Mathematisches Forschungsinstitut Oberwolfach

Report No. 26/2007

Arithmetic and Differential Galois Groups

Organised by
David Harbater (Philadelphia)
B. Heinrich Matzat (Heidelberg)
Marius van der Put (Groningen)
Leila Schneps (Paris)

May 13th – May 19th, 2007

Abstract. Galois theory is the study of symmetries in solution spaces of polynomial and differential equations and more generally of the relation between automorphism groups (or group schemes respectively) and the structure of algebraic and differential extensions. The lectures of this workshop were focused around the following five main topics: the absolute Galois group $G_{\mathbb{Q}}$ and the Grothendieck-Teichmüller group, étale fundamental groups and the anabelian conjecture, arithmetic Galois realizations and constructive Langlands program, local and global differential modules and the p-curvature conjecture, as well as Galois theory for nonlinear and partial differential equations.

Mathematics Subject Classification (2000): 12Fxx,12Gxx,12Hxx, (13Nxx,14Lxx,34Gxx).

Introduction by the Organisers

Galois theory is the study of symmetries in solution spaces of polynomial and differential equations and more generally of the relation between automorphism groups (or group schemes) and the structure of algebraic and differential extensions.

Many of the important problems in this area are connected to the classification of (algebraic or differential) Galois extensions and the study of the respective fundamental groups, e. g. via inverse problems. Other interesting points are the direct problem, i. e., the computation of (ordinary or differential) Galois groups, and related constructive aspects.

This workshop gave an overview on some important new results and developments. A second goal was the discussion of ideas for proving some open questions and conjectures as well as of new directions of research.

The main topics of the workshop were:

- The absolute Galois group $G_{\mathbb{Q}}$ and the Grothendieck-Teichmüller group,
- Etale fundamental groups and the anabelian conjecture,
- Arithmetic Galois realizations and constructive Langlands program,
- Local and global differential modules and the p-curvature conjecture,
- Galois theory for nonlinear and partial differential equations.

Besides this main program we had some reports on related subjects like the Cohen-Lenstra heuristics for number fields by J. Klüners and the behaviour of the Tate-Shafarevich group in anticyclotomic field extensions by M. Çiperiani.

It is always difficult to emphasise highlights or unexpected results, but one of them might be the result of F. Pop that henselian fields always are large, which is of great interest in field arithmetic and inverse Galois theory. Another striking result is the existence of G_2-motives over $\mathbb{Q}$ shown by M. Dettweiler which gives a positive answer to an old question of J.-P. Serre. A fruit of common effort in research in arithmetic and differential Galois theory is the development of patching methods for differential modules by D. Harbater and J. Hartmann. This method will allow yet unexpected applications in inverse differential Galois theory and other areas, like K-theory. The talk of B. Malgrange gave a vision of Galois theory for nonlinear differential equations. Exploitation of his work for special types of equations, like Painlevé equations, and the generalization of his ideas to non algebraically closed fields of constants as well as to positive characteristic will keep researchers busy for years.

Surely, many other results presented at the workshop should be pointed out here, too, like M. Raynaud's work on fundamental groups in positive characteristic, D. Bertrand's result on Schanuel's conjecture or Ch. Hardouin's generalization of q-difference equations to roots of unity by creating an iterative q-difference theory.

Altogether, we had a wonderful and inspiring week with lots of interesting lectures and many discussions bearing ideas for future research.

Finally, the organisers want to cordially thank the Oberwolfach administration and its staff for giving us the opportunity to arrange this and earlier workshops on Galois theory as well as for the excellent service.

Workshop: Arithmetic and Differential Galois Groups

Table of Contents

Florian Pop
Henselian implies Large 1447

Michel Raynaud (joint with Tong-Jilong)
Variation of the fundamental group of curves in positive characteristic . 1448

Michael Dettweiler
Arithmetic of G_2-representations 1449

Jerald J. Kovacic
Strongly normal extensions 1451

Tobias Dyckerhoff
The inverse problem of differential Galois theory over the field $\mathbb{R}(z)$ 1453

Lourdes Juan (joint with Arne Ledet)
Generic Picard-Vessiot extensions 1455

Michael F. Singer
Differential Groups and Differential Relations 1458

Irene Bouw
The accessory parameter problem in positive characteristic 1461

Lenny Taelman
t-Motivic Galois Groups 1462

Andreas Röscheisen
Iterative Connections and Abhyankar's Conjecture 1463

Ted Chinburg (joint with Robert Guralnick, David Harbater)
Lifting local group actions on curves 1466

Anna Cadoret
A moduli formulation of torsion conjectures for jacobians 1468

Magali Rocher
On smooth curves endowed with a big automorphism group 1470

Jean-Pierre Ramis (joint with Jacques Sauloy)
Local classification of linear meromorphic q-difference equations 1473

Jürgen Klüners (joint with Étienne Fouvry)
Cohen–Lenstra heuristics and the negative Pell equation 1476

Stefan Wewers (joint with Tamás Szamuely)
The arithmetic π_1 and diophantine geometry 1479

Scott Corry (joint with Florian Pop)
A Hom-form of the pro-p birational anabelian conjecture 1482

Daniel Bertrand (joint with Anand Pillay)
Schanuel's conjecture over function fields and differential Galois theory 1484

David Harbater (joint with Julia Hartmann)
Patching over fields 1487

Julia Hartmann (joint with David Harbater)
Differential Galois Groups and Patching 1490

Hiroaki Nakamura (joint with Hiroshi Tsunogai, Seidai Yasuda)
Grothendieck-Teichmüller group and a family of Mordell elliptic curves . 1493

Sarah Carr (joint with Francis Brown, Leila Schneps)
Periods on the moduli space of genus 0 curves 1495

Rachel Pries (joint with Jeffrey Achter)
On the p-rank stratification of the moduli space of curves 1498

Bernard Malgrange
On non linear differential Galois theory 1500

Jakob Stix
On the geometry of higher dimensional anabelian varieties 1501

Mirela Çiperiani
The Λ-corank of $Ш(E/K_\infty)_{p^\infty}$ for supersingular primes 1504

Núria Vila (joint with Luis Dieulefait)
Generically large images of geometric Galois representations 1505

Jing Long Hoelscher
Galois extensions ramified only at one prime 1508

Charlotte Hardouin
Iterative q-difference Galois theory 1511

João Pedro Pinto dos Santos
Fundamental group-schemes in positive characteristic 1514

Abstracts

Henselian implies Large

Florian Pop

The notion "large field" was introduced by the author in Pop [4] in the context of *inverse Galois theory,* but this notion proved useful in other contexts too, like the theory of rationally connected varieties, the model theory of function fields, etc. A field K is called a large field if for every K-curve X one has: If X has a smooth K-rational point, then X has infinitely many K-rational points. Examples of large fields are the PAC fields, real/p-adically closed fields, and more general Henselian valued fields; see loc.cit. for examples and characterizations of large fields.

In order to present the main result announced in my talk, let me first recall that a commutative ring R with identity is said to be Henselian with respect to a (non-trivial) ideal $\mathfrak{a}$, or that $(R, \mathfrak{a})$ is a Henselian pair, if setting $\overline{R} := R/\mathfrak{a}$ and denoting $R[X] \to \overline{R}[X]$, $f \mapsto \overline{f}$, the canonical reduction $\bmod \mathfrak{a}$ homomorphism, for every polynomial $f(X) \in R[X]$ the following holds: If $\overline{a} \in \overline{R}$ is a root of $\overline{f}$ such that $\overline{f}'(\overline{a}) \in \overline{R}^\times$, then there exists a lifting $a \in R$ of $\overline{a}$ such that $f(a) = 0$ and $f'(a) \in R^\times$, i.e., "simple roots" of $\overline{f}$ lift to "simple roots" of f.

Theorem. *Let R be a domain which is Henselian with respect to some non-trivial ideal $\mathfrak{a}$, and $K = \mathrm{Quot}(R)$ be the field of fractions of R. Then K is a large field. In particular, every finite split embedding problem for G_K has $|K|$ different proper regular solutions.*

As applications of the Theorem above one gets wide (and maybe unexpected) generalizations of some results by Harbater–Stevenson [2], as well as of Harbater [1], by using –among other things– Weissauer's Theorem (saying that the quotient field of a Krull domain of dimension > 1 is a Hilbertian field). A further application is new evidence for the Bogomolov's Freeness Conjecture, see e.g. [5], by using –among other things– a result by Colliot-Thélène–Ojanguren–Parimala (on the Brauer group of excellent two-dimensional Henselian rings).

References

[1] D. Harbater, *On function fields with free absolute Galois groups,* Manuscript, June 2006.
[2] D. Harbater and K. Stevenson, *Local Galois theory in dimension two,* Manuscript 2005; see http://www.mathnet.or.kr/papers/Pennsy/Harbater/localgal.pdf
[3] E. Paran, *Algebraic patching over complete domains,* Thesis, Tel Aviv University, 2006.
[4] F. Pop, *Embedding problems over large fields,* Ann. of Math. **1944** (1996), 1–34.
[5] L. Positselski, *Koszul property and Bogomolov's conjecture,* Manuscript 2005, see http://www.math.uiuc.edu/K-theory/0720

Variation of the fundamental group of curves in positive characteristic

Michel Raynaud
(joint work with Tong-Jilong)

Let X be a smooth, proper, connected curve, defined over an algebraically closed field k, with positive characteristic p, and let g be its genus. Its fundamental group $\pi_1(X)$ is a profinite group, which is no longer just determined by g, a main difference with characteristic 0. To study its variation in an algebraic family, one can study the local case. Let $S = \mathrm{Spec}k[[T]]$, with its closed point s and its generic point η. Let X be a smooth and proper relative curve above S, with connected geometric fibers of genus g. Then, following Grothendieck, we have a specialization map

$$sp : \pi_1(X_{\bar{\eta}}) \to \pi_1(X_s),$$

which is surjective, but not necessarily injective. It becomes bijective on the greatest p'-torsion quotients, where p' means "of order prime to p". If X_s can be defined over a finite field, A. Tamagawa has shown that sp is bijective if and only if the curve $X \to S$ is constant.

One can ask if the same conclusion remains valid when one replaces the whole π_1 by a suitable metabelian quotient, which is an extension of a pro p'-group: the Tate module built from the p'-torsion of the homology of X, by a pro p-group $N^{\text{new ord}}$, defined as follows. For each finite étale cover $Y \to X$, cyclic of order n, prime to p, we consider the new part of the p-adic homology $H_1(Y, \mathbb{Z}_p)$ (where Z/nZ acts with characters of order exactly n) and we say it is ordinary if it has maximal possible rank $\varphi(n)(g-1)$. Then $N^{\text{new ord}}$ is the product of those new ordinary parts when we vary the cyclic cover $Y \to X$.

We get only partial results : suppose X_s can be defined over a finite field and

$$sp^{\text{new ord}} : \pi_1^{\text{new ord}}(X_{\bar{\eta}}) \to (X_s)$$

is bijective. Then, we conclude that the relative curve $X \to S$ is constant when $g = 2$ or when s is supersingular.

Let X^1 be the curve deduced from X by pull-back by the absolute Frobenius of k and let $F : X \to X^1$ be the relative Frobenius, then we get an exact sequence of vector bundles on X :

$$0 \to \mathcal{O}_{X^1} \to F_*(\mathcal{O}_X) \to B \to 0 \ ,$$

where B is the sheaf of locally exact differentials and has rank $p-1$. The sheaf B admits a Θ divisor, which is a positive divisor lying on the jacobian J^1 of X^1 and is algebraically equivalent to $(p-1)\Theta_{\text{clas}}$, where Θ_{clas} defines the classical principal polarization of J^1 . Then, the structure of $\pi_1^{\text{new ord}}(X)$ is closely related with the p'-torsion lying in Θ.

Arithmetic of G_2-representations

Michael Dettweiler

The method of rigidity was first used by B. Riemann in his study of Gauß' hypergeometric differential equations ${}_2F_1 = {}_2F_1(a,b,c)$: Consider the monodromy representation

$$\rho : \pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus \{0,1,\infty\}, s) \to \mathrm{GL}(V_s)$$

which arises from analytic continuation of the vector space $V_s \simeq \mathbb{C}^2$ of local solutions of ${}_2F_1$ at s along paths around the missing points. Then ρ is *rigid* in the sense that it is determined up to isomorphism by the conjugacy classes of $\rho(\gamma_i)$ in $\mathrm{GL}(V_s)$, where γ_i are simple paths around the singularities $0, 1, \infty$ of ${}_2F_1$. One can translate this into the language of local systems (=locally free sheaves), by saying that the local system $L({}_2F_1)$ on $\mathbb{P}^1 \setminus \{0,1,\infty\}$ which is given by the holomorphic solutions of ${}_2F_1$ is *rigid* in the following sense: The monodromy representation of $L({}_2F_1)$ is determined up to isomorphism by the local monodromy representations at the missing points. This definition of rigidity extends in the obvious way to other local systems. Since Riemann's work, the concept of a rigid local system has proven to be a very fruitful and has appeared in many different branches of mathematics and physics.

A key observation, going back to Pochhammer, turned out to be the following: The local sections of the rank two local system $L({}_2F_1)$ can be written as linear combinations of convolutions $f * g$, where f and g are solutions of suitable Fuchsian systems of *rank one;* see the introduction of N. Katz' book *Rigid Local Systems* ([RLS]) for a general discussion. Thus the rank two hypergeometric equation is related to two rank one systems via convolution. By interpreting the convolution as higher direct image and using a transition to étale sheaves, Katz [RLS] proves a vast generalization of Pochhammer's observation: Let F be any irreducible tamely ramified rigid local $\bar{\mathbb{Q}}_\ell$-system F on the punctured sphere over an algebraically closed field (in the sense specified below). Then F can be transformed to a rank one local system by applying a suitable iterative application of *middle convolutions* MC_χ and tensor products with rank one objects to it (loc. cit., Chap. 5). This yields *Katz Existence Algorithm* for irreducible rigid local systems, which tests, whether a given set of local representations comes from an irreducible and rigid local system (loc. cit., Chap. 6).

We call a locally constant constructible étale $\bar{\mathbb{Q}}_\ell$-sheaf F on a smooth scheme S a *local ($\bar{\mathbb{Q}}_\ell$-)system* on S (such sheaves are also called *lisse*. Let k be an algebraically closed field. Let F be an local $\bar{\mathbb{Q}}_\ell$-system on a Zariski open subset $j : U \to \mathbb{P}^1_k$ which is given by a representation of the tame fundamental group $\pi_1^{\mathrm{tame}}(U)$. Call F *rigid*, if the defining representation

$$\rho_F : \pi_1^{\mathrm{tame}}(U, \bar{\eta}) \to \mathrm{GL}(F_{\bar{\eta}})$$

of F is determined up to isomorphism by the conjugacy classes of the induced representations of tame inertia groups I_s^{tame} at the missing points $s \in D := \mathbb{P}^1 \setminus U$.

Then the following holds: If F is an irreducible (and tamely ramified) local system, then F is rigid, if and only if the following formula holds:

$$\chi(\mathbb{P}^1, j_*\underline{\mathrm{End}}(F)) = (2-\mathrm{Card}(D))\mathrm{rk}(F)^2 + \sum_{s\in D} \dim\left(\mathrm{Centralizer}_{\mathrm{GL}(F_{\bar\eta})}(I_s^{\mathrm{tame}})\right) = 2.$$

Recall that there exist only finitely many simple linear algebraic groups over an algebraically closed field which are not isomorphic to a classical group (i.e., a special linear -, an orthogonal -, or a symplectic group). The smallest of them is the group G_2 which admits an embedding into the group GL_7. We prove the following result:

Theorem 1: (S. Reiter, M. Dettweiler) Let k be an algebraically closed field of characteristic > 2 and let ℓ be a prime number different from $\mathrm{char}(k)$.

(1) Then there exists a tamely ramified rigid local $\bar{\mathbb{Q}}_\ell$-system F of rank 7 on $\mathbb{P}^1_k \setminus \{0,1,\infty\}$ whose monodromy group is Zariski dense in the exceptional simple algebraic group $G_2(\bar{\mathbb{Q}}_\ell) \leq \mathrm{GL}_7(\bar{\mathbb{Q}}_\ell)$. The local monodromy of F is of the following type:

$$-\mathrm{Unip}(1)^4 \oplus \mathrm{Unip}(1)^3, \quad \mathrm{Unip}(2)^2 \oplus \mathrm{Unip}(3), \quad \mathrm{Unip}(7),$$

where $\mathrm{Unip}(n)^i$ denotes the i-fold sum of the standard indecomposable unipotent representation of the tame inertia group of rank n at the missing points $0, 1, \infty$ (resp.).

(2) If $k = \bar{\mathbb{Q}}$, then the defining representation

$$\rho_F : \pi_1(\mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0,1,\infty\}) \to \mathrm{GL}_7(\bar{\mathbb{Q}}_\ell)$$

of F can be extended to a representation of $\pi_1(\mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\})$.

From the Galois representations which result from Thm. 1 (ii), we obtain by specialization Galois representations

$$\rho_s : G_{\mathbb{Q}} \to G_2(\mathbb{Q}_\ell), \quad s \in \mathbb{Q} \setminus \{0,1\}.$$

We prove density results for these Galois representations, if the specialization point s has odd primes dividing the nominator and the denominator (joint work with N. Katz).

References

[RLS] N. Katz, *Rigid Local Systems*, Annals of Math. Studies, Princ. Univ. Press **139** (1996)

Strongly normal extensions

Jerald J. Kovacic

The theory of strongly normal extensions is ripe for study. It has been neglected, possibly because Kolchin used his own axiomatic definition of algebraic group. Instead, we use differential schemes, another area ripe for study.

We start with a sketch of Picard-Vessiot theory. For detailed treatments see Kaplansky [3], Kolchin [4] and [8], Magid [15], or van der Put and Singer [20]. For the treatment here see Kovacic [13].

Fix an ordinary differential field K of characteristic 0 with algebraically closed field of constants C and let L be a Picard-Vessiot extension of K. This means that $L = K(\alpha)$ for some $\alpha \in \mathrm{GL}(n, L)$, $\ell\delta\alpha = \alpha'\alpha^{-1} = A \in \mathrm{Mat}(n, K)$ and the field of constants of L is C. Denote the Galois group of all differential automorphisms of L over K by $\mathrm{Gal}(L/K)$.

The Picard-Vessiot ring is defined to be $P = K[\alpha, \alpha^{-1}]$. It is independent of the choice of α. We let D be the ring of constants of $P \otimes_K P$. The following is the main structure theorem of Picard-Vessiot theory.

Theorem. *The differential homomorphism $P \otimes_C D \to P \otimes_K P$ defined by*

$$a \otimes_C d \mapsto (a \otimes_K 1)d$$

is an isomorphism.

Using Sweedler corings (Sweedler [19]) we induce the structure of Hopf algebra on D and make P a D-comodule algebra. The theorem states that Picard-Vessiot theory is an example of a Hopf-Galois theory (Montgomery [17], Chapter 8).

In terms of algebraic geometry, $\mathrm{Spec}\, D$ is an affine group scheme over $\mathrm{Spec}\, C$ and $\mathrm{Spec}\, P$ is a torsor for $\mathrm{Spec}\, D$.

Theorem. *The mapping $D \to P \otimes_C D$ induces a bijection between maximal ideals of D and maximal differential ideals of $P \otimes_C D$.*

For $\sigma \in \mathrm{Gal}(L/K)$ we define

$$\overline{\sigma}\colon P \otimes_K P \to P, \qquad a \otimes_K b \mapsto a\sigma b,$$

and let $\mathfrak{p}_\sigma$ be the kernel of $\overline{\sigma}$.

Theorem. *The mapping $\sigma \to \mathfrak{p}_\sigma$ gives a bijection from* $\mathrm{Gal}(L/K)$ *onto the set of all maximal differential ideals of $P \otimes_K P$.*

Corollary. *The Galois group is canonically isomorphic to the set of maximal ideals of D, i.e. the closed points of* $\mathrm{Spec}\, D$.

But there is another approach to Galois theory. A field extension L of K is normal if every isomorphism (into some extension field of L) is an automorphism. The corresponding condition in differential algebra is *strongly normal*. This was first studied in Kolchin [5] and [6]. For the treatment here see Kovacic [12], for definitions and properties of Diffspec see Kovacic [11].

Let L be a strongly normal extension of K. Then we define

$$X = \text{Diffspec}\,(L \otimes_K L).$$

If $\sigma \in \text{Gal}(L/K)$ then we define

$$\overline{\sigma}\colon L \otimes_K L \to L, \qquad \overline{\sigma}(a \otimes_K b) = a\sigma b$$

and let

$$\mathfrak{p}_\sigma = \ker \overline{\sigma}.$$

Theorem. *The mapping $\sigma \to \mathfrak{p}_\sigma$ is a bijection from* $\text{Gal}(L/K)$ *onto the set of closed points of X.*

This makes X a differential group scheme; however we want a group scheme. In the Picard-Vessiot theory we had an isomorphism

$$P \otimes_K P \approx P \otimes_C D,$$

where D was a certain ring of constants. We do a similar thing for strongly normal extensions.

Define X^Δ to be the ringed space with the same topological space as X and with $\mathcal{O}_{X^\Delta}(U)$ being the ring of constants of $\mathcal{O}_X(U)$. In general X^Δ is merely a local ringed space, not a scheme. However for $X = \text{Diffspec}\,(L \otimes_K L)$, where L is strongly normal over K, we have the following theorem.

Theorem. X^Δ *is a group scheme of finite type over C and*

$$X \approx L \times_C X^\Delta$$

(This means $\text{Diffspec}\, L \times_{\text{Diffspec}\, C} X^\Delta$.)

There is a "factory" for producing strongly normal extensions, namely the logarithmic derivative (Buium [1], p. 23). Using this factory we may produce a strongly normal extension having as group any given connected algebraic group.

Finally we observe that there are differential equations that have no solution contained in a strongly normal extension. The first Painlevé equation is an example of such (Nishioka [18]). For first order equations Matsuda [16] has determined which have solutions contained in a strongly normal extension; precisely those with no "moveable singularities". At this time there is no good characterization of higher order differential equations with solutions in a strongly normal extension.

References

[1] A. Buium, *Differential function fields and moduli of algebraic varieties*, Lecture Notes in Math., 1226, Springer, Berlin, 1986. MR0874111 (88e:14010).

[2] G. Janelidze, Galois theory in categories: the new example of differential fields, in *Categorical topology and its relation to analysis, algebra and combinatorics (Prague, 1988)*, 369–380, World Sci. Publ., Teaneck, NJ. MR1047912 (91h:12018).

[3] I. Kaplansky, *An introduction to differential algebra*, Second edition, Hermann, Paris, 1976. MR0460303 (57 #297).

[4] E. R. Kolchin, *Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. (2) **49** (1948), 1–42. MR0024884 (9,561c). Reprinted in [9].

[5] ———, *Galois theory of differential fields*, Amer. J. Math. **75** (1953), 753–824. MR0058591 (15,394a). Reprinted in [9].
[6] ———, *On the Galois theory of differential fields*, Amer. J. Math. **77** (1955), 868–894. MR0073588 (17,455a). Reprinted in [9].
[7] ———, *Abelian extensions of differential fields*, Amer. J. Math. **82** (1960), 779–790. MR0132066 (24 #A1913). Reprinted in [9].
[8] ———, *Differential algebra and algebraic groups*, Academic Press, New York, 1973. MR0568864 (58 #27929).
[9] ———, *Selected works of Ellis Kolchin with commentary*, Amer. Math. Soc., Providence, RI, 1999. MR1677530 (2000g:01042).
[10] E. Kolchin and S. Lang, *Algebraic groups and the Galois theory of differential fields*, Amer. J. Math. **80** (1958), 103–110. MR0094596 (20 #1109). Reprinted in [9].
[11] J. J. Kovacic, Differential schemes, in *Differential algebra and related topics (Newark, NJ, 2000)*, 71–94, World Sci. Publ., River Edge, NJ. MR1921695 (2003i:12010).
[12] ———, *The differential Galois theory of strongly normal extensions*, Trans. Amer. Math. Soc. **355** (2003), no. 11, 4475–4522 (electronic). MR1990759 (2004i:12008).
[13] ———, *Geometric characterization of strongly normal extensions*, Trans. Amer. Math. Soc. **358** (2006), no. 9, 4135–4157 (electronic). MR2219014 (2007e:12006).
[14] ———, *Hyperelliptic Jacobians in differential Galois theory*, KSDA lecture notes, `http://mysite.verizon.net/jkovacic/ksda/hyper-ksda.dvi`, (2003).
[15] A. R. Magid, *Lectures on differential Galois theory*, Amer. Math. Soc., Providence, RI, 1994. MR1301076 (95j:12008).
[16] M. Matsuda, *First-order algebraic differential equations*, Springer, Berlin, 1980. MR0576060 (82d:12015).
[17] S. Montgomery, *Hopf algebras and their actions on rings*, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1993. MR1243637 (94i:16019).
[18] K. Nishioka, *A note on the transcendency of Painlevé's first transcendent*, Nagoya Math. J. **109** (1988), 63–67. MR0931951 (89c:12003).
[19] M. Sweedler, *The predual theorem to the Jacobson-Bourbaki theorem*, Trans. Amer. Math. Soc. **213** (1975), 391–406. MR0387345 (52 #8188).
[20] M. van der Put and M. F. Singer, *Galois theory of linear differential equations*, Springer, Berlin, 2003. MR1960772 (2004c:12010).

The inverse problem of differential Galois theory over the field $\mathbb{R}(z)$

Tobias Dyckerhoff

Let F be a differential field of characteristic zero with field of constants K. Given a matrix $A \in \mathrm{Mat}_n(F)$, we denote the corresponding linear differential equation $\partial(y) = Ay$ by $[A]$. A differential field extension E/F is called a **Picard-Vessiot extension** for a matrix A (or the corresponding equation $[A]$), if

(1) there exists $Y \in \mathrm{GL}_n(E)$ such that $\partial(Y) = AY$,
(2) $E = F(Y_{ij} |\ 1 \leq i, j \leq n)$,
(3) $\{e \in E |\ \partial(e) = 0\} = K$.

Given a Picard-Vessiot extension E/F, there exists an affine algebraic group scheme G over K such that for every algebraic field extension L/K one has

$$G(L) \cong \mathrm{Aut}^{\partial}(E \otimes_K L / F \otimes_K L).$$

Indeed, each $E \otimes_K L / F \otimes_K L$ is again a Picard-Vessiot extension. The group scheme G is called the **differential Galois group of** E/F.

The inverse problem of differential Galois theory asks which groups occur as differential Galois groups of Picard-Vessiot extensions over a given differential field F. For the classical case $F = \mathbb{C}(z)$, the first complete answer was given by C. Tretkoff and M. Tretkoff in [3].

Theorem A. *Given any linear algebraic group G over $\mathbb{C}$, there exists a Picard-Vessiot extension $E/\mathbb{C}(z)$ whose differential Galois group is isomorphic to G.*

The main ingredient of the proof is the Riemann-Hilbert Correspondence. The latter states that the category of regular singular differential equations over $\mathbb{C}(z)$ with singularities contained in a finite set $S \subset \mathbb{P}^1$ is equivalent to the category of complex linear representations of the fundamental group of $\mathbb{P}^1 \backslash S$ (cf. [1]). This equivalence is given by associating to a differential equation its monodromy representation.
In [2], we generalize the classical result to the following theorem.

Theorem B. *Given any linear algebraic group G over $\mathbb{R}$, there exists a Picard-Vessiot extension $E/\mathbb{R}(z)$ whose differential Galois group is isomorphic to G.*

To prove the theorem, we combine the Riemann-Hilbert Correspondence with a theory of Galois descent for Picard-Vessiot extensions developed in [2]. The following lemma provides the link between descent theory and Riemann-Hilbert Correspondence.

Lemma. *Let $\tilde{E}/\mathbb{C}(z)$ be a Picard-Vessiot extension for the matrix $A \in \mathrm{Mat}_n(\mathbb{C}(z))$. If the equation $[A]$ is gauge equivalent to its complex conjugate $[\bar{A}]$ (i.e. there exists $C \in \mathrm{GL}_n(\mathbb{C}(z))$ such that $\bar{A} = C^{-1}AC - C^{-1}\partial(C)$), then $\tilde{E}/\mathbb{C}(z)$ descends to a Picard-Vessiot extension $E/\mathbb{R}(z)$.*

Sketch of the proof of Theorem B. Given a linear algebraic group $G \subset \mathrm{GL}_n$ over $\mathbb{R}$, it is well known that there exist finitely many matrices $C_1, \ldots, C_r$ which generate $G(\mathbb{C})$ in the Zariski topology. We choose the set $S \subset \mathbb{P}^1$ to consist of r points in the upper half plane, their complex conjugates as well as ∞. Consider the complex linear representation of $\pi_1(\mathbb{P}^1 \backslash S)$ defined by mapping the generators to the matrices indicated in Figure 1.

By the Riemann-Hilbert Correspondence there exists a differential equation $[A]$ having this prescribed monodromy representation. The Picard-Vessiot extension $\tilde{E}/\mathbb{C}(z)$ for $[A]$ has the group $G \otimes_{\mathbb{R}} \mathbb{C}$ as differential Galois group. Indeed, in the case of regular singularities the image of the monodromy representation is a Zariski dense subgroup of the differential Galois group and so the last assertion follows directly from the choice of the matrices C_i.

