{S}$ closed extensions of Hilbertian fields

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

This is a report on a work in progress.

Let K be a countable Hilbertian field of characteristic 0 (e.g. a finitely generated extension of $\mathbb{Q}$) and S a finite set of inequivalent absolute values of K. For each $v \in S$ let $\hat{K}_v$ be the completion of K at v. Assume that the fields $\hat{K}_v$ with $v \in S$ as well as the algebraic closure $\tilde{K}$ of K are embedded in a common algebraically closed field. Then let $K_v = \tilde{K} \cap \hat{K}_v$. Thus, K_v is a real closure or the algebraic closure of K at v, if v is metric, and a Henselian closure of K at v, if v is ultrametric. Let $\tau = (\tau_1, \ldots, \tau_e) \in \mathrm{Gal}(K)^e$. Denote by $L = K_{\mathrm{tot},S}[\tau]$ the maximal Galois extension of K contained in all the K_v and fixed by $\tau_1, \ldots, \tau_e$.

Our aim is to describe the absolute Galois group $\mathrm{Gal}(K_{\mathrm{tot},S}[\tau])$ of this field. More exactly, we want to prove

Theorem A. *For almost all τ (in the sense of the Haar measure on $\mathrm{Gal}(K)^e$)*

$$\mathrm{Gal}(K_{\mathrm{tot},S}[\tau]) \cong \hat{F}_\omega * \coprod_{v \in S} \coprod_{\sigma \in \Sigma_v} \mathrm{Gal}(K_v^\sigma). \tag{1}$$

For this purpose we are firstly interested in case $e = 0$, which reads as follows:

Theorem B. *Let $K_{\mathrm{tot},S}$ be the* **field of totally S-adic numbers**, *that is, the maximal Galois extension of K in which each $v \in S$ totally splits. Then*

$$\mathrm{Gal}(K_{\mathrm{tot},S}) = \coprod_{v \in S} \coprod_{\sigma \in \Sigma_v} \mathrm{Gal}(K_v^\sigma). \tag{2}$$

for some closed subsets Σ_v of $\mathrm{Gal}(K)$.

Pop [1] proves this result (under more general assumptions). However, that proof is indirect – and hence does not lead to (1):

Let $S' = S \cup \{v'\}$, where v' is an absolute value of K inequivalent to any of the absolute values of S. Then the field $K_{\mathrm{tot},S'}$ is a Galois extension of K which is properly contained in $K_{\mathrm{tot},S}$. One can choose a Hilbertian extension L of $K_{\mathrm{tot},S'}$ in $K_{\mathrm{tot},S}$ such that $LK_{v'}$ is the algebraic closure of K.

Now, $K_{\mathrm{tot},S'}$ is pseudo closed with respect to the family $\{K_v^\sigma \mid v \in S', \sigma \in \mathrm{Gal}(K)\}$. Therefore L is pseudo closed with respect to $\{LK_v^\sigma \mid v \in S', \sigma \in \mathrm{Gal}(K)\}$. As $LK_v^\sigma = K_v^\sigma$ for $v \in S$ and $LK_{v'}$ is the algebraic closure of K, we get that L is pseudo closed with respect to $\{K_v^\sigma \mid v \in S, \sigma \in \mathrm{Gal}(K)\}$. This has two consequences:

(a) $\mathrm{Gal}(L)$ is projective with respect to $\{\mathrm{Gal}(K_v^\sigma) \mid v \in S, \sigma \in \mathrm{Gal}(K)\}$
and

(b) every finite split embedding problem over L has a solution over $L(t)$.
But L is Hilbertian, hence

(c) every finite split embedding problem over L has a solution (over L).

A heavy Iwasawa-like argument then allows to deduce from (a) and (c) that

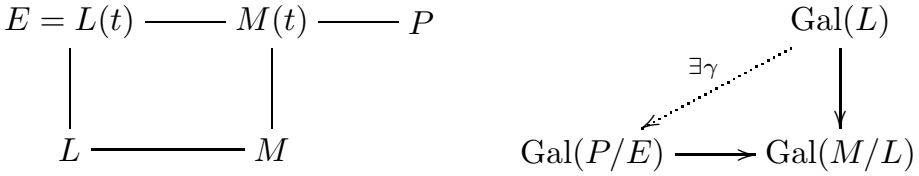
$$\mathrm{Gal}(L) \cong \hat{F}_\omega * \coprod_{v \in S} * \coprod_{\sigma \in \Sigma_v} \mathrm{Gal}(K_v^\sigma), \tag{2}$$

where Σ_v is a closed system of representatives of $\mathrm{Gal}(K)/\mathrm{Gal}(K_{\mathrm{tot},S})$. It is now possible to recognize $\mathrm{Gal}(K_{\mathrm{tot},S})$ in $\mathrm{Gal}(L)$ as the second factor of the free product on the right hand side. Thus we get (2).

As a first step in our programme, we supply a direct proof of Theorem A:

Put $L = K_{\mathrm{tot},S}$. Then (a) , (b) hold. Also —instead of (c)—

(c') L is "$\mathcal{S}$-Hilbertian": Consider an embedding problem



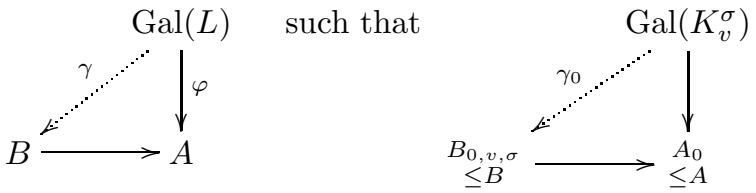
on the right, which arises from the diagram of fields on the left; here M/L and $P/E = L(t)$ are finite Galois extensions such that $M \subseteq P$. Then there exists a homomorphism γ which solves the embedding problem on the right handed side such that

$$\gamma(\{\mathrm{Gal}(K_v^\sigma) \mid v \in \sigma \in \mathrm{Gal}(K)\}) = \{\mathrm{Gal}(P/P \cap E_w^\tau) \mid v|w, v \in S, \tau \in \mathrm{Gal}(E)\}.$$

In particular, if $\mathrm{Gal}(P)$ is generated by the right handed side, then γ must be an epimorphism.

Use (a),(b) to deduce from (c'):

(d) Consider an embedding problem



in which $B = \langle B_{0,v,\sigma} \mid v\sigma \rangle$. Then there is an epimorphism $\gamma\colon \mathrm{Gal}(L) \to B$ such that $\alpha \circ \gamma = \varphi$ and $\gamma(\{\mathrm{Gal}(K_v^\sigma) \mid v, \sigma\}) = \{B_{0,v,\sigma} \mid v\sigma\}$.
Finally, we use an analog of Iwasawa Theorem:

(e) (1) There is a unique second countable profinite group, which, together with a distinguished family of closed subgroups, satisfies (d).
(2) The group $\coprod_{v\in S} \coprod_{\sigma\in\Sigma_v} \mathrm{Gal}(K_v^\sigma)$ satisfies (d), hence $\mathrm{Gal}(L)$ is isomorphic to it.

The proof of our type of Iwasawa's theorem relies heavily on the assumption that the local groups are finitely generated. This restricts K in our result to be of characteristic 0.

References

[1] F. Pop, *Embedding Problems Over Large Fields*, Annals of Mathematics **144** (1996), 1–34.

Local Galois theory in dimension two

David Harbater and Katherine F. Stevenson

This talk proves a generalization of Shafarevich's Conjecture, for fields of Laurent series in two variables over an arbitrary field. This result says that the absolute Galois group G_K of such a field K is *quasi-free* of rank equal to the cardinality of K, i.e. every non-trivial finite split embedding problem for G_K has exactly $\mathrm{card}\, K$ proper solutions. We also strengthen a result of Pop and Haran-Jarden on the existence of proper regular solutions to split embedding problems for curves over large fields; our strengthening concerns integral models of curves, which are two-dimensional.

Let k be a field and let $K = k((x,y))$ with absolute Galois group $G_K = \mathrm{Gal}(K^{sep}/K)$. For this field, the inverse Galois problem asks which finite groups G occur as Galois groups over K, or equivalently as images of surjective homomorphisms $\alpha : G_K \to G$. The answer is that *all* finite groups occur in this way [8]. Thus it is natural to ask how these surjections "fit together." To make the question more precise we consider embedding problems for G_K. A *finite embedding problem* (FEP) for G_K is a pair of surjections $(\alpha : G_K \to G,\ f : \Gamma \to G)$. A *weak solution* to $(\alpha,\ f)$ consists of a homomorphism $\lambda : G_K \to \Gamma$ such that $f \circ \lambda = \alpha$. A solution is called *proper* if it is surjective. Notice that a proper solution to (α, f) corresponds to a Γ-Galois field extension of K that dominates the given G-Galois extension corresponding to α.

A finite embedding problem (α, f) for which there is a splitting $s : G \to \Gamma$ of f is called a *finite split embedding problem* (FSEP). Notice that every finite split embedding problem has a weak solution given by $s \circ \alpha$. A profinite group Π is called *projective* if every FEP for Π has a weak solution. This is equivalent to saying that every FEP is dominated by a FSEP.

Theorem 1 (Chatzidakis, Melnikov [2])**.** *Given a profinite group* Π *and an infinite cardinal* m*,* Π *is free of rank* m *if and only if every non-trivial finite embedding problem has exactly* m *solutions.*

One application of this theorem appeared in the result of Harbater [4] and Pop [9] that if k is an algebraically closed field then $G_{k(x)}$ is free of rank card $k(x)$. This proof used that that $G_{k(x)}$ is projective (being of cohomological dimension 1), along with patching techniques for curves over $k((t))$, to build a proper solution from the weak solution (provided by projectivity). For $k = \bar{\mathbb{F}}_p$, this result is the geometric (function field) case of the following conjecture of Shafarevich.

Conjecture 1 (Shafarevich)**.** *If* K *is a global field then* $G_{K^{\mathrm{cycl}}}$ *is free of countable rank.*

The arithmetic (number field) case of this conjecture remains open.

Given an embedding problem $\mathcal{E} = (\alpha, f)$ for a profinite group Π, let $PS(\mathcal{E})$ be the set of all proper solutions to $\mathcal{E}$. If $\lambda : \Pi \to \Gamma$ is a weak solution to $\mathcal{E}$ with image G', we get a FSEP $\mathcal{E}' = (\lambda : \Pi \to G', f' : \Gamma \times_G G' \to G')$ for Π that dominates $\mathcal{E}$. We prove the following lemma.

Lemma 1 ([6])**.** *The natural map* $PS(\mathcal{E}') \to PS(\mathcal{E})$ *is an injection.*

Using this lemma and Theorem 1 we prove the following result.

Theorem 2 ([6])**.** *Let* Π *be a profinite group and* m *an infinite cardinal. The group* Π *is free of rank* m *if and only*

(1) Π *is projective and*
(2) *Every non-trivial FSEP for* Π *has exactly* m *solutions.*

Definition 1. For m an infinite cardinal, a profinite group Π is *quasi-free of rank* m if every non-trivial FSEP has exactly m proper solutions.

This definition suggests a generalization of the Shafarevich conjecture for fields K for which G_K is not projective: Is $G_{K^{\mathrm{cycl}}}$ quasi-free?

We consider the case $K = k((x,t))$, for k arbitrary. There G_K is not projective (and hence not free) since its cohomological dimension is greater than 1. (In [5], there is an explicit example of a FEP for G_K with no weak solution.) Even without taking the maximal cyclotomic extension of K, we obtain:

Theorem 3 ([6])**.** *The profinite group* $G_{k((x,t))}$ *is quasi-free of rank* $\operatorname{card} k((x,t))$*.*

This result holds without any restrictions on the field k. It strengthens and generalizes the result in [5] for the case $k = \mathbb{C}$. That proof relied heavily on the fact that $\mathbb{C}$ is algebraically closed and characteristic zero, so that all covers of

$\mathbb{C}((x))$ are tame and cyclic and Abhyankar's Lemma applies. Theorem 3 shows that $G_{k((x,t))}$ is "as free as possible" given that it is not projective. Moreover it supports a conjecture of Debes and Dechamps that states that if F is Hilbertian (as $k((x,t))$ is) then every FSEP for G_F has a proper solution [1].

Idea of proof: Let $X^* = \operatorname{Spec} k[[x,t]]$. Let $\mathcal{E} = (\alpha : G_K \to G, f : \Gamma \to G)$ be a FSEP for G_K. Then α corresponds to a G-Galois cover $Y^* \to X^*$. After a change of variables, we may assume that it is unramified at the generic point of $(t = 0)$. Let $Y_0^* \to X_0^*$ be the fibre over $(t = 0)$. Using the Katz-Gabber result [7], there is a (disconnected) G-Galois cover $Y_0 \to X_0 := \mathbf{P}^1_k$ that agrees with $Y_0^* \to X_0^*$ over $k((x))$. By formal patching there is a G-Galois cover $\bar{Y} \to \bar{X} = \mathbf{P}^1_{k[[t]]}$ with this closed fibre away from $(x = 0)$, such that its pullback to the complete local ring at $(x = t = 0)$ is $Y^* \to X^*$. Taking the open fibre, we have a split embedding problem for curves over $k((t))$, which can be solved by a result of Pop [10] and Haran-Jarden [3]. We then wish to normalize that solution over $\bar{X}$ and restrict to X^* to obtain a solution to the given embedding problem (in fact we want $m := \operatorname{card} k((x,t))$ solutions). A difficulty is to guarantee irreducibility of this restriction. So we prove a strengthening of the result of Pop and Haran-Jarden, for models of curves over $k[[t]]$, saying that a finite split embedding problem has m proper solutions $\bar{Z} \to \bar{Y} \to \bar{X}$ such that $\bar{Z} \to \bar{Y}$ is totally ramified at a given point of $\bar{Y}$. Applying this in our case with the point over $(x = t = 0)$, we obtain the desired local irreducibility and hence the result.