Next, one checks that the monodromy representations associated to $[A]$ and $[\bar{A}]$ are equivalent which, again applying the Riemann-Hilbert Correspondence, implies the equivalence of $[A]$ and $[\bar{A}]$. Using the above lemma, we conclude that the extension $\tilde{E}/\mathbb{C}(z)$ descends to a Picard-Vessiot extension $E/\mathbb{R}(z)$. Some further reasoning shows that $E/\mathbb{R}(z)$ actually realizes G as differential Galois group. $\square$

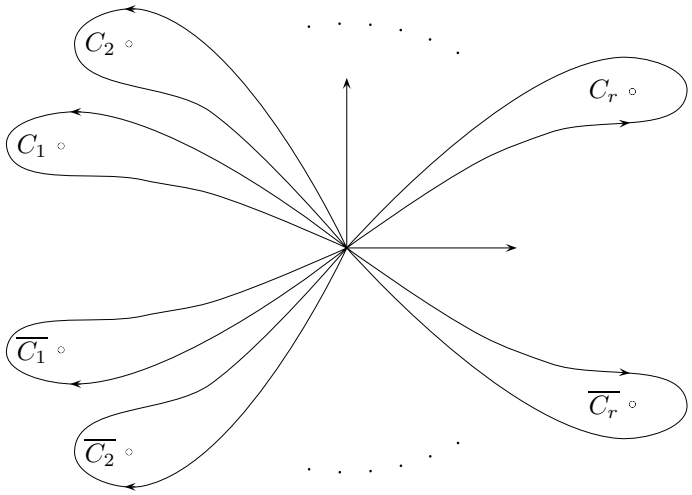

FIGURE 1. Monodromy representation of $[A]$

REFERENCES

[1] D. V. Anosov and A. A. Bolibruch, *The Riemann-Hilbert Problem*, Aspects of Mathematics (1994)

[2] T. Dyckerhoff, *The inverse problem of differential Galois theory over the field* $\mathbb{R}(z)$, submitted to J. Reine Angew. Math.

[3] C. Tretkoff and M. Tretkoff, *Solution of the inverse problem of differential Galois theory in the classical case*, Amer. J. Math. **101** (1979), 1327–1332.

Generic Picard-Vessiot extensions

LOURDES JUAN

(joint work with Arne Ledet)

We work in the standard differential Galois theory context, thus all the differential fields considered are of characteristic zero and have an algebraically closed subfield of constants $\mathcal{C}$.

Given a linear algebraic group G over $\mathcal{C}$, the *generic form of the inverse problem in differential Galois theory* asks whether there are a differential field $\mathcal{F}$ with field of constants $\mathcal{C}$ and a Picard-Vessiot extension (PVE) $\mathcal{E} \supset \mathcal{F}$, with differential Galois group isomorphic to G, such that $\mathcal{E}$ is generated over $\mathcal{F}$ by elements satisfying universal relations, i.e., such that every PVE with differential Galois group isomorphic to G of a differential field with field of constants $\mathcal{C}$ is generated by elements satisfying at least those relations.

For example, let

$$X = \frac{1}{x^2+y^2+z^2+w^2} \times \begin{pmatrix} x^2+y^2-z^2-w^2 & 2xw+2yz & 2yw-2xz \\ 2yz-2xw & x^2-y^2+z^2-w^2 & 2xy+2zw \\ 2xz+2yw & 2zw-2xy & x^2-y^2-z^2+w^2 \end{pmatrix}$$

denote the generic point of SO_3 given by Euler's parametrization, and put

$$P = \begin{pmatrix} \sqrt{a} & & \\ & \sqrt{b} & \\ & & 1/\sqrt{ab} \end{pmatrix},$$

with a, b differentially independent indeterminates over $\mathcal{C}$. The entries of the matrix XP are universal generators for SO_3 extensions (see [8]).

For G finite, this problem and the corresponding notions of generic equation and extension have been extensively studied by Saltman, DeMeyer, Smith, Ledet, Kemper and others and go as far back as the work of Emmy Noether. Generic extensions help understand polynomial Galois extensions with a given Galois group by providing an explicit description of the extensions in terms of generators whose relations are known.

Goldman [2] and Bhandari and Sankaran [1] developed notions of generic linear differential equations while studying a differential analogue of the Noether problem [14, 3] for some families of linear groups.

If F is a differential field and S is a set of elements in a differential domain containing F, $F\langle S\rangle$ denotes the differential field generated by S and F. We use the terminology "Picard-Vessiot G extension", with the obvious meaning "PVE with differential Galois group isomorphic to G".

We have developed the following notions and used them to solve the generic inverse problem for various groups, namely, SO_n, PGL_3, O_n, the infinite multiplicative and additive dihedral groups and the infinite quaternion group [8, 9, 10]:

Let $\mathfrak{gl}_m(\cdot)$ denote the Lie algebra of $m \times m$ matrices with coefficients in some specified field and let $\mathcal{F} = \mathcal{C}\langle Z_1, \ldots, Z_k\rangle$, with Z_i differentially independent indeterminates over $\mathcal{C}$. Let $\mathcal{E} \supset \mathcal{F}$ be a Picard-Vessiot G extension for an equation $X' = X\mathcal{A}(Z_1, \ldots, Z_k)$, with $\mathcal{A}(Z_1, \ldots, Z_k) \in \mathfrak{gl}_m(\mathcal{F})$.

Definition 1. $\mathcal{E} \supset \mathcal{F}$ is said to be a *generic extension for* G if for every Picard-Vessiot G extension $E \supset F$ there is a specialization $Z_i \to f_i \in F$, such that the equation $X' = X\mathcal{A}(f_1, \ldots, f_k)$ gives rise to $E \supset F$ and any fundamental solution matrix maps to one for the specialized equation.

The following stronger version generalizes an analogue in polynomial Galois theory [12]:

Definition 2. $\mathcal{E} \supset \mathcal{F}$ is said to be a *descent generic extension for* G when the following condition holds: for any differential field F with field of constants $\mathcal{C}$ there is a PVE $E \supset F$ with differential Galois group $H \leq G$ if and only if there is a

specialization $Z_i \to f_i \in F$ such that the equation $X' = X\mathcal{A}(f_1, \ldots, f_k)$ gives rise to the extension $E \supset F$ and any fundamental solution matrix maps to one for the specialized equation.

Our method for constructing generic PVE's with group G relies on the structure of Picard-Vessiot G extensions as function fields of irreducible G torsors. The results presented here extend the work in [4, 5, 6] to the situation in which the torsors for the group can be described 'generically'. We briefly summarize the previous results since it is still the case that for many groups a good description of the all the torsors is not available:

(1) The case when G is connected and only PVE's of the form $F(G) \supset F$ where $F(G)$ is the function field of the trivial torsor are considered. This case was first addressed in [4] and then completely solved in [5] for all connected groups. A descent property (more restricted than Definition 2) was achieved in this case as well.

(2) The case when G is non-connected of the form $H \ltimes G^0$, with H finite, G^0 connected, and the adjoint H action on the Lie algebra of G^0 is faithful. The extensions considered are the function fields of G torsors of the form $W \times G^0$ for some irreducible H torsor W. The construction here generalizes (1) and uses tools from the constructive solution, by Mitschi and Singer [13], of the inverse problem for solvable-by-finite groups. A generalization of a result in [13] is obtained, which allows an extension of the descent theorem from (1) to this case. This case is completely solved in [6].

We have attacked the most general case, i.e., the construction of generic extensions which simultaneously describe function fields of trivial and non-trivial torsors by using the bijective correspondence between isomorphism classes of G torsors and the equivalence classes of crossed homomorphisms in the first Galois cohomology set, a particularly helpful feature when a good interpretation of the latter (in a sense explained in [9]) is available.

The generic equations of Goldman and Bhandari and Sankaran have been also studied in the language of rings and homomorphisms [11], the main tool being *the ring of generic solutions* – the analogue to the coordinate ring of a 'generic' torsor.

References

[1] A. K. Bhandari and N. Sankaran, *Generic differential equations and Picard-Vessiot extensions*, Ren. Sem. Mat. Univ. Pol. Torino **52** (1994), 353–358.

[2] L. Goldman, *Specialization and Picard–Vessiot theory*, Trans. Amer. Math. Soc. **85** (1957), 327–356.

[3] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications, Cambridge University Press (2002).

[4] L. Juan, *Principal differential ideals and a generic inverse differential Galois problem for* GL_n, Comm. Algebra **30** (2002), 6071-6103.

[5] L. Juan, *Pure Picard-Vessiot extensions with generic properties*, Proc. Amer. Math. Soc., **9** (2004), 2549-2556.

[6] L. Juan, *Generic Picard-Vessiot extensions for connected by finite groups*, J. Alg. **312** (2007), 194–206.

[7] L. Juan and A. Ledet, *Equivariant vector fields on non-trivial* SO_n*-torsors and differential Galois theory*, J. Alg., to appear (doi:10.1016/j.jalgebra.2007.01.005)
[8] L. Juan and A. Ledet, *On generic differential* SO_n *extensions*, preprint (2006), available at www.math.ttu.edu/∼ljuan
[9] L. Juan and A. Ledet, *On Picard-Vessiot extensions with group* PGL_3, preprint (2007), available at www.math.ttu.edu/∼ljuan
[10] L. Juan and A. Ledet, *Generic Picard-Vessiot extensions for non-connected groups*, preprint (2007), available at www.math.ttu.edu/∼ljuan
[11] L. Juan and A. Magid, *Generic rings for Picard-Vessiot extensions and generic differential equations*, J. Pure Appl. Algebra **209** (2007), 793–800.
[12] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139-141.
[13] C. Mitschi and M. Singer, *Solvable-by-finite groups as differential Galois groups*, Ann. Fac. Sci. Toulouse Math. **11** (2002), 403–423.
[14] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1916), 221–229.

Differential Groups and Differential Relations

Michael F. Singer

In 1886, Otto Hölder showed [4] that the Gamma function satisfies no algebraic differential equation, that is, that there is no nonzero polynomial $F(x, y, y', y'', \ldots)$ with complex coefficients such that $F(x, \Gamma(x), \Gamma'(x), \Gamma''(x), \ldots) = 0$. This result has been given many proofs over the years (for a survey of this and related results, see [7].) Recently, C. Hardouin used the Galois theory of linear difference equations and facts concerning linear algebraic groups to prove generalizations of this result (see [2, 3]; the latter paper also contains a subsequent approach and concise proof due to M. van der Put). Motivated by these results, we developed a Galois theory of linear difference equations where the Galois groups are linear *differential* algebraic groups whose differential properties (*e.g.*, differential dimension) measure the differential properties of the difference equation.

By a *$\sigma\delta$-ring* we mean a ring R together with an automorphism σ and a derivation δ such that $\sigma(\delta(r)) = \delta(\sigma(r))$ for all $r \in R$. Similarly, we can define a *$\sigma\delta$-field* (all fields considered will be of characteristic zero). Examples of $\sigma\delta$-fields include: $k = \mathbb{C}(x), \sigma(x) = x + 1, \delta = \frac{d}{dx}$; $k = \mathbb{C}(x), \sigma(x) = qx$ $(q \in \mathbb{C}\backslash\{0\}), \delta = x\frac{d}{dx}$; $k = \mathbb{C}(x, t), \sigma(x) = x + 1, \sigma(t) = t, \delta = \frac{\partial}{\partial t}$. For k a $\sigma\delta$-field we shall consider difference equations of the form

$$\sigma(Y) = AY, \quad A \in \mathrm{GL}_n(k) \tag{1}$$

Definition 1. A *$\sigma\delta$-Picard-Vessiot ring ($\sigma\delta$-PV-ring)* over k for equation (1) is a $\sigma\delta$-ring R containing k satisfying:

(1) R is a simple $\sigma\delta$-ring, *i.e.,* R has no ideals that are invariant under σ and δ
(2) There exists a matrix $Z \in \mathrm{GL}_n(R)$ such that $\sigma(Z) = AZ$.
(3) R is generated as a δ-ring over k by the entries of Z and $1/\det(Z)$, *i.e.,* $R = k\{Z, 1/\det(Z)\}_\delta$

Note that when δ is identically zero, this corresponds to the usual definition of a Picard-Vessiot extension for a difference equation. To prove existence and uniqueness of Picard-Vessiot extensions, one needs to assume that the field of σ-invariant elements of k is algebraically closed. In the case of $\sigma\delta$-PV extensions, $k^\sigma = \{c \in k \mid \sigma(c) = c\}$ is a differential field with derivation δ and we need to assume that this field is *differentially closed* (see Section 9.1 of [1] for the definition and references.)

Proposition 2. Let k be a $\sigma\delta$-field with k^σ a differentially closed field. There exists a $\sigma\delta$-PV ring for (1) and it is unique up to $\sigma\delta$-k-isomorphism.

We define the *$\sigma\delta$-Galois group* $\mathrm{Gal}_{\sigma\delta}(R/k)$ of the $\sigma\delta$-PV ring R (or of (1)) to be

$$\mathrm{Gal}_{\sigma\delta}(R/k) = \{\phi \mid \ \phi \text{ is a } \sigma\delta\text{-}k\text{-automorphism of } R\} \ .$$

As in the usual theory of linear difference equations, once one has selected a fundamental solution matrix of (1) in R, this group may be identified with elements of $\mathrm{GL}_n(k^\sigma)$. It has an additional structure as does R.

Theorem 3. Let k be a $\sigma\delta$-field and assume that k^σ is a differentially closed field. Let R be a $\sigma\delta$-PV extension of k.

(1) We may identify $\mathrm{Gal}_{\sigma\delta}(R/k)$ with the set of k^σ-points of a linear δ-differential algebraic group G defined over k^σ.
(2) R is a reduced ring and is the coordinate ring of a G-torsor V defined over k. The action of G on V induces an action of $G(k^\sigma)$ on R that corresponds to the action of $\mathrm{Gal}_{\sigma\delta}(R/k)$ on R under the above identification.

In the above result we use the terms "coordinate ring" and "G-torsor" in the differential sense (see Sections 4 and 9.4 of [1] for definitions of these terms as well as other definitions, facts and references concerning linear differential algebraic groups.) One can furthermore show that $R = R_0 \oplus \ldots \oplus R_{t-1}$ is the finite direct sum of integral k-algebras R_i where $\sigma : R_{i \bmod t} \to R_{i+1 \bmod t}$ isomorphically. In particular, the quotient fields of the R_i all have the same differential transcendence degree over k (see [5], Ch. II.10). Abusing language, we define this to be the *differential transcendence degree* $\mathrm{difftr}(R/k)$ *of* R *over* k. The above theorem implies that the $\mathrm{difftr}(R/k)$ is the same as the differential dimension of (the identity component) of G.

We give two applications of Theorem 3. Let $k \subset R$ be differential rings. We say that elements $z_1, \ldots, z_n \in R$ are *differentially dependent* over k if there exists a nonzero differential polynomial $f \in k\{y_1, \ldots, y_n\}$ such that $f(z_1, \ldots, z_n) = 0$. Using Cassidy's classification of differential subgroups of $\mathbf{G}_a^n$ (see Chapter 4 of [1] and references there) and the above theorem on can deduce

Proposition 4. Let k be a $\sigma\delta$-field with k^σ differentially closed and let $f_1, \ldots, f_n \in k$. Let R be a $\sigma\delta$-PV extension of k containing $z_1, \ldots, z_n$ such that

$$\sigma(z_i) - z_i = f_i \text{ for } i = 1, \ldots, n \ .$$

Then $z_1, \ldots, z_n$ are diffferentially dependent over k if and only if there is a homogeneous linear differential polynomial L with coefficients in k^σ such that

$$L(z_1, \ldots, z_n) = g \in k \ .$$

This latter condition is equivalent to $L(f_1, \ldots, f_n) = \sigma(g) - g$.

Using a descent argument, we can deduce the following

Corollary 5. Let $f_1, \ldots, f_n \in \mathbb{C}(x), \sigma(x) = x + 1, \delta = \frac{d}{dx}$ and let $z_1, \ldots, z_n$ be meromorphic functions satisfying

$$\sigma(z_i) - z_i = f_i, \quad i = 1, \ldots, n.$$

Then $z_1, \ldots, z_n$ are differentially dependent over $\mathcal{F}(x)$ ($\mathcal{F}$ is the field of 1-periodic functions) if and only if there is a homogeneous linear differential polynomial L over $\mathbb{C}$ such that

$$L(z_1, \ldots, z_n) = g, \quad g \in \mathbb{C}(x).$$

This latter condition is equivalent to $L(f_1, \ldots, f_n) = \sigma(g) - g$.

Letting $z(x) = \frac{\Gamma'(x)}{\Gamma(x)}$, one sees that $z(x+1) - z(x) = \frac{1}{x}$. For any linear differential operator L with complex coefficients, $L(\frac{1}{z})$ has precisely one pole while for any rational function g, $g(x+1) - g(x)$ will never have exactly one pole. Applying the Corollary when $n = 1$, we have that the Gamma function satisfies no polynomial differential equation.

One can deduce a similar statement for q-difference equations and also characterize differential dependence among solutions of equations of the form $\sigma(y) = f_i y, f_i \in k$. This was first done in [2, 3] (using the usual Galois theory) where explicit criteria are also given just in terms of the divisors of the f_i.

Our techniques, together with Cassidy's classification of Zariski dense differential subgroups of simple linear differential algebraic groups also allow us to show

Proposition 6. Let k be as above and $A \in \mathrm{GL}_n(k)$. Assume that the (usual) difference Galois group of (1) is a simple noncommutative linear algebraic group of dimension t. Let R be the associated $\sigma\delta$-PV ring. The differential transcendence degree of R over k is less than t if and only if it exists $B \in \mathrm{gl}_n(k)$ such that $\sigma(B) = ABA^{-1} + \delta(A)A^{-1}$.

A descent argument allows one to prove a corollary of Proposition 6 analogous to Corollary 5 and using this one can show, for example, that if y_1, y_2 are linearly independent solutions of $y(x+2) - xy(x+1) + y = 0$, then $y_1(x), y_2(x)$ and $y_1(x+1)$ are differentially independent over $\mathcal{F}(x)$.

Finally we note that Theorem 3 allows one to establish a Galois correspondence between linear algebraic subgroups of the $\sigma\delta$-Galois group and $\sigma\delta$-k-subrings $k \subset S \subset K$ of the total ring of quotients K of a $\sigma\delta$-PV-ring R satisfying the property that all nonzerodivisors in S are invertible in S (cf., Theorem 1.29 of [6]).

This material is based upon work supported by the National Science Foundation under Grant No. CCF-0634123.

References

[1] P.J. Cassidy, M.F. Singer, *Galois theory of parameterized differential equations and linear differential algebraic groups*, Differential Equations and Quantum Groups (IRMA Lectures in Mathematics and Theoretical Physics Vol. 9), ed. D. Bertrand, B. Enriquez, C. Mitschi, C. Sabbah, R. Schaefke, EMS Publishing house, (2006), 113- 157.

[2] C. Hardouin, *Hypertranscendance et Groupes de Galois aux différences*, preprint, `http://arxiv.org/abs/math.QA/0609646`, (2006).

[3] C. Hardouin, *Hypertranscendance des systèmes diagonaux aux différences*, preprint, (2007).

[4] O. Hölder, *Über die Eigenschaft der Gammafunktion keiner algebraischen Differentialgleichung zu genügen*, Mathematische Annalen **28** (1886), 1-13.

[5] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, (1973).

[6] M. van der Put, M.F. Singer, *Galois Theory of Difference Equations*, Lecture Notes in Mathematics, **1666**, Springer-Verlag, (1997).

[7] L.A. Rubel, *A Survey of Transcendentally Transcendental Functions*, The American Mathematical Monthly, **96:9** (1989), 777-788.

The accessory parameter problem in positive characteristic

Irene Bouw

Let $k = \bar{k}$ be an algebraically closed field of positive characteristic and $X = \mathbb{P}^1_k$. We choose a parameter t on X. We consider differential operators

$$L = \left(\frac{\partial}{\partial t}\right)^2 + p_1\left(\frac{\partial}{\partial t}\right) + p_2, \qquad p_1, p_2 \in k(t),$$

with regular singularities in $x_1, \ldots, x_r = \infty$. The goal of this talk is to study algebraic solutions $u \in k[\![t]\!]$ of L. A result of Honda ([4]) states that if L has an algebraic solution then L also has a polynomial solution.

We now suppose that the local exponents of L at x_i $(i \neq r)$ (resp. $x_r = \infty$) are $(0,0)$ (resp. $(r/2-1, r/2-1)$). This means that all local monodromy matrices are nilpotent. Under this assumption, L has nilpotent p-curvature if and only of L has a polynomial solution $u \in k[t]$. We may assume, moreover, that

$$p_1 = \sum_{i=1}^{r-1} \frac{1}{t - x_i}, \qquad p_2 = \frac{(1-r/2)^2 t^{r-3} + \beta_{r-4} t^{r-4} + \cdots \beta_0}{\prod_{i \neq r}(t - x_i)}.$$

The β_i's are the *accessory parameters*.

Let $\mathcal{N}_{0,r}$ be the space of differential operators L which have a polynomial solution, and $\mathcal{N}_{0,r}[d] \subset \mathcal{N}_{0,r}$ the subspace of differential operators for which the minimal degree of a polynomial solution is d. A result from Dwork ([2]) and Mochizuki ([5]) states that the natural projection $\pi : \mathcal{N}_{0,r} \to \mathcal{M}_{0,r}$, which sends L to the set of singularities, is finite and flat of degree p^{r-3}. The accessory parameter problem asks to determine the structure of $\mathcal{N}_{0,r}$ and $\mathcal{N}_{0,r}[d]$.

Theorem 1. *Suppose $p > r-2$. Then $\mathcal{N}_{0,r}[d]$ is nonempty if and only if*

$$\begin{cases} d \equiv 1 - r/2 \pmod{p}, \\ 0 \leq d \leq (r-2)(p-1)/2. \end{cases}$$

The necessity of the conditions follows from the Riemann relation and work of Dwork ([3, Lemma 10.1]).

The proof of the theorem first uses a deformation argument ([5]) to reduce to the case that r is odd and $d = (p - r + 2)/2$. In this case, we construct an explicit L which admits a solution of degree d. Details can be found in [1]. A theorem of Mochizuki shows that for d as in the theorem every irreducible component of $\mathcal{N}_{0,r}[d]$ has dimension $r - 3$.

References

[1] I.I. Bouw, *The accessory parameter problem in positive characteristic*, arXiv: 0705.0458v1

[2] B. Dwork, *Differential operators with nilpotent p-curvature*, *Amer. J. Math.*, 112:749–786, 1990.

[3] B. Dwork, *Lectures on p-adic differential equations*, Grundlehren der mathematischen Wissenschaften 253, Springer-Verlag, 1982.

[4] T. Honda, *Algebraic differential equations*, In *Symposia Mathematica, Vol. XXIV (Sympos. INDAM, Rome, 1979)*,

[5] S. Mochizuki, *Foundations of p-adic Teichmüller theory*, Number 11 in Studies in Advanced Math. AMS/IP, 1999.

t-Motivic Galois Groups

Lenny Taelman

The category of motifs depends on the data of a coefficient field (typically the field $\mathbb{Q}$ of rational numbers), and a base field (say, a number field, or the field of complex numbers).

Now let k be a finite field. Denote by $k(t)$ the field of rational functions in one variable t. Let K be any field containing $k(t)$ and fix an injective morphism $k(t) \to K$. One should think of $k(t)$ as the *coefficient* field, and of K as the base field. The chosen morphism $k(t) \to K$ plays the role of the canonical embedding of $\mathbb{Q}$ into any field of characteristic zero. The category of t-motifs [1] depends on this data.

This category shares many (proven) properties with the (conjectured) category of motifs. Most notably:

(1) It is neutral Tannakian over $k(t)$ [3] [4] (*vs.* neutral Tannakian over $\mathbb{Q}$).
(2) With its objects are naturally associated "λ-adic" Galois representations (one for every prime λ of $k[t]$) and this association is a fully faithful functor [5] (*vs.* the Tate conjecture).

With a motif one can also associate a de Rham-Betti realisation: a triple consisting of a vector space over the base field (de Rham cohomology), a vector space over the coefficient field $\mathbb{Q}$ (singular cohomology), and an isomorphism between their complexifications (the Grothendieck-de Rham isomorphism). It has been conjectured [2, 7.1.7.4] that this de Rham-Betti functor is fully faithful.

The results [3] of Papanikolas regarding a kind of Grothendieck period conjecture for t-motifs suggest that one should be able to add the following to the above list:

(3) With its objects are naturally associated "de Rham-Betti structures" and this association is fully faithful (*vs.* the fully faithfulness of the de Rham-Betti functor on motifs).

In this talk we show how to associate such structures with t-motifs, and suggest how the results of Papanikolas [3] imply that this defines a fully faithful realisation functor.

References

[1] G. Anderson, *t-Motives*, Duke Math. J. **53** (1986), 457–502.
[2] Y. André, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, Panoramas et Synthéses [Panoramas and Syntheses], 17. *Soc. Math. de France*, Paris, 2004.
[3] M. A. Papanikolas, *Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms*, `arXiv:math.NT/0506078`.
[4] L. Taelman, *On t-Motifs*, thesis, University of Groningen (2007).
[5] Y. Taguchi, *The Tate conjecture for t-motives*, Proc. Amer. Math. Soc. **123** (1995), no. 11, 3285–3287.

Iterative Connections and Abhyankar's Conjecture

Andreas Röscheisen

In classical theory, one regards modules with connections resp. integrable connections over a certain ring R containing a field K (cf. [2]). If $\mathrm{char}(K) = 0$ and R satisfies some conditions (e.g. $\mathrm{Spec}(R)$ is a smooth, integral scheme of finite dimension over K), the category of these modules forms a neutral Tannakian category over the field K. Thus the general Tannakian approach gives rise to a Galois theory for this category. The first part of this abstract provides a generalisation for arbitrary characteristic which I developed in my dissertation ([5]). All the details omitted here can be found there.

1. Iterative Connections

Definition 1. *For a commutative graded algebra* $\bigoplus_{i=0}^{\infty} B_i$*, we call* $B := \prod_{i=0}^{\infty} B_i$ *the completion of a graded algebra (***cga** *for short). (In fact, B is the completion of* $\bigoplus_{i=0}^{\infty} B_i$ *with respect to the topology given by the grading, cf.* [1]*). We call B_i the i-th homogeneous component of B. If B_0 is isomorphic to a given ring R, B is called a R-cga. B is also an algebra with multiplication given by the Cauchy-product.*

Throughout this abstract, we use the following
Notation: K is a perfect field, R a finitely generated K-algebra such that $\mathrm{Spec}(R)$ is a smooth, integral scheme with a K-rational point, B is a R-cga and M a finitely generated R-module.

Definition 2. *A* **higher derivation** *of R to B over K is a homomorphism of K-algebras $\psi : R \to B$ such that $\mathrm{pr}_0 \circ \psi = \mathrm{id}_R : R \to B \to B_0 = R$. For such a higher derivation, we set $\psi^{(k)} := \mathrm{pr}_k \circ \psi : R \to B_k$. A higher derivation $\psi : R \to R[[T]]$ (the power series ring $R[[T]]$ is the completion of the polynomial ring) is called an* **iterative derivation**, *if for all $i, j \in \mathbb{N}$: $\psi^{(i)} \circ \psi^{(j)} = \binom{i+j}{i}\psi^{(i+j)}$ as maps from R to $R \cdot T^{i+j} \cong R$.*
Similarly, for a given higher derivation $\psi : R \to B$, we define a higher ψ-derivation on the R-module M to be a K-linear map $\Psi : M \to B \otimes_R M$ with $\mathrm{pr}_0 \circ \Psi = \mathrm{id}_M$ and $\Psi(rm) = \psi(r)\Psi(m)$ for all $r \in R$ and $m \in M$.

As for usual derivations, we then have

Theorem 3. *Up to isomorphism, there exists a unique R-cga $\hat{\Omega}_{R/K}$ (which we call the algebra of* **higher differentials***) together with a higher derivation $\mathrm{d}_R : R \to \hat{\Omega}_{R/K}$ satisfying the following universal property:*
For each R-cga B and higher derivation $\psi : R \to B$ there exists a unique grading preserving homomorphism of R-algebras $\tilde{\psi} : \hat{\Omega}_{R/K} \to B$ with $\tilde{\psi} \circ \mathrm{d}_R = \psi$.

Now, the crucial point for the whole theory is that this universal higher derivation can be extended to a K-algebra-automorphism $\mathrm{d}_{\hat{\Omega}} : \hat{\Omega}_{R/K} \to \hat{\Omega}_{R/K}$ that fulfills $\mathrm{d}_{\hat{\Omega}}^{(i)} \circ \mathrm{d}_{\hat{\Omega}}^{(j)} = \binom{i+j}{i}\mathrm{d}_{\hat{\Omega}}^{(i+j)}, i, j \in \mathbb{N}$. Here $\mathrm{d}_{\hat{\Omega}}^{(i)}$ denotes that part of $\mathrm{d}_{\hat{\Omega}}$ that "increases degrees by i", i. e. for all $k \in \mathbb{N}$, we have $\mathrm{d}_{\hat{\Omega}}^{(i)}|_{\hat{\Omega}_k} = \mathrm{pr}_{i+k} \circ \mathrm{d}_{\hat{\Omega}}|_{\hat{\Omega}_k}$.
Using this automorphism, we can define the main object:

Definition 4. *Let M be a finitely generated R-module. An* **iterative connection** *on M is a K-linear map $\nabla : M \to \hat{\Omega}_{R/K} \otimes_R M$ satisfying:*

(1) $\nabla^{(0)} := (\mathrm{pr}_0 \otimes \mathrm{id}_M) \circ \nabla = \mathrm{id}_M$.
(2) $\forall r \in R, m \in M : \nabla(rm) = \mathrm{d}_R(r)\nabla(m)$.
(3) *Letting ${}_{\hat{\Omega}}\nabla : \hat{\Omega}_{R/K} \otimes_R M \to \hat{\Omega}_{R/K} \otimes_R M, \omega \otimes m \mapsto \mathrm{d}_{\hat{\Omega}}(\omega)\nabla(m)$, we have for all $i, j \in \mathbb{N}$:*

$$ {}_{\hat{\Omega}}\nabla^{(i)} \circ {}_{\hat{\Omega}}\nabla^{(j)} = \binom{i+j}{i} {}_{\hat{\Omega}}\nabla^{(i+j)}. $$

(Again ${}_{\hat{\Omega}}\nabla^{(i)}$ denotes that part that "increases degrees by i".)

For every higher derivation $\psi : R \to B$, we then get a higher ψ-derivation on M by $\nabla_\psi := (\tilde{\psi} \otimes \mathrm{id}_M) \circ \nabla : M \to B \otimes_R M$.
∇ is called **integrable iterative**, *if in addition for all commuting iterative derivations $\psi_1, \psi_2 : R \to R[[T]]$ (i. e. for all $k, l \in \mathbb{N}$: $\psi_1^{(k)} \circ \psi_2^{(l)} = \psi_2^{(l)} \circ \psi_1^{(k)}$) the higher derivations ∇_{ψ_1} and ∇_{ψ_2} commute.*

With the assumptions on the ring R made in the beginning, one can show that every finitely generated R-module M that admits an iterative connection, is in fact a projective module. Hence the modules with iterative connection form an abelian category. (Morphism being the homomorphism commuting with the iterative connection.) Moreover, we have:

Theorem 5. *The category* $\mathbf{ICon}(R/K)$ *of modules with iterative connection and the category* $\mathbf{ICon}_{int}(R/K)$ *of modules with integrable iterative connection are neutral Tannakian categories over* K*. Furthermore, if* $\mathrm{char}(K) = 0$*, these categories are equivalent to the categories of modules with connections resp. integrable connections, where the equivalence is given by* $(M, \nabla) \mapsto (M, \nabla^{(1)})$*.*

Remarks. *If the transcendence degree of* R *over* K *is one, every iterative connection on a module is automatically integrable and the category* $\mathbf{ICon}(R/K)$ *is equivalent to the category of differential modules (if* $\mathrm{char}(K) = 0$*) respectively to the category of iterative differential modules as given in* [3] *(if* $\mathrm{char}(K) \neq 0$*).*
One can easily generalise the above to modules over schemes (cf. [5]*, Ch. 4.2).*

2. Abhyankar's Conjecture

By the general theory, a neutral Tannakian category over a field K is equivalent to $\mathrm{Rep}_K(\mathcal{G})$, the category of finite dimensional representations of some proalgebraic group $\mathcal{G}$ defined over K. Moreover for every object M, the full Tannakian subcategory generated by M is equivalent to $\mathrm{Rep}_K(G_M)$, where G_M is a quotient of $\mathcal{G}$ and in fact a linear algebraic group over K. The natural question, which linear algebraic groups occur if we take objects of $\mathbf{ICon}(R/K)$ or $\mathbf{ICon}_{int}(R/K)$, leads in a special case to a differential version of Abhyankar's Conjecture.

Differential Abhyankar Conjecture. *Let* $K \neq \overline{\mathbb{F}}_p$ *be an algebraically closed field of characteristic* $p > 0$*. Let* X *be a smooth projective curve over* K*,* $S \subset X$ *a finite subset and* $R = \mathcal{O}_X(X \setminus S)$ *(i.e.* $\mathrm{Spec}(R) \cong X \setminus S$*). Then a linear algebraic group* G *occurs as* $G_{(M,\nabla)}$ *for* $(M, \nabla) \in \mathbf{ICon}(R/K)$ *if and only if* $G/U(G)$ *does. (*$U(G)$ *denoting the unipotently generated subgroup of* G*.)*

In the setting of iterative differential modules, this conjecture is already stated in [4], without the assumption $K \neq \overline{\mathbb{F}}_p$. However in my dissertation, I proved that the conjecture is false if one drops this assumption. Moreover, I could prove that the conjecture is true for connected groups. I even showed a stronger result, namely that each reduced connected linear algebraic group occurs if S contains at least two points.

References

[1] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics 150, Springer (1995)

[2] N. Katz, *On the calculation of some differential Galois groups*, Inv. Math. **87** (1987), 13–61.

[3] B. H. Matzat, *Differential Galois Theory in Positive Characteristic*, notes written by J. Hartmann, IWR-Preprint 2001-35 (2001)

[4] B. H. Matzat, M. van der Put, *Iterative Differential Equations and the Abhyankar Conjecture*, J. Reine Angew. Math. **557** (2003), 1–52.

[5] A. Röscheisen, *Iterative Connections and Abhyankar's Conjecture*, Heidelberg University Library, Dissertation (2007) (http://www.ub.uni-heidelberg.de/archiv/7179/)

Lifting local group actions on curves

Ted Chinburg
(joint work with Robert Guralnick, David Harbater)

Let k be an algebraically closed field of characteristic $p > 0$. Suppose that $\phi : G \to \mathrm{Aut}_k(k[[t]])$ is an embedding of a finite group G into the group of continuous k-automorphisms of the power series ring $k[[t]]$. This report concerns the question of whether there is a complete discrete valuation ring R of characteristic 0 which has residue field k for which ϕ can be lifted to an embedding $\Phi : G \to \mathrm{Aut}_R(R[[t]])$. If such an R and Φ exist, we will say ϕ can be lifted to characteristic 0.

Our results concern a lifting obstruction which is due to Bertin [1]. Let a_ϕ be the Artin character associated to ϕ. Bertin showed that if a lifting Φ of the above kind exists, there must be a finite G-set S with the following properties. The stabilizer of each $s \in S$ is a non-trivial cyclic subgroup of G. The character χ_S of the permutation representation of G associated to S is given by $\chi_S = mr_G - a_\phi$, where r_G is the character of the regular representation of G and $0 \leq m \in \mathbb{Z}$.

In an earlier talk at Oberwolfach we reported on a determination of all finite groups G for which the Bertin obstruction of every ϕ as above vanishes. By similar methods we have now determined the G for which the Bertin obstruction of some ϕ vanishes; call such G weak local Bertin groups.

We conjecture that when G and k are fixed, every (resp. some) ϕ lifts to characteristic 0 if and only if the Bertin lifting obstruction of every (resp. some) ϕ vanishes. Examples of Pagot [3] show, however, that the Bertin obstruction of a particular ϕ may vanish even though ϕ cannot be lifted to characteristic 0.

To state our result concerning weak local Bertin groups, we must define another set of groups.

Definition 1. *Let $W(k)$ be the ring of infinite Witt vectors over k. We will call a finite group G a Green-Matignon group for k if G is the semi-direct product of a normal p-group P by cyclic subgroup C of order prime to p and if the following conditions hold.*

a. *For each non-trivial element t of C, the centralizer $C_G(t)$ of t in G is cyclic and equal to the product group $C_P(t) \times C$.*
b. *Suppose T is a cyclic subgroup of P and that the centralizer $C_C(T)$ of T in C is not trivial. Then $C_C(T) = C$ and*

$$\sum_{\Gamma \in S(T)} \mu([\Gamma : T]) \equiv 0 \mod \#C\mathbb{Z}$$

where the sum is over the set $S(T) = S_G(T)$ of cyclic subgroups of G which contain T, and $\mu(x)$ is the Mobius μ function.
c. *There is a faithful character $\Theta : C \to W(k)^*$ for which the following is true. Suppose T is a cyclic subgroup of P and $C_C(G)$ is trivial. The restriction of Θ to the normalizer $N_C(T)$ of T in C takes values in $\mathbb{Z}_p^*$, and*

$$xyx^{-1} = y^{\Theta(x)}$$

for $y \in T$ and $x \in N_C(T)$. Furthermore,

$$\sum_{P \not\supset \Gamma \in S(T)} \mu([\Gamma : T]) \equiv 0 \mod \#N_C(T)\mathbb{Z}$$

We will say G is hereditarily Green-Matignon for k, or simply hereditarily GM, if the above conditions also hold, with the same character Θ, when G is replaced by any quotient $G/J = (P/J).C$ by a normal subgroup J of G contained in P.

It is not hard to show that a group G which is hereditarily GM for one algebraically closed field k of characteristic p will be so for every algebraically closed field k of characteristic p.

Theorem 2. *Let G be the semi-direct product of a normal p-group G by cyclic subgroup C of order prime to p. Then G is a weak local Bertin group (i.e. there is an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ which has vanishing Bertin obstruction) if and only G is hereditarily GM for k.*

Example 3. *If G is a p group then there is a ϕ for which the Bertin obstruction vanishes.*

Example 4. *Green and Matignon proved in* [2] *that if the center $Z(G)$ of G is neither cyclic nor a p-group then the Bertin obstruction of every ϕ associated to G is non-trivial. Suppose p is odd. Let G be the semi-direct product of a normal cyclic group of order p with $\mathbb{Z}/4$, with a generator of $\mathbb{Z}/4$ acting by inversions on the p-Sylow of G. Then $Z(G)$ is cyclic, so the Green and Matignon result does not apply. However, Theorem 2 shows that the Bertin obstruction of every ϕ associated to G is non-trivial.*

The proof of Theorem 2 involves converting the Bertin obstruction into a statement about the non-negativity and integrality of the elements of a set $\{b_T : T \in \mathcal{C}\}$ of rational numbers, where $\mathcal{C}$ is a set of representatives for the conjugacy classes of cyclic subgroups of G. The b_T arise from a_ϕ and Artin's theorem that if 1_T^G is the induction to G of the one-dimensional trivial character of T, then $\{1_T^G\}_{T \in \mathcal{C}}$ is a basis over $\mathbb{Q}$ for the $\mathbb{Q}$-vector space of characters of G having rational values. We prove various formulas for the b_T involving the higher ramification groups of G. We then show that if there is a ϕ for which the Bertin obstruction vanishes, G must be hereditarily GM. The proof of the converse involves constructing a ϕ for which the Bertin obstruction vanishes. This is done by induction on the length of a composition series for G.

References

[1] J. Bertin, *Obstructions locales au relèvement de revêtements galoisiens de courbes lisses*, C. R. Acad. Sci. Paris, Ser. I Math. **326** (1998), no. 1, 55–58.

[2] B. Green, B. and M. Matignon, *Liftings of galois covers of smooth curves*, Compositio Mathematica **113** (1998), 237–272.

[3] G. Pagot, *$\mathbb{F}_p$-espaces vectoriels de formes différentielles logarithmiques sur la droite projective*, J. of Number Theory **97** (2002), 58–94.

A moduli formulation of torsion conjectures for jacobians

Anna Cadoret

Given a finite group G and two integers $r,\ g \geq 0$ denote by $\mathcal{H}_{g,G,r}$, $\mathrm{H}_{g,G,r}$ the stack and coarse moduli spaces for G-curves Y with group G such that Y/G has genus g and the resulting G-cover $Y \to Y/G$ has degree r branch divisor. Similarly, denote by $\mathcal{H}_{G,r}$, $\mathrm{H}_{G,r}$ the stack and coarse moduli spaces for G-covers of the projective line with group G and degree r branch divisor. Recall that there is a canonical stack morphism $\mathcal{H}_{G,r} \to \mathcal{H}_{0,G,r}$.

The aim of this work is to describe a strategy to prove the following q-part of the weak torsion conjecture for specific families of jacobian varieties.

Conjecture: *For any number field k, integer $r \geq 2$ and primes $p,\ q$ with $p \not| 2r$ there exists a constant $n_k(p,q,r) \geq 1$ such that for any $f : Y \to \mathbb{P}^1_k \in \mathcal{H}_{\mathbb{Z}/p,2r}(k)$ there is no embedding $\mu_{q^n k} \hookrightarrow \mathrm{J}_{Y|k}$ for $n \geq n_k(p,q,r)$.*

Our approach relies on the following observations.

Let $Y \to k$ be a k-curve of genus $g \geq 1$ and set $J := \mathrm{Pic}^0_{Y|k}$, $P := \mathrm{Pic}^1_{Y|k}$. Denote by $\alpha : \pi_1(Y)^{(ab)} \to \pi_1(P)$ the morphism induced by the canonical embedding $Y \hookrightarrow P$ (Here $\pi_1(Y)^{(ab)}$ denotes the quotient of $\pi_1(Y)$ modulo the derived subgroup of $\pi_1(Y_{\overline{k}})$); note that α restricts to a Γ_k-equivariant isomorphism $\alpha_{\overline{k}} : \pi_1(Y_{\overline{k}})^{ab} \to \pi_1(P_{\overline{k}})$. Using that P is a J-torsor and Kunneth formula, one can show that:

Lemma 1. *There is a canonical Γ_k-equivariant isomorphism $i_{\overline{k}} : \pi_1(J_{\overline{k}}) \to \pi_1(P_{\overline{k}})$. In particular α is an isomorphism.*

So, if, for instance, $P(k) \neq \emptyset$ then any etale G-cover of J with group M induces an etale G-cover of Y with group M.

In our situation, one can even construct a $\mathbb{Z}/p$-invariant section by observing that $P(k)^{\mathbb{Z}/p} \neq \emptyset$. Indeed, denote by $\mathbf{t}$ the branch divisor of $Y \to \mathbb{P}^1_k$ and take any $t_0 \in \mathbb{P}^1(k) \setminus \{\infty\}$. As $p \not| 2r$, there exists two integers $u,\ v \in \mathbb{Z}$ such that $2ru + vp = 1$ and one can take $D := uf^{-1}(\mathbf{t}) + vf^{-1}(t_0) \in P(k)^{\mathbb{Z}/p}$. This and lemma 1 implies:

Lemma 2. *Let $Y_{q^m} \to Y$ be a degree q^m cyclic etale k-G-cover then the Galois closure $\hat{Y}_{q^m} \to \mathbb{P}^1_k$ of $Y_{q^m} \to Y \xrightarrow{f} \mathbb{P}^1_k$ is again a k-G-cover with group $G_{p,q^m} = M_{p,q^m} \rtimes \mathbb{Z}/p$, where M_{p,q^m} is an irreducible representation of $\mathbb{Z}/p$ over $\mathbb{Z}/q^m$ and inertia canonical invariant $\mathbf{C} = C_1 + \cdots C_r$ such that the elements in C_i have the same order as those in $C_i \bmod M_{q^m}$.*

For instance if $r = 2$, $p = 3$, $m = 1$ one has:

- If $3|q-1$ then $G_{3,q} = \mathbb{Z}/q \rtimes \mathbb{Z}/3$ with a generator u of $\mathbb{Z}/3$ acting *via* $u \cdot 1 = \zeta$, $\zeta^2 + \zeta + 1 = 0$.
- If $3|q+1$ then $G_{3,q} = (\mathbb{Z}/q)^2 \rtimes \mathbb{Z}/3$ with a generator u of $\mathbb{Z}/3$ acting *via* $u \cdot (1,0) = (0,1)$, $u \cdot (0,1) = (-1,-1)$.
- If $3 = q$ then $G_{3,3} = \mathbb{Z}/3 \times \mathbb{Z}/3$.

As a result any embedding $\mu_{q^n k} \hookrightarrow J$ induces a k-rational point on $\mathcal{H}_{G_{p,q},2r}$ hence on $\mathrm{H}_{0,G_{p,q},2r}$. So, by Mordell-Weil one gets:

Corollary. *If* $\mathrm{H}_{0,G_{p,q},2r}(k)$ *is finite then the conjecture holds for* k, r, p, q.

Proving that $\mathrm{H}_{0,G_{p,q},2r}(k)$ is finite is, in general, a difficult question. However, when $r = 2$, $\mathrm{H}_{0,G_q,4}$ is a curve which, *via* the branch divisor map, can be regarded as a finite cover $\mathrm{H}_{0,G_{p,q},4} \to \mathbb{P}^1$ branched at 0, 1, ∞. So the ramification type of $\mathrm{H}_{0,G_{p,q},4} \to \mathbb{P}^1$ can be described in a purely group theoretical way by the action of $\gamma_0,\ \gamma_1,\ \gamma_\infty \in \overline{H}_4$ on the reduced Nielsen class $\overline{\mathrm{ni}}_4(G_{p.q})$. Here:

- H_4 denotes the Hurwitz braid group given by the generators Q_1, Q_2, Q_3 and the relations $Q_iQ_jQ_i = Q_jQ_iQ_j$, $1 \le i \ne j \le 3$, $Q_1Q_3 = Q_3Q_1$, $Q_1Q_2Q_3^2Q_2Q_1 = 1$.
- $\mathrm{ni}_4(G_{p.q})$ denotes the set of all 4-tuples $\mathbf{g} = (g_1, ..., g_4) \in G_{p,q}$ which generate G_q and satisfy $g_1 \cdots g_4 = 1$ modulo inner conjugation by $G_{p,q}$.
- H_4 acts on $\mathrm{ni}_4(G_{p.q})$ by $Q_1 \cdot \mathbf{g} = (g_2^{g_1}, g_1, g_3, g_4)$,
  $Q_2 \cdot \mathbf{g} = (g_1, g_3^{g_2}, g_2, g_4)$,
  $Q_3 \cdot \mathbf{g} = (g_1, g_2, g_4^{g_3}, g_3)$.
- $\bar{\cdot}$ denotes quotient modulo the quaternionic subgroup $< (Q_1Q_2Q_3)^2, Q_1Q_3^{-1} >$.
- $\gamma_0,\ \gamma_1,\ \gamma_\infty$ denote the images of Q_1Q_2, $Q_1Q_2Q_3$, Q_2 in $\overline{H}_4$ respectively.

So, proving our conjecture for $r = 2$ amounts (Faltings) to proving that all the geometrically irreducible components of $\mathrm{H}_{0,G_{p,q},4}$ have genus ≥ 2 that is, equivalently (Riemann-Hurwitz), to computing the orbits of $\gamma_0,\ \gamma_1,\ \gamma_\infty$ acting on $\overline{\mathrm{ni}}_4(G_{p.q})$. Because of the specific structure of $G_{p,q}$, the latter problem can be handled by technics of linear algebra. For $p = 3$ (the only case entirely computed at the time of the writing) one obtains:

- $\mathrm{H}_{0,G_{3,2},4}$ has two geometrically irreducible components $\mathbb{Q}$-birational to $\mathbb{P}^1_{\mathbb{Q}}$.
- $\mathrm{H}_{0,G_{3,3},4}$ has three geometrically irreducible components $\mathbb{Q}$-birational to $\mathbb{P}^1_{\mathbb{Q}}$.
- For $q \ne 2,\ 3$, $\mathrm{H}_{0,G_{3,q},4}$ is geometrically irreducible with genus $(q-1)(\frac{q-1}{6} - 2)$ if $3|q-1$ and $\frac{q^2-1}{6}(q^2 - 3q - 10)$ if $3|q+1$.

Corollary. *The conjecture holds for* k, $r = 2$, $p = 3$, $q \ge 11$.

Remarks:

(1) For $q = 2,\ 3,\ 7$ all the geometrically irreducible components of $\mathrm{H}_{0,G_{3,q},4}$ are birational to $\mathbb{P}^1_{\mathbb{Q}}$ (Riemann-Roch) and $\mathrm{H}_{0,G_{3,5},4}$ has genus 1. In this case, the ramification data computed above do not show that there is a degree 1 $\mathbb{Q}$-rational divisor on it. Assume it has one, then $\mathrm{H}_{0,G_{3,5},4}$ is an elliptic curve with good reduction outside 3 and 5. However, according to Cremona's tables, there can be such elliptic curves with either zero or positive rank.

(2) It is natural to ask whether our method does not lead to examples for which uniform bounds are known to exist. The sharpest result in this direction is the following corollary of Clark-Xarles' analysis of the uniform boundedness for the torsion of abelian varieties over l-adic fields. Given a l-adic field k, say that an abelian variety $A \to k$ has isotropic reduction if the 0-component of the reduction of its Neron model contains $\mathbb{G}_m$.

Theorem. *For any number field $k/\mathbb{Q}$ and places $v_1,\ v_2$ of k with residue characteristics $p_1 \neq p_2$, for any g-dimensional abelian variety $A \to k$ with anisotropic reduction above $v_1,\ v_2$ one has*

$$|\mathrm{Tors}(A(k))| \leq (\lfloor 1 + p_1^{\frac{d}{2}} \rfloor \lfloor 1 + p_2^{\frac{d}{2}} \rfloor)^g.$$

However, for any integer $N \geq 1$ one can construct infinitely many $Y \to \mathbb{P}^1_k \in \mathcal{H}_{\mathbb{Z}/3,4}(k)$ with isotropic reduction at all primes $l \leq N$, $l \neq p$. For this, choose a prime $q \neq p$ and $q > N$ and set $\mathbf{t}(\lambda,\mu) := \{\lambda\zeta_p,\ \lambda\zeta_p^{-1},\ \mu\zeta_p,\ \mu\zeta_p^{-1}\}$ with $\lambda,\ \mu \in \mathbb{Q}$ such that $\mathbf{t}(\lambda,\mu)$ is pairwise adjusted (Liu, Pop) for the l-adic valuations, $l \leq N$. Then, by rigid patching, one can construct for all $m \geq 1$ a G-cover $Y_{\lambda,\mu,q^m} \to \mathbb{P}^1_{\hat{k^l}}$ with group of type G_{p,q^m}, inertia canonical invariant $2(C + C^{-1})$ ((where C denotes the conjugacy class of u)) and branch divisor $\mathbf{t}(\lambda,\mu)$ (here, $\widehat{k^l}$ denotes the completion of k at any place above l). Then, $Y_{\lambda,\mu} := Y_{\lambda,\mu,q^m}/M_{p,q^m}$ is defined over k (rigidity and $\mathbf{t}(\lambda,\mu)$ k-rational) with the property that $\mu_{q^m \widehat{k^l}} \hookrightarrow \mathrm{J}_{Y_{\lambda,\mu}\widehat{k^l}}$ hence that $\mathrm{J}_{Y_{\lambda,\mu}\widehat{k^l}}$ has isotropic reduction (Clark-Xarles and $q \neq l$), $l \leq N$. One obtains the annouced conclusion by letting λ and μ vary.
(3) The computation above for $p = 3$ is, essentially, a test for our method and analyzing more precisely the arithmetico-geometric properties of the $\mathrm{H}_{0,G_{3,q^m},4}$ to get bounds depending only on $[k : \mathbb{Q}]$, q (q-strong torsion conj.), k (torsion conj.) or even $[k : \mathbb{Q}]$ (strong torsion conj.) should show how far we can go since, in this precise example, all these bounds are known to exist. Indeed, by the classification of automorphism groups of genus 2 curves any such curve which contains an order 3 element in its automorphism group has reduced automorphism group isomorphic to D_6 (or D_{12}) hence its jacobian is isogeneous, *via* a degree ≤ 4 isogeny, to a product of elliptic curves. Now, for elliptic curves, the strong torsion conjecture holds (Merel).

On smooth curves endowed with a big automorphism group

Magali Rocher

Let k be an algebraically closed field of characteristic $p > 0$ and let C/k be a connected smooth projective curve with genus $g \geq 2$. Then, the order of the full automorphism group $Aut_k(C)$ is bounded by a polynomial in g. Because of the appearance of wild ramification, this bound may be very large, in comparision with the case $char(k) = 0$. Following [Na], we study curves endowed with a big p-group of automorphisms.

Proposition 1 ([L-M])**.**
Let G be a p-subgroup of $Aut_k(C)$. (C,G) is called a "big action" if $\frac{|G|}{g} > \frac{2p}{p-1}$.

1. *Then, there is a point of C (say ∞) such that G is the wild inertia subgroup of G at ∞. Moreover, $C/G \simeq \mathbb{P}^1_k$ and the ramification locus (resp. branch locus) of the cover $\pi : C \to C/G$ is the point ∞ (resp. $\pi(\infty)$).*
2. *Let us denote by G_i the ramification groups at ∞ in lower notation. Then, $G = G_1 \neq G_2$, $G_2 \neq \{1\}$, $C/G_2 \simeq \mathbb{P}^1_k$ and G/G_2 acts as a group of translations of the affine line $C/G_2 - \{\infty\}$.*
3. *Let H be a normal subgroup of G such that $g_{C/H} > 0$. Then, $(C/H, G/H)$ is also a big action.*

We use this third point to go back to the well-known case: $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Theorem 2 ([L-M]). *Let (C, G) be a big action with $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.*

(1) *Then, C is birational to: $W^p - W = XS(X) + cX$, where $S \in k\{F\}$ is an additive polynomial, with degree s in F, the Frobenius operator.*
(2) *Furthermore, the wild inertia subgroup of $Aut_k(C)$ at ∞: $Aut_{\infty,1}(C)$, is a central extension of $\mathbb{Z}/p\mathbb{Z}$ by an elementary abelian p-group: $(\mathbb{Z}/p\mathbb{Z})^{2s}$. The center of $Aut_{\infty,1}(C)$ is equal to its commutator subgroup and is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. For $p > 2$, $Aut_{\infty,1}(C)$ is the unique extraspecial group with exponent p and order p^{2s+1}.*

When k is a finite field, a way to produce big actions is to consider the ray class fields of function fields studied by K. Lauter ([Lau]) and R. Auer ([Au]).

Definition 3. *Let $K := \mathbb{F}_q(X)$, $q = p^e$, let S be the set of all finite rational places, let m be an integer and let us fix K^{alg} an algebraic closure of K.*
We define $K_S^m \subset K^{alg}$ as the largest abelian extension L/K with conductor $\leq m\infty$, such that every place of S totally splits in L. We denote by $G_S(m)$ the corresponding Galois group. It is is a finite p-group.

Proposition 4. *Let $C_m/\mathbb{F}_q$ be the smooth projective curve with function field K_S^m. As the translations: $X \to X + v$, $v \in \mathbb{F}_q$, stabilize S and ∞, they can be extended to $\mathbb{F}_q$-automorphisms of K_S^m. We thus get an action of a p-group $G(m)$ on C_m with:*

$$0 \longrightarrow G_S(m) \longrightarrow G(m) \longrightarrow (\mathbb{F}_q, +) \longrightarrow 0$$

To know if $(C_m, G(m))$ is a big action, we calculate the genus of the curve.

Proposition 5 ([Au]).

$$g_{C_m} = 1 + n_m(-1 + \frac{m}{2}) - \frac{1}{2}\sum_{j=0}^{m-1} n_j, \qquad n_j := \mid G_S(j) \mid .$$

Consequently, $(C_m, G(m))$ is a big action as soon as $\frac{q}{-1+\frac{m}{2}} > \frac{2p}{p-1}$. Then, the second ramification group at ∞: G_2, is equal to $G_S(m)$.

Theorem 6 ([Lau]). *The smallest conductor such that the exponent of $G_S(m)$ is stricly greater than p is $m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$, where $\lceil e/2 \rceil$ is the upper integer part of $e/2$.*

Remark 7. *Therefore, for $e > 3$, $(C_{m_2}, G(m_2))$ is an example of big action with G_2 abelian of exponent stricly greater than p.*

We now search for a classification of big actions and focus on those satisfying

$$M_1 := \frac{4}{(p^2-1)^2} \leq \frac{\mid G \mid}{g^2} \leq M_2 := \frac{4p}{(p-1)^2} \quad (*)$$

The upper bound M_2 always holds for big actions, whereas the lower bound M_1 has been chosen for G_2 to be abelian, with exponent p and order dividing p^3. Indeed, in this case, $\frac{|G|}{g^2}$ only takes a finite number of values:

Theorem 8. *For all $M > 0$, the set $E := \{\frac{|G|}{g^2}\}$ for (C,G) a big action with G_2 abelian of exponent p and such that $\frac{|G|}{g^2} \geq M$, is finite.*

To list all the values of $\frac{|G|}{g^2}$ and to find a parametrization of the curves in each case, it is necessary to shift to an embedding problem.

Assume $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $L := k(C)$, $k(X) := L^{G_2}$.
C is parametrized by: $\forall\ i \in \{1,..,n\}$, $W_i^p - W_i = f_i(X) \in k[X]$, with specific conditions imposed on the degree of $f_i(X)$.
$A := \frac{\wp(L)\cap k[X]}{\wp(k[X])}$ ($\wp := F - \mathrm{id}$) is an $\mathbb{F}_p$-vector space dual of G_2.

From the exact sequence induced by the ramification filtration

$$0 \longrightarrow G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow G = G_1 \longrightarrow V := \frac{G_1}{G_2} \simeq (\mathbb{Z}/p\mathbb{Z})^v \longrightarrow 0,$$

we can deduce a representation $\phi : V \to Aut(G_2) \simeq GL(n, \mathbb{F}_p)$, whose image can be seen as a subgroup of the upper triangular matrices with id on the diagonal. By duality, the adapted choice of basis for G_2 corresponds to the choice of the functions f_i as a basis for A.

A dual representation of ϕ is given by the action of V on A by translation $X \mapsto X + y$. The following proposition expresses the equivalence of the two representations.

Proposition 9. *$G_2 \subset Z(G) \Leftrightarrow \forall\ i \in \{1,..,n\}$, $f_i(X) = XS_i(X) + c_iX$ mod $\wp(k[X])$, with $S_i \in k\{F\}$. If we write $S_i = \sum_{j=0}^{m_i} a_j F^j$, with $a_{m_i} \neq 0$, we can define the "palindromic polynomial" of f_i as: $Ad_{f_i} := \frac{1}{a_{m_i}} F^{m_i}(\sum_{j=0}^{m_i} a_j F^j + F^{-j} a_j)$. It follows that $V \subset \bigcap_{i=1}^{n} Z(Ad_{f_i})$.*

We conclude with a table giving all the values of $\frac{|G|}{g^2}$ for a big action satisfying condition $(*)$, when $p \geq 3$. In each case, we can describe the functions f_i.