Recall from [10] that a field F is called *large* (or *ample*) if every smooth F-curve with an F-point has infinitely many F-points. The field $k((t))$ is large, and the result of Pop and Haran-Jarden holds more generally for split embedding problems for curves over arbitrary large fields F. This can be proven by using the result for $F((t))$, descending to a finite type subalgebra of $F((t))$, and then specializing to an F-point using that F is large. Similarly, our strengthened version, which was used in the above proof, carries over to arbitrary large fields:

Theorem 4 ([6])**.** *Let F be a large field and let X be a smooth projective connected F-curve, with function field K.*

(1) *Every finite split embedding problem $(\alpha : G_K \to G,\ f : \Gamma \to G)$ for K has card(F) proper solutions $Z \to Y \to X$. These may be chosen so that Z is totally split over a given finite closed subset of the G-Galois cover Y.*
(2) *Hence the absolute Galois group of K is quasi-free.*

The cardinality assertion in Theorem 4 is a bit stronger than as stated in reference [6], and it uses

Theorem 5 (Pop)**.** *If F is a large field of (infinite) cardinality m and X is a smooth F-curve with an F-point P, then the cardinality of $X(F)$ is m.*

Proof. It suffices to prove $\operatorname{card}(X(F)) \geq m$. We easily reduce to the case that $(0,0) \in X \subset \mathbb{A}^2_F$, with X defined by a polynomial f such that $\partial f/\partial y \neq 0$ at $(0,0)$. It suffices to construct an injection $i : F \hookrightarrow X(F) \times X(F)$. For $a \in F$, define

$V_a \subset X \times X \subset \mathbb{A}^4_F$ by $f(X_1, Y_1) = 0,\ f(X_2, Y_2) = 0,\ X_1 - aX_2 = 0$, where $\mathbb{A}^4_F$ has coordinates X_1, Y_1, X_2, Y_2. The origin is a smooth point of V_a, and its irreducible component C_a is a curve. Since F is large, there exists $i(a) := (x_1, y_1, x_2, y_2) \in C_a(F)$ with $x_2 \neq 0$. Note $a = x_1/x_2$. So this map i is injective.

References

[1] P. Dèbes, B. Deschamps, *The regular inverse Galois problem over large fields*, "Geometric Galois actions", vol. 2 (L. Schneps and P. Lochak, eds.), London Math. Soc. Lec. Note Ser. **243**, Cambridge U. Press, (1997), 119-138.

[2] M. Fried, M. Jarden, "Field Arithmetic", Ergebnisse Math. series, **11**, Springer-Verlag, (1986).

[3] D. Haran, M. Jarden, *Regular split embedding problems over complete valued fields*, Forum Mathematicum, **10** (1998), 329-351.

[4] D. Harbater, *Fundamental groups and embedding problems in characteristic p*, In "Recent Developments in the Inverse Galois Problem" (M. Fried, et al., eds.), AMS Contemporary Mathematics Series **186**, (1995), 353-369.

[5] D. Harbater, *Patching and Galois theory* In "Galois Groups and Fundamental Groups" (L. Schneps, ed.), MSRI Publications series, **41**, Cambridge University Press, (2003), 313-424.

[6] D. Harbater, K. Stevenson, *Local Galois theory in dimension two*, Advances in Mathematics Vol. 198, Issue 2 (2005) 623-653.

[7] N. Katz, *Local-to-global extensions of representations of fundamental groups*, Ann. l'inst. Fourier, **3**6 (1986), 69-106.

[8] T. Lefcourt, *Galois groups and complete domains*, Israel J. Math. **114** (1999), 323-346.

[9] F. Pop, *Étale Galois covers of affine smooth curves*, Invent. Math., **120** (1995), 555-578.

[10] F. Pop, *Embedding problems over large fields*, Ann. Math., **144** (1996), 1-34.

Profinite HNN–constructions

Wolfgang Herfort

(joint work with Pavel A. Zalesskii)

There are various embedding theorems in profinite group theory. A. Lubotzky and J. Wilson [4] proved the profinite analog of the Higman, Neumann and Neumann theorem [5] asserting that every topologically countably generated profinite group embeds in a two generated profinite group. However, their construction did not allow to control the torsion. So Z. Chatzidakis [1] returned to the original construction of Higman, Neumann and Neumann to make it work in the profinite (resp. pro-p) case to prove that one can embed a countably generated profinite (respectively, pro-p) group in a two generated profinite (respectively, pro-p) group E such that every torsion element is conjugate to an element of G. The same construction has been used in [10] to embed any cyclic subgroup separable group in a two generated cyclic subgroup separable group and in [2] to prove the existence of a 2-generated torsion free residually p-group whose pro-p completion contains every finite p-group. In the present paper we use an HNN-construction in the category of pro-$\mathcal{C}$ groups with the objective to deminish torsion in a virtually torsion free pro-$\mathcal{C}$ groups. Our result is in the spirit of the Higman, Neumann and Neumann theorem stating that any countable group can be emebedded in a countable group

in which all elements of the same order are conjugate.
More precisely, we prove the following

Theorem 1. *Let $\mathcal{C}$ be a class of finite groups closed under forming subgroups, products, and, extensions. Let G be a virtually torsion free pro-$\mathcal{C}$ group and F a torsion free open subgroup of G. Then G can be embedded in a semidirect product $\tilde{G} = E \rtimes G/F$ such that every finite subgroup of $\tilde{G}$ is conjugate to a subgroup of G/F. Moreover, the cohomological dimensions $cd(F) = cd(E)$ coincide.*

The precise reformulation of the Higman Neumann Neumann result can not hold for infinite profinite groups. First, every infinite profinite group is non-countable, so one has to talk about second countable profinite groups. Secondly, a p-element of infinite order in a profinite group can not be conjugate to its p-power, since its image and the pth power of it in some finite quotient have different orders. So, a profinite version of the Higman Neumann Neumann result can be stated only for elements of infinite order. However even then the profinite version of it does not hold (see the Example at the end of the report). Nevertheless, the profinite analog of the Higman Neumann Neumann result is valid for virtually torsion free profinite groups.

Corollary 1. *Let G be a any virtually torsion free profinite group. Then G embeds into a profinite group $\tilde{G}$ where all elements of the same order are conjugate. Moreover, virtual homological dimensions, $vcd(G)$ and $vcd(\tilde{G})$ coincide.*

Our Theorem has in part been motivated by a result of C. Scheiderer [9] – a homological version reads as follows:

Theorem 2. *Let G be a profinite group of virtual cohomological dimension $d < \infty$ and suppose that G does not contain subgroups isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Let $\mathcal{T}$ be the set of all finite subgroups of G on which G acts from the right by conjugation. Then*

$$\bigoplus_{t \in \mathcal{T}} H_n(G, \mathbb{F}_p[[tG]]) \longrightarrow H_n(G, \mathbb{F}_p)$$

is an isomorphism for all $n > d$.

Now one would like to apply Shapiro's lemma to express the homology of G in terms of the homologies of centralizers of torsion elements, but one needs to do it continuously and that requires a continuous section $T/G \longrightarrow T$. Such a section does not always exists (see [8], example 5.6.9). For virtually free pro-p groups as well as for Kurosh subgroup theorem the existence of a continuous section is even more important (see [11], [6], [3]. So it is desirable to embed G coherently into a profinite group with similar structure where the corresponding continuous section would exist. To illustrate this we apply our result to deduce the following

Theorem 3. *Let G be a pro-p group having free pro-p subgroup F such that $G/F \cong C_{p^n}$ with F maximal with respect to this property. Then G embeds into a free product $\tilde{G} = C_{\tilde{G}}(C_p) \amalg H$ of a free pro-p group F and the centralizer $C_{\tilde{G}}(C_p)$ of a group C_p of order p. Moreover,*

(i) *$\tilde{G}$ possesses a free pro-p subgroup $\tilde{F}$ such that $\tilde{G}/\tilde{F} \cong C_{p^n}$;*

(ii) *The quotient group $C_{\tilde{G}}(C_p)/C_p$ has a structure similar to $\tilde{G}$ with the inductive continuation.*

We introduce a pro-$\mathcal{C}$ analogue of the concept of an HNN-group, see [5], p. 180. This generalizes the concept of pro-$\mathcal{C}$ HNN-extension (see [8], 9.4).

Definition 1. Let G be a pro-$\mathcal{C}$ group and $\partial_0, \partial_1 : (\mathcal{G}, T) \to G$ a fiber monomorphisms. A specialization of $(\beta, \beta_1) : (G, \phi, T) \longrightarrow K$ of a triple (G, ϕ, T) into a $\mathcal{C}$-group K consists of a homomorphism $\beta : G \longrightarrow K$ and a continuous map $\beta_1 : T \longrightarrow K$ such that for $t \in T$ and $g \in \mathcal{G}(e)$, one has $\beta(g) = \beta(\partial_0(g))$ and $\beta(\partial_0(g)) = \beta_1(t)^{-1}\beta(\partial_1(g))\beta_1(t)$.

The pro-$\mathcal{C}$ HNN-group is then a pro-$\mathcal{C}$ group $HNN(G, \mathcal{G}, T)$ having a specialization $(\upsilon, \upsilon_1) : (G, \mathcal{G}, T) \longrightarrow HNN(G, \mathcal{G}, T)$, with the following universal property: for every pro-$\mathcal{C}$ group K and every specialization $(\beta, \beta_1) : (G, \mathcal{G}, T) \to K$, there exists a unique homomorphism

$$\omega : HNN(G, \mathcal{G}, T) \longrightarrow K,$$

such that $\omega\upsilon_1 = \beta_1$ and $\beta = \omega\upsilon$.

The following criterion for embedding a pro-$\mathcal{C}$ group G as a base group into a pro-$\mathcal{C}$ HNN-extension $HNN(G, A, f)$, whose proof is based upon the ideas of Zoé Chatzidakis in [1] turns out essential.

Theorem 4. *Let H be a pro-$\mathcal{C}$ group and $f : A \longrightarrow B$ an isomorphism between two closed subgroups of H. Form the pro-$\mathcal{C}$ HNN-extension*

$$G := HNN(H, A, f, t) := \langle H, t \mid \text{ relations: } f(a)^{-1}a^t, a \in A\rangle.$$

Then the HNN-extension is proper, i.e., the natural embedding of $\phi : G \longrightarrow H$ is mono, if and only if for every open normal subgroup U of H there exists an open normal subgroup V of G contained in U such that

$$f(A \cap V) = f(A) \cap V$$

and the abstract HNN-extension $HNN^{abs}(H/V, AV/V, f_V)$ is residually $\mathcal{C}$, where $f_V : AV/V \longrightarrow BV/V$ is the isomorphism induced by f.

Example. Let $G = \prod C_i$ an infinite cartesian product of groups C_i of order 2. Choose a sequence of elements g_n different from 1 that converges to 1. Suppose $\tilde{G}$ embeds into a profinite group where all elements of equal order are conjugate. Then g_0 is conjugated to all of g_n in $\tilde{G}$ and so by continuity has to be conjugate to 1, a contradiction.

References

[1] Z. M. Chatzidakis, Some remarks on profinite HNN extensions, Isr. J. Math. **85**, No.1-3, (1994) 11-18.

[2] Z. M. Chatzidakis, Torsion in pro-p completions of torsion free groups, J. Group Theory **2** (1999), 65–68.

[3] D. Haran, On closed subgraphs of free products of profinite groups, *J. London Math.Soc.* (3) **55** (1987), 266–298.
[4] A. Lubotzky and J.S. Wilson, An embedding theorem for profinite groups, Arch. Math. **42** (1984) 397-399.
[5] R. C. Lyndon and P. E. Schupp, Combinatorial Group Theory, Springer 1977.
[6] O. V. Mel'nikov, Subgroups and Homology of Free Products of Profinite Groups, Math. USSR Izvestiya, **34**, 1, (1990), 97-119.
[7] D. Quillen, The spectrum of an equivariant cohomology ring. I, II. Ann. of Math. (2) 94 (1971), 549–572; ibid. (2) 94 (1971), 573–602.
[8] L. Ribes and P.A. Zalesskii, Profinite Groups, Springer 2000.
[9] C. Scheiderer, Real and étale cohomology. Lecture Notes in Mathematics, 1588. Springer-Verlag, Berlin, 1994.
[10] J.S. Wilson and P.A. Zalesskii, An embedding theorem for certain residually finite groups Arch. Math., **67** (1996) 177-182.
[11] P.A. Zalesskii, Virtually projective groups, J. für die Reine und Angewandte Mathematik (Crelle's Journal) bf 572 (2004) 97-110.

New aspects of anabelian geometry

Jochen Koenigsmann

1. The main result presented in this talk is that, in most cases, a field K can be recovered from the absolute Galois group of the rational function field $K(t)$ over K.

To be more precise, we call a field K **almost arbitrary (a.a)** if K is neither separably closed nor real closed, and if in characteristic $p > 0$ the absolute Galois group G_K of K is not a pro-p group. So K is a.a. iff $l^2 \mid \sharp G_K$ for some prime $l \neq \text{char } K$.

Main Theorem *Let K and K' be perfect fields and assume that K is a.a. Then*

$$G_{K(t)/K} \cong G_{K'(t)/K'} \iff K \cong K'$$

Here we denote by $G_{K(t)/K}$ or, more generally, by $G_{K(\mathcal{C})/K}$ for any smooth projective curve $\mathcal{C}$ over K with function field $K(\mathcal{C})$, the canonical projection (restriction map) $pr_{\mathcal{C}/K} : G_{K(\mathcal{C})} \twoheadrightarrow G_K$, and we write $G_{K(\mathcal{C})/K} \cong G_{K'(\mathcal{C}')/K'}$ if there is an isomorphism $\phi : G_{K(\mathcal{C})} \to G_{K'(\mathcal{C}')}$ of profinite groups inducing via restriction an isomorphism $\overline{\phi} : G_K \to G_{K'}$ and a commutative diagram

$$\begin{array}{ccc} G_{K(\mathcal{C})} & \xrightarrow{\phi} & G_{K'(\mathcal{C}')} \\ \downarrow & & \downarrow \\ G_K & \xrightarrow{\overline{\phi}} & G_{K'} \end{array}$$

Without the assumption of K being a.a. or of K and K' being perfect the Main Theorem becomes false.