$\mid G \mid / g^2$	$\mid G_2 \mid$	$\phi(V)$	deg f_1	deg f_2	deg f_3	$dim_{\mathbb{F}_p} V$	
$\frac{4}{(p^2-1)^2}\ p(p+1)^2$	p	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$			$2s$	$s \geq 1$
$\frac{4}{(p^2-1)^2}\ (p+1)^2$	p	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$			$2s-1$	$s \geq 1$
$\frac{4}{(p^2-1)^2}\ p^2$	p^2	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$	$1+p^s$		$2s$	$s \geq 1$
$\frac{4}{(p^2-1)^2}\ \frac{p^2(p+1)^2}{(1+2p)^2}$	p^2	$\phi(V) \neq \{\mathrm{id}\}$	$1+p$	$1+2p$		2	$p \geq 3$
$\frac{4}{(p^2-1)^2}\ \frac{(p+1)^2}{p}$	p	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$			$2s-2$	$s \geq 1$
$\frac{4}{(p^2-1)^2}\ p$	p^2	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$	$1+p^s$		$2s-1$	$s \geq 2$
$\frac{4}{(p^2-1)^2}\ \frac{p^3(p+1)^2}{(1+p+p^2)^2}$	p^3	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$	$1+p^s$	$1+p^s$	$2s$	$s \geq 2$
$\frac{4}{(p^2-1)^2}\ \frac{p(p+1)^2}{(1+2p)^2}$	p^2	$\phi(V) \neq \{\mathrm{id}\}$	$1+p^2$	$1+2p^2$		3	$p \geq 3$
$\frac{4}{(p^2-1)^2}\ \frac{p^3(p+1)^2}{(1+p+2p^2)^2}$	p^3	$\phi(V) \neq \{\mathrm{id}\}$	$1+p^2$	$1+p^2$	$1+2p^2$	4	$p \geq 5$
$\frac{4}{(p^2-1)^2}\ \frac{p^3(p+1)^2}{(1+2p+2p^2)^2}$	p^3	$\phi(V) \neq \{\mathrm{id}\}$	$1+p$	$1+2p$	$1+2p$	2	$p \geq 5$
$\frac{4}{(p^2-1)^2}\ \frac{(p+1)^2}{p^2}$	p	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$			$2s-3$	$s \geq 1$
$\frac{4}{(p^2-1)^2}\ \frac{p^2(p+1)^2}{(p^2+1)^2}$	p^2	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$	$1+p^{s+1}$		$2s$	$s \geq 3$
$\frac{4}{(p^2-1)^2}$	p^2	$\phi(V) = \{\mathrm{id}\}$	$1+p^s$	$1+p^s$		$2s-2$	$s \geq 3$

References

[Au] R. Auer, *Ray Class Fields of Global Function Fields with Many Rational Places*, Dissertation at the University of Oldenburg, www.bis.uni-oldenburg.de/dissertation/ediss.html, (1999).

[Lau] K. Lauter, *A Formula for Constructing Curves over Finite Fields with Many Rational Points*, Journal of Number Theory 74 (1999).

[L-M] C. Lehr, M. Matignon, *Automorphism groups for p-cyclic covers of the affine line*, Compositio Math. 141 (2005).

[Na] S. Nakajima, *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. 303 (1987).

Local classification of linear meromorphic q-difference equations

Jean-Pierre Ramis

(joint work with Jacques Sauloy)

Our talk was devoted to the local meromorphic classification of q-difference modules. In [5] we gave such a classification in Birkhoff style, using normal forms and index theorems; this classification is complete in the "integral slope case". (One could extend it to the general case using some results of [1].) In [8] (cf. also [6]) appeared another version of our classification, using non abelian cohomology of sheaves on an elliptic curve.

Our aim was to present a new version of the classification, based upon a "fundamental group" and its finite dimensional representations, in the style of the Riemann-Hilbert correspondence for linear differential equations. At some abstract level, such a classification exists: The fundamental group is the Tannakian Galois group of the Tannakian category of our q-modules. But we want more information: Our essential aim is to get a *smaller* fundamental group which is Zariski dense in the Tannakian Galois group and to describe it *explicitly*. (As a byproduct, we shall also get a complete description of the Tannakian Galois group itself.) Our talk was based upon [3, 4]

For our purposes *Tannakian categories* are an essential tool. Assume $\mathcal{E}$ is a *neutral Tannakian category*, with fiber functor ω to the category of $\mathbb{C}$-vector spaces. Then $Aut^{\otimes}(\omega)$ has a structure of a *complex pro-algebraic affine group scheme*; we shall call it the Tannakian group of the Tannakian category $\mathcal{E}$. The category $\mathcal{E}$ is isomorphic to the category of finite dimensional representations[1] of $Aut^{\otimes}(\omega)$. Conversely, if G is a complex pro-algebraic group, its category of complex representations $Rep_{\mathbb{C}}(G)$ is a neutral Tannakian category with a natural fiber functor ω_G (the obvious forgetful functor) and $G = Aut^{\otimes}(\omega_G, Rep_{\mathbb{C}}(G))$; the complex space $\mathbf{aut}^{\otimes}(\omega_G, Rep_{\mathbb{C}}(G))$ of Lie-like $\otimes$-endomorphisms of the fiber functor ω_G is the Lie-algebra of $Aut^{\otimes}(\omega_G, Rep_{\mathbb{C}}(G))$.

[1]Each time we speak of representations of a pro-algebraic group, they are tacitly assumed to be morphisms for the pro-algebraic structure (i.e. *rational* representations).

Assuming that Γ is a *finitely generated* group, a *pro-algebraic completion* of Γ is, by definition, a *universal* pair $(\iota_{al}, \Gamma^{al})$ where $\iota_{al} : \Gamma \to \Gamma^{al}$ is a group homomorphism from Γ to a *pro-algebraic group* Γ^{al}. It is unique up to an isomorphism of pro-algebraic groups.

An example is the category of local meromorphic regular-singular connections, or equivalently the category $\mathcal{D}_f^{(0)}$ of regular singular $\mathcal{D}$-modules, where $\mathcal{D} = \mathbb{C}(\{z\})[d/dz]$. A meromorphic connection is equivalent to an equivalence class of differential systems $\Delta_A : \frac{dY}{dx} = AY$ up to the gauge-equivalence. We consider the fundamental group $\pi_1(D^*, d)$ of a germ at zero of punctured disc, pointed on a germ of direction d. We have an isomorphism $\mathbb{Z} \to \pi_1(D^*, d)$. Then, by a very simple application of the Riemann-Hilbert correspondence, the category $\mathcal{D}_f^{(0)}$ is equivalent to the category of finite dimensional representations of the fundamental group.

We can apply the Tannakian machinery to the group $\Gamma = \mathbb{Z} \approx \pi_1(D^*, d)$. Then the category $\mathcal{D}_f^{(0)}$ is equivalent to the category of representations of $\pi_1(D^*, d)$ (a regular singular $\mathcal{D}$-module M "is" a representation ρ_M of the topological fundamental group). It is also equivalent to the category of representations of the pro-algebraic completion $\pi_1^{\otimes}(D^*, d)$ of $\pi_1(D^*, d)$: a regular singular $\mathcal{D}$-module "is" a representation $\rho_M^{\otimes}$ of the Tannakian fundamental group $\pi_1^{\otimes}(D^*, d)$. The topological group $\pi_1(D^*, d)$ is the "small fundamental group" and $\pi_1^{\otimes}(D^*, d)$ is the "big fundamental group". The small group is *Zariski-dense* in the big group: the image of ρ_M is the monodromy group of M, it is Zariski-dense in the image of $\rho_M^{\otimes}$ which "is" the differential Galois group of M.

In order to understand the structure of the pro-algebraic completion of $\mathbb{Z}$, we can use the Tannakian machinery [7]: the pro-algebraic hull of $\mathbb{Z}$ is $\mathbb{Z}^{al} = Aut^{\otimes}(\omega)$, it is commutative and the product of its semi-simple part $\mathbb{Z}_s^{al}$ and its unipotent part $\mathbb{Z}_u^{al}$, where $\mathbb{Z}_s^{al} = Hom_{gr}(\mathbb{C}^*, \mathbb{C}^*)$, $\mathbb{Z}_u^{al} = \mathbb{C}$.

Our aim is to describe the q-analogues of the differential fundamental groups [2]. The construction is independent of the construction of the differential case; yet, like in that case it is done in three steps: (1) regular-singular or fuchsian equations, (2) formal or pure equations, (3) arbitrary equations. We shall limit ourselves to the integral slopes case. The first two steps are already well known and the difficult part is the last one.

Notations. We fix $q \in \mathbb{C}$ such that $|q| > 1$.

(1) We begin with the *regular singular case*: a germ of a meromorphic system at the origin $\sigma_q Y = AY$ is regular singular if and only if it is meromophically equivalent to a *fuchsian* system $\sigma_q Y = BY$ ($B(0) \in \mathrm{GL}_n(\mathbb{C})$). We call the corresponding category $\mathcal{E}_f^{(0)}$ the category of *fuchsian modules*, its Tannakian Galois group is isomorphic to $Hom_{gr}(\mathbf{E}_q, \mathbb{C}^*) \times \mathbb{C}$, where $\mathbf{E}_q = \mathbb{C}^*/q^{\mathbb{Z}}$ is (the underlying abstract group of) the elliptic curve associated to q (cf. [7] 2.2.2).

(2) The next step is the study of the category $\mathcal{E}_{form}$ of *formal* q-difference modules. We shall limit ourselves to the integral slope case: the category $\mathcal{E}_{form,int}$ (or equivalently, the category $\mathcal{E}^{(0)}_{p,1}$ of pure meromorphic modules with integral slopes). It is a neutral Tannakian category. As in the differential case, in order to compute the corresponding "fundamental groups", it is necessary to understand the formal classification of q-difference equations of order one. These equations are classified by the abelian group $\mathbb{C}^*/q^{\mathbb{Z}} \times (z^m)_{m\in\mathbb{Z}} \simeq \mathbf{E}_q \times \mathbb{Z}$. The "basic" irregular equation is $\sigma_q y - zy = 0$, it admits a Jacobi theta function θ_q as a solution and its q-difference Galois group is isomorphic to $\mathbb{C}^*$. Then one can prove that the Tannakian Galois group $G_{form,int}$ of the category $\mathcal{E}_{form,int}$ is isomorphic to the topological dual group of $\mathbf{E}_q \times \mathbb{Z}$ (where $\mathbf{E}_q$ is interpreted as the inductive limit of its finitely generated subgroups), that is to $\mathbb{C}^* \times (Hom_{gr}(\mathbf{E}_q, \mathbb{C}^*) \times \mathbb{C})$, where $\mathbb{C}^*$ is by definition the *theta torus* – the q-analogue of the exponential torus in the differential case [2].

(3) The last step is the study of the category $\mathcal{E}^{(0)}_1$ of q-difference modules whose Newton polygon admits only integral slopes. It is a neutral Tannakian category, we can prove that there exists a *semi-direct* decomposition of its Tannakian Galois group $G^{(0)}_1 = \mathfrak{St} \rtimes G^{(0)}_{p,1}$, where $\mathfrak{St}$ is a unipotent pro-algebraic group, and we can describe the Lie algebra $\mathfrak{st}$ of $\mathfrak{St}$: Like in the differential case, this Lie algebra is a "pro-algebraic completion" of a *free* complex Lie algebra generated by a family of "q-alien derivations" $\left(\dot{\Delta}^{(\delta)}_{\bar{c}}\right)_{\delta\in\mathbf{N}^*,\bar{c}\in\mathbf{E}_q}$.

These q-alien derivations are indexed by labels $(\delta, \mathbf{c})$ (which are the q-analogues of the labels $(q, \mathbf{d})$ in the differential case): δ is by definition a weight on the θ-torus $\mathbb{C}^*$ (that is, an element of the topological dual group $\mathbb{Z}$; actually, only the $\delta > 0$ have a non trivial action, so that we take $\delta \in \mathbf{N}^*$), and $\mathbf{c}$ is a pair formed by $c \in \mathbf{E}_q$ (*i.e.* a q-direction, representing a germ of q-spiral at the origin) and an element ξ of the semi-simple part of the q-local fundamental group $\pi_{1,q,f}$. In order to define the q-alien derivations, we use, as in the differential case, some summability tools [8], but the approach is different: we no longer use solutions but replace them by fiber functors. We deal with meromorphic families of Lie-like automorphisms of fiber functors (the variable being the q-direction of summability) and extract their singularities by a residue process.

In [3], we defined the q-alien derivations in all generality and compute them in the one-level case using a q-Borel transform; we also proved that, in this case, q-alien derivations are *a complete set of irregularity invariants*. We extended recently these results [4], proving that, in the general case also, q-alien derivations are a complete set of irregularity invariants and that the q-resurgence group is Zariski dense in $\mathfrak{St}$.

References

[1] M. van der Put M, M. Reversat, *Galois theory of q-difference equations*, Ann. Fac. Sci. de Toulouse, vol. **XVI**, no 2 (2007), 1–54.

[2] J.P. Ramis, *About the Inverse Problem in Differential Galois Theory: The Differential Abhyankar Conjecture*, The Stokes Phenomenon and Hilbert's 16-th Problem, Braaksma et al. editor, World Scientific (1996), 261–278.
[3] J.P. Ramis, J. Sauloy, *The q-analogue of the wild fundamental group (I)*, RIMS Kôkyûroku Bessatsu **B2** (2007), 167-193.
[4] J.P. Ramis, J. Sauloy, *The q-analogue of the wild fundamental group (II)*, to appear.
[5] J.P. Ramis, J. Sauloy and C. Zhang, *La variété des classes analytiques d'Équations aux q-différences dans une classe formelle*, C. R. Math. Acad. Sci. Paris, Ser. I, **338**, no. 4 (2004), 277–280.
[6] J.P. Ramis, J. Sauloy, C. Zhang, *Développement asymptotique et sommabilité des solutions des Équations linéaires aux q-différences*, C. R. Math. Acad. Sci. Paris, Ser. I, **342**, no. 7 (2006), 515–518.
[7] J. Sauloy, *Galois theory of Fuchsian q-difference equations*, Ann. Sci. École Norm. Sup. **36** (2003), no. 6, 925–968.
[8] J. Sauloy, *Algebraic construction of the Stokes sheaf for irregular linear q-difference equations*, Analyse complexe, systèmes dynamiques, sommabilité des séries divergentes et théories Galoisiennes. I, Astérisque **296** (2004), 227–251.

Cohen–Lenstra heuristics and the negative Pell equation

Jürgen Klüners
(joint work with Étienne Fouvry)

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field of discriminant D. Denote by Cl_D the ordinary class group of K and by C_D the narrow class group of K. We remark that these two groups are always the same if $D < 0$. For a prime ℓ we denote by $\mathrm{rk}_\ell(A) := \dim_{\mathbb{F}_\ell}(A/A^\ell)$ the ℓ–rank of an abelian group A. Furthermore we introduce the 4–rank $\mathrm{rk}_4(A) := \mathrm{rk}_2(A^2)$.

The goal of this talk is to report on some proven cases of the so-called Cohen–Lenstra [1] heuristics which was stated in 1983 for odd primes ℓ and extended in 1987 by Gerth [6] to $\ell = 2$. In order to state these conjectures we need the following notation.

Definition 1. *Let $f(D)$ be a numerical function. Then $f(D)$ has a mean value over positive fundamental discriminants, if there exists a number $M^+(f(D))$ such that*

$$\frac{\sum\limits_{0<D<X} f(D)}{\sum\limits_{0<D<X} 1} \underset{X\to\infty}{\longrightarrow} M^+(f(D)).$$

Define $M^-(f(D))$ for the corresponding limit over negative fundamental discriminants.

Now we are able to state one case of the Cohen–Lenstra–Gerth heuristics.

Conjecture 1. *Let ℓ be a prime and $k > 0$. Then*

- $M^-(\prod\limits_{0\le i<k} (\ell^{\mathrm{rk}_\ell(C_D^2)} - \ell^i)) = 1$,
- $M^+(\prod\limits_{0\le i<k} (\ell^{\mathrm{rk}_\ell(C_D^2)} - \ell^i)) = \ell^{-k}$.

We remark that in the original conjecture of Cohen and Lenstra there was no squaring of the class group. This makes no difference for odd primes. The idea of Gerth was to consider the 4–rank instead of the 2–rank for $\ell = 2$ which can be done by squaring the class group. Let us write down the special case for $k = 1$ which was considered very often in literature.

Conjecture 2. *Let ℓ be a prime. Then*

- $M^-(\ell^{\mathrm{rk}_\ell(C_D^2)}) = 2$,
- $M^+(\ell^{\mathrm{rk}_\ell(C_D^2)}) = 1 + 1/\ell$.

A little bit surprising is the fact that the constant 2 in the imaginary quadratic case is independent of the prime ℓ, where in the real quadratic case we get a dependency. Let us remark that before our work there was only one proven case of Conjecture 1 for $\ell = 3$ and $k = 1$. This is the well known Davenport–Heilbronn theorem [2].

Another series of conjectures which can be found in [1, 6] concern the density of fundamental discriminants D such that $\mathrm{rk}_\ell(C_D^2) = r$ for a given integer $r \geq 0$.

Conjecture 3. *Let ℓ be a prime and $r \geq 0$. Then the density of fundamental discriminants D such that $\mathrm{rk}_\ell(C_D^2) = r$ is equal to*

- $\ell^{-r^2}\eta_\infty(\ell)\eta_r(\ell)^{-2}$ *for negative D's,*
- $\ell^{-r(r+1)}\eta_\infty(\ell)\eta_r(\ell)^{-1}\eta_{r+1}(\ell)$ *for positive D's,*

where we define

$$\eta_k(t) := \prod_{j=1}^{k}(1 - t^{-j}) \text{ for } k \in \mathbb{N} \text{ or } k = \infty.$$

Conjectures 1 and 3 have been made based on some heuristics which fit to a lot of computations done so far. Out of this heuristics these conjectures came out independently. In [3] we are able to prove that Conjecture 1 implies Conjecture 3 in the following sense.

Theorem 1. *Let ℓ be a prime and restrict to positive (negative) fundamental discriminants. Assume that Conjecture 1 is true for ℓ and for all $k > 0$. Then Conjecture 3 is true for ℓ and all $r \geq 0$.*

In order to prove this theorem it is nice to have the following reformulation of Conjecture 1 which is given in [4]. We denote by $\mathcal{N}(k, \ell)$ the number of $\mathbb{F}_\ell$–vector subspaces of $\mathbb{F}_\ell^k$.

Theorem 2. *Let ℓ be a prime and $m > 0$ be an integer. Then for negative discriminants the following statements are equivalent:*

(1) *For all $1 \leq k \leq m$:* $M^-(\prod_{0 \leq i < k}(\ell^{\mathrm{rk}_\ell(C_D^2)} - \ell^i)) = 1$.

(2) *For all $1 \leq k \leq m$:* $M^-(\ell^{k\mathrm{rk}_\ell(C_D^2)}) = \mathcal{N}(k, \ell)$.

Let ℓ be a prime and $m > 0$ be an integer. Then for positive discriminants the following statements are equivalent:

(1) *For all $1 \leq k \leq m$:* $M^+(\prod_{0 \leq i < k} (\ell^{\mathrm{rk}_\ell(C_D^2)} - \ell^i)) = \ell^{-k}$.

(2) *For all $1 \leq k \leq m$:* $M^+(\ell^{k\mathrm{rk}_\ell(C_D^2)}) = \ell^{-k}(\mathcal{N}(k+1,\ell) - \mathcal{N}(k,\ell))$.

The new version of Conjecture 1 is for $\ell = 2$ better suited for proofs. The following theorem is proved in [4].

Theorem 3. *Let $\ell = 2$. Then Conjectures 1 and 3 are true for all $k > 0$ and all $r \geq 0$.*

The main idea of the proof is to express the 4–part of the narrow class group by (norm-)symbols which lead to oscillating sums. In order to control those sums we apply techniques from analytic number theory like Siegel-Walfisz theorem and large sieve techniques introduced by Heath-Brown [7].

As an application we can consider the so-called negative Pell equation (NPE):

$$x^2 - Dy^2 = -1.$$

By looking modulo p it is easy to see that this equation is not solvable in $\mathbb{Z}^2$ if $D < 0$ or if a prime $p \equiv 3 \bmod 4$ divides D. Therefore it is natural to consider the subset of special discriminants:

$$\mathcal{D} := \{D > 0 : D \text{ fundamental}, p \mid D \Rightarrow p \equiv 1, 2 \mod 4\}.$$

Peter Stevenhagen formulates the following conjecture [8]:

Conjecture 4. *Let $\alpha := \prod_{j=1}^{\infty}(1 + 2^{-j})^{-1} = 0.419422\ldots$ Then*

$$\lim_{X \to \infty} \frac{\#\{D \in \mathcal{D} : D \leq X \text{ and the NPE is solvable for } D\}}{\#\{D \in \mathcal{D} : D \leq X\}} = 1 - \alpha = 0.580578\ldots$$

It is well known that for a special discriminant D the negative Pell equation is solvable if and only if $\mathrm{Cl}_D = C_D$, i.e. the two class groups coincide. We remark that for special discriminants the 2–ranks of the two class groups always coincide.

In [5] we formulate and prove similar statements as in Conjectures 1 and 3, where we now restrict to consider the averages and densities in the special set $\mathcal{D}$. In the special set $\mathcal{D}$ it makes a difference if we consider the ordinary or the narrow class group. We prove the above statements in both versions. Using the above mentioned results we can control the 4–ranks of those groups. We use the following well known statements:

(1) Let $D \in \mathcal{D}$ such that $\mathrm{rk}_4(C_D) = 0$. Then the negative Pell equation for D is solvable.

(2) Let $D \in \mathcal{D}$ such that $\mathrm{rk}_4(C_D) \neq \mathrm{rk}_4(\mathrm{Cl}_D)$. Then the negative Pell equation for D is not solvable.

Using this we are able to prove.

Theorem 4. *A positive density of $D \in \mathcal{D}$ have the property that the negative Pell equation is solvable. Furthermore a positive density of such D's have the property that the negative Pell equation is unsolvable.*

References

[1] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, In: Number theory, Noordwijkerhout 1983, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[2] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. London Ser. A, **322**, (1971),:405–420.

[3] É. Fouvry and J. Klüners, it Cohen–Lenstra heuristics of quadratic number fields, In : F. Hess, S. Pauli, and M. Pohst (ed.) ANTS Proceedings Berlin, LNCS **4076** (2006), 40–55.

[4] É. Fouvry and J. Klüners, *On the 4–rank of class groups of quadratic number fields*, Inv. Math. **167**, (2007), 455–513.

[5] É. Fouvry and J. Klüners, *On the negative Pell equation*, Preprint, 2007.

[6] F. Gerth, III, *Extension of conjectures of Cohen and Lenstra*, Exposition. Math. **5(2)**, (1987) 181–184.

[7] D.R. Heath–Brown, *A mean value estimate for real characters sums*, Acta. Arith. **72**, (1995) 235–275.

[8] P. Stevenhagen, *The number of real quadratic fields with units of negative norms*, Experiment. Math. **2**, (1993) 121–136.

The arithmetic π_1 and diophantine geometry

Stefan Wewers

(joint work with Tamás Szamuely)

1. The nonabelian Chabauty method

Let X be a smooth and absolutely irreducible algebraic curve, defined over $\mathbb{Q}$. Let g denote the genus of X and $r := |(\bar{X} - X)(\bar{\mathbb{Q}})|$ the number of 'points at infinity' (where $\bar{X}$ is the smooth projective model of X). Fix a rational point $x_0 \in X(\mathbb{Q})$. The *arithmetic* π_1 of X is a profinite group attached to the pointed $\mathbb{Q}$-scheme (X, x_0), sitting in the middle of a split short exact sequence, as follows:

$$1 \to \pi_1(X_{\bar{\mathbb{Q}}}, x_0) \to \pi_1(X, x_0) \to \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to 1. \tag{1}$$

While the group on the left (the *geometric* π_1) is determined, up to isomorphism, by the two invariants g and r alone, the whole sequence (1) encodes much more information on X itself. For instance, if X is projective hyperbolic (i.e. $r = 0$ and $g \geq 2$) then the *Section Conjecture* of Grothendieck predicts that the Kummer map

$$\kappa : X(\mathbb{Q}) \to H^1(\mathbb{Q}, \pi_1(X_{\bar{\mathbb{Q}}}, x_0)), \tag{2}$$

which sends a rational point $x \in X(\mathbb{Q})$ to the cohomology class measuring the difference between the two sections of (1) coming from x_0 and x, is a bijection.

At the moment, a proof of the Section Conjecture seems to be out of reach. Nevertheless, M. Kim ([4],[5]) has recently suggested an interesting new method (the *nonabelian Chabauty method*) to control the set of rational or integral points via the arithmetic π_1. Using this method, Kim has obtained the following results:

(a) Finiteness of integral points if $(g, r) = (0, 3)$ or if $(g, r) = (1, 1)$ (the latter is joint work with A. Tamagawa).

(b) Finiteness of rational points for $g \geq 2$, assuming certain conjectures on mixed motives, e.g. the Bloch-Kato Conjecture.

Note that (a) is a special case of the Siegel-Mahler-Lang theorem, while (b) is Faltings' theorem, restricted to the case of the base field $\mathbb{Q}$.

Here is a very brief sketch of the Chabauty method. For simplicity we only consider rational points (and hence assume $g \geq 2$ and $r = 0$). Fix a prime number p at which (X, x_0) has good reduction and an integer $n \geq 2$. We write $\pi_1(X_{\bar{\mathbb{Q}}}, x_0)^{(n)} \subset \pi_1(X_{\bar{\mathbb{Q}}}, x_0)$ for the nth step in the descending central series, and we set

$$\Pi^{\mathrm{et},n} := \big(\pi_1(X_{\bar{\mathbb{Q}}}, x_0)/\pi_1(X_{\bar{\mathbb{Q}}}, x_0)^{(n+1)}\big) \otimes \mathbb{Q}_p.$$

More precisely, $\Pi^{\mathrm{et},n}$ is the group of $\mathbb{Q}_p$-points of the unipotent completion of $\pi_1(X_{\bar{\mathbb{Q}}}, x_0)$ with index of unipotence $\leq n$. From the sequence (1) we deduce a continuous action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\Pi^{\mathrm{et},n}$. We also have a Kummer map

$$\kappa_n : X(\mathbb{Q}) \to H^1_f(\mathbb{Q}, \Pi^{\mathrm{et},n}). \tag{3}$$

Here the subset $H^1_f \subset H^1$ is defined by suitable local conditions. A crucial fact is that $H^1_f(\mathbb{Q}, \Pi^{\mathrm{et},n})$ has a natural structure of an affine variety over $\mathbb{Q}_p$. For $n = 2$ it is even a $\mathbb{Q}_p$-vector space and corresponds to the classical Selmer group. It is therefore appropriate to call $H^1_f(\mathbb{Q}, \Pi^{\mathrm{et},n})$ a *nonabelian Selmer variety*.

Unlike the map (2), κ_n cannot be expected to be a bijection. The fundamental insight of Kim is that for n large, the nonabelian Selmer variety should nevertheless give sufficient control over the set $X(\mathbb{Q})$ in order to show its finiteness.

Philosophically, the group $\Pi^{\mathrm{et},n}$, together with its natural Galois action, should be considered as the étale realization of $\Pi^{\mathrm{mot},n}$, the *motivic fundamental group* of X truncated at level n, see [3]. So far, $\Pi^{\mathrm{mot},n}$ has only been constructed for $g = 0$. However, independently of the existence of $\Pi^{\mathrm{mot},n}$, one can define its *de Rham realization* $\Pi^{\mathrm{dR},n}$. This is a unipotent algebraic group over $\mathbb{Q}_p$, equipped with a Hodge filtration (F^i). The analogue of the Kummer map (3) is the p-adic unipotent *Albanese map*

$$\alpha_n : X(\mathbb{Q}_p) \to \Pi^{\mathrm{dR},n}/F^0. \tag{4}$$

It can be defined by p-adic integration, so it is locally analytic.

Using p-adic Hodge theory (in particular, a comparison isomorphism between $\Pi^{\mathrm{et},n}$ and $\Pi^{\mathrm{dR},n}$), one constructs a map c_n making the following diagram commute:

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\subset} & X(\mathbb{Q}_p) \\ \big\downarrow{\scriptstyle \kappa_n} & & \big\downarrow{\scriptstyle \alpha_n} \\ H^1_f(\mathbb{Q}, \Pi^{\mathrm{et},n}) & \xrightarrow{c_n} & \Pi^{\mathrm{dR},n}/F^0. \end{array} \tag{5}$$

The map c_n is a morphism between affine algebraic varieties over $\mathbb{Q}_p$. Kim conjectures the following:

Conjecture 1 (Kim)**.** *For $n \gg 0$ we have $\dim H^1_f(\mathbb{Q}, \Pi^{\mathrm{et},n}) < \dim(\Pi^{\mathrm{dR},n}/F^0)$. In particular, the image of c_n is not Zariski dense.*

If the conjecture is true, then an easy argument essentially due to Chabauty [2] shows that $X(\mathbb{Q})$ is finite, proving Faltings' theorem in this case.

Conjecture 1 is proved in the case $g = 0$, $r \geq 3$ (see [4]), with modified local conditions defining $H^1_f \subset H^1$ in order to control integral points. In [6] it is shown how to modify these local conditions further in order to deal with the case $(g, r) = (1, 1)$. In [5] it is shown that certain natural conjectures on mixed motives imply Conjecture 1 in general.

2. Higher dimension

It would be very interesting to have an example where the nonabelian Chabauty method gives an unconditional proof of a new diophantine theorem. Since the basic finiteness theorems in dimension one (the theorems of Siegel and Faltings) are already known, it is natural to try this for varieties X of dimension at least two. Here the conjectures of Lang and Vojta predict a tight connection between diophantine finiteness and hyperbolicity, as in dimension one; however, there are only few general results.

Joint work with Tamás Szamuely aims at proving the following conjecture.

Conjecture 2. *Let $D \subset \mathbb{P}^2_{\mathbb{Q}}$ be a normal crossing divisor in the projective plane over $\mathbb{Q}$. Set $X := \mathbb{P}^2_{\mathbb{Q}} - D$ and choose an affine embedding $X \hookrightarrow \mathbb{A}^n_{\mathbb{Q}}$. Let S be a finite set of prime numbers. If the degree of D is at least four, then the set of S-integral points on X (with respect to the chosen embedding) is not Zariski dense.*

The condition on the divisor D given in the above conjecture implies that the surface X is of log-general type. Conjecture 2 is therefore a very special case of a conjecture of Vojta, see [7], IX, §4.

Conjecture 2 is known to be true if the divisor D has at least four irreducible components; see [1], §5.2, in particular Theorem 5.8, which is due to Levin and Autissier and builds on work of Corvaja and Zannier. The proof relies on the Subspace Theorem. It seems that the general case of Conjecture 2 (e.g. the case of an irreducible divisor D) is not easily accessible by this or any other method currently used in diophantine geometry.

We expect to be able to prove Conjecture 2, using an extension of Kim's method. The basic idea is this. We fix an S-integral point $x_0 \in X$ and consider the pencil of lines through x_0. All but finitely many of theses lines intersect D transversally in $d = \deg(D) \geq 4$ points. Hence we obtain a fibration of a Zariski open subset of X by affine rational curves each of which contains only finitely many integral points, by Siegel's theorem. So what we need is some sort of 'relative Siegel theorem'. Our main observation is that Kim's method can indeed be extended to such a relative situation. However, this extension is highly nontrivial.

Very likely, our argument will prove something more general, but it is too early to predict how far our method can be pushed. At the moment, it seems that the essential limitation of our method is the restriction to the ground field $K = \mathbb{Q}$ and to the case of affine rational varieties.

References

[1] Y.F. Bilu, *The many faces of the Subspace Theorem*, Séminaire Bourbaki, 59ème année, 2006-2007, no. 967.
[2] C. Chabauty, *Sur les points rationnels des courbes algébriques*, C.R.Acad. Sci. Paris **212** (1941), 882-885.
[3] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, in *Galois groups over* $\mathbb{Q}$, Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, 79–297.
[4] M. Kim, *The motivic fundamental group of the projective line minus three points and the theorem of Siegel*, Invent. Math. **161** (2005), 629 – 656.
[5] M. Kim, *The unipotent Albanese map and Selmer varieties for curves*, preprint `math.AG/0510441`.
[6] M. Kim, A. Tamagawa, *The l-component of the unipotent Albanese map*, preprint `math.NT/0611384`.
[7] S. Lang, *Survey of Diophantine Geometry*, Springer-Verlag, 1997.
[8] T. Szamuely, S. Wewers, *The nonablian Chabauty method in higher dimension*, in preparation.

A Hom-form of the pro-p birational anabelian conjecture

Scott Corry
(joint work with Florian Pop)

Grothendieck's philosophy of anabelian geometry [2] can be roughly stated as follows: for certain types of fields, k, there should be interesting categories, $\mathcal{C}$, of k-varieties such that the fundamental group functor, π_1, embeds $\mathcal{C}$ as a subcategory of the category of profinite groups with outer continuous G_k-homomorphisms. In other words, the k-varieties in $\mathcal{C}$ should be completely determined by their fundamental groups. Grothendieck termed such k-varieties "anabelian", indicating that their fundamental groups should be "far from" or "beyond" abelian.

The subject of this talk is the birational version of Grothendieck's philosophy, in which k-varieties are replaced by their function fields, and the fundamental group is the Galois group. Moreover, we fix a prime number p, and we assume that k is a sub-p-adic field (i.e. a subfield of a finitely generated field over $\mathbb{Q}_p$). In this context, S. Mochizuki proved the following form of the birational Grothendieck conjecture:

Theorem 1. ([3], Theorem 17.1) *Suppose that $K|k$ and $L|k$ are finitely generated field extensions in which k is relatively algebraically closed (i.e. regular function fields). Then the Galois group functor yields a canonical bijection*

$$\mathrm{Hom}_k(K,L) \to \mathrm{Out}^{\mathrm{open}}_{G_k}(G_L, G_K),$$

where the right hand side denotes open outer G_k-homomorphisms of profinite groups.

In fact, Mochizuki derives this result as a corollary to a much stronger result in the pro-p setting. In order to describe the pro-p setting, we need a little group theory. If $K|k$ is a regular function field, then we have the canonical exact sequence

$$1 \to G_{K\overline{k}} \to G_K \to G_k \to 1.$$

Let N denote the kernel of the projection onto the maximal pro-p quotient $G_{K\overline{k}} \to G_{K\overline{k}}^{(p)}$. Then N is a characteristic subgroup of the geometric Galois group $G_{K\overline{k}}$, hence is normal in G_K. Define $\Pi_K := G_K/N$, which fits into the exact sequence

$$1 \to G_{K\overline{k}}^{(p)} \to \Pi_K \to G_k \to 1,$$

and hence is called the "Galois by pro-p" fundamental group of $K|k$. Then Mochizuki's birational result in this pro-p setting is the

Theorem 2. ([3], Theorem 16.5, birational version) *Suppose that $K|k$ and $L|k$ are regular function fields with* $\mathrm{trdeg}(K|k)$*=1. Then the Galois by pro-p fundamental group functor,* Π*, yields a canonical bijection*

$$\mathrm{Hom}_k(K, L) \to \mathrm{Out}_{G_k}^{\mathrm{open}}(\Pi_L, \Pi_K).$$

Mochizuki obtains Theorem 1 from Theorem 2 by induction on the transcendence degree of $K|k$. But this inductive procedure is ill-suited to the pro-p situation, and hence he obtains only a profinite result, which is weaker than the corresponding pro-p assertion. The aim of this talk is to describe a proof of the following pro-p version of Theorem 1. Our proof is not inductive in nature, but rather makes repeated use of Theorem 2 together with ideas involving Kummer Theory and Projective Geometry coming from [4].

Theorem 3. ([1], Theorem 1) *Suppose that $K|k$ and $L|k$ are regular function fields over the sub-p-adic field k. Then the Galois by pro-p fundamental group functor yields a canonical bijection*

$$\mathrm{Hom}_k(K, L) \to \mathrm{Out}_{G_k}^{\mathrm{open}}(\Pi_L, \Pi_K).$$

References

[1] S. Corry, F. Pop, *A Hom-form of the pro-p birational anabelian conjecture*, preprint, arXiv:math.AG/0610268

[2] A. Grothendieck, *letter to G. Faltings* (June 1983), in: P. Lochak, L. Schneps, *Geometric Galois Actions; 1. Around Grothendieck's Esquisse d'un Programme*, London Math. Soc. Lect. Note Ser. **242**, Cambridge Univ. Press (1997).

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

[4] F. Pop, *The birational anabelian conjecture – revisited*, unpublished manuscript, available at www.math.upenn.edu/∼pop

Schanuel's conjecture over function fields and differential Galois theory

Daniel Bertrand
(joint work with Anand Pillay)

In this joint work with Anand Pillay, we study extensions of Ax's work on Schanuel's conjecture to non-constant algebraic groups. Differential Galois theories can be used in the two extreme cases corresponding to Grothendieck's conjecture on logarithms (i.e. generalized periods), and to the Lindemann-Weierstrass theorem on exponentials.

1. Schanuel's conjecture.

Let K be the algebraic closure of a function field in one variable over $\mathbb{C}$, let ∂ be a non-trivial derivation on K and let $\hat{K}$ be a differential closure of K. Consider a commutative algebraic group $\mathcal{G}$ defined over $\mathbb{C}$, and let $L\mathcal{G}$ be its Lie-algebra. The vector space $L\mathcal{G} \otimes_{\mathbb{C}} K$ carries a canonical connection $\partial_{L\mathcal{G}}$, with $(L\mathcal{G})^{\partial} = L\mathcal{G}(\mathbb{C})$ as space of horizontal vectors over $\hat{K}$. Similarly, following Kolchin, $\mathcal{G}$ admits a canonical logarithmic derivative $\partial\ell n_{\mathcal{G}}$ with values in $L\mathcal{G}$, with $\mathcal{G}^{\partial} = \mathcal{G}(\mathbb{C})$ as kernel over $\hat{K}$. For a $\hat{K}$-rational point $(x, y) \in L\mathcal{G} \times \mathcal{G}$, a way (up to constants, and in particular, periods) of expressing that $y = exp_{\mathcal{G}}(x)$ is the exponential of x, or that $x = log_{\mathcal{G}}(y)$ is a logarithm of y, consists in requiring that (x, y) satisfy the differential relation

$$\partial\ell n_{\mathcal{G}}(y) = \partial_{L\mathcal{G}}(x). \qquad (*)$$

We may then consider the field of definition $K(x, y)$ of (x, y) over K, whose transcendence degree satisfies:

Theorem 1. (Ax [2]) *Let $\mathcal{G}$ be an algebraic group over $\mathbb{C}$, admitting no non-trivial morphism to a vectorial group (cf.* [3]*). Let $(x, y) \in (L\mathcal{G} \times \mathcal{G})(\hat{K})$ satisfy $(*)$, and suppose that no proper algebraic subgroup H of $\mathcal{G}$ over $\mathbb{C}$ satisfies: $x \in LH(\hat{K}) + (L\mathcal{G})^{\partial}$ (or, equivalently: $y \in H(\hat{K}) + \mathcal{G}^{\partial}$). Then,* $\mathrm{trdeg}(K(x, y)/K) \geq \dim(\mathcal{G})$.

In general, neither $K(x, y)$ nor $\mathbb{C}(x, y)$, which Ax actually studies, are differential subfields of $\hat{K}$ - and not suprisingly, no Galois group enters the proof. In fact, this result concerns the leaves of the foliation $d\ell n_{\mathcal{G}} y - d_{L\mathcal{G}} x = 0$, and is likely to pertain to Malgrange's Galois theory, where the ambiant variety $L\mathcal{G} \times \mathcal{G}$ is viewed over $Spec(\mathbb{C})$, with no choice of an intermediate base (i.e. no choice of distinguished variables). On the other hand, Theorem 1 is equivalent to a group theoretic statement in

i) the "logarithmic" case where $y \in \mathcal{G}(K)$: then, $Aut_{\partial}(K(x)/K) \simeq (L\mathcal{G})^{\partial}$;
ii) the "exponential" case where $x \in L\mathcal{G}(K)$: then $Aut_{\partial}(K(y)/K) \simeq \mathcal{G}^{\partial}$.

These are the statements we now try to extend to non-isoconstant algebraic groups, using Picard-Vessiot theory for the first one, and Pillay's theory [6] for the second one.

2. General setting and the logarithmic case.

Let $\mathcal{G}/K$ be an algebraic D-group in the sense of Buium [5], i.e. equipped with an extension to $\mathcal{O}_\mathcal{G}$ of the derivation ∂ respecting the group structure. Denoting Lie algebras (now over K) by L, we write $\partial\ell n_\mathcal{G} : \mathcal{G} \to L\mathcal{G}$ for the corresponding logarithmic derivative on $\mathcal{G}$, in the sense of [6]. Its kernel $\mathcal{G}^\sharp$ is a differential algebraic group over K, and we denote by $\mathcal{G}^\partial := \mathcal{G}^\sharp(\hat{K})$ the group of its $\hat{K}$-points. The differential at the origin of $\partial\ell n_\mathcal{G}$ provides the K-vector space $L\mathcal{G}$ with a canonical connection $\partial_{L\mathcal{G}} : L\mathcal{G} \to L\mathcal{G}$, which may also be viewed as the logarithmic derivative of an algebraic D-group structure on the vectorial group $L\mathcal{G}/K$; in particular, $(L\mathcal{G})^\sharp(\hat{K}) := (L\mathcal{G})^\partial$ is the $\mathbb{C}$-vector space of horizontal vectors of $\partial_{L\mathcal{G}}$. The differential relation $(*)$ still makes sense in this general setting.

Let now G be a semi-abelian variety defined over K, and let A, T be its abelian and toric parts. Its universal vectorial extension $\tilde{G}$ - an extension of G by the vectorial group W dual to $H^1(A, O_A)$ - admits a canonical structure of algebraic D-group over K, to which the above setting applies. Furthermore, the connection $\partial_{L\tilde{G}}$ on $L\tilde{G}$ is the dual of the Gauss-Manin connection on $H^1_{dR}(G/K)$ (the latter one is an extension, in the category of ∂-modules over K, of the direct sum of $\dim(T)$ copies of the trivial connection $\mathbf{1} = (K, \partial)$ by the standard Gauss-Manin connection on $H^1_{dR}(A/K)$).

Assume now that G is a split extension $T \times A$. Then, the ∂-module $L\tilde{G}$ is semi-simple. Let $Ext_{\partial-mod./K}(\mathbf{1}, L\tilde{G}) \simeq L\tilde{G}(K)/\partial_{L\tilde{G}}(L\tilde{G}(K))$ be the $\mathbb{C}$-vector space of extensions of $\mathbf{1}$ by the ∂-module $L\tilde{G}$. Following Manin, we define a map $M : G(K) \to Ext_{\partial-mod./K}(\mathbf{1}, L\tilde{G})$ by attaching to a point $\overline{y} \in G(K)$ the class $M(\overline{y})$ of the extension defined by the inhomogeneous linear differential equation

$$\partial_{L\tilde{G}}(x) = b, \text{ with } b = \partial\ell n_{\tilde{G}}(y) \in L\tilde{G}(K)$$

where y is any lift to $\tilde{G}(K)$ of $\overline{y}$; this is well defined, because $\partial\ell n_{\tilde{G}}$ and $\partial_{L\tilde{G}}$ coincide on $W \simeq LW$. Furthermore, by Manin's kernel theorem, $M(\overline{y}) = 0$ (i.e. the extension splits over K, i.e. the equation above admits a K-rational solution x) if and only if some non-zero multiple of $\overline{y}$ lies in $G_0(\mathbb{C})$, where $G_0 = T \times Tr_{K/\mathbb{C}}A$ (i.e., for G's of such shape, $\overline{y}$ lifts to a point $y \in \tilde{G}^\sharp(K)$). This implies:

Theorem 2. (André [1]) *Assume that $G = T \times A$, and set $\mathcal{G} = \tilde{G}$ and let $K_{L\mathcal{G}}$ be the field of definition of $(L\mathcal{G})^\partial$. Let $(x, y) \in (L\mathcal{G} \times \mathcal{G})(\hat{K})$ satisfy $(*)$. Suppose that $y \in \mathcal{G}(K)$ and that no proper algebraic subgroup H of $\mathcal{G}$ over K satisfies: $y \in H(K) + \mathcal{G}^\sharp(K)$. Then, $Aut_\partial(K_{L\mathcal{G}}(x)/K_{L\mathcal{G}}) \simeq (L\mathcal{G})^\partial$.*

The result does not extend to general semi-abelian varieties, mainly because the Picard-Vessiot group of the ∂-module $L\tilde{G}$ then ceases to be reductive. See [3] for the case of semi-abelian surfaces.

3. The Lindemann-Weierstrass theorem.

Let $\mathcal{G}$ be an algebraic D-group over K. We now assume that x is a K-rational point in $L\mathcal{G}$, and study the differential equation

$$\partial\ell n_{\mathcal{G}}(y) = a, \text{ with } a = \partial_{L\mathcal{G}}(x) \in L\mathcal{G}(K).$$

Assume that $\mathcal{G}$ is K-large in the sense of [6], i.e. that $\mathcal{G}^\sharp(\hat{K}) = \mathcal{G}^\sharp(K)$ (this occurs, for instance, when $\mathcal{G}$ is defined over $\mathbb{C}$, or when $\mathcal{G}$ is the universal extension of an abelian variety with maximal Kodaira-Spencer rank). Then, the field $K(y)$ generated by any solution $y \in \mathcal{G}(\hat{K})$ depends only on a, and Pillay's theory attaches to the equation its "Galois group" : an algebraic D-subgroup $\mathcal{H}$ of $\mathcal{G}$, defined over K, with the property that $Aut_\partial(K(y)/K) \simeq \mathcal{H}^\partial$, and with a Galois correspondence. We then have:

Theorem 3. (see [4]) *Let G/K be a semi-abelian variety, let $\tilde{G}$ be the algebraic D-group attached to its universal vectorial extension, and let U be a vectorial D-subgroup of $\tilde{G}$, defined over K. Assume that the algebraic D-group $\mathcal{G} = \tilde{G}/U$ is K-large. Let $(x, y) \in (L\mathcal{G} \times \mathcal{G})(\hat{K})$ satisfy $(*)$. Suppose that $x \in L\mathcal{G}(K)$ and that no proper algebraic subgroup H of $\mathcal{G}$ over K satisfies: $x \in LH(K) + (L\mathcal{G})^\sharp(K)$. Then, $Aut_\partial(K(y)/K) \simeq \mathcal{G}^\partial$.*

Proof. Suppose the Galois group $\mathcal{H}$ of the equation does not fill up $\mathcal{G}$. As in the proof of Kolchin's classical theorem, we then get a similar equation on the quotient $\mathcal{G}/\mathcal{H}$ with trivial Galois group, i.e. with a K-rational solution $y \bmod(\mathcal{H})$. The hypothesis on x can be shown to descend to the quotient, and the resulting relation contradicts Theorem 2. □

In fact, the hypothesis of K-largeness on $\mathcal{G}$ can be somewhat relaxed, using arguments from the differential algebraic proof of the geometric Mordell-Lang theorem (see Anand's talk at the Leeds meeting next month).

References

[1] Y. André, *Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part*, Compo. Math., 82, 1992, 1-24.

[2] J. Ax, *Some topics in differential algebraic geometry I : analytic subgroups of algebraic groups*, Amer. J. Maths, 94, 1972, 1195-1204.

[3] D. Bertrand, *Schanuel's conjecture for non-isoconstant elliptic curves over function fields*, Model Theory and Appl., Cambridge UP, to appear.

[4] D. Bertrand, A. Pillay, *Lindemann-Weierstrass for semi-abelian varieties over function fields*, in preparation.

[5] A. Buium, *Differential algebraic groups of finite dimension*, Springer LN 1506, 1992.

[6] A. Pillay. *Algebraic D-groups and differential Galois theory*, Pacific J. Maths, 216, 2004, 343-360.

Patching over fields

David Harbater[1]
(joint work with Julia Hartmann)

1. Background.

Patching is a method that has been used to prove results in Galois theory, e.g. concerning the inverse Galois problem for function fields of curves, solutions to embedding problems, and the structure of absolute Galois groups. There are several versions of patching that have appeared in the literature, which go by the names "formal", "rigid" and "algebraic" patching. (For example, see [Ha2], [Ra], [Po], [HV]; and see [Ha3] for an overview.) Here we present another version of patching that is more elementary than formal or rigid patching, and is more general than algebraic patching. It also can be applied to other situations that require working over fields rather than over rings, e.g. differential Galois theory and division algebras.

In patching, one begins with a space $X = U_1 \cup U_2$, with $U_0 = U_1 \cap U_2$, and we want to build a "structure" over X (e.g. a sheaf of modules, or a Galois branched cover) by doing so over the U_i's compatibly. For example if these are schemes, with the U_i's being Zariski open subsets, this is the usual way of constructing sheaves of modules. Unfortunately, this approach does not help in constructing branched covers via the Zariski topology, since giving such a cover over a Zariski open dense subset is already equivalent to giving it globally. Instead, to apply patching to Galois theory, one uses "smaller open sets", as in the formal, rigid or algebraic contexts. This is done over a complete field K, e.g. $K = k((t))$, where the small open sets roughly correspond to neighborhoods in the t-adic topology. This parallels the use of metric discs when patching analytically over the complex numbers. Analytically, one cites Riemann's Existence Theorem (e.g. see [Ha3, Theorem 2.1.1]) or GAGA [Se] to conclude that the analytic object that has been constructed is in fact algebraic. In the other forms of patching, one uses analogs of GAGA, e.g. Grothendieck's Existence Theorem [Gr, Cor. 5.1.6] (which is a "formal GAGA"), or analogs of underlying results such as Cartan's Lemma [Ca].

In formal patching, one uses rings like $k[x][[t]]$, corresponding to a "formal thickening" of the affine x-line. In rigid patching, one uses the same rings with t inverted; these are then viewed as rings of power series in x converging on a closed t-adic disc. The same rings are used in algebraic patching, though without reliance on the machinery of formal schemes or rigid analytic spaces. In the version of patching presented here, we instead use the fraction fields of these rings. This will make the method more amenable to being applied, in particular, to differential Galois theory, where taking derivatives of functions like $x^{1/2}$ or $\log x$ introduces denominators.

[1]Supported in part by NSF Grant DMS-0500118.

2. Main result.

We consider the following situation: X is a smooth projective curve over a field k and $\hat{X} = X \times_k k[[t]]$; we regard X as the closed fibre of $\hat{X}$. Let U_1, U_2 be Zariski affine open subsets of the closed fibre such that $X = U_1 \cup U_2$; let $U_0 = U_1 \cap U_2$; $U_i = \operatorname{Spec} R_i$; $\hat{R}_i = R_i[[t]]$; $F_i = \operatorname{frac} \hat{R}_i$; and let F be the function field of $\hat{X}$. Our result asserts that every patching problem for the F_i's has a unique solution over $\hat{X}$. More precisely,

Theorem 1 (Main Theorem)**.** *In the above situation, given finite dimensional F_i-vector spaces V_i (for $i = 1, 2$) and an isomorphism $\phi : V_1 \otimes_{F_1} F_0 \to V_2 \otimes_{F_2} F_0$, there exists a finite dimensional F-vector space V together with isomorphisms $\alpha_i : V \otimes_F F_i \to V_i$ that are compatible with ϕ. Moreover this choice is unique up to isomorphism; and V is the intersection of V_1 and V_2 with respect to the identifications given by the above isomorphisms.*

This result can also be rephrased as an equivalence of categories,

$$\operatorname{Vect}(F) \to \operatorname{Vect}(F_1) \times_{\operatorname{Vect}(F_0)} \operatorname{Vect}(F_2)$$

given by base change, whose inverse image is given by the fibre product of modules. Here Vect denotes the category of finite dimensional vector spaces over a given field.

In fact, we can state and prove a version of this result for more general complete discrete valuation rings than $k[[t]]$, but we state just this case here for simplicity. Also, the U_i's can be more general than stated above.

The equivalence of categories in the above theorem provides us with analogous results for algebras, covers, etc. It can therefore be used in applications such as the realization of arbitrary finite groups as Galois groups over function fields over an algebraically closed field.

3. Proof of the Main Theorem.

By Proposition 2.1 of [Ha1], it suffices to verify the following two conditions:

(i) $F = F_1 \cap F_2$;
(ii) For every element $D_0 \in \mathrm{GL}_n(F_0)$ there exist $D_i \in \mathrm{GL}_n(F_i)$ for $i = 1, 2$ such that $D_0 = D_1 D_2$.

In order to verify these conditions, we prove the following key result:

Proposition 2. *In the situation of the Main Theorem, if $D \in M_n(\hat{R}_0)$ has non-zero determinant, then there exist $B \in M_n(\hat{R}_1 R_2)$ and $C \in \mathrm{GL}_n(\hat{R}_2)$ such that $D = BC$.*

Here $\hat{R}_1 R_2$ denotes the compositum of $\hat{R}_1$ and R_2 in $\hat{R}_0$.

Sketch of Proof. It suffices to construct sequences of matrices $B_i \in M_n(R_0[t])$, $C_i \in M_n(R_2[t])$ such that $D \equiv B_i C_i \pmod{t^{i+1}}$, $B_i \equiv B_{i-1} \pmod{t^i}$, $C_i \equiv C_{i-1} \pmod{t^i}$, $C_0 \equiv I \pmod{t}$, and the coefficients of the entries of the matrices B_i have uniformly bounded poles at the points of $U_1 - U_0$. This can be done inductively using the Strong Approximation Theorem [FJ, Prop. 3.3.1] (or the

Riemann-Roch Theorem) to find the coefficients of successive powers of t with these bounds on the poles. □

This proposition yields the following matrix version of the Weierstrass Preparation Theorem:

Theorem 3. *With notation as above, if $U = \operatorname{Spec} R \subset X$ is an affine open set, and $\hat{R} = R[[t]]$, then every $D \in M_n(\hat{R})$ with non-zero determinant can be written as $D = BC$ with $B \in \mathrm{GL}_n(F)$ and $C \in \mathrm{GL}_n(\hat{R})$.*

Namely, write $X = U_1 \cup U_2$ where $U_2 = U$, and apply the proposition above. Using this theorem we obtain condition (ii) above, by choosing a non-zero $h \in \hat{R}_0$ such that $hD_0 \in M_n(\hat{R}_0)$ and then applying the theorem to D_0 and (in the 1×1 case) to h. We also obtain condition (i) above, writing $f \in F_1 \cap F_2$ as a_i/b_i with $a_i, b_i \in \hat{R}_i$ (for $i = 1, 2$) and then applying the 1×1 case of the above theorem to b_1 and b_2. As a result, we obtain our Main Theorem.

References

[Ca] H. Cartan, *Sur les matrices holomorphes de n variables complexes*, Journal de Mathématiques pures et appliquées, Series 9, **19** (1940), 1-26.

[FJ] M. Fried, M. Jarden, *Field arithmetic*, second edition. Ergebnisse Math. series, vol. 11, Springer-Verlag, 2005.

[Gr] A. Grothendieck. *Élements de géométrie algébrique (EGA) III*, Publ. Math. IHES, 1^e partie, vol. 11 (1961).

[HV] D. Haran, H. Völklein, *Galois groups over complete valued fields*, Israel J. Math. **93** (1996), 9-27.

[Ha1] D. Harbater, *Convergent arithmetic power series*, Amer. J. Math., **106** (1984), 801-846.

[Ha2] D. Harbater, *Galois coverings of the arithmetic line*; in *Number Theory: New York, 1984-85*. Springer LNM, vol. 1240 (1987), pp. 165-195.

[Ha3] D. Harbater, *Patching and Galois theory*, In *Galois Groups and Fundamental Groups* (L. Schneps, ed.), MSRI Publications series, vol. 41, Cambridge University Press, 2003, pp. 313-424.

[Po] F. Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), 1-34.

[Ra] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar*, Invent. Math. **116** (1994), 425-462.

[Se] J.-P. Serre, *Géométrie algébrique et géométrie analytique*, Annales de L'Institut Fourier **6** (1956), 1-42.

Differential Galois Groups and Patching

Julia Hartmann
(joint work with David Harbater)

1. Introduction

Differential Galois theory is the algebraic theory of (linear, homogeneous) differential equations. These equations are given over some differential field F (i.e., a field equipped with a derivation) in the form of differential modules: A differential module M over F is a finite dimensional vector space over F together with an additive map $\partial : M \to M$ that satisfies the Leibnitz rule $\partial(fm) = \partial(f)m + f\partial(m)$ for $f \in F$ and $m \in M$.
A Picard-Vessiot extension E/F for M is a minimal differential field extension such that $M \otimes_F E$ has a full set of solutions, i.e., so that there exist n elements in $M \otimes_F E$ that map to zero under ∂ and are F-linearly independent. The differential Galois group is the group of all differential automorphisms of E which fix F and carries the structure of a linear algebraic group over the field of constants K of F (we refer the reader to [PS03] for details).
In analogy with classical Galois theory, the *inverse problem* is the question which linear algebraic groups $\mathcal{G}$ occur as differential Galois groups. The answer to this question depends on $\mathcal{G}$ and F. Over algebraic function fields, one generally expects all linear algebraic groups to occur. In the case of $\mathbb{C}(x)$, this was shown to be true by Tretkoff and Tretkoff in [TT79]; when C is an arbitrary algebraically closed field, there are results of Singer for certain classes of groups ([Sin93]), the cases of connected and solvable-by-finite groups were treated by Mitschi and Singer ([MS96], [MS02], and the case of arbitrary groups over $C(x)$ was solved in [Hart05]. These results translate to algebraic function fields over C ([MS96], [Obe03]). For function fields with nonalgebraically closed field of constants, not much is known (see, however, [Dyc07] for the case of $\mathbb{R}$).
The aim of this talk is to present an application of patching over fields ([Harb07]) to inverse differential Galois theory.

2. Patching of differential modules

Let k be a field of characteristic zero and let $\mathcal{X}/k$ be a smooth projective curve. Consider affine open subsets $U_1, U_2 \subseteq \mathcal{X}$ which cover $\mathcal{X}$ and let U_0 be their intersection. Define rings R_i so that $\mathrm{Spec}(R_i) = U_i$, and set $\hat{R}_i := R_i[[t]]$. Let $F_i = \mathrm{Quot}(\hat{R}_i)$ be their fraction fields, and let F be the function field of $\mathcal{X} \times_k k[[t]]$. Fix a variable $x \in k(\mathcal{X})$ and equip all F_i and F with the derivation $\frac{d}{dx}$. Note that $K := k((t))$ is the common field of constants of F and all F_i.