The Main Theorem is a special case of a rather general conjecture of birational anabelian geometry:

Conjecture *Let K be a.a. and perfect, and let $\mathcal{C}$ be a smooth projective curve over K. Then $K(\mathcal{C})$ is up to isomorphism encoded in $G_{K(\mathcal{C})/K}$: if K' is another perfect field, $\mathcal{C}'$ a smooth projective curve over K' then*

$$G_{K(\mathcal{C})/K} \cong G_{K'(\mathcal{C}')/K'} \iff K(\mathcal{C})/K \cong K'(\mathcal{C}')/K'.$$

Here $K(\mathcal{C})/K \cong K'(\mathcal{C}')/K'$ means that there is an isomorphism $K(\mathcal{C}) \to K'(\mathcal{C}')$ of fields inducing via restriction an isomorphism $K \to K'$.

The conjecture has been proved for finitely generated fields by Pop ([P]) and for sub-p-adic fields by Mochizuki ([M]) (building on work by Nakamura and Tamagawa - cf. [MNT]). An analogue for higher dimensional varieties over fields containing all roots of unity was proved by Bogomolov and Tschinkel ([BT]).

2. The proof of the Theorem is based on a purely group theoretic interpretation of K-rational points of a smooth projective curve $\mathcal{C}$ over K inside $G_{K(\mathcal{C})/K}$:

Main Lemma (for K a.a., perfect and, for simplicity, non-henselian, cf. [K], Theorem 4.1)
The map

$$\begin{array}{rccl} \delta: & \mathcal{C}(K) & \to & \{\textit{conj. classes of max. geom. subgps. } D \leq G_{K(\mathcal{C})} \textit{ over } G_K\} \\ & P & \mapsto & [D_P] \end{array}$$

is a bijection.

Here D_P denotes a decomposition subgroup of $G_{K(\mathcal{C})}$ w.r.t. P, and a subgroup $D \leq G_{K(\mathcal{C})}$ is called **geometric over** G_K if it is of the form $D \cong R \rtimes (C \rtimes G)$, where $pr_{\mathcal{C}/K}\,|_G \colon G \to G_K$ is an isomorphism (i.e. G is the image of a section of $pr_{\mathcal{C}/K}$) and

$$\begin{array}{ll} R = 1 \text{ and } C \cong \hat{\mathbb{Z}} & \text{if char } K = 0 \\ R \neq 1 \text{ is pro-}p \text{ and } C \cong \prod_{q \neq p} \mathbb{Z}_q & \text{if char} K = p > 0 \end{array}$$

(We should emphasize that $G_{K(\mathcal{C})/K}$ sees the characteristic of K, so the image of δ *is* given in purely group theoretic terms.)

If K is henselian, δ is still injective but, in general not onto. In this case the group theoretic description of the image becomes more complicated.

The Main Lemma which remains true over finite extensions of K is used to obtain a Galois code for the group of divisors and the group of principal divisors of $\mathcal{C}$ over $\overline{K}$ respecting the Galois action. If $\mathcal{C} = \mathbb{P}^1_K$ (so $K(\mathcal{C}) = K(t)$ as in the Main Theorem) this provides a Galois code for $K \cup \{\infty\}$. One then recovers the field operations of K from $G_{K(t)/K}$ by a Galois code for the group law on a suitable choice of elliptic curves over K (using the Galois code for the principal divisors of these curves).

3. The Main theorem can be modified into a Galois axiomatization for any a.a. perfect field via the elementary theory of $G_{K(t)/K}$ in a suitable first order language for profinite groups. This is a many sorted language which, following Cherlin, van den Dries, Macintyre and Chatzidakis, talks about the 'finite quotients' of

$G_{K(t)/K}$. It gives a dictionary translating the elementary theory of a field K into the elementary theory of $G_{K(t)/K}$:

Theorem *Let K and K' be a.a. perfect fields. Then*

(1) $K \equiv K' \iff G_{K(t)/K} \equiv G_{K'(t)/K'}$
(2) *K and $G_{K(t)/K}$ are bi-interpretable*

In particular, decidability of K is equivalent to decidability of $G_{K(t)/K}$.

As a consequence, an altogether new approach to longstanding questions of decidability presents itself. The hope is to prove this way undecidability of $\mathbb{C}(x)$ and decidability of $\mathbb{F}_p((t))$ or at least of $\mathbb{F}_p((t))^{\mathrm{perf}}$. The method may also apply to Hilbert's 10th problem over $\mathbb{Q}$.

References

[BT] F. Bogomolov, Y. Tschinkel, *Reconstruction of function fields*, http://www.math.princeton.edu/∼ytschink/publications.html

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

[M] S. Mochizuki, *The local pro-p anabelian geometry of curves*, Invent. math. **138** (1999), 319–423.

[MNT] S. Mochizuki, H. Nakamura, A. Tamagawa, *The Grothendieck Conjecture on the fundamental groups of algebraic curves*, Sugaku Expositions **14(1)** (2001), 31–53.

[P] F. Pop, *On Grothendieck's conjecture of birational anabelian geometry I*, Ann. of Math. **138** (1994), 147–182, and *II*, Heidelberg-Mannheim Preprint Series Arithmetik II **16** (1995).

Iterative Differential Equations and Finite Groups

Bernd Heinrich Matzat

It is an old question to characterize those differential equations or differential modules, respectively, whose solution spaces consist of functions which are algebraic over the base field. The most famous conjecture in this context is due to A. Grothendieck and relates the algebraicity property with the p-curvature which appears as the first integrability obstruction in characteristic p. Here we prove a variant of Grothendieck's conjecture for differential modules with vanishing higher integrability obstructions modulo p – these are iterative differential modules – and give some applications.

1. Pseudo Picard-Vessiot Rings over Number Fields

To fix our notation let F/K be a function field of one variable over a number field K with a derivation ∂_F normalized by $\partial_F(t) = 1$ for some $t \in F$. Then $F/K(t)$ is a finite field extension, and ∂_F is the unique extension of $\partial_t := \frac{d}{dt}$ to F. Any linear differential equation over F defines a finite dimensional differential module

(D-module) M over F. This is an F-vector space equipped with a derivation $\partial_M : M \to M$ which is an additive map with

$$\partial_M(x \cdot a) = \partial_M(x) \cdot a + x \cdot \partial_F(a) \text{ for } x \in M, a \in F.$$

With respect to some basis $B = \{b_1, ..., b_m\}$ of M the derivation is given by a matrix $A \in F^{m \times m}$.

Now we are interested in finding a minimal differential extension field E/F such that the solution space $\mathrm{Sol}_E(M)$ of M in E, defined by $\partial_E(\underline{y}) = A \cdot \underline{y}$ for $\underline{y} = (y_1, \ldots, y_m)^{\mathrm{tr}} \in E^m$, has dimension m. Such a field can be constructed in the following way (compare [7], Ch. 1.3): The coordinate ring of the affine group GL_m over F

$$U := F[\mathrm{GL}_m] = F[x_{ij}, \det(x_{ij})^{-1}]_{i,j=1}^m$$

becomes a differential ring (D-ring) by defining $\partial_U(X) = A \cdot X$ for $X = (x_{ij})_{i,j=1}^m$. Then the residue ring R of U by a maximal differential ideal $P \lhd U$ is a D-ring and a domain containing a matrix $Y \in \mathrm{GL}_m(R)$ with $\partial_R(Y) = A \cdot Y$ and ∂_R obtained from ∂_U. Thus R contains a fundamental solution matrix of M, and for $E := \mathrm{Quot}(R)$ holds $\dim_K(\mathrm{Sol}_E(M)) = m$.

In order to find an R without new constants we assume that F/K contains a prime $\wp$ of degree one which is regular for M, i. e., $\wp$ is a regular point. Since M has only finitely many singular points, such a $\wp$ always exists in the case $F = K(t)$ or after a finite extension by constants. Choosing a local parameter $u \in F$ for $\wp$, the D-module M possesses a fundamental solution matrix $Y \in \mathrm{GL}_m(K[[u]])$ which can be normalized by $Y(\wp) \in \mathrm{GL}_m(K)$. Denoting by P the kernel of the differential homomorphism $\pi : U \to K((u))$ defined by $\pi(X) = Y$, the D-ring $R := U/P$ is regular over K. Obviously all fundamental solution matrices $Y \in \mathrm{GL}_m(K[[u]])$ with $Y(\wp) \in \mathrm{GL}_m(K)$ only differ by matrices $C \in \mathrm{GL}_m(K)$. Hence R is uniquely determined up to differential isomorphisms by the property above. It further depends neither on the chosen local parameter nor on the chosen regular rational point $\wp$. In the following the D-ring (R, ∂_R) is called a *pseudo Picard-Vessiot ring* (PPV-ring) and its field of fractions (E, ∂_E) a *PPV-field*.

The F-automorphisms of E commuting with ∂_E form a group $\mathrm{Aut}_{\mathrm{D}}(E/F)$ and define an affine group scheme $\mathcal{G} \leq \mathrm{GL}_m$ over K with $\mathcal{G}(K) \cong \mathrm{Aut}_{\mathrm{D}}(E/F)$, called the *Galois group scheme of* E/F. In case the fixed field $E^{\mathcal{G}(K)}$ equals F, the ring R/F or E/F respectively are called *Picard-Vessiot ring* (PV-ring) or *PV-field*, and $\mathcal{G}(K) =: \mathrm{Gal}_{\mathrm{D}}(E/F)$ is the *differential Galois group of* E/F. It is well known that for connected groups the notion of a PPV-ring and a PV-ring coincide.

By the assumptions above we obtain the following variant of T. Dyckerhoff of the differential Galois correspondence due to E. Kolchin valid over number fields:

Theorem 1. ([2]): *Let (F, ∂_F) be a D-field of one variable over a number field K and (M, ∂_M) be a D-module over F with regular rational point $\wp$ in F. Then the following hold:*

(a) *There exists a PPV-field E/F for M without new constants. E/F is uniquely determined by $Y(\wp) \in \mathrm{GL}_m(K)$ up to differential isomorphisms.*

(b) *There exists a Galois correspondence between the subgroup schemes of the Galois group scheme $\mathcal{G}$ and the differential intermediate fields of E/F.*

2. Grothendiecks p-Curvature Conjecture

By the first section the algebraicity of the solutions of a D-module, the algebraicity of the corresponding PPV-field E/F and the finiteness of $\mathrm{Gal}_{\mathrm{D}}(E/F)$ are equivalent. In case E/F and thus $E/K(t)$ are algebraic, the property $\partial_t^p \equiv 0 \pmod p$ of $K(t)$ implies $\partial_E^p \equiv 0 \pmod p$ for almost all primes. According to A. Grothendieck (1970), this property should be characteristic. To be more precise, let (M, ∂_M) be a D-module over F. Then the p-curvature of M is the p-th iterate ∂_M^p of ∂_M. It is called trivial in the case $\partial_M^p \equiv 0 \pmod p$.

P-Curvature Conjecture. *Let (F, ∂_F) be a D-field of one variable over a number field K and (M, ∂_M) be a D-module over F. Then the following are equivalent:*

(1) *M admits a full system of algebraic solutions.*
(2) *The p-curvature of M is trivial for almost all primes p.*

An equivalent condition has been detected by P. Cartier using reduction. For this purpose let $\mathfrak{p}$ denote a prime divisor (place) dividing p in K, $\mathfrak{p}_t$ its Gauss extension to $K(t)$ and $\mathfrak{P}$ a place F extending $\mathfrak{p}_t$. Then the reduction $F_{\mathfrak{P}}$ of F modulo $\mathfrak{P}$ is a function field with finite field of constants. In case (M, ∂_M) is a D-module over F with representing matrix $A \in F^{m\times m}$ of ∂_M, for almost all $\mathfrak{P}$ the reduced matrix $A_{\mathfrak{P}} \in F_{\mathfrak{P}}^{m\times m}$ exists and defines the derivation of a D-module $M_{\mathfrak{P}}$ over $F_{\mathfrak{P}}$. The same procedure works for any of the matrices $A^{(k)}$ corresponding to the higher derivation $\partial_M^{(k)} := \frac{1}{k!}\partial_M^k$. Fortunately these can be computed iteratively using the so-called Taylor recursion:

$$A^{(0)} = I, A^{(1)} = A, kA^{(k)} = \partial_F\left(A^{(k-1)}\right) + A^{(k-1)} \cdot A.$$

In the case $\partial_M^p \equiv 0 \pmod p$, the formulas above show that

$$Y_{\mathfrak{P}} := (\sum_{k=0}^{p-1} A_{\mathfrak{P}}^{(k)}(-u)^k)^{-1} \in \mathrm{GL}_m(F_{\mathfrak{P}})$$

is a fundamental solution matrix of the reduced D-module $M_{\mathfrak{P}}$, i.e., $M_{\mathfrak{P}}$ is trivial over $F_{\mathfrak{P}}$.

Lemma of Cartier: *Let (F, ∂_F) be a D-field of one variable over a number field K and (M, ∂_M) be a D-module over F. Then (2) is equivalent to:*

(3) *The reduced D-module $M_{\mathfrak{P}}$ is trivial for almost all $\mathfrak{P}$.*

The Lemma of Cartier shows that in this way D-modules over F with algebraic solutions are reduced to D-modules over $F_{\mathfrak{P}}$ with rational (=trivial) solutions. Comparing with algebraic field extensions this property looks quite unnatural.

3. Iterative Differential Modules

In order to preserve by reduction the degree of algebraicity we have to use in addition higher derivations. But then we have to work with infinitely many $\partial_F^{(k)}$ and $A^{(k)}$ and thus to give more care on our D-rings. For this purpose let $\mathbb{P}'_K \subseteq \mathbb{P}_K$ be a cofinite set of primes $\mathfrak{p}$ in K and $\mathcal{O}'_K$ the intersection of their valuation rings $\mathcal{O}_\mathfrak{p}$. Further let $\mathbb{P}'_F$ be the set of all places $\mathfrak{P}$ in F extending the Gauss valuation $\mathfrak{p}_t$ in $K(t)$ for $\mathfrak{p} \in \mathbb{P}'_K$. Then $\mathcal{O}'_F := \bigcap_{\mathfrak{P} \in \mathbb{P}'_F} \mathcal{O}_\mathfrak{P}$ is a Dedekind ring in F. It is called a *global iterative differential ring* (ID-ring) if

$$\partial_F^{(k)}(\mathcal{O}'_F) \subseteq \mathcal{O}'_F \text{ and } \partial_F^{(k)}(\mathfrak{P}) \subseteq \mathfrak{P} \text{ for all } k \in \mathbb{N} \text{ and } \mathfrak{P} \in \mathbb{P}'_F.$$

Obviously any function field of one variable F/K contains infinitely many such global ID-rings. In a similar way we define *global ID-modules* M to be free $\mathcal{O}'_F$-modules of finite rank with higher derivations $\partial_M^{(k)} := \frac{1}{k!}\partial_M^k : M \to M$.