Theorem 1. *Let M_1 and M_2 be differential modules over F_1, F_2, and let*

$$\phi : M_1 \otimes_{F_1} F_0 \to M_2 \otimes_{F_2} F_0$$

be a differential isomorphism. Then

(1) *There exists a differential module M over F for which $M \otimes_F F_i \cong M_i$ compatibly with ϕ.*
(2) *Suppose that E_i is a Picard-Vessiot extension for M_i, and let $\mathcal{G}_i \leq \mathrm{GL}_{n,K}$ be its differential Galois group ($n = \dim_{F_i}(M_i)$). Then there exists a Picard-Vessiot extension for M and its differential Galois group is $\langle \mathcal{G}_1, \mathcal{G}_2 \rangle \leq \mathrm{GL}_{n,K}$.*

Sketch of Proof. The existence of M as a vector space is given by Theorem 1 in [Harb07]. In fact, M is the intersection of M_2 and $\phi(M_1)$ in $M_2 \otimes_{F_2} F_0$, and thus becomes a differential module by restricting the derivations (which agree on M since ϕ is a differential isomorphism). To prove the second claim, we use the construction of a Picard-Vessiot extension as the fraction field of a quotient of the coordinate ring of GL_n by a maximal differential ideal. We first show that the maximal differential ideals in $F_i[\mathrm{GL}_n]$ defining E_i restrict to a maximal differential ideal in $F[\mathrm{GL}_n]$ that defines a Picard-Vessiot extension (i.e., there are no new constants in the quotient). The characterization of differential Galois groups as stabilizers of maximal differential ideals is then used to finish the proof. □

Theorem 1 allows the construction of differential Galois groups from a set of generating subgroups. We call the differential modules corresponding to such subgroups *building blocks*.

3. Realization of K-split groups

Definition 1. *Let $\mathcal{G}$ be a linear algebraic group over K. We say that $\mathcal{G}$ is K-split, if $\mathcal{G}$ is generated (as a K-group) by a finite number of copies of $\mathbb{G}_m$, $\mathbb{G}_a$, and finite cyclic groups.*

Note that if K is algebraically closed, every linear algebraic group is K-split.
In order to realize K-split groups as differential Galois groups, we provide building blocks corresponding to $\mathbb{G}_m$, $\mathbb{G}_a$, and finite cyclic groups. These are constructed as differential modules over F which have the required group over F_1 (for some open U_1) and have trivial differential Galois group over F_2 (for some open U_2 with $U_1 \cup U_2 = \mathcal{X}$), to ensure the existence of the differential isomorphisms required for patching. As an example, consider the case of $\mathbb{G}_a$ and assume $\mathcal{X} = \mathbb{P}^1$ is the projective x-line, $U_1 = \mathbb{P}^1 \setminus \{\infty\}$, $U_2 = \mathbb{P}^1 \setminus \{0\}$. Consider the formal power series $f = \sum_{r=0}^{\infty} \frac{t^r x^{-r}}{r} \in k[x^{-1}][[t]] \subseteq F_2$. Then $\frac{df}{dx} \in F$, and so f is a solution to a differential equation over F. Moreover, a calculation involving the Hilbert matrix shows that $f \notin \mathrm{Quot}(k[[x,t]])$ and hence $f \notin F_1$. Since the additive group has no proper nontrivial closed subgroups, we conclude that the differential equation has differential Galois group $\mathbb{G}_a$ over F_1, but has trivial differential Galois group over F_2 (since $f \in F_2$).

With notation as above, we obtain the following theorem:

Theorem 2. *Every K-split linear algebraic group over K is a differential Galois group over F.*

4. From K to k?

It is possible to recover the solution to the inverse problem over $k(x)$ for k algebraically closed from our results. Let $\mathcal{G}$ be a linear algebraic group over k. Then as noted above, $\mathcal{G}$ is k-split and hence K-split, so by Theorem 2, $\mathcal{G}$ is a differential Galois group over $K(x) = k((t))(x)$. By construction, the differential equation realizing $\mathcal{G}$ is already defined over a finitely generated $\bar{\mathbb{Q}}$-algebra $R \subseteq \bar{\mathbb{Q}}[[t]]$. A result of Hrushovski [Hru02] then allows to specialize these parameters to obtain a differential equation over $\bar{\mathbb{Q}}(x)$, while preserving the differential Galois group. Hence, $\mathcal{G}$ is a differential Galois group over $k(x)$.
Although the good points for Hrushovski's specialization do not form a Zariski open set, we expect that the condition on k that makes the specialization possible can be weakened from algebraically closed to large (cf. [Harb03], Thm 3.3.6).

5. Final Remarks

We would like to point out that the results mentioned here are only a small subset of the expected applications of patching to differential Galois theory. First, the case of nonsplit groups can be dealt with using descent techniques (work in progress). The new methods also apply to embedding problems. Moreover, as the field patching itself works over fields of arbitrary characteristic, the differential patching should also be applicable to the iterative differential modules in characteristic $p > 0$ (as defined in [MP03]).

References

[Dyc07] T. Dyckerhoff, *The inverse problem of differential Galois theory over the field $\mathbb{R}(z)$*, this volume.

[Harb03] D. Harbater, *Patching and Galois Theory*, In: Galois groups and fundamental groups, Math. Sci. Res. Inst. Publ., **41**, Cambridge Univ. Press, Cambridge, 2003, 313–424.

[Harb07] D. Harbater, *Patching over fields*, this volume.

[Hart05] J. Hartmann, *On the inverse problem in differential Galois theory*, J. reine angew. Math. **586** (2005), 21–44.

[Hru02] E. Hrushovski, *Computing the Galois group of a linear differential equation*, in: Differential Galois Theory, Banach Center Publications, Volume **58** (2002), 97–138.

[MP03] B.H. Matzat, M. van der Put, *Iterative differential equations and the Abhyankar conjecture*, J. Reine Angew. Math. **557** (2003), 1–52.

[MS96] C. Mitschi, M. Singer, *Connected groups as differential Galois groups*, J. Algebra **184** (1996), 333–361.

[MS02] C. Mitschi, M. Singer, *Solvable by finite groups as differential Galois groups*, Ann. Fac. Sci. Toulouse Math. **6** 11/3 (2002), 403–423.

[Obe03] T. Oberlies, *Einbettungsprobleme in der Differentialgaloistheorie*, Dissertation, Heidelberg 2003 (http://www.ub.uni-heidelberg.de/archiv/4550).

[PS03] M. van der Put, M. Singer, *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 328. Springer-Verlag, Berlin, 2003.

[Sin93] M. Singer, *Moduli of linear differential equations on the Riemann sphere with fixed Galois groups*, Pac. J. Math. **106** (1993), 343–395.

[TT79] C. Tretkoff, M. Tretkoff, *Solution of the inverse problem of differential Galois theory in the classical case*, Am. J. Math. **101** (1979), 1327–1332.

Grothendieck-Teichmüller group and a family of Mordell elliptic curves

Hiroaki Nakamura

(joint work with Hiroshi Tsunogai, Seidai Yasuda)

Due to Belyi's fundamental theorem, the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ can be embedded into $\mathrm{Aut}(\hat{F}_2)$, with $\hat{F}_2$ regarded as $\pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0,1,\infty\}, \vec{01})$ – the free profinite group $\langle x, y, z \mid xyz = 1\rangle$ (x, y, z : loops around $0, 1, \infty$). The elements $\sigma \in G_{\mathbb{Q}}$ are parametrized by pairs $(\lambda_\sigma, f_\sigma) \in \hat{\mathbb{Z}}^\times \times \hat{F}_2'$, where $\lambda : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$ is the cyclotomic character and f_σ is a uniquely determined element (for each σ) in the commutator subgroup $\hat{F}_2'$ of $\hat{F}_2$ so that $\sigma \in G_{\mathbb{Q}}$ acts as $\sigma(x) = x^{\lambda_\sigma}$, $\sigma(y) = f_\sigma^{-1} y^{\lambda_\sigma} f_\sigma$. Studies of behaviors of the mysterious parameter f_σ on $G_{\mathbb{Q}}$ lead to various versions of the Grothendieck-Teichmüller group $\widehat{GT} \subset \mathrm{Aut}(\hat{F}_2)$ defined by a finite number of functional equations in (λ, f) found satisfied by elements of $G_{\mathbb{Q}}$ (Drinfeld, Ihara, others).

As a first step toward Galois-Teichmüller lego structures through "special loci" *inside* the moduli spaces of curves, Lochak-Schneps and Serre (cf. [LS]) introduced certain accessory parameters g and $h : \widehat{GT} \to \hat{F}_2$ so as to decompose (uniquely) the main parameter $f : \widehat{GT} \to \hat{F}_2$ as follows ($\sharp$):

$$f(x,y) = g(y,x)^{-1} g(x,y) = \begin{cases} y^{-\frac{\lambda-1}{2}} h(y,z)^{-1} h(x,y) & (\lambda \equiv 1 \mod 6), \\ y^{-\frac{\lambda-1}{2}} h(y,z)^{-1} y^{-1} h(x,y) & (\lambda \equiv -1 \mod 6), \end{cases}$$

where $z = (xy)^{-1} \in \hat{F}_2$. On the other hand, we showed in [NT-I] that the parameters g and h can actually be directly written by (λ, f) on the image of $G_{\mathbb{Q}}$ in $\widehat{GT}$, and presented several new-type equations satisfied by the Galois image.

Our motivating problem in this talk concerns with the matrix specialization of these parameters f, g, h, when $x, y \in \hat{F}_2$ are specialized to free generator matrices of the level 2 modular group $\Gamma(2) \subset \mathrm{SL}_2(\mathbb{Z})$. Noting that the profinite completion $\widehat{\mathrm{SL}_2(\mathbb{Z})}$ has still a big kernel to $\mathrm{SL}_2(\hat{\mathbb{Z}})$, we consider specializations in the latter group as a first stage investigation. In [N-I] Corollary 4.13, one explicitly computes the matrix $f_\sigma\left(\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\-2&1\end{smallmatrix}\right)\right) \in \mathrm{SL}_2(\hat{\mathbb{Z}})$, which turned out later in [NS] Remark 2.7 to be decomposed as the following "intriguing" form ($\flat$):

$$f_\sigma\left(\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\-2&1\end{smallmatrix}\right)\right) = (-1)^{\frac{\lambda_\sigma - 1}{2}} \left(\begin{smallmatrix}1&0\\-8\rho_2(\sigma)&1\end{smallmatrix}\right) \left(\begin{smallmatrix}\lambda_\sigma^{-1}&0\\0&\lambda_\sigma\end{smallmatrix}\right) \left(\begin{smallmatrix}1&-8\rho_2(\sigma)\\0&1\end{smallmatrix}\right).$$

Here, $\rho_2 : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}$ designates the Kummer 1-cocycle along the positive roots of 2. The matrix specialization $g_\sigma\left(\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\-2&1\end{smallmatrix}\right)\right)$, $h_\sigma\left(\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\-2&1\end{smallmatrix}\right)\right) \in \mathrm{SL}_2(\hat{\mathbb{Z}})$, that should

decompose the right hand side of the above formula ($\flat$) according to their defining properties ($\sharp$), can be explicitly given in the language of special values of the Anderson-Ihara adelic beta function ([NT-II], [NTY]; joint works with H.Tsunogai and S.Yasuda). In the talk, ingredients of a proof (for h_σ) were discussed in connection with twofold illustrations of the Mordell elliptic curve $Y^2 = X^4 - X$ (Legendre form, 6-cyclic cover over $\mathbf{P}^1$.) Upon putting them together in the Cardano-Ferrari picture of the resolvent map from quartics to cubics, we use a certain 1-parameter family of 2 point punctured Mordell elliptic curves with specially nice properties. More explicitly, the families of quartics $f_s^{lem}(X) = X^4 - \frac{3}{2}sX^2 - sX + \frac{1}{16}s(s-4)$, $f_s^{mor}(X) = X^4 - \frac{3}{2}sX^2 + sX - \frac{3}{16}s^2$ play crucial roles in [NT2], [NTY] respectively with the properties for each case $* \in \{lem, mor\}$; (i) the equation $Y^2 = f_s^{lem}(X)$ (resp. $Y^2 = f_s^{mor}(X)$) gives a family of twice punctured {lemniscate, mordell} elliptic curves over $\mathbf{P}^1_s - \{0, 1, \infty\}$; (ii) the monodromy map $s \mapsto f_s^*(X)$ gives an embedding of $\pi_1(\mathbf{P}^1_s - \{0, 1, \infty\})$ into the Artin braid group $B_4/\langle center\rangle$ that factors through the triangle group of type $(4, \infty, 2)$, $(3, \infty, 2)$ for $* = lem, mor$ respectively; (iii) in the mapping (ii), a certain finite index subgroup of the triangle group corresponding to the fundamental group of the once-punctured {lemniscate, mordell} elliptic curve hits onto the kernel of Cardano-Ferrari homomorphism $B_4 \to B_3$.

References

[A] G. Anderson, *The hyperadelic gamma function*, Invent. Math. **95** (1989), 63–131.

[B] G.V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk. SSSR **8** (1979), 267–276 (in Russian); *English transl. in* Math. USSR Izv. **14** (1980), 247–256.

[Dr] V.G. Drinfeld, *On quasitriangular quasi-Hopf algebras and a group closely connected with* $\mathrm{Gal}(\bar{Q}/Q)$, Algebra i Analiz **2** (1990), 149–181 (in Russian); *English transl. in* Leningrad Math. J. **2(4)** (1991) 829–860.

[G] A. Grothendieck, *Esquisse d'un Programme*, 1984 in *Geometric Galois Actions I, P.Lochak, L.Schneps (eds.)* London Math. Soc. Lect. Note Ser. **242** (1997) 5–48.

[Ih] Y. Ihara, *On beta and gamma functions associated with the Grothendieck-Teichmüller modular group*, in *Aspects of Galois Theory (H. Voelklein et.al (eds.))* London Math. Soc. Lect. Note Ser. **256** (1999) 144–179; Part II, J. reine angew. Math. **527** (2000) 1–11.

[LS] P. Lochak, L. Schneps, *A cohomological interpretation of the Grothendieck-Teichmüller group*, Invent. Math. **127** (1997) 571–600.

[Na] H. Nakamura, *Limits of Galois representations in fundamental groups along maximal degeneration of marked curves, I* , Amer. J. Math. **121** (1999) 315–358; Part II, Proc. Symp. Pure Math. **70** (2002) 43–78.

[N98] —, *Tangential base points and Eisenstein power series*, in *Aspects of Galois Theory, H.Voelklein et. al. (eds.)* London Math. Soc. Lect. Note Ser. **256** (1999) 202–217.

[N01] —, *Some arithmetic in fundamental groups of affine elliptic curves*, talk at Euresco Conference at Acquafredda Maratea (2001).

[NS] H. Nakamura, L. Schneps, *On a subgroup of the Grothendieck-Teichmüller group acting on the tower of profinite Teichmüller modular groups*, Invent. Math. **141** (2000) 503–560.

[NT] H. Nakamura, H. Tsunogai, *Harmonic and equianharmonic equations in the Grothendieck-Teichmüller group*, Forum Math. **15** (2003) 877–892; Part II, *in "Primes and Knots" (T.Kohno, M.Morishita eds.)* AMS Contemporary Mathematics **416** (2006), 197–211.

[NTY] H. Nakamura, H. Tsunogai, S. Yasuda, *Harmonic and equianharmonic equations in the Grothendieck-Teichmüller group, III*, in preparation.

Periods on the moduli space of genus 0 curves

Sarah Carr
(joint work with Francis Brown, Leila Schneps)

A recent theorem in the thesis of Francis Brown proves that any period over a connected component of the real part of $\mathfrak{M}_{0,n}(\mathbb{C})$ is a $\mathbb{Q}$-linear combination of multizeta values. By studying the cohomology and geometry of $\mathfrak{M}_{0,n}(\mathbb{C}) = \mathfrak{M}_{0,n}$, we have found a method to formally represent these periods as linear combinations of pairs of n-polygons, one of which represents a connected component, or *cell*, of the real part of $\mathfrak{M}_{0,n}$, and the other a certain differential form which we call a *cell form*. These pairs of polygons form an algebra for the shuffle product. In this talk, we will outline the combinatorial structure of this algebra. As consequences, we obtain an explicit basis for the cohomology group, $H^{n-3}(\mathfrak{M}^{\delta}_{0,n})$, of differential forms converging on the boundary divisors which bound standard associahedron, δ, and hence a new method for studying multizeta values.

We denote by $(0, t_1, ..., t_{n-3}, 1, \infty)$ a point in $\mathfrak{M}_{0,n}$ and by $\mathfrak{M}_{0,n}(\mathbb{R}) \subset \mathfrak{M}_{0,n}$ the points whose marked points are in $\mathbb{R}$. We can identify an oriented n-gon to a connected component, or *cell*, in $\mathfrak{M}_{0,n}(\mathbb{R})$ by labelling the n-gon with the marked points. This n-gon is associated to the cell given by the clockwise cyclic ordering of the labelled edges of the polygon. For example, a polygon cyclically labelled $(0, t_1, t_3, 1, t_2, \infty)$ is identified with the cell $0 < t_1 < t_3 < 1 < t_2 < \infty$ in $\mathfrak{M}_{0,n}(\mathbb{R})$.

Similarly we can associate an n-gon labelled by the marked points to a differential $(n-3)$-form which we call a *cell form*. A cell form is defined as $dt_1 \wedge ... \wedge dt_{n-3}/\Pi(s_i - s_{i-1})$, where the s_i are the cyclically labelled sides of the polygon. We leave the side labelled ∞ out of the product. For example, the polygon cyclically labelled $[0, 1, t_1, t_3, \infty, t_2]$ gives the cell form $dt_1 dt_2 dt_3/((t_1 - 1)(t_3 - t_1)(-t_2))$.

We consider a *period* on $\mathfrak{M}_{0,n}$ to be convergent integral, over a connected component in $\mathfrak{M}_{0,n}(\mathbb{R})$, of a differential form which is holomorphic on the interior of $\mathfrak{M}_{0,n}$ and which has at most logarithmic singularities on $\overline{\mathfrak{M}}_{0,n} \setminus \mathfrak{M}_{0,n}$. Up to a variable change corresponding to permuting the marked points, all periods can be written as integrals over the standard cell, $\delta := 0 < t_1 < ... < t_{n-3} < 1$.

According to the above definitions, we can associate a pair of polygons to a cell and a cell form. Therefore, we have a map from pairs of n-gons to periods (and divergent integrals) given by mapping the pair to the integral of the cell form over the cell. This association and Brown's thesis have allowed us to prove some results and approach some conjectures about multizeta values and formal multizeta values.

Theorem 1. *The 01-cell forms given by polygons* $[..., 0, 1, ..., \infty]$ *form a basis for* $H^{n-3}(\mathfrak{M}_{0,n})$ *of differential* $(n-3)$*-forms convergent on the interior of* $\mathfrak{M}_{0,n}$ *and with at most logarithmic singularities on the boundary divisors,* $\overline{\mathfrak{M}}_{0,n} \setminus \mathfrak{M}_{0,n}$.

To prove this, it was enough to express Arnol'd's well-known basis in terms of 01-cell forms.

Definitions 2. *Let $\mathcal{P}_n$ be the vector space generated by oriented n-gons decorated by the marked points in $\mathfrak{M}_{0,n}$.*

Recall that the shuffle product of lists A and B is defined as

$$A \sqcup\!\sqcup B = \sum_{\sigma \in \mathfrak{S}} \sigma(A \cdot B),$$

where σ runs over the permutations of the concatenation of A and B such that the orders of A and B are preserved.

Let $I_n \subset \mathcal{P}_n$ be the vector subspace generated by shuffle sums with respect to ∞, in other words polygon sums of the form

$$\sum_{W \in A \sqcup\!\sqcup B} [W, \infty]$$

where A, B is a partition of $\{0, t_1, ..., t_{n-3}, 1\}$.

Theorem 3. *$\mathcal{P}_n / I_n$ is isomorphic to $H^{n-3}(\mathfrak{M}_{0,n})$.*

Proof. (Sketch) By the previous theorem, we have a natural surjective map

$$\mathcal{P}_n \twoheadrightarrow H^{n-3}(\mathfrak{M}_{0,n}), \tag{1}$$

which sends a polygon to it's associated cell form. A calculation on rational functions shows that I_n is in the kernel of this map. A dimension count finishes the proof. □

We would like to study cohomology of interesting subspaces of $H^{n-3}(\mathfrak{M}_{0,n})$ such as the space of differential forms which converge on the standard cell, δ. To do this we make use of the kernel I_n to create a basis of convergent 01-forms and what we refer to as *insertion forms*.

Some 01-forms naturally converge on δ. We define a *chord* on a cell form, ω, to be a set of marked points of a subsequence on ω of the length between 2 and $\lfloor \frac{n}{2} \rfloor$. The 01-forms which do not have any chords in common with δ converge on δ. However, some linear combinations of nonconvergent 01-forms converge on δ; a certain generating set of these are *insertion forms*. Insertion forms are created according to a recursive procedure of inserting convergent shuffles (those whose shuffle factors have no chords in common with δ) into convergent 01-forms. For example,

$$\omega = [0, 1, t_1, t_2, \infty, t_3] + [0, 1, t_2, t_1, \infty, t_3] \tag{2}$$

$$= [0, 1, t_1 \sqcup\!\sqcup t_2, \infty, t_3] \tag{3}$$

is an insertion form obtained by inserting the convergent shuffle $t_1 \sqcup\!\sqcup t_2$ into the convergent 01-form $[0, 1, s_1, \infty, s_2]$. The shuffle factors are t_1 and t_2, and are therefore too short to contain any chords.

Theorem 4. *The insertion forms and the convergent 01-cell forms form a basis for $H^{n-3}(\mathfrak{M}^{\delta}_{0,n})$.*

The proof of this theorem is the heart of our recent work and is given in [3]. It exploits the fact that I_n is the kernel of the map (1).

Now that we can explicitly describe the differential forms convergent on δ, we can define an algebra of periods, since by a variable change, all periods can be written as integrals of forms over δ. The algebra of periods has three known sets of relations:

(1) Invariance under the symmetric group action corresponding to a variable change
(2) Forms given by shuffles with respect to one point are identically 0
(3) Product map relations coming from the pullback of maps on moduli space (outlined in [2] and [3]).

The product map relations also allow us to define a multiplication law on periods.

We conjecture that these are the only relations on periods, but this question seems difficult to prove. A more strategic approach is to define a formal algebra on polygon pairs satisfying these and only these relations. Since the algebra of periods is isomorphic to the algebra of multizeta values ([2]), we conjecture that the formal algebra of pairs of polygons, which we call $\mathcal{FC}$, is isomorphic to the formal multizeta value algebra. With this association, we hope to approach some of the main conjectures on formal multizetas such as Zagier's dimension conjecture.

Conjecture 5 (Zagier)**.** *Let $\mathcal{Z}_n$ be the vector space generated by weight n multizeta values. Then $d_n = \dim(\mathcal{Z}_n)$ is given by the recursive formula,*

$$d_n = d_{n-2} + d_{n-3}.$$

This conjecture is true in small weight for $\mathcal{FC}$ and we hope that its combinatorial recursive definition will allow us to make progress on this conjecture.

References

[1] V. I. Arnol'd, *The cohomology of the colored braid group*, Mat. Zameki, no. 5, 1969, pp. 227-231
[2] F. Brown, *Multiple zeta values and periods of moduli spaces* $\overline{\mathfrak{M}}_{0,n}(\mathbb{R})$, PhD thesis, 2006
[3] F. Brown, S. Carr et L. Schneps, *Cellular zeta values*, to appear
[4] X. Buff, J. Fehrenbach, P. Lochak and L. Schneps, *Espaces de modules des courbes, groupes modulaires et théorie des champs*, Panoramas et Synthèses, no. 7, SMF, 1999
[5] H. Furusho, *The multiple zeta value algebra and the stable derivation algebra*, Publications of the Research Institute for Mathematical Sciences (Kyoto), Vol. 39 (2003), p. 695
[6] A.B. Goncharov, *Galois symmetries of fundamental groupoids and noncommutative geometry*, arXiv:math.AG/0208144 v4, June 17, 2004
[7] Y. Ihara, *On the stable derivation algebra associated with some braid groups*, Israel Journal of Mathematics, Vol. 80 (1992), pp. 135-153
[8] M. Kontsevich and D. Zagier, *Periods*, IHES/M/01/22
[9] C. Reutenauer, *Free Lie Algebras*, Oxford University Press, 1993

On the p-rank stratification of the moduli space of curves

Rachel Pries
(joint work with Jeffrey Achter)

We describe the $\mathbb{Z}/\ell$-monodromy and $\mathbb{Z}_\ell$-monodromy of every irreducible component of the moduli space $\mathcal{M}_g^f$ of curves of genus g and p-rank f in characteristic p. In particular, we prove that the $\mathbb{Z}/\ell$-monodromy of every component of $\mathcal{M}_g^f$ is the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$ if $g \geq 3$ and if $\ell \neq p$ is an odd prime. We give applications to the generic behavior of automorphism groups, zeta functions, class groups, and Jacobians of curves of genus g and p-rank f.

Let k be an algebraically closed field of characteristic $p > 0$. Suppose C is a smooth connected projective k-curve of genus g. The Jacobian $\mathrm{Pic}^0(C)$ is a principally polarized abelian variety of dimension g. The number of p-torsion points of $\mathrm{Pic}^0(C)$ is p^f for some integer f so that $0 \leq f \leq g$. Here f is the *p-rank* of C.

Let $\mathcal{M}_g$ be the moduli space parametrizing smooth connected projective k-curves of genus g. The p-rank induces a stratification $\mathcal{M}_g = \cup \mathcal{M}_g^f$ by locally closed reduced subspaces $\mathcal{M}_g^f$.

Suppose $\ell \neq p$ is an odd prime. We compute the ℓ-adic monodromy of every irreducible component of $\mathcal{M}_g^f$. The main result implies that there is no restriction on the monodromy group other than that it preserve the symplectic pairing coming from the principal polarization. Heuristically, this means that imposing p-rank constraints does not force the existence of extra automorphisms (or other algebraic cycles) on a sufficiently general family of curves.

More precisely, let S be a connected k-scheme and let s be a geometric point of S. Let $\phi : C \to S$ be a flat family of smooth, proper curves of genus g over S. Then $\mathrm{Pic}^0(C)[\ell]$ is an étale cover of S with geometric fiber isomorphic to $(\mathbb{Z}/\ell)^{2g}$. The fundamental group $\pi_1(S, s)$ acts linearly on the fiber $\mathrm{Pic}^0(C)[\ell]_s$. The monodromy group $\mathsf{M}_\ell(C \to S, s)$ is the image of $\pi_1(S, s)$ in $\mathrm{Aut}(\mathrm{Pic}^0(C)[\ell]_s)$.

For the main result we compute $\mathsf{M}_\ell(S) := \mathsf{M}_\ell(C \to S)$, where S is an irreducible component of $\mathcal{M}_g^f$, the stratum of $\mathcal{M}_g$ which parametrizes curves of genus g and p-rank f, and $C \to S$ is the tautological curve.

Theorem 1. *Let $\ell \neq p$ be an odd prime. Suppose $g \geq 1$, $0 \leq f \leq g$, and $f \neq 0$ if $g \leq 2$. Let S be an irreducible component of the moduli space $\mathcal{M}_g^f$ of k-curves of genus g and p-rank f. Then $\mathsf{M}_\ell(S) \cong \mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$.*

We also prove that the ℓ-adic monodromy group is $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ in this situation.

We give four applications of Theorem 1. Some of these applications do not use the full strength of the theorem, in that they could be deduced solely from the $\mathbb{Q}_\ell$-monodromy. Application (1) complements [8] and [9], while application (2) complements results in [5]. Applications (3) and (4) build upon [6, 9.7.13] and [7, 6.1 and 3.2.(4)] respectively.

Applications: Let $\mathbb{F}$ be a finite field of odd characteristic. Under the hypotheses of Theorem 1:

(1) there is an $\overline{\mathbb{F}}$-curve $\mathcal{C}$ of genus g and p-rank f with $\mathrm{Aut}_{\overline{\mathbb{F}}}(\mathcal{C}) = \{\mathrm{id}\}$;
(2) there is an $\overline{\mathbb{F}}$-curve $\mathcal{C}$ of genus g and p-rank f with absolutely simple Jacobian;
(3) if $|\mathbb{F}| \equiv 1 \bmod \ell$, about $1/(\ell-1)$ of the $\mathbb{F}$-curves of genus g and p-rank f have a point of order ℓ on their Jacobian;
(4) for most $\mathbb{F}$-curves $\mathcal{C}$ of genus g and p-rank f, the splitting field of the numerator of the zeta function of $\mathcal{C}$ is as large as possible.

The proof of Theorem 1 proceeds by induction on the genus. Consider the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g and its p-rank strata $\mathcal{A}_g^f$. Recent work in [2, 4.7] gives information about the integral monodromy of $\mathcal{A}_g^f$. Namely, the author proves that an irreducible subspace of $\mathcal{A}_g$ which is stable under all Hecke correspondences and is not supersingular has monodromy group $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. The base cases of Theorem 1 rely on the fact that the dimensions of $\mathcal{M}_g^f$ and $\mathcal{A}_g^f$ are equal if $g \leq 3$.

The inductive step uses results in [3] on the boundary of $\mathcal{M}_g^f$. In particular, we show that the closure of every component S of $\mathcal{M}_g^f$ intersects the interior of the boundary component $\Delta_{1,1}$ of $\mathcal{M}_g$. As in [1], this implies that the monodromy group of S contains two non-identical copies of $\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell)$.

We note that [2] is not directly applicable to the strata $\mathcal{M}_g^f$ when $g \geq 4$. When $g \geq 4$, the Torelli locus is very far from being Hecke-stable. Another method for computing integral monodromy is found in [4], where the author shows that certain group-theoretic conditions on the local inertia structure of a $\mathbb{Z}/\ell$-sheaf guarantee that its global monodromy group is the full symplectic group. The lack of information about explicit one-parameter families in $\mathcal{M}_g^f$ makes it difficult to apply this method.

Our techniques can be applied to compute the ℓ-adic monodromy in two other situations. This yields analogues of applications (1)-(4) for both of these situations. The first case involves components of the moduli space $\mathcal{H}_g^{g-1}$ of hyperelliptic curves with genus g and p-rank $f = g-1$. The integral monodromy of hyperelliptic curves with p-rank $f = g$ was computed previously (by J.K.Yu (unpublished), [1], [4]). The second case involves components of the moduli space $\mathcal{T}_g^2$ of curves of genus g with a-number 2. We briefly describe the results.

Theorem 2. *Let $p \geq 3$ and $g \geq 2$. Let $\ell \neq p$ be an odd prime. Let S be an irreducible component of the moduli space $\mathcal{H}_g^{g-1}$ of hyperelliptic k-curves of genus g and p-rank $g-1$. Then $\mathsf{M}_\ell(S) \cong \mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$.*

Theorem 3. *Suppose $p \geq 5$ and $g \geq 3$. Let $\ell \neq p$ be an odd prime. Let S be an irreducible component of the moduli space $\mathcal{T}_g^2$ of k-curves of genus g with a-number 2. Then $\mathsf{M}_\ell(S) \cong \mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$.*

It is interesting that these results can be proven despite a lack of information about the geometry of $\mathcal{M}_g^f$. For example, at this time, the number of irreducible

components of $\mathcal{M}_g^f$ is known only in special cases. Further progress on this could lead to simplified proofs of our results. For example, if $\mathcal{M}_g^0$ is irreducible then the proof of Theorem 1 could reduce to the case that $f = 0$.

The author was partially supported by NSF grant DMS-04-00461.

References

[1] J. D. Achter and R. J. Pries, *The integral monodromy of hyperelliptic and trielliptic curves*, Math. Ann., 338(1):187–206, 2007.

[2] C.-L. Chai, *Monodromy of Hecke-invariant subvarieties*, Pure Appl. Math. Q., 1(2):291–303, 2005.

[3] C. Faber and G. van der Geer, *Complete subvarieties of moduli spaces and the Prym map*, J. Reine Angew. Math., 573:117–137, 2004.

[4] C. Hall, *Big symplectic or orthogonal monodromy modulo ℓ*, August 2006, arXiv:math.NT/0608718.

[5] E. W. Howe and H. J. Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory, 92(1):139–163, 2002.

[6] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society, Providence, RI, 1999.

[7] E. Kowalski, *The large sieve, monodromy and zeta functions of curves*, J. Reine Angew. Math., 601:29–69, 2006.

[8] B. Poonen, *Varieties without extra automorphisms I. Curves* Math. Res. Lett., 7(1):67–76, 2000.

[9] H. J. Zhu, *Hyperelliptic curves over $\mathbb{F}_2$ of every 2-rank without extra automorphisms*, Proc. Amer. Math. Soc., 134(2):323–331 (electronic), 2006.

On non linear differential Galois theory

Bernard Malgrange

Let X be a smooth complex algebraic variety. One works "generically" on X, i.e. one replaces if necessary X by a Zariski open dense set (without saying it explicitly). A foliation on X is a coherent subsheaf $\mathcal{N}$ of the sheaf of 1-forms on X, which satisfies the Frobenius condition. One can suppose that N is generated by p forms $a_1, .., a_p$, which are linearly independent at each point.

Roughly speaking, one defines the "Galois groupoid" of $\mathcal{N}$ as the smallest $\mathcal{D}$-groupoid whose Lie algebra contains the vector fields tangent to the foliation. More precisely, for each integer k, let $J_k(X)$ be the space of invertibles jets of order k of maps from X to X. One looks at the smallest subgroupoid of $J_k(X)$ (generically) whose Lie algebra (or "algebroid") contains the jets of order k of the vector fields of the foliation. One proves that this groupoid can be defined by the usual Picard-Vessiot theory (or its extension to the case of a non-algebraically closed field of constants).

One method is the following: By choosing a projection of dimension $\dim(X) - p$, transverse to the foliation, one is reduced to a differential equation. Then one takes its variational equations (of all orders), and apply to them the Picard-Vessiot theory. Another construction is also given, independent of any projection.

This gives only a partial description of the Galois groupoid; roughly speaking, this gives what corresponds in the non linear case to the Picard-Vessiot extension.

But it does not give the complete description of "what corresponds to the Galois group" (in fact this is not a group but rather a filtered Lie algebra, or, better a filtered Lie coalgebra; due to lack of time, this subject was not developed in the lecture).

On the geometry of higher dimensional anabelian varieties

Jakob Stix

1. Anabelian varieties

The étale fundamental group of a geometrically connected variety X over a field k sits in a short exact sequence

$$1 \to \pi_1 X_{\overline{k}} \to \pi_1 X \to \mathrm{Gal}_k \to 1.$$

Grothendieck conceived that for special varieties, this short exact sequence captures the geometry and arithmetic of the underlying (category of) varieties. Such varieties are called anabelian and coincide in dimension 1 with hyperbolic curves, whereas in higher dimensions the notion of anabelian varieties is unclear. The talk focused on the geometric property of being an algebraic $\mathrm{K}(\pi,1)$ space and derived consequences for the geometry of such varieties.

2. Algebraic $\mathrm{K}(\pi,1)$ spaces

Let X/k be a connected variety. The finite étale site $X_{\mathrm{fét}}$ is by definition via a choice of a base point isomorphic to the classifying site $\mathscr{B}\pi_1 X$ of $\pi_1 X$. The map

$$\gamma : X_{\text{ét}} \to X_{\mathrm{fét}} \cong \mathscr{B}\pi_1 X$$

induces comparison maps $\mathrm{H}^*(\pi_1 X, A) \to \mathrm{H}^*_{\text{ét}}(X, \mathscr{A})$ for each finite continuous $\pi_1 X$-module A with locally constant system $\mathscr{A} = \gamma^* A$. An **algebraic** $\mathrm{K}(\pi,1)$ **space** is a variety, such that all comparison maps are isomorphisms. As cohomology is always killed locally in the respective topology for which it is computed, the Leray spectral sequence for γ_* shows that being an algebraic $\mathrm{K}(\pi,1)$ is equivalent to the following: all $\mathrm{H}^q(X', \mathbb{Z}/n\mathbb{Z})$ for finite étale covers X'/X, $n \in \mathbb{N}$ and $q > 0$ are killed upon restriction to suitable finite étale covers. Hence, the $\mathrm{K}(\pi,1)$ property forces $\pi_1 X$ to be sufficiently rich. The comparison map is always bijective for H^1 and injective for H^2, as classes in H^1 are étale torsors which kill themselves.

Examples for algebraic $\mathrm{K}(\pi,1)$ spaces are: curves except for $\mathbb{P}^1_k$, abelian varieties, and more generally varieties such that for all finite étale covers the cohomology ring is generated by classes in H^1. The latter implies for projective varieties that the Albanese map is finite. Being an algebraic $\mathrm{K}(\pi,1)$ space goes up and down along finite étale covers and behaves well in fibrations in the following sense. Let $f : X \to S$ be a smooth, projective map with $f_* \mathscr{O}_X = \mathscr{O}_S$ and S is connected of characteristic 0. Then one geometric fibre is $\mathrm{K}(\pi,1)$ if and only if all geometric fibres are $\mathrm{K}(\pi,1)$. With X_s being the geometric fibre over $s \in S$ the fibre sequence

$$1 \to \pi_1 X_s \to \pi_1 X \to \pi_1 S \to 1$$

is exact if the base S is $\mathrm{K}(\pi,1)$ or X/S admits a section.

Then comparison of Hochschild–Serre and Leray spectral sequences yields: if two out of fibre X_s, base S and total space X are $\mathrm{K}(\pi,1)$ then also the third. For the exactness of the fibre sequence in case S is a $\mathrm{K}(\pi,1)$ only the injectivity of $\pi_1 X_s \to \pi_1 X$ needs a proof. For this we need to extend any connected G-torsor $\varphi : \pi_1 X_s \twoheadrightarrow G$ of the fibre to a G-torsor $\tilde{\varphi} : \pi_1 X' \to G$, where $X' = X \times_S S'$ with a finite étale cover S'/S. As the nonabelian $\mathrm{R}^1 f_* G$ is locally constant, we may choose, upon substitution of S by a finite étale cover, a global isomorphism class of a G-torsor in $\mathrm{H}^0(S, \mathrm{R}^1 f_* G)$ that restricts to φ in the fibre above s. The obstruction for this class to come from an actual torsor lies in $\mathrm{H}^2(S, Z(G))$ where $Z(G)$ is the center of G and the lien of the corresponding gerbe, because the G-torsor φ is connected. This obstruction vanishes on a finite étale cover of S.

A smooth projective $\mathrm{K}(\pi,1)$ space X of dimension $\dim X \geq 2$ is never a hyperplane section of a smooth projective variety Y. By Lefschetz, the inclusion induces an isomorphism $\pi_1 X \xrightarrow{\sim} \pi_1 Y$ which for an anabelian X would conjecturally lead to an unlikely retraction for the inclusion. In the diagram

$$\begin{array}{ccc} \mathrm{H}^2(\pi_1 Y, \mathbb{Z}_\ell(1)) & \xrightarrow{\cong} & \mathrm{H}^2(\pi_1 X, \mathbb{Z}_\ell(1)) \\ \downarrow & & \downarrow \cong \\ \mathrm{H}^2(Y, \mathbb{Z}_\ell(1)) & \hookrightarrow & \mathrm{H}^2(X, \mathbb{Z}_\ell(1)) \end{array}$$

the Weak Lefschetz Theorem and comparison for H^2 of Y imply the injections. Hence all maps are bijective. In particular, the class h of a hyperplane of Y comes from group cohomology, so that $h^{\dim Y}$ can be computed in the cohomology ring $\mathrm{H}^*(\pi_1 X)$ and hence vanishes, a contradiction.

3. Algebraic $\mathrm{K}(\pi,1)$ spaces and the Minimal Model Program

By Zariski–Nagata purity $\pi_1 X$ is a birational invariant of a smooth projective variety. As birational maps have seldom retractions, a smooth projective anabelian variety must be an absolutely minimal variety in its birational class. This is indeed the case already for smooth projective $\mathrm{K}(\pi,1)$ spaces.

Kollàr defines in [Ko93] Def 2.7 the notion of a variety X with **large algebraic fundamental group**: the image of $\pi_1 Z \to \pi_1 X$ is infinite for all nonconstant algebraic maps $f : Z \to X$. Projective algebraic $\mathrm{K}(\pi,1)$ spaces have large algebraic fundamental group. Arguing by contradiction we may restrict to smooth projective curves Z and finite maps f, such that $\pi_1 f$ is trivial. The degree $\deg_Z f^* \mathscr{L}$ for an ample line bundle $\mathscr{L}$ on X must be positive. On the other hand, by the commutativity of the following diagram

$$\begin{array}{ccccc} \mathrm{Pic}(X) & \xrightarrow{c_1} & \mathrm{H}^2(X, \mathbb{Z}_\ell(1)) & \xleftarrow{\cong} & \mathrm{H}^2(\pi_1 X, \mathbb{Z}_\ell(1)) \\ \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle \mathrm{H}^2(f)} & & \downarrow{\scriptstyle 0} \\ \mathrm{Pic}(Z) & \xrightarrow{c_1} & \mathrm{H}^2(Z, \mathbb{Z}_\ell(1)) & \xleftarrow{} & \mathrm{H}^2(\pi_1 Z, \mathbb{Z}_\ell(1)) \end{array}$$

and the formula $\deg_Z f^* \mathscr{L} = c_1(f^* \mathscr{L}) \in \mathrm{H}^2(Z, \mathbb{Z}_\ell(1)) = \mathbb{Z}_\ell$, the degree vanishes.

Having large fundamental group implies nonexistence of rational curves, which tremendously restricts geometry. Mori's bend and break technique inhibits nontrivial families of pointed maps $(C, c) \to (X, x)$. Moreover, the canonical bundle ω_X is nef and X is already minimal in the sense of the Minimal Model Program.

4. An abelian fibration

Abelian varieties are not really anabelian. Hence it is desirable to get rid of the abelian part of an algebraic $\mathrm{K}(\pi, 1)$ space. The following is inspired by its birational version [Ko93] Thm 6.3. of Kollàr.

An **almost regular fibration** on X is a projective map $\widetilde{f} : \widetilde{X} \to \widetilde{Y}$ defined on a projective birational modification $\sigma : \widetilde{X} \to X$, such that for a dense open $V \subset \widetilde{Y}$ the preimage $\widetilde{f}^{-1}(V)$ is mapped isomorphically by σ onto an open subset $U \subset X$ and the restriction $\widetilde{f}|_U : U \to V$ is smooth projective.

Theorem. *Let X/k be a smooth projective algebraic $\mathrm{K}(\pi, 1)$ space in characteristic 0. Let $\widetilde{f}$ be an almost regular fibration on X such that a general fibre admits a finite étale cover by an abelian variety.*

Then there exists a finite étale cover X'/X and a map $f' : X' \to Y'$ that is birational to the prolongation of $\widetilde{f}$ such that X'/Y' is an abelian scheme and Y' is a smooth projective $\mathrm{K}(\pi, 1)$ space.

Though for algebraic $\mathrm{K}(\pi, 1)$ spaces the proof is easier as in [Ko93] Thm 6.3, the proof follows the strategy of loc. cit. adding a final fourth step. (I) Replacing X by a finite étale cover, we may assume that a given fibre is an abelian variety. Hence all smooth fibres are algebraic $\mathrm{K}(\pi, 1)$ spaces with abelian fundamental group, thus are abelian varieties. (II) From Grothendiecks monodromy description of families of abelian varieties [Gr66], we obtain good reduction of the relative Albanese family over all of $\widetilde{Y}$. Here Kollàr uses a more involved argument via Hodge theory in order to verify Grothendieck's condition. (III) Again replacing X by a finite étale cover, we may assume that $\widetilde{X}/\widetilde{Y}$ is itself a family of abelian varieties. (IV) in the final step, we descend the family of abelian varieties using [Gr66] to the image under σ of the zero section of $\widetilde{X}/\widetilde{Y}$ as an abelian scheme. It turns out, that the necessary contraction of the total space is precisely the map σ, and the abelian fibration on a cover of X is achieved.

Almost abelian fibrations on minimal models are given by: (A) the nef reduction of ω_X as in [Nef01], (B) the Iitaka fibration under a conjecture on Kodaira dimension 0 and numerically trivial ω_X, (C) suitable pluricanonical maps under the abundance conjecture. Conjecturally all three examples agree and lead to a base Y' which is of general type. Following Kawamata Campana and Peternell conclude that the canonical bundle is even ample, see [Ka92] Appendix.

References

[Gr66] A. Grothendieck, *Un Théorème sur les Homomorphisme de Schémas Abéliens*, Invent. Math. **2** (1966), 59–78.

[Ka92] Y. Kawamata, *Moderate degenerations of algebraic surfaces*, Lecture Notes in Math **1507**, 113–133.

[Ko93] J. Kollàr, *Shafarevich maps and plurigenera of algebraic varieties*, Invent. Math. **113** (1993), 177–215.

[Nef01] T. Bauer, F. Campana, T. Eckl, S. Kebekus, T. Peternell, S. Rams, T. Szemberg, L. Wotzlaw, *A reduction map for nef line bundles*, arXiv:math.AG/0106147.

The Λ-corank of $Ш(E/K_\infty)_{p^\infty}$ for supersingular primes

Mirela Çiperiani

Let E be an elliptic curve defined over $\mathbb{Q}$. The L-function of E, $L(E,s)$, is known to have analytic continuation to the whole complex plane by the theorems of Wiles [13] extended by Breuil, Conrad, Diamond and Taylor [2]. This is a consequence of E being modular, i.e. covered by the modular curve by a finite map $\pi : X_0(N) \to E$ for some positive integer N. The minimal such N is called the conductor of E. The L-function can be defined as an Euler product

$$L(E,s) = \prod_{p|N}(1 - a_p p^{-s})^{-1} \cdot \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1}$$

where for $p \nmid N$, $a_p = 1 + p - \#E(\mathbb{F}_p)$ with $\mathbb{F}_p$ denoting the field with p elements and for $p|N$, $a_p = -1, +1,$ or 0. The order of the zero of $L(E,s)$ at $s = 1$ is called the *analytic rank* of $E/\mathbb{Q}$.

Genus one curves defined over $\mathbb{Q}$ with Jacobian E which have a point defined over each completion of $\mathbb{Q}$ but no point defined over $\mathbb{Q}$ correspond to nontrivial elements of $Ш(E/\mathbb{Q})$. This group is known to be torsion and the Birch and Swinnerton-Dyer conjecture predicts that $Ш(E/\mathbb{Q})$ is finite. This is known only in the case when the analytic rank of $E/\mathbb{Q}$ is less than or equal to one, by the combined work of Gross and Zagier [5], Kolyvagin [7], Waldspurger [12], Murty and Murty [9], Bump, Friedberg and Hoffstein [1].

We fix a rational prime p which does not divide N. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We can consider $Ш(E/\mathbb{Q}_\infty)_{p^\infty}$ as a module over $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$. We know that

$$Ш(\widehat{E/\mathbb{Q}_\infty})_{p^\infty} := \mathrm{Hom}(\, Ш(E/\mathbb{Q}_\infty)_{p^\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$$

is finitely generated over Λ and the Λ-corank of $Ш(E/\mathbb{Q}_\infty)_{p^\infty}$ is defined to be equal to the Λ-rank of $Ш(\widehat{E/\mathbb{Q}_\infty})_{p^\infty}$.

In the case when p is a prime of ordinary reduction (i.e. $p \nmid a_p$) by Rubin (CM case) [10] and Kato (non CM case) [6] we know that $Ш(E/\mathbb{Q}_\infty)_{p^\infty}$ has trivial corank. When p is a prime of supersingular reduction (i.e. $p \mid a_p$) Kurihara [8] has shown that the Λ-corank of $Ш(E/\mathbb{Q}_\infty)_{p^\infty}$ is 1 under some conditions which in particular imply that the elliptic curve does not have complex multiplication and its analytic rank is 0.

Let $K/\mathbb{Q}$ be an imaginary quadratic extension such that all the primes dividing the conductor N split and K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension. Using the

modularity of E and the work of Cornut [4] and Vatsal [11] we know that $E(K_\infty)$ contains infinitely many non-torsion Heegner points.

When p is a prime of ordinary reduction and E does not have complex multiplication, Bertolini [3] uses Heegner points to show that $Ш(E/K_\infty)_{p^\infty}$ has trivial Λ-corank, where $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$. We have proven the same result in the case when p is a prime of supersingular reduction.

References

[1] D. Bump, S. Friedberg and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618.

[2] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[3] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*' Compositio Math. **99** (1995), no. 2, 153–182.

[4] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523.

[5] B. H. Gross and D.B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[6] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, preprint

[7] V.A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., **87**, Birkhäuser Boston, Boston, MA, 1990.

[8] M. Kurihara, *On the Tate-Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*, Invent. Math. **149** (2002), no. 1, 195–224.

[9] M.R. Murty and V.K. Murty, *Mean values of derivatives of modular L-functions*, Annals of Math. **133** (1991) 447–475.

[10] K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. math. **93** (1988), 701–713

[11] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), no. 2, 219–261.

[12] J. -L., Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. (9) **60** (1981), no. 4, 375–484.

[13] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

Generically large images of geometric Galois representations

Núria Vila

(joint work with Luis Dieulefait)

The main aim of this talk was to report on recent results concerning generically large images for compatible families of geometric four-dimensional Galois representations. We only consider representations attached to a pure motive defined over $\mathbb{Q}$ with coefficients in an imaginary quadratic field, with different Hodge-Tate numbers. We apply our results to an example constructed by J. Scholten [Sc] obtaining a family of four-dimensional linear groups, and one of unitary groups as Galois groups over $\mathbb{Q}$.

Results on generically large images for compatible families of Galois representations are well known in the two-dimensional case for Galois representations attached to elliptic curves without Complex Multiplication (CM), results of Serre

[S1], and attached to classical modular forms without CM, results of Ribet [R1]. In the three-dimensional case generically large images were obtained by the authors in [D-V1] for compatible families attached to smooth projective surfaces and to cohomological modular forms. For four-dimensional symplectic Galois representations, generically large images are known for Galois representations attached to principally polarized abelian surfaces with trivial endomorphism ring (cf. [S2]), and to cuspidal genus two Siegel eigenform (cf. [D], [D-K-R]). We need to have explicit criteria to control a set of exceptional primes for the images of the residual Galois representation and apply the results to explicit objects, in order to obtain that families of finite linear groups occur as Galois groups over $\mathbb{Q}$ (see [V] and references there).

Let $S/\mathbb{Q}$ be a smooth projective variety of dimension 3. Consider the action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the absolute Galois group over $\mathbb{Q}$ on the étale cohomological group $H^3(S)_\ell := H^3_{et}(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$. Let

$$\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GL}(H^3(S)_\ell)$$

be the ℓ-adic Galois representations. Let N be the product of primes of bad reduction of S. Let K be an imaginary quadratic field, assume that the Galois representations on $H^3(S)_\ell \otimes_{\mathbb{Q}_\ell} K_\ell$ are all reducible, and they contain as subrepresentations a compatible family $\{\sigma_{S,\lambda}\}$ of λ-adic 4-dimensional Galois representations, with λ prime in K dividing ℓ. For this family it also holds that the ramification set is (at most) the set of prime factors of N. We will assume that the traces at Frobenius elements all lie in K and generate K. We will also assume that these representations have four different Hodge-Tate numbers $\{0, 1, 2, 3\}$, and that the determinant of each $\sigma_{S,\lambda}$ is just χ^6, where χ denotes the ℓ-adic cyclotomic character (this last condition can always be satisfied after twisting by a suitable Dirichlet character unramified outside N).

Thus, the families we are considering can be briefly described as a compatible family of 4-dimensional Galois representations:

$$\sigma_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}(W_\lambda) \cong \mathrm{GL}(4, K_\lambda),$$

associated to a pure motive defined over $\mathbb{Q}$ with coefficients in a quadratic field K and Hodge-Tate numbers $\{0, 1, 2, 3\}$ with the simplifying assumption that the determinants are just χ^6.

From the compacity of $G_{\mathbb{Q}}$ and the continuity of the representations σ_λ, it follows that we can assume that the images are contained in $\mathrm{GL}(4, \mathcal{O}_\lambda)$, where $\mathcal{O}$ denotes the ring of integers of K. This implies that we can consider the residual representations $\bar{\sigma}_\lambda$ with values in $\mathrm{GL}(4, \mathbb{F}_\lambda)$, obtained by composing σ_λ with the naive map "reduction modulo λ".

Let a_p denote the trace of $\sigma_\lambda(\mathrm{Frob}\ p)$, for any prime $p \nmid \ell N$. Let $Pol_p(x) = x^4 - a_p x^3 + b_p x^2 - p^3 \bar{a}_p x + p^6$, be the characteristic polynomials of $\sigma_\lambda(\mathrm{Frob}\ p)$ $(p \nmid \ell N)$. We will denote by $c := \mathrm{l.c.m.}\{cond(\sigma_\lambda)\}_\lambda$, the "conductor of the family of representations". To study the images of $\bar{\sigma}_\lambda$ we have two main tools: The classification of maximal subgroups, up to conjugation, of $\mathrm{GL}(4, p^t)$ (cf. [K-L]),

and the description of the image of the inertia at ℓ. We obtain the following result for the generic images:

Theorem. *Let $\{\sigma_\lambda\}$ be a compatible family of geometric pure 4-dimensional Galois representations of $G_{\mathbb{Q}}$ with Hodge-Tate weights $\{0,1,2,3\}$, with determinants χ^6, coefficients in an imaginary quadratic field K. Assume that $K=\mathbb{Q}(\{a_p^2\})$. Then, one of the following is satisfied:*

(i) *$\sigma_\lambda \cong \sigma_{f_1,\ell} \oplus (\sigma_{f_2,\ell}\otimes\chi)$, where f_1 and f_2 are modular forms.*
(ii) *$\sigma_\lambda = Ind_E^{\mathbb{Q}}(\varphi)$, where φ is a one or a two dimensional Galois representation of the absolute Galois group of a number field E.*
(iii) *the image of σ_λ is "as large as possible", for almost every prime, i.e., the image of its projectivization $P(\sigma_\lambda)$ satisfies:*
$\mathrm{PSL}(4,\mathbb{Z}_\ell)\subseteq \mathrm{Image}(P(\sigma_\lambda))\subseteq \mathrm{PGL}(4,\mathbb{Z}_\ell)$, *if ℓ splits in K;*
$\mathrm{Image}(P(\sigma_\lambda))=\mathrm{PSU}(4,\mathbb{Z}_\ell)$, *if ℓ is inert in K.*

Moreover, we can give six explicit conditions in order to guarantee that we are in case iii) of the theorem and to control the exceptional set of primes:
1): There exists a prime $p\nmid N$ such that none of the roots of $Pol_p(x)$ is a number of the form ηp^i, where η denotes an arbitrary root of unity and $i\in\{0,1,2,3\}$.
2): There exists a prime $p\nmid N$ such that none of the roots of $Q_p(x)$, the characteristic polynomial of $\wedge^2(\sigma_\lambda)(\mathrm{Frob}\ p)$, is a number of the form ηp^i, where η denotes an arbitrary root of unity and $i\in\{1,2,3,4,5\}$.
3): For every quadratic character ψ unramified outside N there exists a prime $p\nmid N$ with $\psi(p)=-1$ and $p^3(a_p^2+\bar{a}_p^2)\neq a_p\bar{a}_p b_p$.
4): For every quadratic character ψ unramified outside N there exists a prime $p\nmid N$ with $\psi(p)=-1$ and $a_p\neq 0$.
5): For every cubic character ϕ unramified outside N there exists a prime $p\nmid N$ with $\phi(p)\neq 1$ and $a_p^2 b_p+p^6\neq p^3\bar{a}_p a_p$,
6): There exists a prime $p\nmid N$ such that: $K=\mathbb{Q}(a_p^2)$.
Assuming that the conductor c is known, we can give an algorithm to explicitly bound the finite set of exceptional primes (image not maximal), for a family verifying the six conditions.
We apply our results to $\sigma_{S,\lambda}$ the non-selfdual 4-dimensional ℓ-adic Galois representation given by Scholten [Sc], defined over $K=\mathbb{Q}(\zeta)$, where ζ is a cubic root of unity. We can conclude that the images of the 4-dimensional Galois representations $\sigma_{S,\lambda}$ are "as large as possible", for almost every prime. We cannot bound the set of exceptional primes with an explicit finite set using the algorithm, because the value of the conductor c of the family is unknown. Instead, we take a "fake" value for this conductor: $c=27\cdot 64$, in a similar way as in [D-V1]. Then, we can bound the set of exceptional primes by a small density set of primes. We only consider primes λ such that $\ell\notin D_1\cup D_2$, where, $D_1:=\{\ell\ :\ \ell\equiv 1\pmod{27}\}\cup\{\ell\ :\ \ell\equiv 1\pmod{32}\}$ and $D_2:=\{\ell\ :\ \ell\equiv -1\pmod{27}\}\cup\{\ell\ :\ \ell\equiv\pm 1\pmod{16}\}$. In terms of Dirichlet density, we are excluding 1/6 of the splitting primes and 1/3 of the inert primes. We executed the algorithm in Pari GP and we found that no exceptional prime greater than 11. Then,

Theorem. *The images of the 4-dimensional Galois representations $\sigma_{S,\lambda}$ are "as large as possible" for every prime λ such that $\ell > 11$ and $\ell \notin D_1 \cup D_2$.*

If we consider the projectivizations of these residual representations, we obtain as a corollary two new families of classical groups over finite fields realized as Galois groups over $\mathbb{Q}$.

Corollary. *Let $\ell > 11$ prime and $\ell \notin D_1 \cup D_2$. Then, the following groups are Galois groups of a finite extension of $\mathbb{Q}$ unramified outside 6ℓ:*
1) $\mathrm{PSL}(4, \mathbb{F}_\ell)$, *if* $\ell \equiv 7 \pmod{12}$.
2) $\mathrm{PSU}(4, \mathbb{F}_\ell)$, *if* $\ell \equiv 2 \pmod{3}$.

References

[D-K-R] M. Dettweiler, U. Kühn, S. Reiter, *On Galois representations via Siegel modular forms of genus two*, Math. Res. Lett. **8** (2001), 577–588.

[D] L. Dieulefait, *On the images of the Galois representations attached to genus 2 Siegel modular forms*, J. Reine Angew. Math. **553** (2002), 183-200.

[D-V1] L. Dieulefait, N. Vila, *On the images of modular and geometric three-dimensional Galois representations*, Amer. J. of Math. **126** (2004), 335-361.

[D-V2] Dieulefait, L., Vila, N., *Geometric families of 4-dimensional Galois representations with generically large images*, preprint.