Under these assumptions we can follow Section 1 in order to construct a PPV-ring R for M now over the global ID-ring $\mathcal{O}'_F$ with a fundamental solution matrix $Y \in \mathrm{GL}_m(R)$ and with $Y(\wp) \in \mathrm{GL}_m(\mathcal{O}'_K)$ for some regular prime $\wp$ of degree one of F/K. Since by definition all matrices $A^{(k)}$ belong to $(\mathcal{O}'_F)^{m\times m}$, this PPV-ring R is equipped with an iterative derivation $\left(\partial_R^{(k)}\right)_{k\in\mathbb{N}}$ and thus is itself an ID-ring. In all we obtain the following ID-analogue of Theorem 1.

Theorem 2. ([4])*: Let $(\mathcal{O}'_F, \partial_F)$ be a global ID-ring and (M, ∂_M) be a global ID-module over $\mathcal{O}'_F$ with regular rational prime $\wp$ in $\mathcal{O}'_F/\mathcal{O}'_K$. Then there exists a PPV-ring R_M over $\mathcal{O}'_F$ with ring of constants $\mathcal{O}'_K$. Moreover R_M is unique up to D-isomorphisms by assuming $Y(\wp) \in \mathrm{GL}_m(\mathcal{O}'_K)$.*

If in addition the spezialized matrix $A(\wp)$ belongs to $(\mathcal{O}'_K)^{m\times m}$ - this can be reached by removing a finite set of primes $\mathfrak{P}$ from $\mathbb{P}'_F$ - then $A^{(k)}(\wp) \in (\mathcal{O}'_K)^{m\times m}$ holds for all $k \in \mathbb{N}$ by Taylor recursion. This leads to

Corollary 1. *Assuming in addition $A(\wp) \in (\mathcal{O}'_K)^{m\times m}$, the Taylor expansion of Y for a local parameter u for $\wp$ belongs to $\mathrm{GL}_m(\mathcal{O}'_K[[u]])$.*

In particular, the Taylor expansions in u of the entries y_{ij} of Y are globally bounded in the sense of G. Christol (compare [1], Ch. 4.1). It should be mentioned that any finite Galois extension E/F without new constants can be obtained as field of fractions of a PPV-ring R_M of some global ID-module M over a global ID-ring $\mathcal{O}'_F$. Thus any finite group appears as differential Galois group of such a global ID-module.

4. Reduction of Global ID-Modules.

Let (M, ∂_M) be a global ID-module over a global ID-ring $(\mathcal{O}'_F, \partial_F)$. Then by Theorem 2 there exists a PPV-ring $R_M/\mathcal{O}'_F$ for M. As before, for all $\mathfrak{P} \in \mathbb{P}'_F$ the residue field $F_\mathfrak{P} := \mathcal{O}'_F/\mathfrak{P}$ is a function field of one variable over the finite field $K_\mathfrak{p} := \mathcal{O}'_K/\mathfrak{p}$ and the residue ring $(R_M)_\mathfrak{P} := R_M/R_M\mathfrak{P}$ is an $F_\mathfrak{P}$-algebra.

On the other side the reduced matrices $A_{\mathfrak{P}}^{(k)} \in F_{\mathfrak{P}}^{m\times m}$ define an iterative derivation $(\partial_{M_{\mathfrak{P}}}^{(k)})_{k\in\mathbb{N}}$ on some $F_{\mathfrak{P}}$-vector space $M_{\mathfrak{P}}$. Thus $M_{\mathfrak{P}}$ is an ID-module over $F_{\mathfrak{P}}$ as studied for example in [5], Ch. 5. By [5], Prop. 6.1, there exists a PV-ring for $M_{\mathfrak{P}} \otimes_{K_{\mathfrak{p}}} \overline{K_{\mathfrak{p}}}$ over $F_{\mathfrak{P}} \otimes_{K_{\mathfrak{p}}} \overline{K_{\mathfrak{p}}}$. In case $F_{\mathfrak{P}}$ contains a regular point $\tilde{\wp}$ of degree one for $M_{\mathfrak{P}}$, an argument like the one given in Section 1 shows that there exists an iterative PPV-ring $R_{M_{\mathfrak{P}}}$ over $F_{\mathfrak{P}}$ without new constants. Further $R_{M_{\mathfrak{P}}}$ is uniquely determined up to ID-isomorphisms by the property that a fundamental solution matrix $Y_{\mathfrak{P}}$ of $M_{\mathfrak{P}}$ in $R_{M_{\mathfrak{P}}}$ at $\tilde{\wp}$ has initial values in $\mathrm{GL}_m(K_{\mathfrak{p}})$. The next theorem shows that for almost all $\mathfrak{P} \in \mathbb{P}'_F$ the reduced PPV-ring $(R_M)_{\mathfrak{P}}$ and the PPV-ring $R_{M_{\mathfrak{P}}}$ constructed from the reduced matrices $A_{\mathfrak{P}}^{(k)}$ coincide.

Theorem 3. ([4]): *Let (M, ∂_M) be a global ID-module over a global ID-ring $(\mathcal{O}'_F, \partial_F)$. Then for almost all $\mathfrak{P} \in \mathbb{P}'_F$ the reduced PPV-ring $(R_M)_{\mathfrak{P}}$ and the PPV-ring of the reduced ID-module $M_{\mathfrak{P}}$ are isomorphic as ID-rings.*

The proof of Theorem 3 relies on the compatibility of the Taylor expansions in different characteristics based on the globally boundedness. By the Generic Flatness Lemma then follows

Corollary 2. *For almost all $\mathfrak{P} \in \mathbb{P}'_F$ holds*

$$\dim(R_{M_{\mathfrak{P}}}) = \dim(R_M) - 1 = \dim(R_M/\mathcal{O}'_F).$$

Thus Corollary 2 proves the last conjecture statet in [5]. A D-module is called algebraic if it admits a full system of algebraic solutions over the base ring.

Theorem 4. ([4]): *Let (M, ∂_M) be a global ID-module over a global ID-ring $(\mathcal{O}'_F, \partial_F)$. Then the following hold:*

(a) *$M/\mathcal{O}'_F$ is algebraic if and only if the reduced ID-modules $M_{\mathfrak{P}}/F_{\mathfrak{P}}$ are algebraic for almost all $\mathfrak{P} \in \mathbb{P}'_F$.*

(b) *$\mathrm{Gal}_D(R_M/\mathcal{O}'_F)$ is a finite group G if and only if $\mathrm{Gal}_{\mathrm{ID}}(R_{M_{\mathfrak{P}}}/F_{\mathfrak{P}}) \cong G$ for almost all $\mathfrak{P} \in \mathbb{P}'_F$.*

For global ID-modules this theorem refines Cartier's Lemma in Section 2

5. The Link with Grothendieck's Conjecture

According to Grothendieck's conjecture the following conjecture should be true:

Conjecture 1. *Any global ID-module (M, ∂_M) over a global ID-ring $(\mathcal{O}'_F, \partial_F)$ is algebraic.*

To prove Conjecture 1, by Theorem 4 it would be enough to show that reductions modulo $\mathfrak{P}$ lying in $K_{\mathfrak{p}}[[u]]$ of globally bounded solutions of linear differential equations at a regular point are algebraic over $K_{\mathfrak{p}}(u)$.

The truth of Conjecture 1 would already imply an interesting algebraicity criterion for formal power series over number fields.

Eisenstein's Algebraicity Criterion. *Let $f = \sum_{k\in\mathbb{N}} a_k t^k$ be a formal power series over a number field K. Then the following are equivalent:*

(a) *f is algebraic over $K(t)$,*
(b) *f is regularly differentially finite and globally bounded.*

Here an element $f \in K[[t]]$ is called regularly differentially finite if it is a solution of a linear differential equation over $K(t)$, which is regular at 0. The proof that (a) implies (b) is due to G. Eisenstein (reported in [3]). Eisenstein's intention was to develop at least a necessary condition for the algebraicity of solutions of differential equations. The converse implication (b) to (a) would follow from Conjecture 1. It is known that the property being globally bounded is not sufficient at singular points.

The link with Grothendieck's p-curvature conjecture would then be given by the following second conjecture:

Conjecture 2. *Let (M, ∂_M) be a global D-module over a global D-ring $(\mathcal{O}'_F, \partial_F)$ with vanishing p-curvature for almost all primes $p \in \mathbb{Z}$. Then the solutions of M near a non singular prime $\wp$ of degree one in F for M are given by locally bounded power series over the field of constants K of F.*

Obviously Grothendieck's p-curvature conjecture follows from Conjecture 1 and 2. Thus these two conjectures could indicate a way of approaching its proof.

References

[1] André, Y.: *G-functions and Geometry*. Vieweg, Wiesbaden 1989.
[2] Dyckerhoff, T.: *Picard–Vessiot Extensions over Number Fields*. Diplomarbeit, Heidelberg 2005.
[3] Eisenstein, G.: Über eine allgemeine Eigenschaft der Reihen-Entwicklungen algebraischer Funktionen (Bericht von 1852). *Mathematische Werke II*, S. 765–767, Chelsea Publ. Comp., New York 1975.
[4] Matzat, B. H.: Differential equations and finite groups. J. Algebra, to appear.
[5] Matzat, B. H.; van der Put, M.: Iterative differential equations and the Abhyankar conjecture. J. reine angew. Math. **257** (2003), 1-52.
[6] Matzat, B. H.; van der Put, M.: Constructive differential Galois theory. Pp. 425-467 in L. Schneps (Ed.): *Galois Groups and Fundamental Groups*, MSRI Publications 41, Cambridge Univ. Press 2003.
[7] van der Put, M.; Singer, M.F.: *Galois Theory of Linear Differential Equations*. Springer-Verlag, Berlin etc. 2003.

Solvable points on projective algebraic curves

Ambrus Pál

Let X be a quasi-projective variety over a field F. We say that X has a solvable point over F if X has a rational point defined over a solvable extension of F.

Theorem. *Let F be a local field such that the absolute Galois group of its residue field has quotients isomorphic to a finite list of groups ($S_5 \times S_7$, $S_5 \times S_8$, $PSL_3(\mathbb{F}_2)$ and $PSL_3(\mathbb{F}_3)$). Then there is a smooth, geometrically irreducible projective curve defined over F of genus g without solvable points (over the perfection of F) when g is equal to 6, 8, 10, 11, 15, 16, 20, 21, 22 or it is at least 24.* □

The structure of the proof of the theorem is the following. First we construct a connected, but geometrically reducible stable curve of arithmetic genus g without solvable points over the residue field using the assumption on its absolute Galois group. This construction is essentially combinatorial in nature. Then we use classical results of Deligne and Mumford on the deformation theory of stable curves to construct a flat projective curve over the spectrum of the discrete valuation ring of F such that its generic fiber is smooth and geometrically irreducible and its special fiber is the stable curve above. The generic fiber will be of genus g without solvable points.

On the other hand there are natural numbers g such that there are not any smooth, geometrically irreducible projective curves of genus g defined over an arbitrary field without solvable points:

Theorem. *Let F be any field and let X be a smooth, geometrically irreducible projective curve defined over F such that its genus is 0, 2, 3 or 4. Then X has a solvable point.* □

There is a similar result for surfaces. We will call a variety X defined over a field F geometrically rational if it is irreducible and rational over the algebraic closure of F. The theorem is the following:

Theorem. *Let F be any field and let X be a smooth, geometrically rational projective surface defined over F. Then X has a solvable point.* □

These results are proved by examining the canonical linear system on X in order to construct zero-dimensional cycles on X of low degree defined over a solvable extension of F. In order to prove the second theorem we will also show that the Merkurjev-Suslin theorem implies that every Brauer-Severi variety defined over an arbitrary field has a solvable point.

References

[1] A. Pál, *Solvable points on projective algebraic curves*, Canad. J. Math., **56** (2004), no. 3, 612–637.

On the rank of abelian varieties over large fields

Sebastian Petersen

Let A be a non-zero abelian variety over a number field K. Then $A(K)$ is finitely generated by the Mordell-Weil theorem and it is well-known that $\mathrm{rk}(A(\overline{K})) = \infty$. Interesting problems arise if we ask for the rank of A in other infinite algebraic extensions of K. Frey and Jarden posed the following question in their 1974 paper [1].

Question: (Frey, Jarden) *Is $\mathrm{rk}(A(K_{ab})) = \infty$ for any non-zero abelian variety over a number field K? Here K_{ab} denotes the maximal abelian extension of K.*

We use a specialization theorem [8, Prop. 3.1] (see also [7] and [5]) to establish the following abstract condition for infinite rank over infinite algebraic extensions.

Theorem. *Let K be a Hilbertian field, $T|K$ a smooth variety, $T_0 \subset T$ and $U \subset \mathbb{A}_n$ non-empty open subsets and $A|K$ an abelian variety. Let $p : T_0 \to U$ be a finite étale morphism of degree d. Suppose that there is a non-constant morphism $f : T \to A$. Then there is a sequence of geometric points $(t_j)_{j\in\mathbb{N}} \subset T(\overline{K})$ with the following properties:*

a) *$p(t_j) \in U(K)$ is K-rational and $K(t_j)|K$ is a finite, separable extension of degree d.*
b) *$\bigotimes_{j\in\mathbb{N}} K(t_j)$ is a field.*
c) *The image of $f(t_j)$ in $\frac{A(K(t_j))}{A(K)}$ is of infinite order.*

Let $\Omega = \prod_{j\in\mathbb{N}} K(t_j)$ be the composite field of the residue fields of the points t_j. Then $\mathrm{rk}(A(\Omega)) = \infty$.
If p is a Galois cover with group Γ, then the extensions $K(t_j)|K$ are Galois with group Γ and $\Omega|K$ is Galois with group $\prod_{j\in\mathbb{N}} \Gamma$. If in addition Γ is abelian, then $\mathrm{rk}(A(K_{ab})) = \infty$.

We can derive the following partial answer to the abovementioned question of Frey and Jarden from this theorem.

Corollary. *Let $T|\mathbb{P}_1$ be a smooth, geometrically integral Galois cover with group Γ. Let B be an* arbitrary non-zero quotient *of the Jacobian J_T. Then there is a Galois extension $\Omega|K$ with group $\prod_{j\in\mathbb{N}} \Gamma$ such that* $\mathrm{rk}(B(\Omega)) = \infty$. *If Γ is abelian, then* $\mathrm{rk}(B(K_{ab})) = \infty$.

This corollary generalizes the results in [1], [4], [6], [11], [10] on the question of Frey and Jarden. Among these papers the work [10] of Rosen and Wong offers the most general result, namely that the statement of the above corollary is true *provided K is a number field, Γ is cyclic and $J_T \cong B$*. The proof in [10] is totally different from ours.

Unfortunately we do not know whether any abelian variety can be realized as a quotient of the Jacobian J_T of an *abelian* Galois cover $T|\mathbb{P}_1$. This question seems to be a difficult open problem.

The above theorem can be used to obtain infinite rank results over fields which are large in the sense that their Galois group is finitely generated. Fix an integer $e \geq 1$. For $\sigma \in G_K^e$ denote by $K_s(\sigma)$ the fixed field of the closure of the group $\langle \sigma_1, \cdots, \sigma_e \rangle \subset G_K$ generated by the components of the vector σ. We can slightly generalize a classical result in [1].

Corollary. *Let $A|K$ be a non-zero abelian variety. Then* $\mathrm{rk}(A(K_s(\sigma))) = \infty$ *for almost all $\sigma \in G_K^e$ (in the sense of Haar measure on G_K^e).*

The only novelty here is that we do not assume K to be a *finitely generated* Hilbertian field. Our proof, however, is different from the proof in [1] and in our opinion quite simple. In the proof of this corollary we apply the theorem with

$T = A$ and $f = Id$ and make use of the lemma of Borel-Cantelli. M. Jarden recently proved that one may replace $K_s(\sigma)$ by the maximal Galois extension $K_s[\sigma]$ of K in $K_s(\sigma)$ in the above corollary. This strenghtens a result in [3]. We want to mention a third corollary.

Corollary. *Suppose that A admits a projective embedding of degree d. Let Ω be the composite field of all extension fields of K of degree d. Then* $\mathrm{rk}(A(\Omega)) = \infty$.

In [10] Rosen and Wong have shown this with the composite field Ω' of all extensions of K of degree $\leq d(4\dim(A) + 2)$ instead of Ω.

A detailed discussion of the material[1] mentioned so far can be found in [8].

The author suspects that the answer to the question of Frey and Jarden mentioned at the beginning is yes. He even conjectures:

Conjecture. *Let $A|\mathbb{Q}$ be a non-zero abelian variety. For $D \in \mathbb{Q}^\times/2$ denote by $A^D|\mathbb{Q}$ the twist of A by the extension $\mathbb{Q}(\sqrt{D})|\mathbb{Q}$. Then* $\mathrm{rk}(A^D(\mathbb{Q})) \geq 1$ *for infinitely many $D \in \mathbb{Q}^\times/2$.*

Note that there is an isomorphism

$$\frac{A(\mathbb{Q}(\sqrt{\Delta}))}{A(\mathbb{Q})} \otimes \mathbb{Z}[\frac{1}{2}] \cong \bigoplus_{D \in \Delta \setminus \{1\}} A^D(\mathbb{Q}) \otimes \mathbb{Z}[\frac{1}{2}]$$

for any subgroup $\Delta \subset \mathbb{Q}^\times/2$. Hence the following statements are equivalent:

a) The above conjecture holds true.
b) Any non-zero abelian variety $A|\mathbb{Q}$ acquires infinite rank over the maximal Kummer extension $\mathbb{Q}(\sqrt{\mathbb{Q}^\times})|\mathbb{Q}$ of exponent 2.

There is some of work in progress relating the author's conjecture to a suitable version of the conjecture of Birch and Swinnerton-Dyer (denoted by BSD in the sequel). We briefly describe the main idea: For an abelian variety $B|\mathbb{Q}$ denote by $W(B)$ the root number of B. Note that $W(B)$ can be defined as a product of local terms without assuming any conjectures. Presumably $W(B)$ is the sign in a conjectured functional equation for the L-series of B. If the BSD-conjecture holds true, then $W(A^D) = -1$ implies $\mathrm{rk}(A^D(\mathbb{Q})) \geq 1$. There is a formula [9] of Rohrlich relating $W(A^D)$ to $W(A)$ provided A is an elliptic curve. Sabitova[2] recently found an analoguous formula for abelian varieties of arbitrary dimension. This formula suggests that, in fact, $W(A^D) = -1$ for infinitely many $D \in \mathbb{Q}^\times/2$. We have, however, not yet checked the details.

[1]The author is indebted to his supervisor C. Greither and also to M. Jarden for very helpful suggestions while this work was done.

[2]The author wants to thank T. Chinburg for bringing Sabitova's work to his attention during the workshop in Oberwolfach.

References

[1] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proc. London Math. Soc. **28** (1974), 112–128

[2] M. D. Fried and M. Jarden, *Field Arithmetic, Second Edition, revised and enlarged by Moshe Jarden*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2005

[3] W.-D. Geyer and M. Jarden, *The rank of Abelian varieties over large algebraic fields*, Archiv der Mathematik, to appear

[4] H. Imai, *On the rational points of some Jacobian varieties over large algebraic number fields*, Kodai Math. J. **3** (1980), 56–58

[5] S. Lang, *Fundamentals of Diophantine Geometry*, Springer 1983

[6] N. Murabayashi, *Mordell-Weil rank of the jacobians of the curves defined by* $y^p = f(x)$, Acta Arithmetica **LXIV.4** (1993), 297–302

[7] A. Néron, *Problèmes arithmétiques et géometriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **83** (1952), 101–166

[8] S. Petersen, *On a Question of Frey and Jarden about the Rank of Abelian Varieties* (with an appendix by M. Jarden), Journal of Number Theory, to appear

[9] D. Rohrlich, *Galois theory, elliptic curves and root numbers*, Compositio Math. **100** (1996), 311–349

[10] M. Rosen and S. Wong, *The Rank of Abelian Varieties over Infinite Galois Extensions*, Journal of Number Theory **92** (2002), 182–196

[11] J. Top, *A remark on the rank of jacobians of hyperelliptic curves over* $\mathbb{Q}$ *over certain elementary abelian 2-extensions*, Tôhoku Math. J. **40** (1988), 613–616

On the elementary theory of function fields

Florian Pop

First let us recall/introduce notations as follows:

• For a field K, we denote by $\mathbf{Th}(K)$ its elementary theory, i.e., the set of all first order sentences φ which are true in K.

• We say that fields K and L are elementarily equivalent if they have the same elementary theory, i.e., $\mathbf{Th}(K) = \mathbf{Th}(L)$.

Clearly, if K and L are isomorphic, then they are elementarily equivalent. The converse of this assertion is wrong, but the following well known model theoretical fact is a very good substitute for that:

K and L are elementarily equivalent if and only if there exist ultra-powers $K^I/\mathbf{U}$ and $L^J/\mathbf{V}$ which are isomorphic as fields.

Main Question. What information about K is encoded in $\mathbf{Th}(K)$ in arithmetical/geometrical significant situations, i.e., when K are function fields over some "reasonable" base fields k?

Part of this question is actually the following:

Conjecture (Elementary equivalence versus Isomorphisms)**.** Let $K|k$ and $L|l$ be regular function fields over reasonable base fields k and l. Suppose that K and L are elementarily equivalent. Then k and l are elementarily equivalent, and if $k \cong l$, then $K \cong L$ as fields.

The notation of a reasonable base field k is not completely clarified, but the prime fields $\mathbf{Q}$, $\mathbf{F}_p$, and the so called *large fields* should be reasonable base fields.

• Arithmetic situation: In this case K is a function field over its prime field k_0; or equivalently, if K is a finitely generated field, and its field of constants k is finite over k_0.

• Geometric situation: In this case K is a function field over an algebraically closed field k.

• More general, we will speak about the anti-Mordellic situation, if K is a function field over a large field k satisfying further conditions.

Some results

In my talk I first mentioned some **old results** by Duret, Pierce, Vidaux, concerning the the elementary theory of function fields $K|k$ of curves in the geometric situation: The isomorphy type of K is encoded in $\mathbf{Th}(K)$ if K is not the function field of a CM elliptic curve of some special type. And the very striking result by Rumely saying that for every global field K there exists a sentence φ_K which distinguishes the isomorphy type of K among the global fields: If L is another global field, then φ_K holds in L if and only if $K \cong L$ as fields.

The main focus of my talk was on the following *newer results* by Pop, Poonen, and Poonen-Pop:

Pop (2002):

Arithmetic situation

(1) For every characteristic p there exists a sequence of sentences φ_d, where $d \geq 0$, such that given a finitely generated field K with $\mathrm{char}(K) = p$ one has: φ_d is true in K if and only if $\mathrm{tr.deg.}(K|k) = d$.

In particular, $\mathrm{tr.deg.}(K|k)$ is encoded in $\mathbf{Th}(K)$.

(2) Moreover, for every characteristic p there exist a formula $\phi(t_1, \ldots, t_r)$ with parameters $t_1, \ldots, t_r$ such that given a finitely generated field K with $\mathrm{char}(K) = p$, and a system $(a_1, \ldots, a_r)$ of elements of K, one has: $\phi(a_1, \ldots, a_r)$ is true in K if and only if $(a_1, \ldots, a_r)$ is part of a separable transcendence basis of $K|k$.

In particular, if K and L are finitely generated fields which are elementarily equivalent, then K and L are isogeneous, i.e., there exist separable field embeddings $K \hookrightarrow L$ and $L \hookrightarrow L$.

Therefore, if K and L are as at 2) above, and K is the function field of a variety of general type, then $K \cong L$ as fields.

Geometric situation

(1) There exists a sequence of sentences φ_d such that for every function field $K|k$ as at 3) above one has: φ_d is true in K if and only if $\mathrm{tr.deg.}(K|k) = d$.

Moreover, (for every characteristic p) there exist a formula $\phi(t_1, \ldots, t_r)$ (depending on p) with parameters $t_1, \ldots, t_r$ such that given a finitely generated field K (with $\mathrm{char}(K) = p$), and a system $(a_1, \ldots, a_r)$ of elements of K, one has:

$\phi(a_1, \ldots, a_r)$ is true in K if and only if $(a_1, \ldots, a_r)$ is part of a (separable) transcendence basis of $K|k$.

(2) From this one deduces that if $K|k$ and $L|k$ are elementary equivalent, and $K|k$ is the function field of a k-variety of general type, then K and L are isomorphic as function fields.

Poonen (2005):

(1) There exists a predicate $p(t)$ such that given a finitely generated field K one has: The constant field k of K is definable by $p(t)$ inside K, in other words one has $k = \{a \in K \mid p(a) \text{ true in } K\}$.

(2) There exists a formula $\phi_r(t_1, \ldots, t_r)$ such that given a finitely generated field K, and a system $(a_1, \ldots, a_r)$ of elements of K, one has: $\phi(a_1, \ldots, a_r)$ is true in K if and only if $(a_1, \ldots, a_r)$ are algebraically independent over the prime field of K.

Poonen-Pop (2005):

(1) There exists a predicate $p(x)$ such that given a function field $K|k$ with k large and relatively closed in K one has: k is definable inside K by $p(x)$, i.e., $k = \{a \in K \mid p(a) \text{ true in } K\}$.

(2) One has similar results as at Poonen, 2) above, but a little bit more technical.

Methods of proof

The main new insight is that using the properties of Pfister quadratic forms and their generalizations, one can detect algebraic dependence. (Here the main ingredients are the Galois cohomological characterization of the algebraic independence, combined with the Milnor's Conjecture, proved by Voevodsky et al, Rost, etc. See e.g. [3] and [4], where more can be found.)

Example: Let $K|\mathbf{Q}$ be a function field. Then tr.deg.$(K|\mathbf{Q}) = d$ if and only if the following holds: Every $(d+3)$ fold Pfister form over K becomes isotropic over $K[\sqrt{-1}]$, and there exist $(d+2)$ fold Pfister forms over K which are not isotropic over $K[\sqrt{-1}]$.

In his proofs, Poonen does also uses in a subtle way Rumely's result as well as facts about the the relation between the rational points $E(K)$ and $E(k)$ of some special elliptic curves E, etc.

References

[1] J.-B. Bell and A.-B. Slomson, *Models and ultra-products: an introduction,* Amsterdam 1969.

[2] J.-L. Duret, *Équivalence élémentaire et isomorphisme des corps de courbe sur un corps algebriquement clos,* J. Symbolic Logic **57** (1992), 808–923.

[3] E. Kahn, *La conjecture de Milnor (d'après Voevodsky),* Séminaire Bourbaki, Asterisque **245** (1997), 379–418.

[4] A. Pfister, *On the Milnor conjectures: history, influence, applications,* Jahresbericht DMV **102** (2000), no. 1, 15–41.

[5] D. Pierce, *Function fields and elementary equivalence,* Bull. London Math. Soc. **31** (1999), 431–440.

[6] B. Poonen, *Uniform first-order definitions in finitely generated fields*, Preprint, 2005
[7] B.Poonen and F. Pop, *First order definitions in function fields over anti-Mordellic fields,* See http://arxiv.org/PS_cache/math/pdf/0602
[8] F. Pop, *Elementary equivalence versus Isomorphism,* Invent. Math. **150** (2002), 385-408.
[9] R.-S. Rumely, *Undecidability and definability for the theory of global fields,* Trans. AMS **262** (1980), no. 1, 195–217.
[10] X. Vidaux, *Multiplication complexe et équivalence élémentaire dans le langage des corps,* J. Symbolic Logic **67** (2002), no. 2, 635–648.

Henselian valued fields

Alexander Prestel

In this talk we give a brief summery of the "going down" properties of henselian valuation rings on fields.

Let (K, O) be a field together with a valuation ring O of K. We say that (K', O') extends (K, O) if K' is a field extending K and $O' \cap K = O$. A valued field (K, O) is called *henselian* if the valuation ring O of K has a unique extension to the separable closure K^s of K. Equivalently, (K, O) is henselian if every polynomial $f \in O[X]$ that has a simple root modulo the maximal ideal M of O, has a root in K.

Let $V(K)$ be the set of valuation rings $O \subsetneq K$. Two valuation rings $O_1, O_2 \in V(K)$ induce the same topology on K if and only if the composition O_1O_2 also belongs to $V(K)$. Thus the totality of valuation rings of K inducing a fixed topology forms a tree by the partial ordering of inclusion. For the set $H(K)$ of henselian valuation rings $O \subsetneq K$ even more can be said.

Let $H_1(K)$ be the set of valuation rings $O(K)$ such that O/M is *not* separably closed, while $H_2(K)$ is the set of those $O \in H(K)$ such that O/M is separably closed. Now $H_1(K)$ is linearly ordered and sits on top of the tree formed by $H_2(K)$. If $H_2(K) = \emptyset$, then $H_1(K)$ has a smallest element O^*, called the *canonical* valuation ring of K. If $H_2(K) \neq \emptyset$, then $H_2(K)$ has a maximal element O^* which now is called the canonical valuation ring. Let $H^*(K) = H_1(K) \cup \{O^*\}$. With these notations the following theorems hold:

Theorem 1. *Let K'/K be a normal extension (finite or infinite). Then every henselian $O' \in H^*(K')$ restricts to a henselian $O = O' \cap K \in H^*(K)$.*

Theorem 2. *Let K'/K be a finite extension with K' not being separably closed. Then $O' \in H^*(K')$ implies $O = O' \cap K \in H^*(K)$.*

Theorem 3 (Koenigsmann)**.** *Let p be a rational prime and K' the fixed field of a p-Sylow subgroup of the absolute Galois group $G(K^s/K)$ of K. Then every henselian $O' \in H^*(K')$ restricts to a henselian $O = O' \cap K \in H^*(K)$, unless $p = 2$ and O'/M' is real closed.*

The proofs of the above theorems can be found in [1].

References

[1] A.J. Engler, A. Prestel, *Valued Fields*, Springer Monographs in Math. (2005).

Hilbert's tenth problem, Mazur's conjectures and Poonen's theorem

Alexandra Shlapentokh

At the beginning of the XX century David Hilbert ask the following question:

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

Using modern terms one can ask if there exists a program taking coefficients of a polynomial equation as input and producing "yes" or "no" answer to the question "Are there integer solutions?". This question became known as *Hilbert's Tenth Problem* because it was the problem # 10 on the list of problems some of which were presented by Hilbert at the International Congress of Mathematicians in 1900.

The question of Hilbert was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matijasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of integers are the same as the Diophantine subsets of integers. (See [2] and [3] for more details.)

The question asked by Hilbert can of course be asked about any recursive ring R. In other words we can ask if there is an algorithm which, if given an arbitrary polynomial equation in several variables with coefficients in R, can determine whether this equation has solutions in R. This question is still open for $R = \mathbb{Q}$ and R equal to the ring of integers of an arbitrary number field.

One way to answer the question negatively for a ring R of characteristic 0 is to construct a Diophantine definition of $\mathbb{Z}$ over R or more generally to construct a Diophantine model of $\mathbb{Z}$ over R. Unfortunately, some conjectures formulated by Barry Mazur and a theorem of Gunther Cornelissen and Karim Zahidi indicate that this line of the attack on Hilbert's Tenth Problem over $\mathbb{Q}$ is not likely to succeed. (See [1], [5], [6], [7], [8], for more details on these conjectures and their consequences.)

Given the difficulty of resolving the Hilbert's Tenth Problem over $\mathbb{Q}$ one could attempt to consider the problem over some "intermediate " rings between $\mathbb{Z}$ and $\mathbb{Q}$. We defined these rings below for an arbitrary number field.

Let K be a number field and let $\mathcal{S}$ be an arbitrary set of its non-archimedean primes. Then let $O_{K,\mathcal{S}}$ be the following ring

$$\{x \in K : \mathrm{ord}_{\mathfrak{p}} x \geq 0 \text{ for all } \mathfrak{p} \notin \mathcal{S}\}$$

If $\mathcal{S}$ is finite, we call the corresponding ring a *small* ring, and we call the ring a *big* one otherwise.

Using some ideas of Julia Robinson originally needed for a first-order definition of rational and algebraic integers over number fields (see [10] and [11]), and a proposition of Denef on definability of non-zero elements over subrings of number fields (see [4]), we can give a Diophantine definition of $\mathbb{Z}$ in any small subring of rational numbers. Thus we know that Hilbert's Tenth Problem is undecidable of these rings.

Over large rings the situation proved to be much more complicated. While we have some $\mathbb{Z}$-definability results for big rings for non-trivial totally real extensions of $\mathbb{Q}$ and their extensions of degree two (see [12], [13], [14], [15]), we don't have a Diophantine definition of $\mathbb{Z}$ over any large subring of rational numbers.

However, just as one can consider Diophantine definability of $\mathbb{Z}$ over subrings of $\mathbb{Q}$, one could also consider a version of Mazur's conjectures and Diophantine models over these rings. In pursuing this line of investigation Poonen proved the following theorem in [9].

Theorem.
There exist recursive sets of rational primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of rational primes containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, the following hold:

- *There exists an affine curve E defined over $\mathbb{Q}$ such that the topological closure of $E(O_{\mathbb{Q},\mathcal{S}})$ in $E(\mathbb{R})$ is an infinite discrete set. Thus the ring version of Mazur's conjecture does not hold for $O_{\mathbb{Q},\mathcal{S}}$.*
- *$\mathbb{Z}$ has a Diophantine model over $O_{\mathbb{Q},\mathcal{S}}$.*
- *Hilbert's Tenth Problem is undecidable over $O_{\mathbb{Q},\mathcal{S}}$.*

References

[1] Gunther Cornelissen and Karim Zahidi. Topology of diophantine sets: Remarks on Mazur's conjectures. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 253–260. American Mathematical Society, 2000.

[2] Martin Davis. Hilbert's tenth problem is unsolvable. *American Mathematical Monthly*, 80:233–269, 1973.

[3] Martin Davis, Yurii Matijasevich, and Julia Robinson. Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution. In *Proc. Sympos. Pure Math.*, volume 28, pages 323– 378. Amer. Math. Soc., 1976.

[4] Jan Denef. Diophantine sets of algebraic integers, II. *Transactions of American Mathematical Society*, 257(1):227– 236, 1980.

[5] Barry Mazur. The topology of rational points. *Experimental Mathematics*, 1(1):35–45, 1992.

[6] Barry Mazur. Questions of decidability and undecidability in number theory. *Journal of Symbolic Logic*, 59(2):353–371, June 1994.
[7] Barry Mazur. Speculation about the topology of rational points: An up-date. *Asterisque*, 228:165–181, 1995.
[8] Barry Mazur. Open problems regarding rational points on curves and varieties. In A. J. Scholl and R. L. Taylor, editors, *Galois Representations in Arithmetic Algebraic Geometry*. Cambridge University Press, 1998.
[9] Bjorn Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *Journal of AMS*, 16(4):981–990, 2003.
[10] Julia Robinson. The undecidability of algebraic fields and rings. *Proceedings of the American Mathematical Society*, 10:950–957, 1959.
[11] Julia Robinson. On the decision problem for algebraic rings. In *Studies in mathematical analysis and related topics*, pages 297–304. Stanford Univ. Press, Stanford, Calif, 1962.
[12] Alexandra Shlapentokh. Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator. *Inventiones Mathematicae*, 129:489–507, 1997.
[13] Alexandra Shlapentokh. Defining integrality at prime sets of high density in number fields. *Duke Mathematical Journal*, 101(1):117–134, 2000.
[14] Alexandra Shlapentokh. On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2. *Journal of Number Theory*, 95:227–252, 2002.
[15] Alexandra Shlapentokh. Diophantine Definability and Decidability in the Extensions of Degree 2 of Totally Real Fields. *pre-print*.

Anabelian properties of the moduli spaces of smooth projective curves

Jakob Stix

The talk delivered at the meeting and the report below contain a survey of the results obtained by the author in [3].

1. Rational curves

In [2] Oort constructs non-constant maps $\mathbb{P}^1(k) \to \mathrm{M}_g(k)$ for large, suitable g by exploiting 'Parshin's trick'. Here k is an algebraically closed field and M_g is the coarse moduli variety of smooth, projective, geometrically connected curves of genus g. In contrast, the fine moduli stack $\mathscr{M}_g$ parametrising families of smooth, projective, geometrically connected curves of genus $g \geq 2$ does not contain rational curves. In characteristic 0 this follows for example from the uniformisation of $(\mathscr{M}_g)^{\mathrm{an}}$ by Teichmüller space which is a ball and the simply connectedness of $\mathbb{P}^1$. Indeed, any map $f : T \to (\mathscr{M}_g)^{\mathrm{an}}$ from a simply connected complex variety T must lift to Teichmüller space and hence is forced to be constant if T is proper or by Liouville for T the complex plane. The Brødy hyperbolicity of $(\mathscr{M}_g)^{\mathrm{an}}$ follows.

The moduli space of principally polarised abelian varieties $\mathscr{A}_{g,1}$ behaves similar at first sight. It is uniformised by the Siegel upper half plane. But, again in [2], Oort constructs rational families of abelian varieties in positive characteristic, essentially by using rational families of maps from α_p to a given abelian variety with p-rank exceeding 1. This raises the question of the existence of simply connected

subvarieties of $\mathscr{M}_g$ in positive characteristic and in particular of an algebraic reasoning.

2. Anabelian Geometry

Anabelian geometry deals with the arithmetical/geometrical content of the profinite étale fundamental group of a variety. In homotopy theory, for X an Eilenberg-MacLane $\mathrm{K}(\pi,1)$ space, the fundamental group $\pi_1 X = \pi$ determines all maps up to homotopy from CW-spaces with target X. One consequence is that group cohomology of π with coefficients in F computes the singular cohomology of X with coefficients in the associated locally constant sheaf $\mathscr{F}$.

We define an **algebraic** $\mathrm{K}(\pi,1)$ **space** to be a variety over an algebraically closed field, such that the canonical map

$$\gamma^* : \mathrm{H}^*(\pi_1^{\text{ét}} X, F) \to \mathrm{H}^*(X_{\text{ét}}, \mathscr{F})$$

is an isomorphism for all finite F and associated $\mathscr{F}$. In general, we call the cohomology classes in the image of γ^* **group theoretic** cohomology classes.

One difference between $\mathscr{M}_g$ and $\mathscr{A}_{g,1}$ consists in the pro-finite properties of their respective analytic fundamental groups: the Mapping class group is conjectured to be good in the sense of Serre, whereas $\mathrm{Sp}_{2g}(\mathbb{Z})$ is definitely not good. This might explain why the 'analytic $\mathrm{K}(\pi,1)$ behaviour' of $\mathscr{A}_{g,1}$ does not carry over to the algebraic and moreover positive characteristic setting.

3. Constant maps

Theorem 1. *Let k be an algebraically closed field and X/k a quasi-projective, connected variety such that for some prime ℓ different from the characteristic and for all $n \in \mathbb{N}$ all classes in $H^2(X, \mathbb{Z}/\ell^n\mathbb{Z})$ are group theoretic. Let $f : T \to X$ be a regular map from a proper, reduced and connected variety T/k such that $\pi_1 f$ is the trivial map. Then f must be constant.*

Proof: One just notices that f is constant if and only if it contracts all proper curves in T, which is a numerical condition. The pullback of an ample numerical class can be computed via group cohomology, hence vanishes, and we are done.

In order to apply Theorem 1 to the moduli space of smooth, projective curves we either need to prove that the mapping class group is good in cohomological degree 2 (announced by Boggi) or find different means. The alternative proof deals only with some quotient of the fundamental group of $\mathscr{M}_g$. Thus it yields a much stronger theorem also strengthening the characteristic 0 case, which for the full fundamental group follows from the analytic argument given above as the mapping class group is residually finite.

Let X/S be a family of smooth, projective, geometrically connected curves of genus $g \geq 2$ with S connected. Let $\mathbb{L}$ be a set of primes invertible on S. Then one can proof, see [3] and the comments in loc. cit., that the homotopy sequence

$$\pi_1(\text{fibre}) \to \pi_1 X \to \pi_1 S \to 1$$

yields an outer monodromy representation $\rho : \pi_1 S \to \mathrm{Out}\left(\pi^{\mathbb{L}}\right)$ where $\pi^{\mathbb{L}}$ is the pro-$\mathbb{L}$ completion of the fundamental group of a geometric fibre of X/S. The construction is compatible with pullback, hence comes by composition with the characteristic map from the universal outer representation

$$\rho^{\mathrm{univ}} : \pi_1\big(\mathscr{M}_g \otimes \mathbb{Z}[\frac{1}{\mathbb{L}}]\big) \to \mathrm{Out}\left(\pi^{\mathbb{L}}\right).$$

Theorem 1bis. *Let T be a reduced, connected variety over an algebraically closed field k. Let $f : T \to \mathscr{M}_g$, $g \geq 2$, be a map such that for the associated curve the outer pro-$\mathbb{L}$ representation $\rho : \pi_1 T \to \mathrm{Out}\left(\pi^{\mathbb{L}}\right)$ is the trivial homomorphism for one of the following collections of sets of prime numbers $\mathbb{L}$ and additional conditions on k:*

(A) *$\mathbb{L} = \{\ell\}$ for some prime number ℓ and k is of characteristic 0, or*
(B) *$\mathbb{L} = \{\ell_1, \ell_2\}$ for all pairs of sufficiently large prime numbers ℓ_1, ℓ_2 invertible in k and k is of positive characteristic.*

Then f is constant in the sense that the corresponding T-curve $X/T \in \mathscr{M}_g(T)$ comes by base extension from a curve in $\mathscr{M}_g\big(\mathrm{Spec}(k)\big)$.

The basic idea of the proof is to look at the corresponding family of Jacobians which has constant $\mathbb{L}$-primary torsion by the condition of the theorem. Then use the Torelli theorem. This explains the easier condition in characteristic 0.

But this approach fails in positive characteristic. We only deduce that our Jacobians all have the same p-rank. A construction of auxiliary covers following Tamagawa (after Raynaud) that has already been exploited by Saïdi allows nevertheless to deduce the theorem. It is in the construction of the auxiliary covers that condition (B) on the sets $\mathbb{L}$ comes up.

4. Monodromy controls good reduction

There are several known criteria for good reduction that ask for unramified Galois action. Galois action is nothing but monodromy action in the arithmetic case. The question of good reduction turns out to be the question of extendibility for the representing map to the respective moduli space. Put together, these ideas indicate that extending a map $f : U \to \mathscr{M}_g$ from some open dense subscheme $U \subset S$ in the normal scheme S to a map $\tilde{f} : S \to \mathscr{M}_g$ is controlled by monodromy.

Theorem 2 (Moret-Bailly)**.** *The above f always extends uniquely for S regular and $S \setminus U$ of codimension at least 2.*

This is the purity result for smooth, projective curves of Moret-Bailly in [1]. If we combine Zariski–Nagata's purity of the branch locus, Moret-Bailly's theorem above and the following criterion for good reduction from [4], Thm 5.3,

Theorem 3 (Oda–Tamagawa)**.** *Let S be the spectrum of a discrete valuation ring, and U be the generic point. Then a curve of genus $g \geq 2$ over U extends uniquely over S iff the associated outer pro-ℓ monodromy representation is unramified, i.e., factors over $\mathrm{Gal}_K = \pi_1 \mathrm{Spec}(K) \to \pi_1 S$, for some ℓ invertible in K.*

we obtain the case of regular bases S of the following monodromy criterion of good reduction of smooth, projective curves.

Theorem 4. *Let U be a dense open subscheme of a normal, connected, excellent scheme S. Let X/U be a U-curve in $\mathscr{M}_g(U)$ for some $g \geq 2$. Then X/U extends to an S-curve in $\mathscr{M}_g(S)$ if and only if the pro-$\mathbb{L}$ monodromy representation*

$$\rho : \pi_1\big(U \otimes \mathbb{Z}[\frac{1}{\mathbb{L}}]\big) \to \mathrm{Out}\,\big(\pi^{\mathbb{L}}\big)$$

factors over $\pi_1\big(U \otimes \mathbb{Z}[\frac{1}{\mathbb{L}}]\big) \to \pi_1\big(S \otimes \mathbb{Z}[\frac{1}{\mathbb{L}}]\big)$ for one of the following collections of sets of prime numbers $\mathbb{L}$ and additional conditions on S:

(A) *$\mathbb{L} = \{\ell\}$ for some prime number ℓ and S is of characteristic 0, or*
(B) *$\mathbb{L} = \{\ell_1, \ell_2\}$ for all pairs of sufficiently large prime numbers ℓ_1, ℓ_2 and no additional conditions on S.*

For the proof and details on the matter of this report see [3].

References

[1] L. Moret-Bailly, *Un théorème de pureté pour les familles de courbes lisses*, C. R. Acad. Sci. Paris Sér. I Math. **300** (1985), no. 14, 489–492.
[2] F. Oort, *Subvarieties of moduli spaces*, Inventiones Math. **24** (1974), 95–119.
[3] J. Stix, *A monodromy criterion for extending curves*, Intern. Math. Res. Notices **29** (2005), 1787–1802.
[4] A. Tamagawa, *The Grothendieck conjecture for affine curves*, Compositio Math. **109** (1997), 135–194.

The ex-Ax conjecture (after Kollár)

Tamás Szamuely

A field k is called a *C_1-field* if every homogeneous polynomial $f \in k[x_0, \ldots, x_n]$ of degree $d \leq n$ has a nontrivial zero. More generally, it is a C_1'-field if every system of homogeneous polynomials $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ whose degrees d_i satisfy $\sum d_i \leq n$ has a nontrivial common zero. Classical examples of C_1'-fields are finite fields (Chevalley), function fields of curves over an algebraically closed field (Tsen), and Laurent series fields over an elgebraically closed field (Lang). The notion of C_1-fields stems from E. Artin, who called them quasi-algebraically closed, because their Brauer group is trivial (i.e. there are no nontrivial finite dimensional central division algebras over them). For more on these fields, see e.g. [3], Section 6.2.

On the other hand, k is called a *PAC (pseudo-algebraically closed) field* if every geometrically integral k-variety has a k-point. This notion was introduced in [1]; see [2] for an exhaustive and up-to-date treatment. It is known that every PAC field has cohomological dimension one, and hence trivial Brauer group; the same is true of C_1-fields. The converse is false in both cases.

In his paper [1] cited above, Ax asked whether every perfect PAC field is C_1. This conjecture is now a theorem in characteristic 0 thanks to recent work of J. Kollár:

Theorem 1. (Kollár [4]) *Every PAC field of characteristic 0 is C_1'.*

My lecture at Oberwolfach presented the proof of this theorem.

Step 1. The first idea is to observe that it is enough to prove that the Zariski closed subset $X \subset \mathbf{P}^n$ defined as the zero locus of a system of polynomials $f_1, \dots, f_s$ as in the C_1' condition contains a geometrically integral k-subvariety.

Step 2. For a system of sufficiently general f_i's the subset X above is a smooth complete intersection variety, and in particular geometrically integral, thus we are done. Otherwise by an easy deformation argument one finds a fibration over $\mathbf{P}^1$ that contains X as a special fibre, and whose generic fibre is is a smooth complete intersection variety defined by polynomials g_i of the same degree as the f_i. It then suffices to prove:

Theorem 2. *Let k be a field of characteristic 0, C a smooth projective k-curve, Z an irreducible, projective k-variety and $g : Z \to C$ a proper surjective morphism. Assume that the generic fibre is*

(1) *smooth,*
(2) *geometrically connected, and*
(3) *Fano (that is, its anti-canonical class is ample).*

Then every fibre $g^{-1}(c)$ contains a $k(c)$-subvariety which is geometrically integral.

Note that a smooth complete intersection in $\mathbf{P}^n$ defined by polynomials satisfying the degree condition $\sum d_i \leq n$ is always a Fano variety.

Step 3. Theorem 2 follows from the following variant of the Kollár–Shokurov connectedness theorem:

Theorem 3. *Let Y be a smooth, projective variety, C a smooth projective curve and $f : Y \to C$ a proper surjective morphism with geometrically connected fibres. Let $D = \sum a_i P_i$ be a $\mathbf{Q}$-divisor on Y such that*

(1) $\mathrm{Supp}(D)$ *has simple normal crossings,*
(2) $\mathrm{Supp}(D)$ *is contained in finitely many fibres of f, and*
(3) $-(K_Y + D)$ *is ample, where K_Y is the canonical divisor of Y.*

Then every fibre of $f : \mathrm{Supp}(D_{\geq 1}) \to C$ is geometrically connected.

The proof of this theorem is based on the fundamental Kawamata-Viehweg vanishing theorem, itself a variant of the Kodaira vanishing theorem. These vanishing theorems are false in positive characteristic.

The theorem is applied via the following corollary:

Corollary 3. *Let Y, C and f be as above, and let $D = \sum a_i P_i$ be a $\mathbf{Q}$-divisor on Y such that*

(1) $\mathrm{Supp}(D) + (\text{any fibre of } f)$ *has simple normal crossings,*
(2) $\mathrm{Supp}(D)$ *is contained in finitely many fibres of f,*
(3) $-(K_Y + D)$ *is ample.*

Then for every $c \in C$ the fibre $f^{-1}(c)$ contains a $k(c)$-irreducible component which is geometrically integral.

One derives the corollary by fixing first $c \in C$, and then adding to D a suitably chosen vertical $\mathbf{Q}$-divisor so that the $\mathbf{Q}$-divisor D' thus obtained still satisfies conditions 1–3, and moreover its only component with coefficient ≥ 1 contained in $f^{-1}(c)$ is an irreducible component of $f^{-1}(c)$ (which is smooth by definition). Then the theorem applies to D' and yields the corollary. To guarantee condition 3 for D' one uses the Kleiman ampleness criterion.

Step 4. To derive Theorem 2 from the above corollary, one first observes that if $h : Z' \to Z$ is a dominating morphism of varieties over C and the conclusion of Theorem 2 holds for Z', then it holds for Z. Hironaka's desingularization theorem shows that after blowing up Z finitely many times one finds such a morphism h with Z' smooth, projective, and having normal crossing fibres over C. It remains to secure a suitable divisor D, which one finds, again after suitable blowups, using condition 3 of Theorem 2.

References

[1] J. Ax, The elementary theory of finite fields, *Ann. of Math.* 88 (1968), 239–271.

[2] M. Fried, M. Jarden, *Field Arithmetic*, 2nd ed., Springer-Verlag, 2005.

[3] P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006.

[4] J. Kollár, A conjecture of Ax and degenerations of Fano varieties, preprint, 2005, to appear in *Israel Journal of Mathematics.*

Stable reduction of Lubin–Tate spaces of dimension one

Stefan Wewers

The Lubin–Tate tower Let F be a local field. We denote by $\mathcal{O}$ its ring of integers, by $\wp$ its maximal ideal and by $k = \mathcal{O}/\wp$ its residue class field. Note that k is a finite field; we write q for the cardinality and p for the characteristic of k.

Fix an integer $h \geq 1$. To F and h one can associated a certain projective system

$$\mathsf{X}(\wp^\infty) = \big(\cdots \to \mathsf{X}(\wp^2) \to \mathsf{X}(\wp) \to \mathsf{X}(1) \big)$$

of rigid analytic spaces over the field $\hat{F}^{\mathrm{nr}}$, called the *Lubin–Tate tower*. At a fixed level $n \geq 0$, the rigid analytic space $\mathsf{X}(\wp^n)$ is smooth of dimension $h-1$. At the bottom level, $\mathsf{X}(1)$ is (non-canonically) isomorphic to an open polydisk.

Our notation (which is not the standard one) suggests a relation to modular curves. And indeed, in the special case $F = \mathbb{Q}_p$ and $h = 2$ the space $\mathsf{X}(\wp^n)$ can be identified with a certain open subset of the rigid space over $\mathbb{Q}_p^{\mathrm{nr}}$ associated to the classical modular curve $X(p^n m)$, for some $m \geq 3$ which is prime to p. In the general case, $\mathsf{X}(\wp^n)$ is an example of a *Rapoport–Zink space*, which is a sort of local analogue of a Shimura varity.

Non-abelian Lubin–Tate theory A recent theorem of Harris and Taylor [2] states that the étale cohomology of the tower $\mathsf{X}(\wp^\infty)$ realizes the local Langlands correspondence and the Jacquet–Langlands correspondence for supercuspidal representations of the group $\mathrm{GL}_h(F)$. For $h = 1$ this is nothing but a

restatement of classical Lubin–Tate theory, i.e. the construction of the reciprocity map $F^\times \to \mathrm{Gal}(F^{\mathrm{ac}}/F)^{\mathrm{ab}}$ in terms of division points of certain formal groups. For $h = 2$ the theorem of Harris–Taylor had been proved earlier by Carayol, extending work of Deligne. It was also Carayol who formulated the general conjecture for $h > 2$, see [1].

To be a bit more precise we have to introduce some notation. Let $G := \mathrm{GL}_h(F)$, W_F the Weil group of F and B the division algebra of dimension h^2 over F with invariant $1/h$. The group $\Gamma := G \times B^\times \times W_F$ has a surjective morphism onto $\mathbb{Z}$ such that the kernel Γ_0 of this map acts, in a natural way, on the tower $\mathsf{X}(\wp^\infty)$. So

$$\mathcal{H} := \mathrm{Ind}_{\Gamma_0}^{\Gamma} \mathcal{H}_0, \quad \mathcal{H}_0 := \varinjlim_n H_{\mathrm{et}}^{h-1}(\mathsf{X}(\wp^n)_{\hat{F}^{\mathrm{ac}}}, \bar{\mathbb{Q}}_\ell)$$

defines an (infinite dimensional) representation of Γ. Fix a quasicharacter $\chi : F^\times \to \bar{\mathbb{Q}}_\ell^\times$ and let $\mathcal{H}_\chi$ denote the subspace of $\mathcal{H}$ where G acts with central character χ. Then the main theorem of non-abelian Lubin–Tate theory says the following. For every irreducible supercuspidal representation π of G with central character χ we have an isomorphism

$$\mathrm{Hom}_G(\pi, \mathcal{H}_\chi) \cong \mathrm{JL}(\pi)^\vee \otimes \mathrm{L}(\pi)' \tag{1}$$

of representations of $B^\times \times W_F$. Here $\mathrm{JL}(\pi)$ denotes the supercuspidal representation of $B^\times$ corresponding to π under the Jacquet–Langlands correspondence and $\mathrm{L}(\pi)'$ is, up to normalization, the two-dimensional irreducible representation of W_F corresponding to π under the local Langlands correspondence.

Stable reduction of $\mathsf{X}(\wp^n)$ From now on, we suppose that $h = 2$. Then the spaces $\mathsf{X}(\wp^n)$ are smooth of dimension one and occur naturally as an étale $\mathrm{GL}_2(\mathcal{O}/\wp^n)$-torsor of the open unit disk $\mathsf{X}(1)$. We call a rigid space of this form an *open analytic curve*; one can see this as a non-archimedian analogue of a compact Riemann surface with finitely many closed disks removed. An easy extension of the usual semistable reduction theorem shows that the spaces $\mathsf{X}(\wp^n)$ have an (essentially unique) *stable model* $\mathcal{X}(\varpi^n)$. More precisely, there exists a finite extension $K_n/\hat{F}^{\mathrm{nr}}$ and an integral model $\mathcal{X}(\varpi^n)$ of $\mathsf{X}(\varpi^n)_{K_n}$ with the following properties. Firstly, the special fiber $\bar{X}(\wp^n) := \mathcal{X}(\wp^n)_s$ of $\mathcal{X}(\wp^n)$ is isomorphic to the formal completion $Y|_Z^\wedge$ of a semistable curve Y over k^{ac} along a proper closed subset $Z \subset Y$. Secondly, $\mathcal{X}(\varpi)$ is the minimal integral model satisfying this condition. We call $\bar{X}(\wp^n)$ the *stable reduction* of $\mathsf{X}(\wp^n)$.

Quite recently, the author of these lines has managed to determine the stable reduction of $\mathsf{X}(\wp^n)$, for all local fields F and all integers $n \geq 1$. In particular, he has obtained a description of the graph of components of $\bar{X}(\wp^n)$ and explicit equations for each irreducible component of $\bar{X}(\wp^n)$. All this follows quite easily from the results of [3] and [5].

In the special case $F = \mathbb{Q}_p$ one can deduce (using also results of Katz and Mazur) a description of the stable reduction at the prime p of the classical modular curve $X(N)$, for every integer N. So far, such a description was only known for $N = pm$, $(m, p) = 1$. (In the case $N = p^2 m$ some partial results can be

deduced from a recent preprint of Coleman and McMurdy, which concerns the stable reduction of $X_0(p^3)$).

A local approach to non-abelian Lubin–Tate theory Having a hand on the stable reduction of $\mathsf{X}(\wp^n)$, a natural question to ask is: what is the minimal field extension $K_n/\hat{F}^{\mathrm{nr}}$ over which this stable reduction occurs? Let $I_F := \mathrm{Gal}(\hat{F}^{\mathrm{ac}}/\hat{F}^{\mathrm{nr}})$ denote the inertia group of F. Then K_n is the fixed field of the kernel of the natural *monodromy action* $I_F \to \mathrm{Aut}(\bar{X}(\wp^n))$. Instead of the monodromy action itself it actually suffices to look at the induced action of I_F on the étale cohomology group $H^1_{\mathrm{et}}(\bar{X}(\wp^n), \bar{\mathbb{Q}}_\ell)$. But this action is determined (admittedly in a rather indirect way) by Equation (1). In other words: the extension K_n can be determined by non-abelian Lubin–Tate theory.

Somewhat surprisingly, this argument can be reversed. The methods used in [5] (on which the computation of $\bar{X}(\wp^n)$ relies) do not yield any concrete information on the extension K_n. However, once $\bar{X}(\wp^n)$ is known, it is possible to determine the monodromy action $I_F \to \mathrm{Aut}(\bar{X}(\wp^n)$ (one uses the distribution on $\mathsf{X}(\wp^n)$ of the CM-points associated to quadratic extensions E/F, together with classical Lubin-Tate theory for the local field E). Even better: one can also determine the action of the subgroup $\Gamma_0 \subset \Gamma = G \times B^\times \times W_F$ on $\varprojlim_n \bar{X}(\wp^n)$. If the residue characteristic p is odd then it is not very hard to deduce Equation (1) from this knowledge. In other words: for $p \neq 2$ the results of [5] can be used to give a new and purely local proof of Carayol's theorem, i.e. of non-abelian Lubin–Tate theory for $\mathrm{GL}_2(F)$.

The case $p = 2$ still presents some difficulties, due to the fact that the local Langlands correspondence is not so easy to make explicit in this case. But the author expects to be able to treat the case $p = 2$ in the near future as well.

It would be very interesting if one could give a local proof of Harris and Taylor's theorem for $h > 2$. A partial result in this direction (the part which only concerns the first level $\mathsf{X}(\wp)$ of the Lubin–Tate tower) has been achieved by T. Yoshida [6]. To treat higher levels as well, a natural approach would be to extend the results of [5] to the case $h > 2$. The author thinks that this is a non-trivial but interesting problem.

References

[1] H. Carayol, *Non-abelian Lubin–Tate theory*. In L. Clozel and J.S. Milne, editors, *Automorphic forms, Shimura varieties and L-functions*, volume II, pages 15-39. Academic Press, 1990.

[2] M. Harris and R. Taylor, *The Geometry and Cohomology of Some Simple Shimura Varieties*. Annals of Math. Studies 151, Princeton Univ. Press.

[3] S. Wewers, *Some remarks on open analytic curves over non-archimedian fields*, math.AG/0509434.

[4] S. Wewers, *Swan conductors on the boundary of Lubin–Tate spaces*, math.NT/0511434.

[5] S. Wewers, *Non-abelian Lubin–Tate theory via stable reduction*, in preparation.

[6] T. Yoshida, *On non-abelian Lubin-Tate theory via vanishing cycles*, math.NT/0404375, to appear in Annales de l'Institut Fourier.

Class field theory of arithmetic schemes

Götz Wiesend

Let F be a number field and S a finite set of places of F, including the infinite places. Define the abelian topological group

$$\mathbf{C}_S := \mathrm{coker}(F^\times \to \bigoplus_{v\notin S} \mathbb{Z} \oplus \bigoplus_{v\in S} \hat{F}_v^\times)$$

where $\hat{F}_v$ is the completion of F at v.

Classical class field theory describes abelian extensions of F unramified outside S. Let F_S be the maximal algebraic extension of F unramified outside S. The reciprocity map

$$\mathbf{C}_S \to \mathrm{Gal}(F_S|F)^{\mathrm{ab}}$$

is surjective and its kernel is the connected component of 0.

We generalise this result to the higher dimensional case. Let F be the function field of an arithmetic scheme, i.e. an integral, regular, separated scheme flat and of finite type over Spec $\mathbb{Z}$. Then $\pi_1(X)$ $(= \pi_1^{\text{ét}}(X))$ classifies finite extensions of F unramified over X. Note, if $\dim X = 1$, then $\pi_1(X) = \mathrm{Gal}(F_S|F)$, where S is the set of places of F not related to X.

In [3] K. Kato and S. Saito describe $\pi_1(X)^{\mathrm{ab}}$ by higher dimensional Milnor K-theory. Instead of the completions $\hat{F}_v$ they use higher dimensional local fields associated to X by a flag of subschemes of X.

A. Schmidt [5] uses this theory in the unramified case and deduces a presentation of $\pi_1(X)^{\mathrm{ab,\ tame}}$ without K-theory.

W. Hofmann and I [2] give a desciption of $\pi_1^{\mathrm{ab}}(X)$ for $\dim X = 2$ which also covers the wild case. We need no K-theory. Here this independent approach is generalized to higher dimensions.

Let X be a separated scheme of finite type over Spec $\mathbb{Z}$. A **curve** C on X is an integral, closed subscheme of X of dimension 1. The function field $\kappa(C)$ of C is a global field. Denote by C_∞ the (finite and infinite) places of $\kappa(C)$ which do not correspond to points of the normalisation. I associate to X the abelian topological group

$$\mathbf{C}_X := \mathrm{coker}(\bigoplus_{C\subseteq X} \kappa(C)^\times \to \bigoplus_{x\in X} \mathbb{Z} \oplus \bigoplus_{C\subseteq X} \bigoplus_{v\in C_\infty} \widehat{\kappa(C)}_v^\times)$$

Here $\widehat{\kappa(C)}_v$ is the completion of $\kappa(C)$ at v. Note that for $\dim X = 1$ the group $\mathbf{C}_X$ equals the above $\mathbf{C}_S$, where $S = X_\infty$.

$\mathbf{C}_X$ is a covariant functor from the category of separated schemes of finite type over Spec $\mathbb{Z}$ to abelian topological groups. Using classical local and global class field theory we construct a continuous natural transformation

$$\rho_X : \ \mathbf{C}_X \to \pi_1^{\mathrm{ab}}(X)$$

of covariant functors.

Main Theorem. *Let X be regular, integral and flat over Spec $\mathbb{Z}$. Then*

$$\rho_X : \mathbf{C}_X \to \pi_1^{ab}(X)$$

is surjective and its kernel is the connected component of 0. It induces a bijection between the open subgroups of $\pi_1^{ab}(X)$ and the open subgroups of $\mathbf{C}_X$.

Now let X be regular and flat and proper over Spec $\mathbb{Z}$. The main theorem implies that there is an exact sequence of finite groups

$$\bigoplus_{i=1}^{r} \mathbb{Z}/2 \to \pi_1^{\mathrm{ab}}(X) \to \mathrm{CH}_0(X) \to 0$$

where r is the number of connected components of $X(\mathbb{R})$ and $\mathrm{CH}_0(X)$ is the Chow group of zero cycles on X. In particular this gives an independent and elementary proof of the finiteness of $\mathrm{CH}_0(X)$, originally proved by Bloch, Kato and Saito ([1], [3, Theorem 9.10], [4, Chapter 5]).

Now let X be integral and regular. I prove: For a finite, étale Galois cover $Y|X$ there is an isomorphism

$$\mathbf{C}_X/N_{Y|X}\mathbf{C}_Y \cong \mathrm{Gal}(Y|X)^{\mathrm{ab}}.$$

Let X be integral and regular, let n be an integer which is invertible on X. There is an isomorphism

$$\mathbf{C}_X/n \cong \pi_1^{\mathrm{ab}}(X)/n.$$

The proof of the main theorem is based on the paper [6]. Consider the following data: For each curve C on X is given a connected abelian étale covering, such that the inertia degrees are equal at the points of intersection. It is shown in [6] that there exists a unique connected abelian, étale covering of X compatible with this data.

References

[1] Bloch, S.: Algebraic K-theory and class field theory for arithmetic surfaces. *Annals of Mathematics* **114**, 229 – 265 (1981)

[2] Hofmann, W. and Wiesend, G.: Non-abelian Class Field Theory for Arithmetic Surfaces. *Mathematische Zeitschrift* **250**, 203–224 (2005)

[3] Kato, K. and Saito, S.: Global class field theory of arithmetic schemes. *Contemporary Mathematics* **55**, 255–331 (1986)

[4] Raskind, W.: Abelian class field theory of arithmetic schemes. In: *Jacob, Bill (ed.) et al., K-theory and algebraic geometry: connections with quadratic forms and division algebras. Summer Research Institute on quadratic forms and division algebras, July 6-24, 1992, University of California, Santa Barbara, USA. Providence, RI: American Mathematical Society. Proc. Symp. Pure Math.* **58***, Part 1, 85-187* (1995)

[5] Schmidt, A.: Tame class field theory for arithmetic schemes. *Invent. math.* **160**, 527–565 (2005)

[6] Wiesend, G.: On the Fundamental Group of Arithmetic Schemes. *Journal of Number Theory*, in print

[7] Wiesend, G.: Class field theory of arithmetic schemes. preprint, Essen 2005

Reporter: Walter Hofmann

Participants

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

Prof. Dr. Serban A. Basarab
Institute of Mathematics
"Simion Stoilow"
of the Romanian Academy
P.O. Box 1-764
014700 Bucharest
ROMANIA

Prof. Dr. Frauke M. Bleher
Dept. of Mathematics
University of Iowa
Iowa City, IA 52242-1466
USA

Prof. Dr. Irene Bouw
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

David Brink
Mathematical Institute
University of Copenhagen
Universitetsparken 5
DK-2100 Copenhagen

Prof. Dr. Anna Cadoret
Universite des Sciences et
Technologies de Lille (Lille I)
Laboratoire Paul Painleve
F-59655 Villeneuve d'Ascq Cedex

Prof. Dr. Zoe Chatzidakis
U. F. R. de Mathematiques
Case 7012
Universite Paris VII
2, Place Jussieu
F-75251 Paris Cedex 05

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

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

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

Tobias Dyckerhoff
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA

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

Prof. Dr. Yuri L. Ershov
Institute of Mathematics SO RAN
Akademic Koptyug prospect 4
630090 Novosibirsk 90
RUSSIA

Prof. Dr. Gerhard Frey
FB 6 - Mathematik
Universität Duisburg-Essen
45117 Essen

Prof. Dr. Wulf-Dieter Geyer
Mathematisches Institut
Universität Erlangen-Nürnberg
Bismarckstr. 1 1/2
91054 Erlangen

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

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
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

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

Walter Hofmann
Mathematisches Institut
Universität Erlangen-Nürnberg
Bismarckstr. 1 1/2
91054 Erlangen

Armin Holschbach
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA

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

Prof. Dr. Christian Ulrik Jensen
Matematisk Afdeling
Kobenhavns Universitet
Universitetsparken 5
DK-2100 Kobenhavn

Dr. Jochen Koenigsmann
Mathematisches Institut
Universität Freiburg
Eckerstr.1
79104 Freiburg

Dr. Claus Lehr
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

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

Prof. Dr. Peter Müller
Mathematisches Institut
Lehrstuhl für Mathematik I
Universität Würzburg
Am Hubland
97074 Würzburg

Salah Najib
U. F. R. Mathematiques
Universite de Lille 1
F-59655 Villeneuve d'Ascq Cedex

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

Prof. Dr. Ambrus Pal
CNRS - I.H.E.S.
Le Bois Marie
35, route de Chartres
F-91440 Bures-sur-Yvette

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

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

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. Chris Rasmussen
Dept. of Mathematics
Rice University
P.O. Box 1892
Houston, TX 77005-1892
USA

Dr. Aharon Razon
3 Bet-Zuri st.
Tel-Aviv 69122
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
Achatweg 5
69181 Leimen

Prof. Dr. Claus Scheiderer
Fakultät für Mathematik
Universität Konstanz
Postfach 5560
78434 Konstanz

Prof. Dr. Alexandra Shlapentokh
Dept. of Mathematics
East Carolina University
Greenville NC 27858-4353
USA

Prof. Dr. Jack Sonn
Department of Mathematics
Technion
Israel Institute of Technology
Haifa 32000
ISRAEL

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

Dr. Jakob M. Stix
Mathematisches Institut
Universität Bonn
Beringstr. 1
53115 Bonn

Prof. Dr. John Swallow
Davidson College
Box 7046
209 Ridge Road
Davidson NC 28035-7046
USA

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

Prof. Dr. Helmut Voelklein
Institut für Experimentelle Mathematik
Ellernstr. 29
45326 Essen

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

Sven Wagner
Fachbereich Mathematik u. Statistik
Universität Konstanz
Universitätsstr. 10
78457 Konstanz

Dr. Yann Walkowiak
Departement Informatique
Universite de Lille 1
F-59655 Villeneuve d'Ascq Cedex

Prof. Dr. Stefan Wewers
Mathematisches Institut
Universität Bonn
Beringstr. 1
53115 Bonn

Dr. Götz Wiesend
Institut für Experimentelle Mathematik
Universität Essen
Ellernstr. 29
45326 Essen

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

Prof. Dr. Leonardo Zapponi
Institut Mathematiques de Jussieu
Universite Pierre et Marie Curie
175, Rue du Chevaleret
F-75013 Paris