[K-L] P. Kleidman, M. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. LNS 129, Cambridge University Press, 1990.

[R1] K. A. Ribet , *On ℓ-adic representations attached to modular forms*, Invent. Math. **28**, (1975) 245-275

[Sc] J. Scholten, *A non-selfdual 4-dimensional Galois representation*, www.math.uiuc.edu/-Algebraic-Number-Theory/0183.

[S1] J.-P.Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[S2] ——— , Oeuvres, vol. 4, 1-55, Springer, 2000.

[V] N. Vila, *Arithmetical-Geometrical Galois Representations and the Inverse Galois Problem*, in Algebra, Arithmetic and Geometry with Applications, 775-782, Springer, 2004.

Galois extensions ramified only at one prime

Jing Long Hoelscher

Motivation

For any finite group G, a Dedekind domain D and a finite set S of primes in D, is there a Galois extension $L/Frac(D)$ with ramification only at S? The answer is "No, in general." With given ramification, not every finite group can occur as a Galois group. As the number and the size of ramified primes increases, more finite groups are allowed to occur as Galois groups. And in the "limit", we expect all finite groups to occur.

Question. *Which finite groups can occur as Galois groups of finite branched covers of "curves" with specified branch locus?*

We can ask the above question in the following four settings:

1. Curves over an algebraically closed field k of characteristic 0;
2. Curves over an algebraically closed field k of characteristic $p > 0$;
3. Curves over a finite field;
4. "Curves" of the form $U_n = \mathrm{Spec}(\mathbb{Z}[\frac{1}{n}])$.

The question in the first setting is completely answered by Riemann's Existence Theorem. Abhyankar's Conjecture has answered the question in the second setting. This talk will focus on the last two settings.

Curves over a finite field

By combining the Frobenius action with the branch cycle description of a lift of a tame cover to characteristic 0, we can give some restriction on Galois groups occurring tamely over function fields $\mathbb{F}_q(t)$.

Proposition. *Let K be the function field of a geometric Galois cover of the affine line over $\mathbb{F}_p$ with Galois group G and ramified only at a finite prime $\mathfrak{f}$ and possibly at ∞, with all ramification tame. Then there exist $x_1, x_2, ..., x_d, x_\infty \in G$ such that*

$$\langle x_1, ..., x_d, x_\infty \rangle = G \quad \textit{and} \quad x_1 ... x_d x_\infty = 1$$

with $x_1^p \sim x_2, ..., x_d^p \sim x_1$ and $x_\infty^p \sim x_\infty$ (i.e. conjugate in G). Moreover, the order of each of $x_1, \ldots, x_d$ is equal to the ramification index over $\mathfrak{f}$, and the order of x_∞ is the ramification index at ∞.

Denote $\pi_A^t(U_f)$ the set of finite groups that can occur as Galois groups over $\mathbb{P}^1_{\mathbb{F}_p(t)}$ ramified only at f, we have the following corollaries:

Corollary. *For any integer $k \geq 1$ and any prime f, the dihedral group $D_{4k} \notin \pi_A^t(U_f)$. For the case of D_{4k+2}, when the degree of the prime f is odd, we have $D_{4k+2} \notin \pi_A^t(U_f)$.*

Corollary. *In the case $p = 2$, any symmetric group $S_n \notin \pi_A^t(U_f)$ for any prime f of $\mathbb{F}_p(t)$ and any integer $n > 2$. If $p \neq 2$ and f is of odd degree, then any symmetric group $S_n \notin \pi_A^t(U_f)$ for $n > 2$.*

Cyclotomic function fields

Considering abelian extensions over $\mathbb{F}_q(t)$ ramified at only one prime $f \in \mathbb{F}_q[t]$, i.e. cyclotomic function fields, we have an explicit description of these abelian extensions. We consider a degree d irreducible polynomial $f = \prod_{i=1}^{d}(t - \alpha_i)$, where $\alpha_i \in \mathbb{F}_{q^d}$ are the d roots of f, for $1 \leq i \leq d$.

Theorem. *For $f = \prod_{i=1}^{d}(t-\alpha_i)$ as above, the cyclotomic function field $\mathbb{F}_q(t)(\lambda_f)$ over $\mathbb{F}_q(t)$ is the unique maximal cyclic geometric sub-extension K_0 of the extension $K = \mathbb{F}_{q^d}(t)(y_0)$ over $\mathbb{F}_q(t)$ such that the residue degree of the prime f is 1, where K is the Kummer extension $\mathbb{F}_{q^d}(t)(y_0)/\mathbb{F}_{q^d}(t)$ of degree q^d-1 over the constant extension $\mathbb{F}_{q^d}(t)/\mathbb{F}_q(t)$ and*

$$y_0^{q^d-1} = \prod_{i=1}^{d}(x-\alpha_i)^{q^{d-i}}.$$

We can also get descriptions for general cyclotomic function fields $\mathbb{F}_q(t)(\lambda_f)$ for a general polynomial f. As an application to develop an Iwasawa theory for cyclotomic function fields, I believe I can prove the following:

Conjecture. *Suppose F is any function field of characteristic p. Given F_∞/F ramified only at one prime f with Galois group $\mathrm{Gal}\,(F_\infty/F) \cong \mathbb{Z}_p^2$ and sub-extensions F_{2n+k} for $0 \le k < 2, n \ge 0$ chosen like those in an infinite cyclotomic function fields. If f is totally ramified in F_∞/F, then there exist integers λ, μ_1, μ_2 and ν depending on f such that*

$$e_{2n+k} = \mu_1 p^{2n} + (\lambda n + \mu_2)p^n + \nu.$$

"Curves" of the form $U_n = \mathrm{Spec}(\mathbb{Z}[\frac{1}{n}])$

In this section, we consider finite extensions over $\mathbb{Q}$ ramified only at one finite prime. In the solvable case, we have the following result:

Theorem. *Let K be a finite Galois extension of $\mathbb{Q}$ ramified only at a single finite prime $p > 2$, with the Galois group $G = \mathrm{Gal}\,(K/\mathbb{Q})$ solvable. Let $K_0/\mathbb{Q}$ be an intermediate abelian extension of $K/\mathbb{Q}$. Let $N = \mathrm{Gal}\,(K/K_0)$ and $p(N)$ be the quasi p-part of N. Suppose N is solvable. Then either*

(i) *$N/p(N) \subset \mathbb{Z}/(p-1)$; or*
(ii) *there is a non-trivial abelian unramified subextension $L/K_0(\zeta_p)$ of $K(\zeta_p)/K_0(\zeta_p)$ of degree prime to p with L Galois over $\mathbb{Q}$.*

The above theorem is a generalization of Proposition 2.17 in [Ha] in the case $p = 2$, and it gives evidence for Conjecture 2.1 in [Ha]. Applying the theorem above to dihedral groups or small primes, we have the following corollaries:

Corollary. *Suppose $p \equiv 1 \pmod 4$ is a regular prime such that the class number of $\mathbb{Q}(\sqrt{p})$ is 1 (for example, in the range $2 \le p \le 100$, this is the case when $p = 5, 13, 17, 29, 41, 53, 61, 73, 89, 97$). Then there are no dihedral groups in $\pi_A(U_p)$ except D_2, the cyclic group of order 2.*

The corollary above strengthens the result in [JY], there Jensen and Yui showed that any dihedral extension with Galois group D_{2n} over $\mathbb{Q}$ ramified only at p satisfying that $p \equiv 1 \pmod 4$ is a regular prime has degree not divisible by p.

Corollary. *If G is a solvable group in $\pi_A(U_3)$, then either G is cyclic, or $G/p(G) \cong \mathbb{Z}/2$, or G has a cyclic quotient of order 27.*

Corollary. *Suppose $K/\mathbb{Q}$ is a Galois extension with nontrivial Galois group G, ramified only at 3 and possibly at ∞, with ramification index e. Then 9 divides e unless $G/p(G) \cong \mathbb{Z}/2$ or $G \cong \mathbb{Z}/3$.*

In the non-solvable case, using the Odlyzko discriminant bound, local class field theory and group theory, we can rule out certain non-solvable groups as Galois groups over $\mathbb{Q}$ ramified only at one finite prime.

Proposition. *Let $p < 23$ be a prime number. Then A_5, S_5 and $SL(3,2)$ can not occur as Galois groups over $\mathbb{Q}$ ramified only at the prime p.*

Proposition. *Let $p < 23$ be a prime number. If G is a Galois group over $\mathbb{Q}$ ramified only at the prime p with order ≤ 300, then G is solvable.*

Lastly, we have examples of number fields ramified over $\mathbb{Q}$ at only one prime which admit infinite class towers.

References

[Ha] D. Harbater, *Galois groups with prescribed ramification*, Contemporary Mathematics, **174** (1994), 35-60.

[JY] C. Jensen and N. Yui, *Polynomials with D_p as Galois group*, Journal of Number Theory, **15** (1982).

[LH] J. L. Hoelscher, *Galois extensions ramified at one prime*, thesis, the University of Pennsylvania. (2007)

Iterative q-difference Galois theory

Charlotte Hardouin

Initially, the Galois theory of q-difference equations has been built for q unequal to a root of unity (see for instance [5]). This choice was made in order to avoid the increase of the field of constants to a transcendental field. However, Peter Hendricks has studied this problem in his PhD thesis under the supervision of Marius van der Put (see [2]). In chapter 6 he gave a notion of Galois groups for q-difference equations over $\mathbb{C}(z)$ with $q^m = 1$. His idea was to compare the category $Diff_{\mathbb{C}(z)}$ of q-difference modules over $\mathbb{C}(z)$ with the category $FMod_Z$ of modules over the ring $\mathbb{C}(z^m)[t, t^{-1}]$. He thus obtained an equivalence of categories and a fiber functor from $Diff_{\mathbb{C}(z)}$ with value in the category $Vect_{\mathbb{C}(z^m)}$ of vector spaces of finite dimension over $\mathbb{C}(z^m)$. But this construction is not totally satisfying because we do not want to have such transcendental base fields for Galois groups. By q-deformation of the Iterative differential Galois theory of B.H. Matzat and M. van der Put (see [3]), we consider a family of *iterative q-difference operators* instead of considering just one q-difference operator, and in this way we stop the increase of the constant field and succeed to set up a Picard-Vessiot theory for q-difference equations where q is a root of unity, which is compatible to the classical difference Galois theory of Singer, van der Put.

We will now define the notion of **iterative q-difference rings**. To this purpose, we recall some basic tools of q-difference algebra.

Let C be an algebraically closed field and $q \neq 1$ an element of C. Let $F = C(t)$ be the field of rational functions over C and let σ_q be the automorphism of F given by $\sigma_q(f)(t) = f(qt)$.

Let $k \in \mathbb{Z}$, we denote by $[k]_q! \in C$ the q-factorial of k and by $\binom{r}{k}_q \in C$ the q-binomial coefficient of r to k (see [1]). These elements are the q-analogue of the classical arithmetical factorial and binomial.

Definition 1. *Let R be a q-difference ring extension of F and let $\delta_R^* := (\delta_R^{(k)})_{k\in\mathbb{N}}$ be a collection of maps from R to R. The family δ_R^* is called an **iterative q-difference** of R, if all the following properties are satisfied*

(1) $\delta_R^{(0)} = id.$
(2) $\delta_R^{(1)} = \frac{\sigma_q - id}{(q-1)t}$
(3) $\delta_R^{(k)}(x+y) = \delta_R^{(k)}(x) + \delta_R^{(k)}(y)$
(4) $\delta^{(k)}(ab) = \sum_{i+j=k} \sigma_q^i(\delta_R^{(j)}(a))\delta_R^{(i)}(b).$
(5) $\delta_R^{(i)} \circ \delta_R^{(j)} = \binom{i+j}{i}_q \delta_R^{(i+j)}$

*for all $a, b \in R$ and all $i, j, k \in \mathbb{N}$. The set of such iterative q-differences is denoted by $ID_q(R)$. For $\delta_R^* \in ID_q(R)$, the tuple (R, δ_R^*) is called an **iterative q-difference ring** (ID_q-ring). We say that an element c of R is a constant if $\forall k \in \mathbb{N}^*, \delta_R^{(k)}(c) = 0$. We will denote by $C(R)$ the ring of constants of R.*

I just want to mention that the definition of iterative q-difference is obtained by q-deformation of the notion of iterative derivation of Matztat, van der Put. For instance if q goes to 1, $\delta_R^{(1)}$ goes to the usual derivation $\frac{d}{dt}$ and we also retrieve all the formulas satisfied by iterative derivations.

Main example Let us define an iterative q-difference over the field $F = C(t)$ by setting $\delta_F^{(k)}(t^r) := \binom{r}{k}_q t^r$ for $(r, k) \in (\mathbb{N}^*)^2$ and extending this definition to F by C-linearity and point 4 of the previous definition. Since $\delta_F^{(m)}(t^m) = 1$, the constant field is equal to C.

Till the end, q denotes an n-th prime root of unity, (L, δ_L^*) (resp. (R, δ_R^*)) will denote an ID_q-field (resp. ring), with algebraically closed constant field C. In a very natural way, we can define the notion of iterative q-difference modules over R and we denote this set by $IDM_q(R)$. We then obtain the following theorem.

Theorem 2. *The category $IDM_q(L)$ is a neutral Tannakian category over L with unit object (L, δ_L^*).*

Let us yet define the notion of iterative q-difference equation. To put together the case of zero and positive characteristic, we will need the following notations.

Notations 3.
(1) *If the characteristic of the constants field C of L is zero then let us denote by $(k_C)_{k\in\mathbb{N}}$ the family $(k)_{k\in\mathbb{N}}$,*
(2) *if the characteristic of the constants field C of L is positive equal to p then let us denote by $(k_C)_{k\in\mathbb{N}}$ the family $\{1, (np^k)_{k\in\mathbb{N}}\}$.*

For all $M \in IDM_q(L)$ we can associate a so called **iterative q-difference equation** (ID_qE), i.e a family of equations $\{\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}\}_{k\in\mathbb{N}}$ where the A_k's satisfy some specific relations. As in the classical q-difference Galois theory there is a one to one correspondence between $ID_q(L)$-modules and ID_q-equations.

Now let us define the notion of iterative q-difference Picard-Vessiot ring.

Definition 4. *Let $\{\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}\}_{k\in\mathbb{N}}(ID_qE)$ be an **iterative q-difference equation** defined over L (ID_qE). Let (R, δ_R^*) be an iterative q-difference extension of (L, δ_L^*). A matrix $Y \in Gl_n(R)$ is called a **fundamental solution matrix** for the ID_qE if $\delta_R^{(k_C)}(Y) = A_kY$, $\forall k \in \mathbb{N}$. The ring R is called an **iterative q-difference Picard-vessiot ring** for $ID_qE(M)$ $(IPV_q$-ring) if it fulfills the following conditions :*

(1) *R is a simple ID_q-ring (that means that R contains no proper iterative q-difference ideal),*
(2) *The ID_qE has a fundamental solution matrix Y with coefficients in R,*
(3) *R is generated by the coefficients of Y and $det(Y)^{-1}$.*
(4) *$C(R) = C(L)$*

The fact that the constant field C of L is algebraically closed assures the existence and the uniqueness up to ID_q-isomorphism of iterative q-difference Picard-Vessiot ring. Till the end we will fix R an **iterative q-difference Picard-Vessiot ring** for some ID_qE defined over L. We are now able to define the iterative q-difference Galois group associated to R.

Definition 5. *The group* $\mathrm{Gal(R/L)} := \mathrm{Aut_{ID_q}(R/L)}$ *of all iterative q-difference automorphisms, which induce the identity on L, is called the **iterative q-difference Galois group** of the extension R/L.*

For simplicity, we will assume that the iterative q-difference Picard-Vessiot ring R/L is a domain and that its quotient field E is a separable extension of L. Similarly to the usual difference Galois theory, the iterative q-difference Galois group Gal(R/L) is embedded in $\mathrm{GL}_n(C(L))$ and has a structure of reduced linear algebraic group $\mathcal{G}$ defined over C. Moreover, $Spec(R)$ is a $\mathcal{G}$-torsor. As attended, we obtain the usual Galois correspondence.

Theorem 6 (Galois Correspondence)**.** *There exists an anti-isomorphism of lattices between*

$$\mathfrak{H} = \{\mathcal{H} | \mathcal{H} \subset \mathcal{G} \text{ is a Zariski closed reduced linear algebraic subgroup}\},$$

and

$$\mathfrak{L} = \{T | T \text{ is an intermediate iterative difference field s.t. } E/T \text{ is separable } L \subset T \subset E\}.$$

Moreover if $\mathcal{H} \subset \mathcal{G}$ is a Zariski closed reduced normal subgroup, then $T := E^{\mathcal{H}(C)}$ is an iterative Picard-Vessiot extension of L with Galois group $(\mathcal{G}/\mathcal{H})(C)$.

We could work in more generality by considering schemes, but since it is a work in progress we will restrict ourselves to the previous case.

The interests of building such a theory are multiple. First of all, it fulfils the gap in the q-difference Galois theory generated by the roots of unity. But this study could also provide a good functor of confluence from iterative q-difference modules to iterative differential modules, by following the work of A. Pulita [4]. This idea of a confluence functor is at the moment giving birth to a collaboration with Julia Hartmann. Another goal of this theory will be to obtain a iterative q-difference version of the Grothendieck Conjecture following the work of Lucia di Vizio [1] and the work of Peter Hendricks.

References

[1] L. Di Vizio, *Arithmetic theory of q-difference equations: the q-analogue of Grothendieck-Katz's conjecture on p-curvature*, *Invent. Math.,* 150(3): 517-578, 2002.

[2] P.A. Hendriks, *Algebraic aspects of linear differential and difference equations*, Ph.D Thesis, University of Groningen, 1996.

[3] B.H. Matzat, M. van der Put, *Iterative differential equations and the Abhyankar conjecture*, J. reine angew. Math., 557 (2003),1–52.

[4] A. Pulita, *p-Adic confluence of q-difference equations*, submitted december 4, 2006.

[5] M. van der Put, M. F. Singer, *Galois theory of difference equations*, volume 1666 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1997.

Fundamental group-schemes in positive characteristic

João Pedro Pinto dos Santos

Introduction – The topic of this talk is the study of the Tannakian group scheme associated to the category of stratified sheaves (D-modules) on a smooth scheme over an algebraically closed field of positive characteristic. The details and further references are in [3]. This work is based on [4], [6] and [7].

Let k be an algebraically closed field of positive characteristic p. Let X be a smooth k-scheme. The absolute Frobenius morphism of X will be denoted by F. Let $\mathscr{D}_X$ be the $\mathscr{O}_X$-algebra of k-linear differential operators on X as defined in EGA IV_4, 16.7. Another reference for differential operators is [1, Ch. 2].

Definition 1. *The category of stratified sheaves* $\mathbf{str}(X)$ *is the category whose:*

Objects are: $(\mathscr{E}, \nabla)$ *with* $\mathscr{E}$ *a coherent* $\mathscr{O}_X$*-module and* $\nabla : \mathscr{D}_X \longrightarrow \mathrm{End}_k(\mathscr{E})$ *a homomorphism of* $\mathscr{O}_X$*-algebras.*

Arrows are: *homomorphisms of* $\mathscr{D}_X$*-modules.*

Remark: Our terminology follows that introduced by Grothendieck in [5].

The category $\mathbf{str}(X)$ is abelian, k-linear and tensor. A stratified sheaf is a generalization of an integrable connection. In fact, if Θ_X denotes the sheaf of tangent vectors of X/k (k-linear derivations), then $\Theta_X \subseteq \mathscr{D}_X$ and the condition that ∇ above is a homomorphism of $\mathscr{O}_X$-algebras implies that $\nabla|\Theta_X$ is an integrable connection on $\mathscr{E}$. In characteristic zero these notions are equivalent (see [1, Ch. 2])

but in positive characteristic a stratification is a much stronger condition, as the following lemma shows:

Lemma 2 ([1]). *If $(\mathscr{E}, \nabla)$ is a stratified sheaf, then $\mathscr{E}$ is locally free.*

Note that the $k[x]$-module $k[x]/(x^p)$ is endowed with an integrable connection but is certainly not locally free.

A more convenient description of the category $\mathbf{str}(X)$ can be obtained by iterating Cartier's result on the p-curvature and Frobenius pull-backs. First a definition:

Definition 3. *The category of F-divided sheaves $\mathbf{Fdiv}(X)$ is the category whose:*

Objects are: *sequences of coherent $\mathscr{O}_X$-modules $\{\mathscr{E}_i\}_{i\in\mathbb{N}}$ and isomorphisms of $\mathscr{O}_X$-modules $\sigma_i : F^*\mathscr{E}_{i+1} \longrightarrow \mathscr{E}_i$.*

Arrows are: *projective systems; $\{\alpha_i\} : \{\mathscr{E}_i, \sigma_i\} \longrightarrow \{\mathscr{F}_i, \tau_i\}$ with α_i $\mathscr{O}_X$-linear and $\tau_i \circ F^*(\alpha_{i+1}) = \alpha_i \circ \sigma_i$.*

By flatness of Frobenius, it is easy to see that $\mathbf{Fdiv}(X)$ has a structure of an abelian k-linear category. There is also an obvious tensor product. If $\{\mathscr{E}_i\}$ is an object of $\mathbf{Fdiv}(X)$, then $\mathscr{E}_0$ is locally free. Using this (and the above hinted result of Cartier) we have:

Theorem 4 (N. Katz, [4]). *The categories $\mathbf{Fdiv}(X)$ and $\mathbf{str}(X)$ are equivalent k-linear tensor categories.*

Since all the sheaves in $\mathbf{str}(X)$ and $\mathbf{Fdiv}(X)$ are locally free, given $x_0 \in X(k)$ we obtain the following definition.

Definition 5. *The fundamental group scheme of X at the point x_0,*

$$\Pi_X = \Pi(X, x_0),$$

is the Tannakian group scheme associated to $\mathbf{Fdiv}(X)$ via the fibre functor x_0^*.

For the construction of the Tannakian group scheme see [2, Thm. 2.11].

Structural properties of Π_X – By using a method of Nori which interprets exact tensor functors $\mathscr{L} : \mathrm{Rep}_k(G) \longrightarrow \mathrm{coh}(X)$ we can show:

Theorem 6. *The Frobenius homomorphism $F : \Pi_X \longrightarrow \Pi_X$ is an isomorphism.*

Corollary 7. *i) Any quotient of Π_X is reduced.*
ii) Any pro-finite quotient of Π_X is pro-étale.

The same method of Nori allows us to show that the group of connected components of $\pi_0(\Pi_X)$ is none other than the étale fundamental group seen as a constant group scheme. This is another manifestation of the property "differential equations with finite monodromy are étale coverings". This is silently used in the next result.

Theorem 8. *Assume that X is proper over k. Then the largest unipotent quotient of Π_X, Π_X^{uni}, coincides with the largest unipotent quotient of the étale fundamental group.*

The reader should notice that this is quite particular to positive characteristic as one can see from the example of an elliptic curve over $\mathbb{C}$. The above theorem will enable us to derive more precise information about Π_X from known information on the étale fundamental group π_1^{et}.

THE CASE OF AN ABELIAN VARIETY – Using the results above we come to a good description of Π_X in the case where X is an abelian variety.

Theorem 9. *There is a natural isomorphism*

$$\Pi_X \xrightarrow{\cong} T_p(X) \times \mathrm{Diag}(P),$$

where $T_p(X)$ is the p-adic Tate module (of k-rational points) and $\mathrm{Diag}(P)$ *is the diagonal group scheme* [8, 2.2] *whose character group is*

$$P = \varprojlim \left(\cdots \xrightarrow{[p]} \mathrm{Pic}^0 \xrightarrow{[p]} \mathrm{Pic}^0 \xrightarrow{[p]} \cdots \right).$$

REFERENCES

[1] P. Berthelot and A. Ogus, *Notes on crystalline cohomology*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.

[2] P. Deligne and J. Milne, *Tannakian categories*, Lecture Notes in Mathematics 900, pp. 101–228, Springer-Verlag, Berlin-New York, 1982.

[3] J. P. P. dos Santos, *Fundamental groups for stratified sheaves*, to appear in Journal of Algebra. Available at http://dx.doi.org/10.1016/j.jalgebra.2007.03.005

[4] D. Gieseker, *Flat vector bundles and the fundamental group in non-zero characteristics*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 2 (1975), no. 1, 1–31.

[5] A. Grothendieck, *Crystals and the de Rham cohomology of schemes*. In Dix Exposés sur la Cohomologie des Schémas pp. 306–358 North-Holland, Amsterdam; Masson, Paris, 1968.

[6] M. V. Nori, *On the representations of the fundamental group*, Compositio Math. 33 (1976), no. 1, 29–41.

[7] M. V. Nori, *Ph.D Thesis*, Proc. Indian Acad. Sci. Math. Sci. 91 (1982), no. 2, 73–122.

[8] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, 66. Springer-Verlag, New York-Berlin, 1979.

Reporter: Andreas Röscheisen

Participants

Colas Bardavid
U. F. R. Mathematiques
I. R. M. A. R.
Universite de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex

Prof. Dr. Daniel Bertrand
Institut de Mathematiques
Universite Pierre et Marie Curie
Tour 46, 5eme etage
4 place Jussieu
F-75252 Paris Cedex 05

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

Louis Brewis
Universität Ulm
Abteilung Reine Mathematik
89069 Ulm

Prof. Dr. Anna Cadoret
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Sarah Carr
Institut de Mathematiques
Analyse Algebrique
Universite Pierre et Marie Curie
4, place Jussieu, Case 247
F-75252 Paris Cedex 5

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

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

Prof. Dr. Elie Compoint
Inst. de Mathematiques de Jussieu
Theorie des Nombres Case 247
Universite de Paris VI
4, Place Jussieu
F-75252 Paris

Scott Corry
Department of Mathematics
University of Pennsylvania
Philadelphia , PA 19104-6395
USA

Prof. Dr. Jean-Marc Couveignes
Departement de Mathematiques et
Informatique; UFR S.E.S.
Universite Toulouse II
5, Allee Antonio Machado
F-31058 Toulouse Cedex 9

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

Dr. Joao Pedro dos Santos
U. F. R. Mathematiques
I. R. M. A. R.
Universite de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex

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

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

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

Dr. Charlotte Hardouin
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Dr. Julia Hartmann
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Jing Long Hoelscher
Department of Mathematics
David Rittenhouse Laboratory
University of Pennsylvania
209 South 33rd Street
Philadelphia , PA 19104-6395
USA

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

Prof. Dr. Lourdes Juan
Department of Mathematics
Texas Tech. University
Lubbock , TX 79409-1042
USA

Prof. Dr. Jürgen Klüners
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

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

Prof. Dr. Jerald K. Kovacic
29 E 10th Street
2nd floor
New York , NY 10003
USA

Dr. Arne Ledet
Department of Mathematics
Texas Tech. University
Lubbock , TX 79409-1042
USA

Prof. Dr. Andy R. Magid
Dept. of Mathematics
University of Oklahoma
601 Elm Avenue
Norman , OK 73019-0315
USA

Prof. Dr. Bernard Malgrange
Institut Fourier
UMR 5582; CNRS/UJF
Universite de Grenoble I
100 rue de Maths
F-38402 Saint-Martin d'Heres

Prof. Dr. Gunter Malle
Fachbereich Mathematik
T.U. Kaiserslautern
Erwin-Schrödinger-Straße
67653 Kaiserslautern

Prof. Dr. Michel Matignon
Mathematiques et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

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

Prof. Dr. Claudine Mitschi
Institut de Recherche
Mathematique Avancee
ULP et CNRS
7, rue Rene Descartes
F-67084 Strasbourg Cedex

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

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

An Khuong Nguyen
Mathematisch Instituut
Rijksuniversiteit Groningen
Postbus 800
NL-9700 AV Groningen

Dr. Brian Osserman
Department of Mathematics
University of California
Berkeley , CA 94720-3840
USA

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

Prof. Dr. Rachel Pries
Dept. of Mathematics
Colorado State University
Weber Building
Fort Collins , CO 80523-1874
USA

Prof. Dr. Marius van der Put
Mathematisch Instituut
Rijksuniversiteit Groningen
Postbus 800
NL-9700 AV Groningen

Prof. Dr. Jean-Pierre Ramis
Mathematiques
Laboratoire Topologie et Geometrie
Universite Paul Sabatier
118 route de Narbonne
F-31062 Toulouse Cedex

Prof. Dr. Michel Raynaud
Laboratoire de Mathematiques
Universite Paris Sud (Paris XI)
Batiment 425
F-91405 Orsay Cedex

Magali Rocher
Mathematiques et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Andreas Röscheisen
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg

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

Prof. Dr. Michael F. Singer
Department of Mathematics
North Carolina State University
Campus Box 8205
Raleigh , NC 27695-8205
USA

Dr. Jakob M. Stix
School of Mathematics
Institute for Advanced Study
1 Einstein Drive
Princeton , NJ 08540
USA

Lenny Taelman
Mathematisch Instituut
Rijksuniversiteit Groningen
Postbus 800
NL-9700 AV Groningen

Prof. Dr. Felix Ulmer
U. F. R. Mathematiques
I. R. M. A. R.
Universite de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex

Prof. Dr. Nuria Vila
Facultat de Matematiques
Universitat de Barcelona
Gran Via, 585
E-08071 Barcelona

Prof. Dr. Jacques-Arthur Weil
Mathematiques
Universite de Limoges
U. E. R. des Sciences
123, rue Albert Thomas
F-87060 Limoges Cedex

Dr. Stefan Wewers
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg