Mathematisches Forschungsinstitut Oberwolfach

Report No. 25/2006

Pro-p Extensions of Global Fields and pro-p Groups

Organised by
Nigel Boston (Madison)
John Coates (Cambridge)
Fritz Grunewald (Düsseldorf)

May 21st – May 27th, 2006

Mathematics Subject Classification (2000): 11-06,20-06.

Introduction by the Organisers

The meeting *Pro-p Extensions of Global Fields and pro-p Groups* was organised by Nigel Boston (Madison), John Coates (Cambridge) and Fritz Grunewald (Düsseldorf). As the name of the meeting conveys, a primary aim was to bring together group theorists working in the field of pro-p groups and number theorists interested in pro-p extensions of global fields. The workshop consisted of over 25 talks, supplemented by informal discussions. Topics included: Galois groups of extensions with restricted ramification, self-similar and automata groups, noncommutative Iwasawa theory, groups acting on rooted trees.

This meeting was well attended with over 50 participants; more than 30 of these came from countries other than Germany. The range of topics and the diverse backgrounds of the participants led to a stimulating exchange of recent results, challenging problems and general ideas. The organisers and participants thank the *Mathematisches Forschungsinstitut Oberwolfach* for providing the setting for this successful workshop.

The following extended abstracts appear in the chronological order of the talks; they were collected and edited by Benjamin Klopsch (Düsseldorf).

Workshop: Pro-p Extensions of Global Fields and pro-p Groups

Table of Contents

Abstracts

Finitely generated profinite groups

D. Segal
(joint work with N. Nikolov)

This is a report of joint work with Nikolay Nikolov. An announcement has appeared in [NS1], and full proofs will appear in [NS2].

Our main result is

Theorem 1. *In a finitely generated profinite group, every subgroup of finite index is open.*

This answers Question 7.37 of the 1980 Kourovka Notebook [K], restated as Open Question 4.2.14 in [RZ]. It implies that the topology of a finitely generated profinite group is completely determined by its underlying abstract group structure, and that the category of finitely generated profinite groups is a full subcategory of the category of (abstract) groups.

The proof depends on properties of certain *verbal subgroups*. A group word w is called *d-locally finite* if $F_d/w(F_d)$ is finite (where F_d is the d-generator free group). Now let G be a d-generator profinite group and N a normal subgroup of finite index. It is easy to cook up a d-locally finite word w such that $w(G) \subseteq N$ (by considering the finitely many homomorphisms from F_d into G/N), so Theorem 1 follows from

Theorem 2. *Let G be a d-generator profinite group and let w be a d-locally finite group word. Then the verbal subgroup $w(G)$ is open in G.*

(By $w(G)$ we mean the subgroup generated *algebraically*, not topologically, by the values of w in G). Though not necessary for Theorem 1, the following variation is also of interest:

Theorem 3. *Let G be a finitely generated profinite group and H a closed normal subgroup of G. Then the subgroup $[H, G]$ generated (algebraically) by all commutators $[h, g]$ ($h \in H$, $g \in G$) is closed in G.*

This implies in particular that *the (algebraic) derived group G' is closed*, and (by an obvious induction) that *every term of the (algebraic) lower central series of G is also closed.*

Thus $w(G)$ is closed if (a) w is a locally finite word or (b) w is one of the words $[x_1, \ldots, x_n]$ with $n \geq 2$. This does *not* hold for arbitrary words, however: Romankov [Ro] has shown that it fails (even in pro-p groups) for the "2nd derived word" $w = [[x_1, x_2], [x_3, x_4]]$. On the other hand, it seems likely that it does hold for the "Burnside words" $w = x^q$; indeed, we can prove that the verbal subgroup G^q is closed in a finitely generated profinite group G provided G does not involve all finite groups as open sections.

If the word w is d-locally finite and G is a d-generator profinite group, then $w(G)$ is open if and only if it is closed. A simple compactness argument then shows that Theorem 2 is equivalent to the following result about finite groups:

Theorem 4. *Let d be a natural number and let w be a d-locally finite group word. Then there exists $f = f_w(d)$ such that if G is any d-generator finite group, then every element of $w(G)$ is equal to a product of f w-values.*

(By *w-values* here we mean elements of the form $w(g_1, \ldots, g_k)^{\pm 1}$.)

Similarly, Theorem 3 follows from

Theorem 5. *Let d be a natural number. Then there exists $g = g(d)$ such that if G is any d-generator finite group and H is any normal subgroup of G, then every element of $[H, G]$ is equal to a product of g commutators $[u, v]$ with $u \in H$ and $v \in G$.*

These theorems are applications of our main technical result, which is as follows. Before stating it let us introduce some notation. For any subset S of a group G and natural number n, $S^{*n} = \{s_1 s_2 \ldots s_n \mid s_1, \ldots, s_n \in S\}$. For $g \in G$ and S, $T \subseteq G$, $[S, g] = \{[s, g] \mid s \in S\}$, $\mathfrak{c}(S, T) = \{[s, t] \mid s \in S,\, t \in T\}$. For an integer q we write $G^{\{q\}} = \{g^q \mid g \in G\}$.

Key Theorem *There exist numerical functions h_1, h_2 and z and an absolute constant D with the following property. Let $G = \langle g_1, \ldots, g_d \rangle$ be a finite group and H a subgroup such that* (i) *$H = [H, G]$,* (ii) *if $H \geq N > Z$, where N and Z are normal subgroups of G and N/Z is non-abelian, then N/Z is neither simple nor the direct product of two isomorphic simple groups. Then*

$$(\mathrm{A}): \qquad H = ([H, g_1] \cdot \ldots \cdot [H, g_d])^{*h_1(d,q)} \cdot (H^{\{q\}})^{*z(q)}$$

for each $q \in \mathbb{N}$, and

$$(\mathrm{B}): \qquad H = ([H, g_1] \cdot \ldots \cdot [H, g_d])^{*h_2(d)} \cdot \mathfrak{c}(H, H)^{*D}.$$

The deduction of Theorem 4 is not quite direct. One applies the Key Theorem not to G itself but to the group $w(G)$, which is generated by a bounded number of w-values $g_1, \ldots, g_{d'}$. We take $q = |C_\infty / w(C_\infty)|$, and find a characteristic subgroup H of $w(G)$ such that (a) the pair $(w(G), H)$ satisfies the hypotheses of the Key Theorem and (b) Theorem 4 is already known for the quotient group G/H. The result then follows from (A) on noting that each element $[h, g_i]$ is a product of two w-values and each element h^q is a w-value. Theorem 5 is deduced in a similar way from Key Theorem (B).

The proof of the Key Theorem is long and elaborate; it is modelled in principle on Hensel's Lemma. Given an arbitrary element $h \in H$ we have to solve an equation of the form $h = \Phi(u_1, \ldots, u_m)$ where Φ is a group word involving the 'unknowns' u_i, to be found in H, and some 'constants' $g_1, \ldots, g_m \in G$. We assume inductively that this can be done modulo K, where K is some small normal subgroup of G inside H, and then have to kill the error term by adjusting the unknowns. This comes down to solving a new system of equations in K (or perhaps a slightly larger normal subgroup), considered as a G-operator group.

The possibility of doing this depends ultimately on properties of the finite simple groups. Let α, β be automorphisms of a group G. For $x, y \in G$, we define the "twisted commutator"

$$T_{\alpha,\beta}(x,y) = x^{-1}y^{-1}x^{\alpha}y^{\beta}.$$

Theorem 6. *There is an absolute constant D such that if S is a finite quasisimple group and α_i, β_i $(i = 1, \ldots, D)$ are any automorphisms of S then*

$$S = T_{\alpha_1,\beta_1}(S,S) \cdot \ldots \cdot T_{\alpha_D,\beta_D}(S,S).$$

Theorem 7. *Let q be a natural number. There exist natural numbers $C = C(q)$ and $M = M(q)$ such that if S is a finite quasisimple group with $|S| > C$, β_i $(i = 1, \ldots, M)$ are any automorphisms of S, and q_i $(i = 1, \ldots, M)$ are any divisors of q, then there exist inner automorphisms α_i of S such that*

$$S = [S, (\alpha_1\beta_1)^{q_1}] \cdot \ldots \cdot [S, (\alpha_M\beta_M)^{q_M}].$$

These generalize several known results about products of commutators and products of powers in simple groups. They are proved by a delicate analysis of the internal structure of the groups, known from the Classification, together with recent results of Liebeck, Pyber and Shalev [LP], [LS].

References

[K] *Kourovka Notebook*, 7th ed., Novosibirsk, 1980.

[LP] M. W. Liebeck and L. Pyber, Finite linear groups and bounded generation, *Duke Math. J.* **107** (2001), 159-171.

[LS] M. W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383-406.

[RZ] L. Ribes and P. A. Zalesskii, *Profinite groups.* Ergebnisse der Math. **40**, Springer, Berlin – Heidelberg , 2000.

[NS1] N. Nikolov and D. Segal, Finite index subgroups in profinite groups, *C. R. Acad. Sci. Paris I* **337** (2003), 303-308.

[NS2] N. Nikolov and D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds; II: products in quasimple groups, *Annals of Math.*, to appear

[Ro] V. A. Roman'kov, Width of verbal subgroups in solvable groups, *Algebra i Logika* **21** (1982), 60-72 (*Russian*); Algebra and Logic **21** (1982), 41-49 (*English*).

Noncommutative Iwasawa algebras

Ken Brown

(joint work with Konstantin Ardakov)

I review the definition of noncommutative Iwasawa algebras, fixing notation for later talks, and give a review of some known and unknown ring-theoretic properties of these algebras. Further details can be found in [2].

1. Definitions. Let G be a compact $p-$adic analytic group, so G is a topological group which has the structure of a p-adic analytic manifold. By work of Lazard,

[5], a topological group G is compact p-adic analytic if and only if G is profinite, with an open subgroup which is pro-p of finite rank, if and only if G is a closed subgroup of $GL_d(\mathbb{Z}_p)$ for some $d \geq 1$. The *Iwasawa algebra of* G is

$$\Lambda_G \quad := \quad \varprojlim \mathbb{Z}_p[G/N],$$

where the inverse limit is taken over the open normal subgroups N of G. Closely related to Λ_G is its epimorphic image Ω_G, defined as

$$\Omega_G \quad = \quad \varprojlim \mathbb{F}_p[G/N],$$

where $\mathbb{F}_p$ is the field of p elements. Often, a property of Λ_G can easily be deduced from the corresponding property of Ω_G, and vice versa; where this is routine we will occasionally save space by stating only one of the two variants.

Suppose that H is an open normal subgroup of the compact p-adic analytic group G. Let $\mathcal{C}_H$ denote the set of open normal subgroups of G which are contained in H. Then clearly $\Lambda_G = \varprojlim \mathbb{Z}_p[G/U]$ where U runs over $\mathcal{C}_H$, and so it follows at once that

$$\Lambda_G \quad \cong \quad \Lambda_H * (G/H), \tag{1}$$

a crossed product of Λ_H by the finite group G/H. We shall see that, combined with a judicious choice of the subgroup H, the isomorphism (1) reduces many questions about Λ_G and Ω_G to the analysis of certain crossed products of finite groups. Usually, the right subgroup H to choose is a *uniform* one, defined as follows.

Let G be a pro-p group. Define $P_1(G) = G$ and $P_{i+1}(G) = \overline{P_i(G)^p[P_i(G), G]}$ for $i \geq 1$. The decreasing chain of characteristic subgroups

$$G = P_1(G) \supseteq P_2(G) \supseteq \cdots \supseteq P_i(G) \supseteq \cdots \supseteq \cap_{i=1}^{\infty} P_i(G) = 1$$

is called the *lower p-series* of G. The group G is *powerful* if $G/\overline{G^p}$ is abelian (for p odd), or $G/\overline{G^4}$ is abelian (when $p = 2$). Finally, G is *uniform* if it is powerful, finitely generated, and

$$|G : P_2(G)| = |P_i(G) : P_{i+1}(G)|$$

for all $i \geq 1$.

Now we can add one further characterisation of a $p-$adic analytic group, also essentially due to Lazard, to those given above: a topological group G is compact p-adic analytic if and only if it has an open normal uniform pro-p subgroup of finite index, [3, Corollary 8.34].

2. Ring-theoretic properties. Consider first the Iwasawa algebra of a uniform group. Crucial to understanding this case is the following result, which essentially dates back to Lazard [5].

Theorem 1. *Let U be a uniform pro-p group, and let I denote the augmentation ideal of the ordinary group algebra $\mathbb{F}_p[U]$.*

(1) Ω_U is isomorphic to the I-adic completion of $\mathbb{F}_p[U]$. There is a similar result for $\mathbb{Z}_p[U]$.

(2) *From the first part, Ω_U is local with Jacobson radical $J := I\Omega_U$. The graded ring of Ω_U with respect to the J-adic filtration is isomorphic to a polynomial ring in $d = \dim U$ variables:*

$$\mathrm{gr}_J \Omega_U \cong \mathbb{F}_p[X_1, \ldots, X_d].$$

Many of the fundamental properties of Ω_G and Λ_G for an arbitrary $p-$adic analytic group G can be deduced from this theorem and the crossed product decomposition (1). Before stating a portmanteau result we recall some terminology. A ring R is *semilocal* if the factor of R by its Jacobson radical $J(R)$ is semisimple artinian. It is *local* if $R/J(R)$ is simple artinian, and *scalar local* if $R/J(R)$ is a division ring. A ring R is *prime* if the product of two nonzero ideals is again nonzero; R is *semiprime* if it has no nonzero nilpotent ideals.

Corollary. *Let G be a compact p-adic analytic group of dimension d..*

(1) *Ω_G and Λ_G are complete noetherian semilocal rings.*

(2) *Ω_G and Λ_G are (scalar) local rings if and only if G is a pro-p group.*

(3) *Ω_G and Λ_G are prime if and only if G has no non-trivial finite normal subgroups.*

(4) *Ω_G is semiprime if and only if G has no non-trivial finite normal subgroups of order divisible by p. Λ_G is always semiprime.*

(5) *Ω_G and Λ_G are domains if and only if G is torsion free.*

(6) *Ω_G and Λ_G have finite global dimension if and only if G has no elements of order p, and in this case their global dimensions are d and $d+1$ respectively.*

(7) *Ω_G and Λ_G are Auslander-Gorenstein rings of dimensions d and $d+1$ respectively.*

The *Auslander-Gorenstein property* is the “correct” generalisation to noncommutative noetherian rings of the commutative Gorenstein property; its precise definition can be found at [2, 3.5], for example. Amongst many advantageous consequences, the presence of this property allows one to introduce a very natural dimension for modules over Iwasawa algebras, called the *canonical dimension*, generalising the Krull dimension of the commutative case. How this works is explained in [2].

The results in the above corollary are due to Lazard, Neumann, Venjakob and Ardakov-Brown. For detailed attributions, see [2].

3. Two-sided ideal structure. One of the first questions asked when studying a noetherian algebra is “what are its two-sided ideals?” It is usually sensible to focus first on the prime ideals. There are two natural mechanisms for constructing prime ideals of Ω_G: one can take (a minimal prime containing) the ideal of Ω_G generated by the augmentation ideal of a normal subgroup of G; and one can take (a minimal prime containing) the ideal $P\Omega_G$ of Ω_G generated by a prime ideal P of the centre $Z(\Omega_G)$ of Ω_G. Both methods are quite well understood, the second by virtue of the

Theorem 2. [1] *Let G be a uniform pro-p group and let Z be its centre. Then the centre of Ω_G equals Ω_Z and the centre of Λ_G equals Λ_Z.*

The above two methods can obviously be combined, applying first the first, then the second to the resulting factor. Naturally, one is led to ask whether *every* prime ideal of Ω_G arises in essentially this way. At present, this question is completely open. A special case is particularly important for applications - suppose that G is *almost simple*, meaning that it is a uniform pro-p group whose Lie algebra has no non-trivial ideals, so that $Z(\Omega_G) = \mathbb{F}_p$ and every nontrivial normal subgroup of G has finite index. The simplest non-trivial example thus arises when G is a congruence subgroup in $SL(2, \mathbb{Z}_p)$. We therefore ask:
Question. Let G be almost simple. Are $\{0\}$ and the Jacobson radical the only prime ideals of Ω_G?

M. Harris [4] claimed to have answered this in the negative, but unfortunately there is a gap in his proof.

References

[1] K. Ardakov, *The centre of completed group algebras of pro-p groups*, Doc. Math **9** (2004), 599-606.
[2] K. Ardakov and K. A. Brown, *Ring-theoretic properties of Iwasawa algebras: a survey*, arXiv math.RA/0511345.
[3] J.D.Dixon, M.P.F. Du Sautoy, A.Mann, D.Segal, *Analytic pro-p groups*, 2nd edition, CUP (1999).
[4] M. Harris, *The annihilators of p-Adic induced Modules*, J.Algebra **67**, 68-71 (1980).
[5] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. IHES **26** (1965), 389-603.

The word width of pro-p groups

A. Jaikin-Zapirain
(joint work with P. Shumyatsky)

Let G be a profinite group, F a free group on k independent generators and $w \in F$. We say that $g \in G$ is a w-**value** in G if there are $g_1, \dots, g_k \in G$ such that $g = w(g_1, \dots, g_k)^{\pm 1}$. We denote by $G^{\{w\}}$ the set of all the w-values in G and by $w(G) = \langle w(g_1, \dots g_k) | g_1, \dots g_k \in G \rangle$ the subgroup of G generated (algebraically) by the w-values of G. A standard argument shows that $w(G)$ is closed if and only if there exists l such that any element from $w(G)$ is a product of at most l elements from $G^{\{w\}}$. The smallest such number l is called the **width** of w in G. In my talk I present the following two results.

Theorem 1. *Let G be a compact p-adic analytic group, F a free group and $w \in F$. Then the group $w(G)$ is closed.*

Theorem 2 (joint result with Pavel Shumyatsky)**.** *Let F be a free group and $w \in F$. Then $w(G)$ is closed for any finitely generated pro-p group G if and only if $w \notin (F')^p F''$.*

Pro-p groups and towers of rational homology spheres

J. S. Ellenberg
(joint work with N. Boston)

In the recent paper [2], Calegari and Dunfield exhibit a sequence of hyperbolic 3-manifolds which have increasing injectivity radius, and which, subject to some conjectures in number theory, are rational homology spheres. We prove unconditionally in [1] that these manifolds are rational homology spheres, and give a sufficient condition for a tower of hyperbolic 3-manifolds to have first Betti number 0 at each level.

We prove this theorem purely by the methods of pro-p group theory, without any appeal to number theory. Consequently, the methods yield unconditional results and are not restricted to arithmetic 3-manifolds. The main idea is that the sequence of 3-manifolds considered by Calegari and Dunfield is in fact a tower of Galois covers of a base manifold M_0, which corresponds to a homomorphism from $\pi_1(M_0)$ to a pro-p p-adic Lie group G. Then the first Betti number of the various covers in this tower can be computed as the $\mathbf{Z}_p$-rank of the abelianization of some finite-index subgroup of the pro-p completion of $\pi_1(M_0)$. The content of our theorem is that this pro-p completion is in fact identical with G; it is then a standard fact that all finite-index subgroups of G have finite abelianization, so that the first Betti numbers of the 3-manifolds described in [2] are all zero.

References

[1] N. Boston and J. S. Ellenberg. Pro-p groups and towers of rational homology spheres. *Geometry and Topology* 10, 331–334 (2006).

[2] F. Calegari and N. Dunfield. Automorphic forms and rational homology 3-spheres. *Geometry and Topology* 10, 295-329 (2006).

Galois groups of unramified pro-p extensions

R. T. Sharifi

Let p be an odd prime, and let F be a number field. For a pro-p Galois extension L of F that is unramified outside a finite set of primes S of F including those above p, we consider the following two questions, in obvious descending order of difficulty:

1. What is the Galois group $\mathcal{G}_L$ of the maximal unramified pro-p extension of L?
2. What is the maximal abelian quotient X_L of $\mathcal{G}_L$?

These groups are in general far from understood. We focus in this talk on the case that L contains the cyclotomic $\mathbf{Z}_p$-extension K of F.

We use Λ to denote the Iwasawa algebra, i.e., the completed $\mathbf{Z}_p$-group ring, of $\mathrm{Gal}(K/F)$. In the fundamental case that $F = \mathbf{Q}(\mu_p)$ for an odd prime p, we have a good but partial understanding of the Λ-module structure of X_K by work of Iwasawa (e.g., [I]), Ferrero-Washington [FW], and Mazur-Wiles [MW], among others. On the other hand, even in this case that $F = \mathbf{Q}(\mu_p)$, we have little understanding of $\mathcal{G}_K$ if the $\mathbf{Z}_p$-rank of X_K is greater than 1. Furthermore, we have little understanding of X_L for L non-abelian over its totally real subfields.

We describe two results by way of example. First, consider the compositum $\tilde{F}$ of all $\mathbf{Z}_p$-extensions of F. Let $\tilde{\Lambda}$ denote the Iwasawa algebra of $\mathrm{Gal}(\tilde{F}/F)$ over $\mathbf{Z}_p$. We say that a $\tilde{\Lambda}$-module M is *pseudo-null* if its annihilator has height at least 2 in $\tilde{\Lambda}$. R. Greenberg made the following conjecture (see [G], for instance).

Conjecture (Greenberg)**.** *For any number field F, the Galois group $X_{\tilde{F}}$ is pseudo-null as a $\tilde{\Lambda}$-module.*

We have the following.

Theorem 1. *Greenberg's conjecture holds for $F = \mathbf{Q}(\mu_p)$ and $p < 1000$.*

As for the Galois group $\mathcal{G}_L$, we have the following.

Theorem 2. *Let $F = \mathbf{Q}(\mu_p)$. The group $\mathcal{G}_K$ is abelian for $p < 1000$ and non-abelian for $p = 1217$, 7069, and 9829.*

As a corollary, the p-Hilbert class tower of $\mathbf{Q}(\mu_p)$ is finite for all primes $p < 1000$, the maximal unramified extension of $\mathbf{Q}(\mu_p)$ being abelian in these cases. For the 14 primes less than 1000 with p-rank at least 2, this runs contrary to previous results in the literature.

The proofs of Theorems 1 and 2 are given in [S3]. We describe only the main ideas here. The key lies in understanding the behavior of Iwasawa modules in $\mathbf{Z}_p$-extensions. In our description, let us take $F = \mathbf{Q}(\mu_p)$. We suppose that E/K is an $\mathbf{Z}_p$-extension that is unramified outside p, and we set $H = \mathrm{Gal}(E/K)$. We then have exact sequences of Λ-modules (see [HS, S1]):

$$0 \to (X_E)_H \to X_K \to H/H_p \to 0 \tag{1}$$

$$0 \to I_H X_E / I_H^2 X_E \to \frac{X_K \otimes_{\mathbf{Z}_p} H}{\mathrm{im}\,\Psi_{E/K}} \to H \otimes_{\mathbf{Z}_p} H/H_p \to 0, \tag{2}$$

where I_H denotes the augmentation ideal in the Iwasawa algebra of H, where H_p denotes the decomposition group at the unique prime above p in K, and where $\Psi_{E/K}$ is a map to be described shortly. More generally, we have longer exact sequences relating X_L to X_K in our original setting, supposing that L/K is a $\mathbf{Z}_p$-extension [S2].

We must describe the homomorphism $\Psi_{E/K}$. Let $\mathcal{U}_K$ denote the group of norm compatible sequences of elements of the p-completion of the p-units in intermediate number fields in K. Let $X_{E/K}$ denote the image of the restriction map $X_E \to X_K$. Then

$$\Psi_{E/K} \colon \mathcal{U}_K \to X_{E/K} \otimes_{\mathbf{Z}_p} H$$

can be defined either as a certain coboundary map or via cup products on certain inverse limits of Galois cohomology groups.

We sketch the proofs very briefly. First, suppose that the map $\Psi_{E/K}$ is surjective. Then the last two terms in (2) are isomorphic, so $X_E \cong (X_E)_H$ has finite

$\mathbf{Z}_p$-rank less than or equal to that of X_K. If we knew this for some E/K abelian over F, then we could conclude that X_E was pseudo-null as a module over the Iwasawa algebra of $\mathrm{Gal}(E/F)$. From this, Greenberg's conjecture would follow.

As for Theorem 2, let M denote the maximal unramified pro-p extension of K, and suppose certain mild conditions on p which imply, for instance, that M is a compositum of unramified $\mathbf{Z}_p$-extensions E of K Galois over F. Knowing the surjectivity for all such E/K is then enough to assure that $X_M = 0$. Of course, since $X_K = \mathrm{Gal}(M/K)$, this forces $\mathcal{G}_K$ to be abelian. Similarly, one can prove a converse to this result.

Theorems 1 and 2 are therefore reduced to verifying the surjectivity of certain of the maps $\Psi_{E/K}$. We need only determine the images of these maps modulo the maximal ideal of Λ. In turn, it is enough for this to compute the values of a pairing

$$\mathcal{O}_{F,S}^{\times} \times \mathcal{O}_{F,S}^{\times} \to A_F \otimes \mu_p,$$

where $\mathcal{O}_{F,S}$ is the ring of p-integers in F and A_F is the p-part of the class group of F. This pairing arises via Kummer theory from the cup product in the Galois cohomology of the maximal unramified outside p extension of the field $F = \mathbf{Q}(\mu_p)$. For $p < 25{,}000$, a conjectural computation of this pairing has been given in terms of tables of its values on cyclotomic p-units [McS]. For $p < 1000$, this conjecture has been verified [S1]. Checking the tables yields the results.

References

[FW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. Math.* **109** (1979), 377–395.

[G] R. Greenberg, Iwasawa theory - past and present, in "Class Field Theory: its Centenary and Prospect," *Adv. Stud. Pure Math.* **30**, Math. Soc. Japan, Tokyo, 335–385.

[HS] Y. Hachimori and R. Sharifi, On the failure of pseudo-nullity of Iwasawa modules, *J. Alg. Geom.* **14** (2005), 567–591.

[I] K. Iwasawa, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Inv. Math.* **76** (1984), 179–330.

[McS] W. McCallum and R. Sharifi, A cup product in the Galois cohomology of number fields, *Duke Math. J.* **120** (2003), 269–310.

[S1] R. Sharifi, Iwasawa theory and the Eisenstein ideal, to appear in *Duke Math. J.*.

[S2] R. Sharifi, The augmentation filtration in Iwasawa theory, in preparation.

[S3] R. Sharifi, On Galois groups of unramified pro-p extensions, in preparation.

Classifying finite p-groups up to isomorphism by coclass

C. R. Leedham-Green

(joint work with B. Eick)

Reporter's Note: *The following summary is based on the speaker's handwritten entry in the Vortragsbuch.*

The objective is to attain the clearly impossible goal of classifying all finite p-groups up to isomorphism. This is to be carried out by reducing the classification of all p-groups of coclass r to a finite calculation for all (p, r), p prime and $r \geq 1$. That is to say, a separate calculation for each pair.

The case $p = 2$ is complete, and produces a more explicit version of a theorem of Marcus du Sautoy. We expect to produce similar but more complicated results for $p > 2$. In this report the assumption, made in all other talks in this workshop, that $p > 2$ is replaced by the assumption that $p = 2$.

Consider the case $r = 1$. The classification of the 2-groups of coclass 1 is a trivial exercise. If $n \geq 4$ there are three isomorphism classes of 2-groups of maximal class whose order is 2^n: D_{2^n}, Q_{2^n}, SD_{2^n}. In the present context we prove this as follows.

Lemma 1. *Let G be a 2-group of coclass 1 whose order is 2^n. Then G has a normal subgroup N such that*

(i) *N is cyclic of order 2^{n-2};*
(ii) *$G/N \cong C_2 \times C_2$;*
(iii) *$G/N = \langle a, b\rangle$ where $x^a = x^{-1}$ and $x^b = x$ for all $x \in N$.*

Thus $G = \mathbb{Z}_2/2^{n-2}\mathbb{Z}_2.R$ where $R = \langle a, b\rangle$ and R acts on $\mathbb{Z}_2$ as in (iii) (but with $x^a = -x$ as $\mathbb{Z}_2$ is written additively), and $2^{n-2}\mathbb{Z}_2$ is the unique R-submodule of $\mathbb{Z}_2$ of index 2^{n-2}. The next step is to compute $\mathrm{H}^2(R, \mathbb{Z}_2/2^{n-2}\mathbb{Z}_2)$.

Lemma 2. *There is a natural isomorphism*

$$\alpha : \mathrm{H}^2(R, \mathbb{Z}_2/2^{n-2}\mathbb{Z}_2) \cong \mathrm{H}^2(R, \mathbb{Z}_2) \oplus \mathrm{H}^3(R, \mathbb{Z}_2).$$

Lemma 3. $\chi \in \mathrm{H}^2(R, \mathbb{Z}_2/2^{n-2}\mathbb{Z}_2)$ *defines a 2-group of coclass 1 if and only if $\alpha(x) = (\theta, \phi)$, where $\theta \in \mathrm{H}^2(R, \mathbb{Z}_2)$ defines $D_{2^\infty} = \varprojlim D_{2^m} = \mathbb{Z}_2 : C_2(\alpha)$.*

Thus the 2-groups of coclass 1 are determined by the elements of $\mathrm{H}^3(R, \mathbb{Z}_2)$.

Lemma 4. $\mathrm{H}^3(R, \mathbb{Z}_2) \cong C_2 \times C_2$.

Lemma 5. *The four cohomology classes in Lemma 4 give rise to three distinct isomorphism classes of groups.*

The calculations required to prove Lemmas 4 and 5 can be avoided as follows. Both of the calculations are transparently independent of n. (In the given context we should perhaps write $\mathrm{H}^3(R, 2^{n-2}\mathbb{Z}_2)$ rather than $\mathrm{H}^3(R, \mathbb{Z}_2)$.)So if we determine the groups of order 2^4 and class 3 in any way whatsoever a similar result will follow for the groups of order 2^n and coclass 1 for any $n \geq 4$.

The surprising fact is that this proof generalises to give a similar result for 2-groups of any coclass: The argument can be generalised to deal with any given coclass by using the full force of the coclass project, as described in [2], and made more precise so as to give parametrised presentations of the groups.

The case of general r depends critically on the deep result that asserts that there are only finitely many isomorphism classes of pro-p-groups of coclass r, for given (p, r), and that these are abelian by finite. Classifying finite p-groups by rank (where the rank of a group G is the least integer r such that $d(H) \leq r$ for all $H \leq G$) would require the analysis of p-adic analytic pro-p-groups as in [1].

The classification of wider classes of pro-p-groups such as the class of hereditarily just infinite pro-p-groups of finite obliquity would be a major advance. We know no way of attacking such problems.

References

[1] F. Klaas, C. R. Leedham-Green, W. Plesken, *Linear pro-p-groups of finite width*, Lecture Notes in Mathematics **1674**, Springer-Verlag, Berlin, 1997.

[2] C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, London Mathematical Society Monographs **27**, Oxford University Press, Oxford, 2002.

Hanoi Towers group on 3 pegs and its pro-finite closure

R. I. Grigorchuk

(joint work with V. Nekrashevych, Z. Šunić)

Hanoi Towers problem

The well known Hanoi Towers Problem on 3 pegs was invented by Edouard Lucas in 1883. Given 3 pegs, labeled by $0, 1, 2$ and n disks of different size, labeled by $1, \ldots, n$ as they increase in size, a configuration is any placement of the disks on the pegs such that no disk is placed on a smaller disk. In a single move a single disk from the top of one peg can be moved to the top of another peg as long as the new placement of disks is a valid configuration. Initially, all disks are placed on one peg, say 0, and the goal is to move them all to another peg in the smallest possible number of moves.

Algebraic model by a self-similar group

Configurations on n disks can be represented by words of length n over the 3-letter alphabet $X = \{0, 1, 2\}$. The word $x_1 \ldots x_n$ represents the unique configuration in which the disk i is placed on peg x_i. The set X^* of words over X ordered by the prefix relation has the structure of a rooted ternary tree, denoted $\mathcal{T}$. For $0 \leq i < j \leq 2$, let a_{ij} be the automorphism of $\mathcal{T}$ defined recursively by

$$a_{ij}(iw) = jw, \qquad a_{ij}(jw) = iw, \qquad a_{ij}(xw) = xa_{ij}(w), \text{ for } x \notin \{i, j\},$$

for $w \in X^*$. The automorphism a_{ij} acts on $\mathcal{T}$ in a such a way that each configuration in the Hanoi Towers Problem is mapped to the configuration resulting after a move is performed between peg i and peg j (configurations in which both peg i and peg j are empty do not change under this move).

Definition. The Hanoi Towers group (on 3 pegs) is the group $H \leq \mathsf{Aut}(\mathcal{T})$, defined by

$$H = \langle\ a_{01},\ a_{02},\ a_{12}\ \rangle$$

The Schreier graph of the action of H on level n in the ternary tree $\mathcal{T}$ is the graph of all configurations on n disks in Hanoi Towers Problem. For example, the Schreier graph for 3 disks is given in the left half of Figure 1 (the meaning of the labels is $a = a_{01}$, $b = a_{02}$ and $c = a_{12}$).

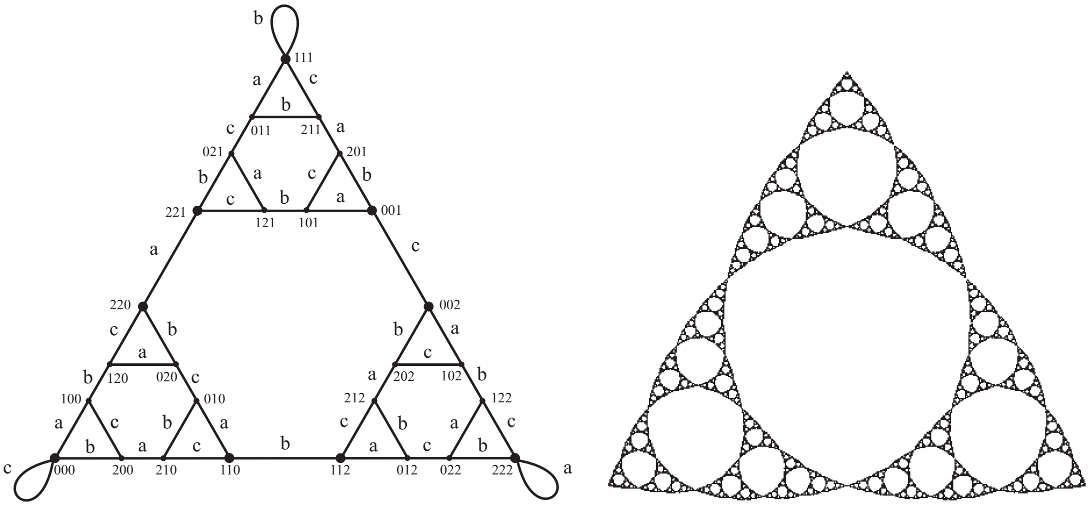


FIGURE 1. Schreier graph of H at level 3 and the limit space of H

Denote by $\bar{H}$ the closure of H in the pro-finite group $\mathsf{Aut}(\mathcal{T})$.

RESULTS

Theorem. *The Hanoi Towers group H has the following properties:*

(i) *H is amenable*

(ii) *H is not elementary amenable (moreover, H is not sub-exponentially amenable)*

(iii) *H is a regular branch group over its commutator subgroup $[H, H]$.*

(iv) *H is not just infinite.*

(v) *H has exponential growth.*

(vi) *H is conjugate in $\mathsf{Aut}(\mathcal{T})$ to the iterated monodromy group $IMG(f)$ of the rational map $f(z) = z^2 - \frac{16}{27z}$, whose self-similar action on the ternary rooted tree $\mathcal{T}$ is given by*

$$\alpha = (01)\ (1, 1, \beta)$$

$$\beta = (02)\ (1, \alpha, 1)$$

$$\gamma = (12)\ (\gamma, 1, 1)$$

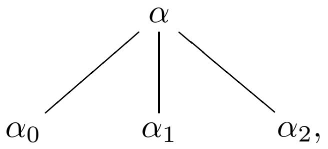
(vii) *The limit space of H and the Julia set of the rational map f are homeomorphic to the Sierpiński gasket.*

(viii) *The closure $\bar{H}$ is the Galois group of the tower of extensions of the field of rational functions $\mathbb{C}(t)$, determined by the polynomial equations*

$$f^{(n)}(z) = t, \quad n = 1, 2, 3, \ldots,$$

where $f^{(n)}$ denotes the n-fold composition of the rational map f.

(ix) *The closure $\bar{H}$ is a finitely constrained group. The forbidden patterns are all the patterns of the form*



where $\alpha, \alpha_0, \alpha_1, \alpha_2$ are permutations in S_3 such that

$$\mathsf{sgn}(\alpha) \neq \mathsf{sgn}(\alpha_0) + \mathsf{sgn}(\alpha_1) + \mathsf{sgn}(\alpha_2).$$

Further details on Hanoi Towers groups, self-similar groups and iterated monodromy groups can be found in [GŠ06] and [Nek05],

References

[GŠ06] Rostislav Grigorchuk and Zoran Šunik̀. Asymptotic aspects of Schreier graphs and Hanoi Towers groups. accepted in C. R. Math. Acad. Sci. Paris, arxiv math.GR/0601592, 2006.

[Nek05] Volodymyr Nekrashevych. *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.

On the leading terms of p-adic L-functions in non-commutative Iwasawa theory

O. Venjakob
(joint work with D. Burns)

In the last few years there have been several significant developments in non-commutative Iwasawa theory.

Firstly, in [5] a main conjecture for elliptic curves without complex multiplication was formulated. More precisely, if F_∞ is any Galois extension of a number field F which contains the cyclotomic $\mathbb{Z}_p$-extension F_{cyc} of F and is such that $\mathrm{Gal}(F_\infty/F)$ is a compact p-adic Lie group with no non-trivial p-torsion, then Coates et al formulated a $\mathrm{Gal}(F_\infty/F)$-equivariant main conjecture for any elliptic curve which is defined over F, has good reduction at all places above p and whose Selmer group (over F_∞) satisfies a certain natural torsion condition.

Then, in [6], Fukaya and Kato formulated a natural main conjecture for any compact p-adic Lie extension of F and any critical motive M which is defined over F and has good ordinary reduction at all places above p.

The key feature of [5] is the use of the localization sequence of algebraic K-theory with respect to a canonical Ore set. However, the more general approach of

[6] is rather more involved and uses a notion of 'localized K_1-groups' together with Nekovar's theory of Selmer complexes and the (conjectural) existence of certain canonical p-adic L-functions. See [18] for a survey.

The p-adic L-functions of Fukaya and Kato satisfy an interpolation formula which involves both the 'non-commutative Tamagawa number conjecture' (this is a natural refinement of the 'equivariant Tamagawa number conjecture' formulated by Burns and Flach in [2] and hence also implies the 'main conjecture of non-abelian Iwasawa theory' discussed by Huber and Kings in [7]) as well as a local analogue of the non-commutative Tamagawa number conjecture. Indeed, by these means, at each continuous finite dimensional p-adic representation ρ of $\mathrm{Gal}(F_\infty/F)$, the 'value $\mathcal{L}(\rho)$ at ρ' $\mathcal{L}(\rho)$ of the p-adic L-function $\mathcal{L}$ is explicitly related to the value at the central critical point of the complex L-function associated to the 'ρ^*-twist' $M(\rho^*)$ of M, where ρ^* denotes the dual representation of ρ. However, if the Selmer module of $M(\rho^*)$ has strictly positive rank (and recent work of Mazur and Rubin [8] shows that this should often be the case), then both sides of the Fukaya-Kato interpolation formula are equal to zero.

The main aim of this project has therefore been to extend the formalism of Fukaya and Kato in order to obtain an interesting interpolation formula for all representations ρ as above. To this end we introduce a notion of 'the leading term $\mathcal{L}^*(\rho)$ at ρ' for elements $\mathcal{L}$ of suitable localized K_1-groups. This notion is defined in terms of the Bockstein homomorphisms that have already played significant roles (either implicitly or explicitly) in work of Perrin-Riou [10, 11], of Schneider [15, 14, 13, 12] and of Greither and the first named author [3, 1] and have been systematically incorporated into Nekovar's theory of Selmer complexes [9].

We briefly sketch the result in the case $M = h^1(A)(1)$ of an abelian variety A over $\mathbb{Q}$ with good ordinary reduction at a fixed prime $p \neq 2$, for more general results and the details see [4]. Let F_∞ be the extension $\mathbb{Q}$ which arises by adjoining the p-power division points $A[p^\infty]$ of A. Then its Galois group G acts by definition faithfully on the p-adic representation $V_p(A)$ (and $V_p(A^\vee)$) attached to A (and its dual abelian variety $A^\vee$), in particular G has a quotient isomorphic to $\mathbb{Z}_p$ corresponding to the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ by the Weil-pairing. By $\Lambda(G)$ we denote the Iwasawa algebra of G with coefficients in $\mathbb{Z}_p$. We write $SC := SC(A/F_\infty)$ for a suitably defined Selmer complex of A over F_∞ (which is quasi-isomorphic to a bounded complex of finitely generated projective $\Lambda(G)$-modules.) The ζ- and ϵ-isomorphism conjectures by Fukaya and Kato are vast generalizations of the (equivariant) Tamagawa Number Conjecture and in particular assume meromorphic continuation of the involved complex L-functions, predict the right order of vanishing of them in terms of motivic cohomology groups and describe their leading terms by arithmetic invariants of A in a functorial, equivariant way; for example they contain the Birch and Swinnerton-Dyer Conjecture. The validity of these 'meta-conjectures' would imply the existence of a p-adic L-function $\mathcal{L}$ of A with an explicit interpolation formula for $\mathcal{L}(\rho)$, whenever for an Artin representation $\rho : G \to GL_n(\mathcal{O}_L)$, L a finite extension of $\mathbb{Q}_p$, the complex $L^n \otimes^{\mathbb{L}}_{\Lambda,\rho^*} SC(A/F_\infty)$ is acyclic.

Nevertheless, if this complex fails to be acyclic, the above assumption on G grants the existence of Bockstein homomorphisms

$$\mathcal{B}_i = \mathcal{B}_i(SC(\rho^*)) : \mathbb{H}_i(G, SC(\rho^*)) \to \mathbb{H}_{i-1}(G, SC(\rho^*))$$

for the hyper-(co)homology groups $\mathbb{H}_i(G, SC(\rho^*)) := \mathrm{H}^{-i}(L^n \otimes^{\mathbb{L}}_{\Lambda,\rho^*} SC(A/F_\infty))$ giving rise to a complex $(\mathbb{H}_\bullet(G, SC(\rho^*)), \mathcal{B}_\bullet)$ and we say that $SC(A/F_\infty)$ is *semisimple at ρ* if this complex is acyclic. If this condition holds, one can define the *leading term $\mathcal{L}^*(\rho)$ of $\mathcal{L}$ at ρ* as an element in $L^\times$ using the complex $(\mathbb{H}_\bullet(G, SC(\rho^*)), \mathcal{B}_\bullet)$.

On the other hand one can show that the Bockstein map $\mathcal{B}_{-1}(SC(\rho^*))$ coincides with the map

$$\mathrm{ad}(h_p(W)) : \mathrm{H}^1_f(\mathbb{Q}, W) \to \mathrm{H}^2_f(\mathbb{Q}, W) \cong \mathrm{H}^1_f(\mathbb{Q}, Z)^*$$

which is induced from Nekovář's p-adic height pairing for $W := V_p(A^\vee)(\rho^*)$

$$h_p(W) : \mathrm{H}^1_f(\mathbb{Q}, W) \times \mathrm{H}^1_f(\mathbb{Q}, Z) \to L$$

and global duality with $Z = W^*(1)$ the Kummer dual of W. Instead of recalling the definition of the finite part $\mathrm{H}^i_f(\mathbb{Q}, -)$ of global cohomology we only remark that, if ρ corresponds to the regular representation of the Galois group $G(K/\mathbb{Q})$ for some finite Galois extension $K/\mathbb{Q}$ contained in F_∞, there is an isomorphism

$$\mathrm{H}^1_f(\mathbb{Q}, W) \cong A^\vee(K) \otimes_{\mathbb{Z}} L.$$

It turns out that $SC(A/F_\infty)$ is semisimple at ρ if and only if the pairing $h_p(W)$ is non-degenerate, which we will assume henceforth. We also assume that the archimedean (Neron-Tate) height pairing $h_\infty(N)$ for the motive $N = M(\rho^*)$ is non-degenerate. The regulators $R_\infty(N)$ and $R_p(N)$ are then defined as the determinants of the induced isomorphisms $\mathrm{ad}(h_\infty(N))$ and $\mathrm{ad}(h_p(W))$ with respect to some rational bases (the ratio $R_p(N)R_\infty(N)^{-1}$ being independent of the choice). Finally, we set $r := r(N) := \dim_L \mathrm{H}^1_f(\mathbb{Q}, W)$.

Theorem ([4, thm. 6.5]). *Let $M = h^1(A)(1)$ be the motive of an abelian variety A over $\mathbb{Q}$ with good ordinary reduction at a fixed prime $p \neq 2$. We assume that the archimedean and p-adic height pairing for the motive $M(\rho^*)$ are non-degenerate and that the above mentioned conjectures by Fukaya and Kato hold.*

Then $SC(A/F_\infty)$ is semisimple at ρ and the leading term $\mathcal{L}^*(\rho)$ is equal to the product

$$(-1)^r \frac{L^*_{K,B}(M(\rho^*))}{\Omega_\infty(M(\rho^*)) \cdot R_\infty(M(\rho^*))} \cdot \Omega_p(M(\rho^*)) \cdot R_p(M(\rho^*)) \cdot \frac{P_{L,p}(\hat{W}^*(1), 1)}{P_{L,p}(\hat{W}, 1)},$$

where $L^*_{K,B}(M(\rho^*))$ denotes the leading term at $s = 0$ of the B-truncated complex L-function of $M(\rho^*)$ with B a certain set of rational primes containing p. Here $\Omega_\infty(M(\rho^*))$ and $\Omega_p(M(\rho^*))$ denote certain archimedean and p-adic periods, while $\frac{P_{L,p}(\hat{W}^*(1),1)}{P_{L,p}(\hat{W},1)}$ describes the modification of the Euler-factor at p.

References

[1] D. Burns, On the values of equivariant Zeta functions of curves over finite fields, Documenta Math. **9** (2004) 357-399.

[2] D. Burns and M. Flach, Equivariant Tamagawa numbers for motives with (non-commutative) coefficients, Documenta Math. **6** (2001) 501-570.

[3] D. Burns and C. Greither, On the equivariant Tamagawa number conjecture for Tate motives, Invent. Math. **153** (2003), no. 2, 303–359.

[4] D. Burns and O. Venjakob, On the leading terms of zeta isomorphisms and p-adic L-functions in non-commutative Iwasawa theory, to appear in Doc. Math. (2006).

[5] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication, Publ. Math., Inst. Hautes Etud. Sci. **101** (2005), 163–208.

[6] T. Fukaya and K. Kato, A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory, to appear in Proc. St . Petersburg Math. Soc. **11** (2005).

[7] A. Huber and G. Kings, Equivariant Bloch-Kato conjecture and non-abelian Iwasawa main conjecture, *in* Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), 149–162, Higher Ed. Press, Beijing, 2002;

[8] B. Mazur and K. Rubin, Finding large Selmer groups, preprint 2005.

[9] J. Nekovar, *Selmer complexes*, preprint (2001).

[10] B. Perrin-Riou, Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes), Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. **108**, Birkhäuser Boston, Boston, MA, 1993, pp. 203–220.

[11] B. Perrin-Riou, p-adic L-functions and p-adic representations, SMF/AMS Texts and Monographs, vol. 3, American Mathematical Society, Providence, RI, 2000.

[12] P. Schneider, Height pairings in the Iwasawa theory of abelian varieties, in *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*, 309–316, Progr. Math., **22**, Birkhäuser, 1982.

[13] P. Schneider, p-adic height pairings. I., Invent. Math. **69** (1982), 401–409.

[14] P. Schneider, Iwasawa L-functions of varieties over algebraic number fields. A first approach, Invent. Math. **71** (1983), no. 2, 251–293.

[15] P. Schneider, p-adic height pairings. II., Invent. Math. **79** (1985), 329–374.

[16] J-P. Serre, Sur le résidue de la fonction zêta p-adique d'un corps de nombres, C.R. Acad. Sci. Paris **278** (1978) 183-188.

[17] J. Tate, Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$ (notes par D.Bernardi et N. Schappacher), Progress in Math., **47**, Birkhäuser, Boston, 1984.

[18] O. Venjakob, From the Birch & Swinnerton-Dyer Conjecture over the Equivariant Tamagawa Number Conjecture to non-commutative Iwasawa theory - a survey, to appear in 'L-functions and Galois representations', Proceedings of the 2004 Durham Symposium, C.U.P., preprint: arXiv:math.NT/0507275 (2005).

Mild pro-p-groups and p-extensions of $\mathbb{Q}$

J. Labute

Let p be a prime $\neq 2$ and let $S = \{q_1, \ldots, q_m\}$ be a set of m rational primes $\equiv 1$ mod p. Let $G = G_S(p)$ be the maximal p-extension of $\mathbb{Q}$ unramified outside S. The pro-p-group G has a minimal presentation with m generators and m relations and so by Golod-Shafarevich it is infinite if $m \geq 4$. That was all we knew about this group in this case, except for the fact that the quotients of the derived series were finite, until we showed in [5] that G has cohomological dimension 2 under certain conditions on S. We also showed that under these conditions the ranks of the lower p-central series quotients grow exponentially.

To describe these conditions we introduce the weighted directed graph $\Gamma_S(p)$ whose vertices are the primes in S. We join q_i to q_j if q_i is not a p-th power mod q_j in which case we attach a weight ℓ_{ij} to the edge q_iq_j. To define this weight we chose a primitive root g_i for each prime q_i. Then ℓ_{ij} is the unique image in $\mathbb{Z}/p\,\mathbb{Z}$ of any integer r satisfying

$$q_i \equiv g_j^{-r} \bmod q_j.$$

Using the Čebotarev density theorem, one can show that, for any given finite directed graph Γ, there is a set of primes S as above with $\Gamma_S(p) \cong \Gamma$ as directed graphs.

We call $\Gamma_S(p)$ a **non-singular circuit** if the the following conditions hold:

(a) There is an ordering $q_1, \ldots, q_m$ of the vertices of Γ such that $q_1q_2\cdots q_mq_1$ is a circuit.

(b) We have $\ell_{ij} = 0$ if i, j are odd and

$$\Delta(q_1, q_2, \ldots, q_m) = \ell_{12}\ell_{23}\cdots\ell_{m-1,m}\ell_{m1} - \ell_{1m}\ell_{21}\ell_{32}\cdots\ell_{m,m-1} \neq 0.$$

In this case we also call $q_1q_2\cdots q_m$ a circular sequence of primes. If $S = \{7, 19, 61, 163\}$ then $\Gamma_S(3)$ is a non-singular circuit. If $\Gamma_S(p)$ is not a non-singular circuit we can add m primes $\equiv 1$ mod p to make it a non-singular circuit.

Note that if (a) holds then $\Delta(q_1, q_2, \ldots, q_m) \neq 0$ if there is an edge q_iq_j of the circuit $q_1q_2\cdots q_mq_1$ such that q_jq_i is not an edge of $\Gamma_S(p)$. Also note that (a) and (b) imply that m is even and ≥ 4. Condition (b) is independent of the choice of primitive roots g_j since

$$\Delta(q_1, q_2, \ldots, q_m) \neq 0 \iff \frac{\ell_{1m}}{\ell_{m-1,m}}\frac{\ell_{21}}{\ell_{m1}}\frac{\ell_{32}}{\ell_{12}}\cdots\frac{\ell_{m,m-1}}{\ell_{m-2,m-1}} \neq 1,$$

where each ratio in the product is independent of the choice of primitive roots.

Theorem A If $\Gamma_S(p)$ is a non-singular circuit then $G_S(p)$ is of cohomological dimension 2.

Corollary. If $S = \{7, 19, 61, 163\}$ then then $\mathrm{cd}(G_S(3)) = 2$.

To prove this we use the fact that, due to Koch [4], the pro-p-group $G = G_S(p)$ has a presentation $G = F/R$ with F the free pro-p-group on $x_1, \ldots, x_m$ and R the closed normal subgroup generated by $r_1, \ldots, r_m$ with

$$r_i \equiv x_i^{q_i-1}\prod_{j=1}^{n}[x_i, x_j]^{\ell_{ij}} \bmod F_3,$$

where F_n denotes the n-th term of the lower p-central series of F. The Lie algebra $L = \mathrm{gr}(F)$ associated to the lower p-central series of F is a free Lie algebra over $\mathbb{F}_p[\pi]$, where the action of the indeterminate π is induced by $x \mapsto x^p$. Let ρ_i be the image of r_i in $\mathrm{gr}_2(F)$ and let $\mathfrak{r}$ be the ideal of L generated by $\rho_1, \ldots, \rho_m$.

Let $\mathfrak{g} = L/\mathfrak{r}$ and let $U_{\mathfrak{g}}$ be the enveloping algebra of $\mathfrak{g}$. Then $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a $U_{\mathfrak{g}}$-module via the adjoint representation.

Theorem B. If $\Gamma_S(p)$ is a non-singular circuit then
(a) $\mathfrak{g}$ is a free $\mathbb{F}_p[\pi]$-module,
(b) M is a free $U_{\mathfrak{g}}$-module on the images of $\rho_1, \ldots, \rho_m$.

We call $\rho_1, \ldots, \rho_m$ **strongly free** if the conditions (a) and (b) of Theorem B hold. In this case we call G **mild**.

Theorem C. If the sequence $r_1, \ldots, r_m$ is strongly free then $\mathrm{gr}(G) = L/\mathfrak{r}$ and $R/[R, R]$ is a free $\mathbb{Z}_p[[G]]$-module.

If $R/[R, R]$ is a free $\mathbb{Z}_p[[G]]$-module, the canonical exact sequence

$$0 \to R/[R, R] \to \mathbb{Z}_p[[G]]^m \to \mathbb{Z}_p[[G]] \to Z_p \to 0$$

together with a result of Brumer [2] shows that the cohomological dimension of G is 2. That $R/[R, R]$ is a free $\mathbb{Z}_p[[G]]$-module is proven by showing that, under the assumption that the sequence $r_1, \ldots, r_m$ is strongly free, the above exact exact sequence lifts the exact sequence

$$0 \to \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}] \to U_{\mathfrak{g}}^m \to U_{\mathfrak{g}} \to F_p[\pi] \to 0.$$

If $\overline{L} = L/\pi L$ and $\overline{\rho}_i$ is the image of ρ in $\overline{L}$ then $\rho_1, \ldots, \rho_m$ is a strongly free sequence in L if and only if $\overline{\rho}_1, \ldots, \overline{\rho}_m$ is a strongly free sequence in $\overline{L}$, which can be identified with the free Lie algebra over $\mathbb{F}_p$ on $\xi_1, \ldots, \xi_m$. The sequence $\rho_1, \ldots, \rho_m$ is strongly free if and only if the Poincaré series of the enveloping algebra of $\mathfrak{g}/\pi\mathfrak{g}$ is

$$P(t) = \frac{1}{1 - mt + mt^2}.$$

In this case one can show that the dimension of the n-th homogeneous component of $L/\mathfrak{r}$ is

$$\sum_{k=1}^{n} \frac{1}{k} \sum_{d|k} \mu(k/d)(\alpha^d + \beta^d),$$

where $1 - mt + mt^2 = (1 - \alpha t)(1 - \beta t)$. Note that $\alpha, \beta > 1$ for $m \geq 4$.

The problem of deciding strong freeness is a difficult one. However, in joint work with Michael Bush [3], we have found an algorithm for strong freeness in the case $m = 4$. In fact, we show that $\rho_1, \ldots, \rho_4$ is a strongly free sequence if and only if the dimensions of the first four homogeneous components of $\mathfrak{g}/\pi\mathfrak{g}$ are $4, 2, 4, 6$. For example, if $p = 3$ and $S = \{7, 13, 19, 31\}$, the sequence $\rho_1, \ldots, \rho_4$ is strongly free. The case $m > 4$ is the subject of ongoing research. Alexander Schmidt [6] has extended our results to give criteria on $\Gamma_S(p)$ for the cohomological dimension of $G_S(p)$ to be 2. We don't know whether in these cases $G_S(p)$ is a mild group.

More generally, a finitely presented pro-p-group G is said to be **mild** if it has a minimal presentation $G = F/R =< x_1, \ldots, x_d \mid r_1, \ldots, r_m >$ where the initial forms of the relators r_i with respect to the lower p-central series form a strongly free sequence; if h_i is largest with $r_i \in F_{h_i}$ then the initial form ρ_i of r_i is the image of r_i in $\mathrm{gr}_{h_i}(F)$.

Theorem C is true in this general context even if $p = 2$ if we assume $r_i \in F^4[F,F]$ for all i. Moreover, the sequence $r_1, \dots, r_m$ is strongly free if and only if the Poincaré series of the enveloping algebra of $\mathfrak{g}/\pi\mathfrak{g}$ is

$$\frac{1}{1 - dt + t^{h_1} + \cdots + t^{h_m}}.$$

In this case, if $1 - dt + t^{h_1} + \cdots + t^{h_m} = (1 - \alpha_1 t) \cdots (1 - \alpha_m)$ then

$$\dim \mathrm{gr}_n(G) = \sum_{k=1}^{n} \frac{1}{k} \sum_{d|k} \mu(k/d)(\alpha_1^d + \cdots + \alpha_m^d).$$

If $h_i = h$ for all i then strong freeness implies $m < d^h/(h-1)e$. If $h = 2$ we can find strongly free sequences $r_1, \dots, r_m$ with $1 \le m \le t(d)$ where $t(d) = d^2/4$ if d is even and $t(d) = (d-1)^2/4$ is d is odd; we conjecture that $t(d)$ is largest possible.

We call a pro-p-group G **tame** if it is mild and has the property **FAB**: every subgroup of G finite index has a finite abelianization. In this case, $m \ge d$. Infinite tame groups lie strictly between the class of free pro-p-groups and p-adic analytic groups but have properties in common with each of these classes. It would be interesting to have a classification of infinite tame groups in view of their relevance to the Fontaine-Mazur Conjecture, cf [1]. It is our belief that infinite tame groups appear often as Galois groups of maximal p-extensions of number fields with restricted tame ramification. See for example the recent work of Vogel [7] in the case of imaginary quadratic number fields.

References

[1] N. Boston, *Reducing the Fontaine-Mazur Conjecture to Group Theory*, (preprint).

[2] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. Algebra 4, 442-470 (1966).

[3] M. Bush, J. Labute. *Mild pro-p-groups with* 4 *generators*, (preprint).

[4] H. Koch, *Galois Theory of p-Extensions*, Springer Verlag, 2002.

[5] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, (to appear in J. Reine Angew. Math.)

[6] A. Schmidt, Circular sets of prime numbers and p-extensions of the rationals, (to appear in J. Reine Angew. Math.)

[7] D. Vogel, *Circular sets of primes of imaginary quadratic number fields*, (preprint).

Profinite groups generated by automata

L. Bartholdi

There has been considerable interest in residually-p groups generated by automata. The construction goes as follows: fix a prime p. By a finite *automaton* we mean a finite directed graph A, such that at every vertex there is an element of $\mathbb{F}_p$ and p outgoing edges labeled by the elements of $\mathbb{F}_p$.

A given vertex $v \in A$ induces a permutation of the set of infinite sequences $\partial T = (\mathbb{F}_p)^\infty$, as follows: let $x_1 x_2 \dots$ be in ∂T. There is a unique path $v_1 v_2 \dots$ in A with $v_1 = v$ and label x_i on the edge from v_i to v_{i+1}. Let n_i be the element of $\mathbb{F}_p$ at vertex v_i. Then set

$$v(x_1 x_2 \dots) = (x_1 + n_1)(x_2 + n_2) \dots . \tag{1}$$

The space ∂T may be interpreted as the boundary of a rooted, p-regular tree T, as follows: vertices of the tree (at distance k from the root) are identified with prefixes (of length k) of infinite sequences. Two prefixes are adjacent in the tree precisely if one is a prefix of the other and their length differs by one.

The p-automorphism group W of the tree T is the group of graph automorphisms of T such that their action, below any vertex, is by a fixed p-cycle. This means that if $g \in W$ maps $v_1 \dots v_k$ to $w_1 \dots w_k$, then there must exist $n_{v_1 \dots v_k} \in \mathbb{F}_p$ such that $g(v_1 \dots v_k v_{k+1}) = w_1 \dots w_k (v_{k+1} + n_{v_1 \dots v_k})$.

It follows readily that W is isomorphic with $W \wr \mathbb{F}_p := W^p \rtimes \mathbb{F}_p$, the isomorphism ϕ being given explicitly by

$$\phi(g) = (g_0, \dots, g_{p-1})n,$$

where $g_i \in W$ and $n \in \mathbb{F}_p$ are defined by $g(v_1 v_2 \dots) = (v_1 + n) g_{v_1}(v_2 \dots)$. Furthermore, W is a pro-p group, with basis of neighbourhoods of the identity given by the fixators of $\mathbb{F}_p^k \subset T$, for all $k \in \mathbb{N}$.

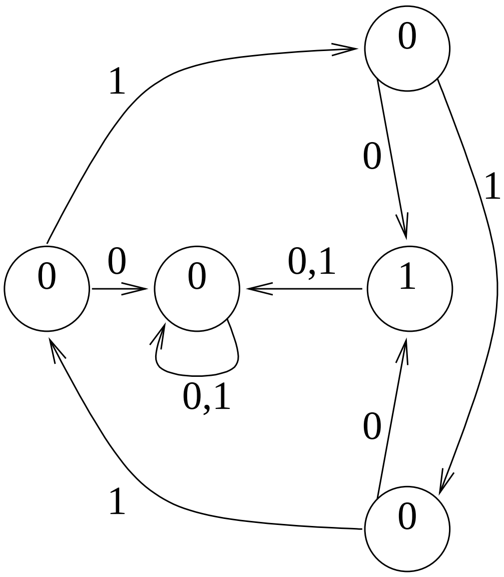
Topologically, $W \cong \{f : T \to \mathbb{F}_p\}$, under the map $\pi : g \mapsto (v_1 \dots v_k \mapsto n_{v_1 \dots v_k})$. The image of $g \in W$ under this correspondence is called its *portrait*. Note that if one writes $\phi(g_v) = (g_{v0}, \dots, g_{v(p-1)})n_v$ for all $v \in T$, then $n_{v_1 \dots v_k}$ is obtained from g by iterating k times (ϕ and projection on coördinate v_i), followed by projection on the last coördinate.

Let $G(A)$ be the group generated by all transformations $v \in A$. This is a residually-p group; indeed there are finite p-quotients given by restricting the action to $(\mathbb{F}_p)^k$. These groups satisfy the condition that $\phi(G(A)) \subset G(A) \wr \mathbb{F}_p$.

It turns out that many interesting groups appear by considering quite small automata. On the other hand, the topological closures (in $\mathrm{Aut}(T)$), or the profinite completions of such groups $G(A)$ seem to have received little attention, and my intent is to indicate interesting, as-yet-unexplored directions. This will be done by considering closer the following examples, which are all obtained with $p = 2$.

The "Grigorchuk" automaton

Taking $p = 2$, the automaton A is the following:



The group $G(A)$ generated by the five vertices of A has many unusual properties, in particular it is an infinite, finitely generated group in which every element has order a power of 2. It has been extensively studied since the early 1980's by Grigorchuk [3]; for a comprehensive list of properties see the survey [2].

A pro-p group W is naturally a metric space, where one sets

$$d(g,h) = \inf\{[W : H]^{-1} : gh^{-1} \in H \text{ an open subgroup of } G\}.$$

There is therefore a notion of Hausdorff dimension for closed subgroups of pro-p groups; for closures G of automata groups it takes the following form [1]:

$$\dim_H(G) = (p-1) \liminf \frac{\log \#G_n}{p^n},$$

where G_n is the quotient of G acting on $(\mathbb{F}_p)^n$. The normalization is chosen so that $\dim_H(W) = 1$.

The profinite completion $G = \widehat{G(A)}$ of Grigorchuk's group is isomorphic to the topological closure of $G(A)$. It is known that the Hausdorff dimension of G is 5/8; however much more is true:

Proposition 1. *The portrait $\pi(G)$ is*

$$\Big\{f : T \to \mathbb{F}_p : \\ f(w0) + \sum_{x\in\mathbb{F}_p} f(w1x) + \sum_{x,y\in\mathbb{F}_p} f(w1xy) = 0 \textit{ for all } w \in T, \\ f(w1) + \sum_{x\in\mathbb{F}_p} f(w0x) + \sum_{x,y\in\mathbb{F}_p} f(w0xy) = 0, \textit{ for all } w \in T \\ f(w0)f(w1) + \sum_{x\in\mathbb{F}_p} f(wx1) + \sum_{x,y\in\mathbb{F}_p} f(wx0y) = 0 \textit{ for all } w \in T\Big\}.$$

There are therefore 3 equations on every depth-3 subtree; this means that, for every depth-3 subtree with $2^3 = 8$ bottom nodes, only $5 = 8 - 3$ degrees of freedom are allowed in portraits of G. This is a general interpretation of the Hausdorff dimension of a subgroup of W.

More results follow immediately from this proposition: for example,

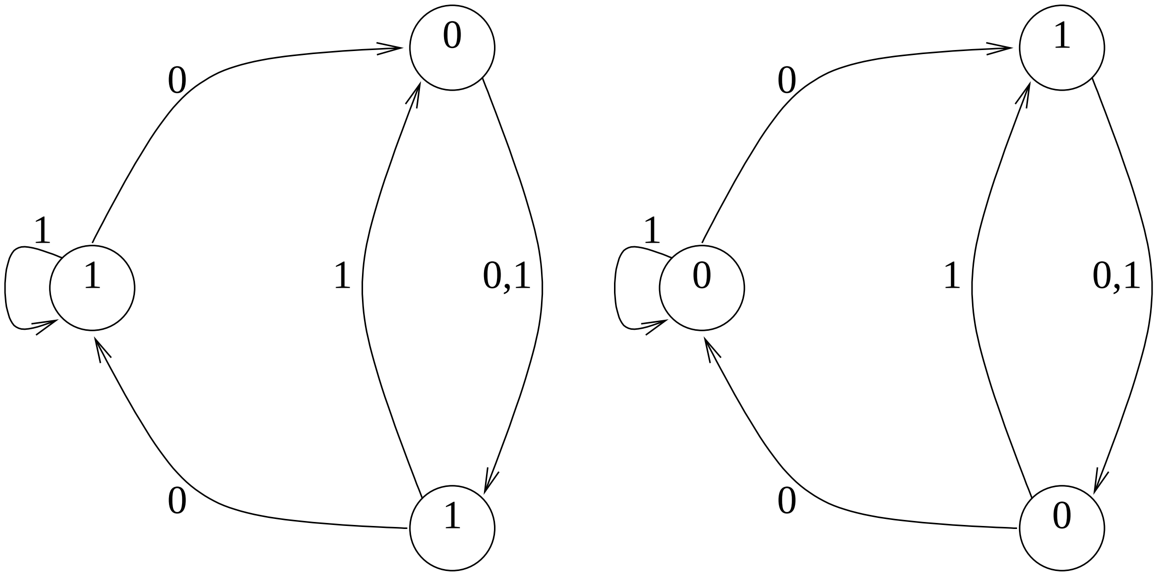
Proposition 2. *Let $t : v_1v_2\ldots \mapsto (v_1+1)(v_2+1)\ldots$ be the automorphism of T that exchanges all 0's and 1's. Then $\dim_H(G \cap G^t) = \frac{1}{2}$.*

Indeed, the first two equations are exchanged by t, while the third gives a genuinely new equation under conjugation by t. The portraits of $G \cap G^t$ therefore have 4 degrees of freedom within every 8 nodes.

This is work in progress with Olivier Siegenthaler.

1. The "Aleshin" and "Baby-Aleshin" automata

Take again $p = 2$. The "Aleshin" (A) and "Baby-Aleshin" (B) are respectively the right and left automata of



It has been shown by Vorobets [5] that $G(A)$ is free of rank 3, and by Muntyan and Savchuk [4, Theorem 1.10.2] that $G(B)$ is isomorphic to $C_2 * C_2 * C_2$.

The topological closures $\overline{G(A)}$ and $\overline{G(B)}$ are very far from the pro-2 completions of $G(A)$ and $G(A)$ respectively. I conjecture that in fact these closures are $\mathbb{Z}_2$-analytic groups.

More precisely, I conjecture that $\overline{G(B)}$ is a pro-2-Sylow of $SL_2(\mathbb{Z}_2)$.

I also conjecture that, for every n, the Schreier graph (with vertex set $(\mathbb{F}_p)^n$ and an edge from x to $v(x)$ for all $x \in (\mathbb{F}_p)^n$ and all $v \in B$) is a "Ramanujan graph", i.e. the spectrum of its adjacency matrix is contained in $[-\sqrt{8}, \sqrt{8}] \cup \{3\}$.

References

[1] A. G. Abercrombie, *Subgroups and subrings of profinite rings*, Math. Proc. Cambridge Philos. Soc. **116** (1994), no. 2, 209–222.

[2] L. Bartholdi, R. I. Grigorchuk, and Z. Šuniḱ, *Branch groups*, Handbook of algebra, Vol. 3, North-Holland, Amsterdam, 2003, pp. 989–1112.

[3] R. I. Grigorchuk, *On Burnside's problem on periodic groups*, Функционал. Анал. и Приложен. **14** (1980), no. 1, 53–54, English translation: Functional Anal. Appl. **14** (1980), 41–43.

[4] V. V. Nekrashevych, Self-similar groups, Mathematical Surveys and Monographs, vol. 117, Amer. Math. Soc., Providence, RI, 2005.

[5] M. Vorobets and Y. Vorobets, *On a free group of transformations defined by an automaton*, arXiv:math.GR/0601231, 2006.

Galois Actions on Rooted Trees

R. Jones

(joint work with N. Boston)

The Galois tower generated by the iterates of a polynomial $f \in \mathbb{Z}[x]$ has a natural action on the regular rooted tree of f-preimages of 0. The study of these "arboreal" Galois representations is quite young, and we propose some analogues to key features of the powerful theory of linear l-adic Galois representations.

Let us describe the natural Galois action on the f-preimages of 0. Given $f \in \mathbb{Z}[x]$ of degree d, let $f^1 = f$ and $f^n = f \circ f^{n-1}$, so that f^n is the nth iterate of f. Suppose that all the iterates f^n are separable. The successive f-preimages of 0 (contained in $\overline{\mathbb{Q}}$) now form a complete rooted d-ary tree. Indeed, for each root α of f^n there is a unique root β of f^{n-1} related to α in the sense that $f(\alpha) = \beta$. Assigning edges according to this relation, the disjoint union $\bigcup_{n=0}^{\infty}\{\text{roots of } f^n\}$ becomes a complete d-ary tree with root 0. In this manner, one has a representation $G_{\mathbb{Q}} \to \mathrm{Aut}(T)$ of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ into the group of automorphisms of the complete rooted d-ary tree T. We call such a representation arboreal. In this talk we consider only the case of $d = 2$, which already presents ample complexity.

There are three important aspects of linear l-adic Galois representations that we wish to highlight: the trace of the Frobenius conjugacy class at p, the study of the images of such representations, and the L-functions associated to them. We discuss the development of arboreal analogues in these three areas, with emphasis on the trace of Frobenius.

To formulate an analogy to the trace of Frobenius in the linear case, we wish to associate a conjugacy-class invariant to the Frobenius class Frob_p at each unramified prime p. The cycle structure of Frob_p is given by the degrees of the irreducible factors of $f^n \bmod p$, and thus we analyze this factorization. The descendants of an irreducible factor h of $f^n \bmod p$ are the irreducible factors of $h \circ f^k$ for $k \geq 1$, while the irreducible factors of $h \circ f$ are called immediate descendants. Call h *f-stable* if all its descendants are irreducible. Consider the example of $f = x^2 + 1$ and $p = 7$. We have the following factorizations of f, f^2, and f^3:

$$f = x^2 + 1$$
$$f^2 = (x^2 + 2x + 3)(x^2 + 5x + 3)$$
$$f^3 = (x^4 + 4x^2 + 6)(x^2 + x + 4)(x^2 + 6x + 4)$$

Note that x^2+2x+3 has only one immediate descendant, namely x^4+4x^2+6, while $x^2 + 5x + 3$ has two, namely $x^2 + x + 4$ and $x^2 + 6x + 4$. Moreover, computations suggest that the factor $x^2 + x + 4$ of f^3 is f-stable. We prove that this is the case, making use of the following definition: the *critical orbit* of a polynomial f is the union of the sets $\{f^n(\gamma) : n \geq 1\}$, where γ ranges over the critical points of f. If $f = ax^2 + bx + c$, then the critical orbit is simply $\{f^n(-b/2a) : n \geq 1\}$.

Proposition. *If $f, h \in \mathbb{F}_p[x]$, $\deg f = 2$, and $\deg h$ is even, then h is f-stable if and only if $h(c)$ is not a square for every element c of the critical orbit of f.*

In the case of $f = x^2 + 1$, $h = x^2 + x + 4$, and $p = 7$, the critical orbit of f is $\{1, 2, 5\}$ and h maps these to $6, 3$, and 6, respectively. Thus h is f-stable. It now is logical to classify each h appearing in the factorization of each f^n by whether $h(1)$, $h(2)$, and $h(5)$ are squares. Thus x^2+x+4 is *nnn*, while for instance x^2+5x+3 is *sns*. Moreover, only certain decay patterns are possible: for example, an *snn* polynomial must have two immediate descendants, and they can be either an *sns*/*nsn* pair or a *ssn*/*nns* pair. On the other hand, an *nnn* polynomial must be stable, and so all its descendants are *nnn*.

We now make the assumption that the possible decay patterns are equally likely over the long run, implying that the long term behavior of the iterates of f is given by an 8-state Markov process that is aperiodic with a sink at *nnn*. Therefore in particular the proportion of the degree of $f^n \bmod p$ occupied by *nnn* (i.e. f-stable polynomials) goes to 1. Extensive computation shows that the behavior of this 8-state Markov process closely describes the actual behavior of iterates of f.

We call $f \in \mathbb{F}_p[x]$ *settled* if the proportion of the degree of f^n occupied by f-stable polynomials goes to 1.

Conjecture. *Any irreducible quadratic polynomial $f \in \mathbb{F}_p[x]$ is settled.*

More generally, if we associate to any irreducible factor h of f^n a string in $\{n, s\}$ based on where h maps elements of the critical orbit of f, we conjecture that the distribution for large n of the factors of f^n is given by the long-term behavior of the appropriate Markov process.

Assuming the above Conjecture, given $f \in \mathbb{Z}[x]$, we can associate a (possibly infinite) partition of unity to each prime p that is unramified in the splitting fields of all iterates of f. If $d_1, \dots, d_r$ are the degrees of the f-stable factors of $f^n \bmod p$, then let $d_1/2^n + \cdots + d_r/2^n$ be the initial segment of what as $n \to \infty$ becomes a partition of unity. For instance, if all iterates of $f \bmod p$ are irreducible then the partition is simply 1 while if $f^3 \bmod p$ factors as four f-stable polynomials then the partition is $4/4$. In the example of $f = x^2 + 1$, $p = 7$ analyzed above, the partition is infinite, with no apparent pattern: $1/4 + 1/8 + 3/16 + 8/64 + 10/128 + \cdots$. This partition is our proposed analogue to the trace of Frobenius. See [1] for more details.

We now address the image of an arboreal representation. By the Tchebotarev Density Theorem, it follows that Frobenius conjugacy classes are dense in the infinite Galois group G_f of all iterates of f. Define a settled automorphism of a regular rooted tree analogously to a settled polynomial, based on the cycle structure of the action on level n of the tree. According to the above Conjecture, Frobenius classes should be settled at least when $\deg f = 2$, so it follows that G_f should have a dense subset of settled elements. We call such a group *densely settled*, and thus we conjecture that in the quadratic case the image of an arboreal Galois representation is densely settled. The image of a linear l-adic Galois representation has been a source of great interest (e.g Serre's theorem [3] on the image of l-adic representations coming from elliptic curves), and we propose densely settled groups as a similarly interesting class.

The images of the arboreal representations associated to some quadratic $f \in \mathbb{Z}[x]$ have been found, and these groups have always turned out to be densely settled. Stoll [4] has shown the Galois groups of iterates of $f = x^2 + a$ are the full group $\mathrm{Aut}(T)$ for an infinite family of $a \in \mathbb{Z}$, while it is also known that iterates of $f = x^2 - kx + k$, $k \notin \{-2, 2, 4\}$, give finite-index subgroups of $\mathrm{Aut}(T)$ [2]. It is easy to see that any finite index subgroup of $\mathrm{Aut}(T)$ is densely settled. It is also known that if $f = x^2 - 2$ then the image of the associated arboreal representation is $\mathbb{Z}_2$, while if $f = (x \pm p)^2 \mp p$ for p an odd prime then the image is the group of affine linear transformations of $\mathbb{Z}_2$, which is isomorphic to $\mathbb{Z}_2 \rtimes \mathbb{Z}_2^*$. Both of these images are settled. A particularly interesting example is given by the polynomial $f = (x+1)^2 - 2$, whose iterates generate fields of degree a power of 2 that are unramified outside 2 and ∞. Thus the associated Galois group is a quotient of the Galois group of the maximal 2-extension unramified outside $\{2, \infty\}$. It is an open question to determine the size of the kernel of the quotient map.

Finally, one would like to have an analogue of L-functions for arboreal representations, as they have made up a very rich part of the theory of linear l-adic Galois representations. As yet there are no compelling candidates. One possibility is to associate a zeta-function to the tree of iterates of f, although how to do this in the right way remains open.

References

[1] Nigel Boston and Rafe Jones, *Densely settled groups and arboreal galois representations*, preprint.

[2] Rafe Jones. *On the density of prime divisors of quadratic recurrences*, preprint.

[3] Jean-Pierre Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math **15(4)** (1972), 259–331.

[4] Michael Stoll. *Galois groups over* $\mathbf{Q}$ *of some iterated polynomials*, Arch. Math. (Basel) **59(3)** (1992), 239–244.

Towards arithmetical description of the Galois group of a local field

V. Abrashkin

Let K be a complete discrete valuation field with residue field of characteristic p. Let Γ_K be the absolute Galois group of K and let $\Gamma_K(p)$ be the Galois group of the maximal p-extension of K. What we can say about its structure? The known cases are:

— if $\operatorname{char} K = p$ then $\Gamma_K(p)$ is pro-p-free;
— if $\operatorname{char} K = 0$ and k is finite (i.e. K is one-dimensional), then
  — if $\zeta_p \notin K$, then $\Gamma_K(p)$ is pro-p-free;
  — if $\zeta_p \in K$, then $\Gamma_K(p)$ is the Demushkin group.

What we can say if K is an N-dimensional local field? (This means that k is an $(N-1)$-dimensional local field.) Notice that "1-dimensional" methods can't be directly generalized to study the higher dimensional case.

Alternative "1-dimensional" approach: characteristic p case

Assume for simplicity that $K = \mathbb{F}_p((t))$. Then the Artin-Schreier theory gives an explicit description of the group $\Gamma_K/\Gamma_K^p C_2(\Gamma_K)$, where $C_2(\Gamma_K)$ is the closed subgroup generated by commutators of order $\geqslant 2$. This group appears as the Galois group of the extension $K(\{T_a \mid (a,p)=1 \text{ or } a=0\})/K$, where $T_a^p - T_a = t^{-a}$. It is an abelian group of exponent p with free generators τ_b, where $b \in \mathbb{N}$, $(b,p)=1$ or $b=0$. The action of τ_b can be given explicitly by the relation $\tau_b(T_a) = T_a + \delta_{ab}$, where δ is the Kronecker symbol.

We can proceed further to obtain the maximal p-extension of K by joining roots $T_{a_1\dots a_s}$, where $s \geqslant 1$ and all a_i's are either zero or natural numbers prime to p, of the equations $T_{a_1\dots a_s}^p - T_{a_1\dots a_s} = T_{a_1\dots a_{s-1}} t^{-a_s}$. This idea has been known for a very long time ago but did not lead to any satisfactory theory because it was not supported by explicit description of the action of elements of $\Gamma_K(p)$ on these structural elements $T_{a_1\dots a_s}$.

Example. *The relation* $(T_{a_1}T_{a_2})^p - T_{a_1}T_{a_2} = T_{a_1}t^{-a_2} + T_{a_2}t^{-a_1} + t^{-(a_1+a_2)}$ *implies for* $(a_1+a_2, p) = 1$, *the relation* $T_{a_1}T_{a_2} = T_{a_1a_2} + T_{a_2a_1} + T_{a_1+a_2}$. *Therefore, when extending the action of* $\tau_{a_1+a_2}$ *to* K_{sep} *we must specify its non-trivial action on at least one of* $T_{a_1a_2}$ *or* $T_{a_2a_1}$. *This problem can be avoided if we assume that* $p > 2$ *and introduce a corrected definition of* $T_{a_1a_2}$ *such that* $T_{a_1a_2}^p - T_{a_1a_2} = T_{a_1}t^{-a_2} + \frac{1}{2}t^{-(a_1+a_2)}$. *Then we obtain "homogeneous" relations* $T_{a_1}T_{a_2} = T_{a_1a_2} + T_{a_2a_1}$ *and a nice description of the extension of the action of* τ_b *on* $T_{a_1a_2}$ *given by the formula* $\tau_b(T_{a_1a_2}) = T_{a_1a_2} + \delta_{ba_1}T_{a_2} + \frac{1}{2}\delta_{ba_1a_2}$.

The situation from the above example can be generalised to correct the elements $T_{a_1\dots a_s}$, where $s<p$. These elements will appear as roots of modified Artin-Schreier equations, they satisfy "homogeneous relations" and their images under a suitable extension of τ_b's are given by explicit and symmetric formulas. This is so-called nilpotent version of the Artin-Schreier theory. It was developed by the author nearly 15 years ago and can be presented as follows.

Denote by $\mathcal{A}$ the pro-free non-commutative unitary $\mathbb{F}_p$-algebra with the set of generators D_a, where $a=0$ or $a\in\mathbb{N}$ and $(a,p)=1$. Set $\mathcal{F}=1+\sum T_{a_1\dots a_s}D_{a_1}\dots D_{a_s}\in\mathcal{A}\hat{\otimes}K_{\mathrm{sep}}$, and $E=\widetilde{\exp}\,(\sum t^{-a}D_a)\in\mathcal{A}\hat{\otimes}K$, where $\widetilde{\exp}(x)=\sum_{0\leqslant s<p}x^s/s!$ is the truncated exponential.

Then all equations for the elements $T_{a_1\dots a_s}$ are consequences of the "equation" $\sigma\mathcal{F}:=1+\sum T^p_{a_1\dots a_s}D_{a_1}\dots D_{a_s}=\mathcal{F}E \bmod \deg p$.

All relations between different $T_{a_1\dots a_s}$ come from the following "relation" $\Delta(\mathcal{F})\equiv\mathcal{F}\hat{\otimes}\mathcal{F}\bmod\deg p$, where Δ is the diagonal map such that for all a, $\Delta(D_a)=D_a\hat{\otimes}1+1\hat{\otimes}D_a$.

For all b, the extension of the action of τ_b is given by the formula $\tau_b(\mathcal{F})=\widetilde{\exp}(D_b)\mathcal{F}\bmod\deg p$.

The above theory has the following interpretation. Let $\widetilde{\mathcal{L}}$ be a pro-free Lie algebra over $\mathbb{F}_p$ with pro-free generators D_a, where as usually $a=0$ or $(a,p)=1$. Set $\mathcal{L}=\widetilde{\mathcal{L}}/C_p(\widetilde{\mathcal{L}})$, where $C_p(\widetilde{\mathcal{L}})$ is the ideal of commutators of order $\geqslant p$. Then $\mathcal{F}\bmod\deg p=\widetilde{\exp}(f)$ with $f\in\mathcal{L}\hat{\otimes}K_{\mathrm{sep}}$. This gives the Artin-Schreier equation

$$\sigma(f)=f\circ(\sum t^{-a}D_a)$$

in $\mathcal{L}\hat{\otimes}K$, where $\circ$ is the Campbell-Hausdorff composition law. The correspondence $\tau\mapsto\tau(f)\circ(-f)$ induces the identification $\Gamma_K/\Gamma_K^pC_p(\Gamma_K)=G(\mathcal{L})$, where $G(\mathcal{L})$ is the group obtained from the elements of the Lie algebra $\mathcal{L}$ via the Campbell-Hausdorff composition law.

Remark. *The above version of nilpotent Artin-Schreier theory admits generalizations to the case of fields K with arbitrary finite residue field (not just $\mathbb{F}_p$) and arbitrary extensions of nilpotent class $<p$ (not just of exponent p). It can be extended also by the description of the images of higher ramification subgroups of Γ_K in $G(\mathcal{L})$.*

2-dimensional local fields: characteristic p case

Consider the simplest case of 2-dimensional local fields of characteristic p. So, let $K=\mathbb{F}_p((t_2))((t_1))$. In this case we do not have a simple description even for the group $\Gamma_K/\Gamma_K^pC_2(\Gamma_K)$. Indeed, the idea of working with generators similarly to 1-dimensional case is destroyed e.g. by the fact that the extension $T^p-T=\sum_{n\geqslant0}t_2^nt_1^{-1}$ is not contained in the composite of the extensions $T_n^p-T_n=t_2^nt_1^{-1}$, $n\geqslant0$. There is a concept of topology (we call it the P-topology) on K (and its algebraic extensions) which brings together two valuation topologies coming from the structure of 2-dimensional field on K. The arithmetic operations on K are sequentially P-continuous and the basis of sequentially P-compact subsets in K consists of $U = \{\sum \alpha_{ab} t_1^a t_2^b\}$ such that there are $A = A(U) \in \mathbb{Z}$ and for all $a \leqslant A$, $A_a = A_a(U)$ such that $\alpha_{ab} = 0$ if either $a < A$ or $a \geqslant A$ but $b < A_a$. Therefore, $\Gamma_K/\Gamma_K^p C_2(\Gamma_K)$ can be provided with the P-topological structure by the Artin-Schreier pairing. Then we can develop the above formalism of nilpotent Artin-Schreier theory which provides us with the identification $\Gamma_K/\Gamma_K^p C_p(\Gamma_K) = G(\mathcal{L})$, where $\mathcal{L}$ is the maximal quotient of nilpotnent class $< p$ of the pro-free P-topological Lie algebra over $\mathbb{F}_p$ with the set of topologcal generators $\{D_{(a,b)} \mid (a,b) > (0,0), (a,b,p) = 1 \text{ or } (a,b) = (0,0)\}$.

Remark. *The above situation admits a generalisation to the case of local fields with an arbitrary last residue field (not just $\mathbb{F}_p$) and an arbitrary dimension N (not just $N = 2$). There is also a ramification theory for such fields and the above identification of the Galois group with $G(\mathcal{L})$ can be extended by the explicit description of the images of the ramification subgroups of Γ_K in $G(\mathcal{L})$.*

1-dimensional local fields: mixed characteristic case

Let $[K : \mathbb{Q}_p] < \infty$. Suppose $M \in \mathbb{N}$ and a primitive p^M-th root of unity $\zeta_{p^M} \in K$. For simplicity we assume that $M = 1$ and the residue field k of K is $\mathbb{F}_p$.

Consider the following special case of the situation, which appears in the theory of the field-of-norms functor. Fix a uniformizer $\pi_0 \in K$ and set $\widetilde{K} = \cup_{s \geqslant 0} K(\pi_s)$, where $\pi_{s+1}^p = \pi_s$ for all $s \geqslant 0$. Then $\mathrm{Gal}(\bar{K}/\widetilde{K})$ can be identified with the Galois group of $\mathcal{K} = \mathbb{F}_p((t))$. $\Gamma_{\mathcal{K}}$ is not normal in Γ_K, but there is an exact sequence of p-groups

$$1 \longrightarrow H \longrightarrow \Gamma_K/\Gamma_K^p C_p(\Gamma_K) \longrightarrow \langle \tau \rangle \longrightarrow 1,$$

where the last gorup is $\mathrm{Gal}(K_1/K)$ and τ is its element such that $\tau(\pi_1) = \zeta_p \pi_1$. There is also a group epimorphism from $G(\mathcal{L}) = \Gamma_{\mathcal{K}}/\Gamma_{\mathcal{K}}^p C_p(\Gamma_{\mathcal{K}})$ to H. This can be rewritten as the exact sequence of $\mathbb{F}_p$-Lie algebras (where J is an ideal in $\mathcal{L}$)

$$0 \longrightarrow \mathcal{L}/J \longrightarrow L \longrightarrow \langle \tau \rangle \longrightarrow 0.$$

The structure of this sequence can be described by the action of $\mathrm{ad}\,\tau$ on $\mathcal{L}$:

— if $(a,p) = 1$, then $(\mathrm{ad}\,\tau)(D_a) = aD_{a+e^0} + \dots$, where $e^0 = pe/(p-1)$; this allows us to kill extra generators coming from $\mathcal{L}$ to L;

— $\mathrm{ad}\,\tau(D_0) = \frac{1}{2}\sum_{a_1+a_2=e^0} a_1[D_{a_1}, D_{a_2}] \bmod C_3(\mathcal{L})$ — this is the Demushkin relation.

2-dimensional local fields: mixed characteristic case

Suppose K is 2-dimensional, $\mathrm{char}\, K = 0$, all other residue fields of K are of characteristic p and K admits a system of local parameters π_1 and π_2, where π_1 is algebraic over $\mathbb{Q}_p$ (K is so-called standard local field). Also assume that $\zeta_p \in K$.

In this situation there is a construction of an analogue of the Fontaine-Wintenberger field-of-norms functor (it was recently developed by the author). This provides us with the exact sequence

$$1 \longrightarrow H \longrightarrow \Gamma_K/\Gamma_K^p C_p(\Gamma_K) \longrightarrow \langle\tau_1\rangle \times \langle\tau_2\rangle \longrightarrow 1,$$

where $\tau_i(\sqrt[p]{\pi_j}) = \zeta_p^{\delta_{ij}} \sqrt[p]{\pi_j}$ for $i, j = 1, 2$. Recall that all objects are provided with additional P-topological structure. We also have an epimorphic P-continuous map from $G(\mathcal{L})$ to H. As earlier, we must describe the operators $\operatorname{ad}\tau_1$ and $\operatorname{ad}(\tau_2)$ on $\mathcal{L}$.

— if $(a, b) \neq (0, 0)$, then $\operatorname{ad}\tau_1(D_{(a,b)}) = aD_{(a+e^0,b)} + \dots$ and $\operatorname{ad}\tau_2(D_{(a,b)} = bD_{(a+e^0,b)} + \dots$. These relations allow us to kill extra generators but also imply that $b\operatorname{ad}\tau_1 - a\operatorname{ad}\tau_2$ commutes with $D_{(a,b)}$. This situation needs a very careful study, because (according to explanations of F. Pop) one can't expect the appearance of commuting pairs in the Galois group modulo second term of its p-central series.

— for $(a, b) = (0, 0)$ we have also the relation

$$(\operatorname{ad}\tau_2)(D_{(0,0)}) = \tfrac{1}{2} \sum_{a_1+a_2=e^0 b_1+b_2=0} b_1[D_{(a_1,b_1)}, D_{(a_2,b_2)}] \operatorname{mod} C_3(\mathcal{L}).$$

This relation can be considered as an analogue of the Demushkin relation.

Almost commuting elements in small Galois groups

F. Pop

Recall the following two theorems which give rise to valuations via Galois theory:

Theorem (Ware, Mináč, Arason-Elman-Jacob, Koenigsmann, Efrat, ...). *Let ℓ be a prime number, and let K be a field with $\ell \neq \operatorname{char}(K)$ and $\mu_\ell \subseteq K$. Let $G_K(\ell)$ be the Galois group of the maximal pro-ℓ extension of K. Then for every closed subgroup $\Delta = \overline{\langle\sigma, \tau\rangle} \leq G_K(l)$, fitting into an exact sequence*

$$1 \to \mathbb{Z}_\ell \to \Delta \to \mathbb{Z}_\ell \to 1,$$

in particular Δ meta-cyclic, there exists a valuation v on K and a prolongation v^ℓ of v on $K(\ell)$, such that denoting by $I(v^\ell|v) \subset D(v^\ell|v)$ the inertia, respectively the decomposition group of $v^\ell|v$, and by Kv the residue field of v, one has:

- $\Delta \leq D(v^\ell|v)$,
- $\Delta \cap I(v^\ell|v) \neq 1$,
- $\operatorname{char}(Kv) \neq \ell$.

Theorem (Bogomolov, Bogomolov-Tschinkel). *Let k be an algebraically closed field, $K|k$ a field extension, and $\ell \neq \operatorname{char}(K)$ a prime number. Let K' be a maximal pro-ℓ abelian extension of K, and $K''|K'$ a maximal pro-ℓ central extension of $K'|K$. Denote by $G''_K \to G'_K$ the corresponding projection between Galois groups. Let $\Delta = \overline{\langle\sigma, \tau\rangle} \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \leq G'_K$ such that its preimage Δ'' in G''_K is abelian. Then there exists a valuation v on K such that*

- $\Delta \leq D_v \leq G'_K$,
- $\Delta \cap I_v \neq \{1\}$,
- $\mathrm{char}(Kv) \neq \ell$.

Here, $I_v \subset D_v$ denote the inertia, respectively the decomposition group, of some prolongation of v to K'.

In the talk the following common generalization of the above results was explained, which at the same time extends some previous results by Mináč, Mahé-Mináč-Smith of the case $\ell = 2$. For a profinite group G, call $\sigma, \tau \in G$ *almost commuting*, if $\overline{\langle \sigma, \tau \rangle}$ is met-abelian. Then one has fact:

Theorem. *Let K be a field, $\ell \neq \mathrm{char}(K)$ such that $\mu_{\ell^m} \subseteq K$ for some $m > 0$, and $m > 1$ if $\ell = 2$. Let K' be a maximal abelian l^m-elementary extension of K, $K''|K'$ a maximal ℓ^m-elementary central extension of $K'|K$, and $G''_K \to G'_K$ the corresponding projection of Galois groups. Let σ, τ be elements of G'_K such that $\Delta := \overline{\langle \sigma, \tau \rangle} \cong \mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z} \leq G'_K$, and suppose that σ, τ have some almost commuting preimages σ', τ' in G''_K. Then there exists a valuation v of K such that*

- $\Delta \leq D_v \leq G'_K$,
- $\Delta \cap I_v \neq \{1\}$,
- $\mathrm{char}(K_v) \neq \ell$.

Here, $I_v \subset D_v$ denote the inertia, respectively the decomposition group, of some prolongation of v to K'.

For the proof one employs the method of constructing valuations of a field as developed by Jacobs, Mináč, Ware, etc., together with some ideas from Bogomolov-Tschinkel.

References

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

[2] F. A. Bogomolov, *On two conjectures in birational algebraic geometry,* in Algebraic Geometry and Analytic Geometry, ICM-90 Satellite Conference Proceedings, ed A. Fujiki et all, Springer Verlag Tokyo 1991.

[3] F. A. Bogomolov and Y. Tschinkel, *Reconstruction of function fields,* Manuscript, March 2003.

[4] I. Efrat, *Construction of valuations from K-theory,* Mathematical Research Letters 6 (1999), 335-344.

[5] A. J. Engler and J. Koenigsmann, *Abelian subgroups of pro-p Galois groups,* Trans. AMS **350** (1998), no. 6, 2473–2485.

[6] L. Mahé and J. Mináč and T. L. Smith, *Additive structure of multiplicative subgroups of fields and Galois theory*, Documenta Math. **9** (2004) 301–355.

Some remarkable groups

A. Zuk

Reporter's Note: *The speaker did not submit an extended abstract of his talk. The following short summary is based on my own notes.*

In his talk Zuk described several automata groups on the alphabet $\{0,1\}$ which, despite the simplicity of the underlying automata, possess remarkable properties.

His first topic was Atiyah's question regarding the rationality of L^2 Betti numbers of closed manifolds. Zuk explained how to construct a closed manifold whose third L^2 Betti number equals $1/3$ and is not related to the torsion of the associated fundamental group. His second topic was amenability. In this context Zuk displayed an example of a (finitely presented) group which is amenable but not contained in the smallest class of groups including all groups of sub-exponential growth and closed under taking subgroups, quotients, direct limits and extensions.

Representation growth of nilpotent groups and Igusa's local zeta functions

C. Voll

A finitely generated, torsion-free nilpotent group Γ has – up to twisting with a linear character – only finitely many irreducible complex characters of each finite degree n. Let us call this number a_n. The study of the *representation growth* of Γ seeks to understand how the sequence (a_n) behaves as n tends to infinity. One way to make this sequence tractable is to encode it into a Dirichlet series

$$\zeta_\Gamma^{\mathrm{irr}}(s) := \sum_{n=1}^{\infty} a_n n^{-s},$$

where s is a complex variable. Owing to the nilpotency of Γ, this *representation zeta function* has an Euler product decomposition

$$\zeta_\Gamma^{\mathrm{irr}}(s) = \prod_{p \text{ prime}} \zeta_{\Gamma,p}^{\mathrm{irr}}(s)$$

into local representation zeta functions, enumerating characters of p-power degree. By a theorem of Hrushovski and Martin ([2]), these local representation zeta functions of Γ are rational functions in p^{-s}. The model-theoretic proof of this result, however, sheds little light on the explicit form of these local factors, or their dependence on the prime. We have

Theorem. *Let Γ be a finitely generated, torsion-free nilpotent group. Almost all local representation growth zeta functions are explicitly computable in terms of Igusa's local zeta functions associated to the degeneracy loci of certain matrices of linear forms. In particular, for almost all primes, a functional equation of the following form holds:*

$$\text{(FE)} \qquad \zeta_{\Gamma,p}^{\mathrm{irr}}(s)|_{p\to p^{-1}} = p^n \zeta_{\Gamma,p}^{\mathrm{irr}}(s),$$

where n is the Hirsch length of the derived group $\Gamma' = [\Gamma, \Gamma]$.

Via an explicit formula for Igusa's local zeta functions, essentially due to Denef ([1]), this result shows that the dependence of the local factors $\zeta^{\mathrm{irr}}_{\Gamma,p}(s)$ on the prime p reflects how the numbers of $\mathbb{F}_p$-points on certain smooth projective algebraic varieties defined over $\mathbb{F}_p$ vary with p. The local functional equation (FE) is 'inherited' from an analogous symmetry of Igusa's local zeta function, first observed by Denef and Meuser ([3]), who derived it from properties of the Hasse-Weil zeta functions associated to smooth projective varieties over finite fields.

Our main tool to obtain this result is the use of a 'Kirillov-theory' developed by Howe in the 1970ies for these groups ([4]). It describes a correspondence between irreducible characters and co-adjoint orbits in the dual of a Lie algebra associated to Γ.

References

[1] J. Denef, *On the degree of Igusa's local zeta function*, Amer. J. Math. **109** (1987), no. 6, 991–1008.

[2] E. Hrushovski and B. Martin, *Zeta functions from definable equivalence relations*, Preprint, 2004.

[3] J. Denef and D. Meuser, *A functional equation of Igusa's local zeta function*, Amer. J. Math. **113** (1991), no. 6, 991–1008.

[4] R. Howe, *On representations of discrete, finitely generated, torsion-free, nilpotent groups*, Pacific J. Math. **73** (1977), no. 2, 281–305.

Divisibility of special Values of Automorphic L-Functions and Denominators of Eisenstein classes

G. Harder

I discuss some conjectural relations between the integral structure of the cohomology of an arithmetic group and arithmetic properties of certain special values of L-functions attached to automorphic forms. This relation predicts that primes dividing an certain L -values attached to automorphic forms f also divide the denominators of Eisenstein cohomology classes attached to f. The divisibility of these denominators by certain primes creates congruences between systems of Hecke-eigenvalues on inner cohomology classes and eigenvalues on Eisenstein classes.

In my talk I first explained a very classical example and gave also a comparison between two different ways of speaking about these denominators. We consider the stack $S/\mathrm{Spec}(\mathbb{Z})$ of elliptic curves, on this stack we have the universal elliptic curve $\mathcal{E}/S$. We can compactify this stack by adding a point ∞ at infinity over which we have the groupoid of Tate curves, we write $\mathcal{E}^\vee/S^\vee$. We can define a line bundle $\omega/S^\vee$ such that $\omega^2/S^\vee$ is the bundle of differentials and we can enlarge it to $\omega^{\times 2}/S^\vee(\log)$ where we allow a first order pole at ∞.

We pick an even integer $k \geq 0$ and consider the free $\mathbb{Z}$ modules of sections

$$H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}) \hookrightarrow H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}(\log)).$$

It is a well known fact from the theory of modular forms and the theory of the moduli stack that $H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}(\log)) =$ Module of modular forms f of weight $k+2$ whose q expansions

$$f(q) = a_0 + a_1 q + a_2 q^2 \dots$$

have coefficients in $\mathbb{Z}$. The submodule $H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2})$ corresponds to the space of cusp forms, i.e. those for which $a_0 = 0$. The mapping sending f to a_0 is a residue map. For $k > 0$ we get an exact sequence

$$0 \to H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}) \to H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}(\log)) \to \mathbb{Z}_{\mathrm{DR}}(= \mathbb{Z} \cdot 1_{\mathrm{DR}}) \to 0$$

We define the topological space $S(\mathbb{C}) = \mathrm{Sl}_2(\mathbb{Z})\backslash\mathbb{H}$, on this space have a sheaf $\tilde{\mathcal{M}}_k$ which is obtained from the standard representation of $\mathrm{Sl}_2(\mathbb{Z})$ on the homogenous polynomials $\sum a_\nu X^\nu Y^{k-\nu}$ where the $a_\nu \in \mathbb{Z}$.

We consider the cohomology with coefficients in this sheaf (See [3] Chap. 2 and 3) and we get the exact sequence in cohomology

$$0 \to H^1_!(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \to H^1(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \to H^1(\partial S(\mathbb{C}), \tilde{\mathcal{M}}_k) \to H^2_c(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \to 0$$

Now we have the following facts

(i) On all these modules we have an action of the Hecke algebra, which is built up from the commuting family of endomorphisms T_p, $p = 2, 3, 5, \dots$. These operators commute with all arrows (also the arrows still to come)

(ii) If we tensorize by the complex numbers then we have a canonical injection

$$H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}(\log)) \otimes \mathbb{C} \hookrightarrow H^1(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \otimes \mathbb{C}$$

this (part of) is the Eichler-Shimura isomorphism.

(iii) The Hecke operator T_p acts on $\mathbb{Z}_{\mathrm{DR}}$ by the eigenvalue $p^{k+1} + 1$, and $H^1(\partial S(\mathbb{C}), \tilde{\mathcal{M}}_k)$ contains a unique summand $\mathbb{Z} \cdot 1_{\mathrm{B}}$ on which T_p acts by the same eigenvalue. We have $H^1(\partial S(\mathbb{C}), \tilde{\mathcal{M}}_k) = \mathbb{Z} \cdot 1_{\mathrm{B}} \oplus$ torsion and T_p acts nilpotently on the torsion and on the torsion module $H^2_c(S(\mathbb{C}), \tilde{\mathcal{M}}_k)$.

Now it is a classical result that the system of eigenvalues $\{p^{k+1} + 1\}$ does not occur neither in $H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}) \otimes \mathbb{C}$ nor in $H^1_!(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \otimes \mathbb{C}$ and therefore we get canonical splittings

$$H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}) \otimes \mathbb{Q} \oplus \mathbb{Q}E^{\mathrm{DR}}_{k+2} = H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}(\log)) \otimes \mathbb{Q}$$

and

$$H^1_!(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \otimes \mathbb{Q} \oplus \mathbb{Q}E^{\mathrm{B}}_{k+2} = H^1(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \otimes \mathbb{Q}$$

The question we ask is: What are the denominators of these Eisenstein classes, i.e. what are the smallest (with respect to divisibility) integers $\Delta_{\mathrm{DR}}(k), \Delta_{\mathrm{B}}(k)$ such that

$$\Delta_{\mathrm{DR}}(k) E^{\mathrm{B}}_{k+2} \in H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2})$$

$$\Delta_{\mathrm{B}}(k) E^{\mathrm{DR}}_{k+2} \in \mathrm{Im}(H^1(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \to H^1(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \otimes \mathbb{Q}).$$

We may weaken the question slightly and ask for the primes ℓ dividing the denominators. In the case of the de-Rham cohomology the class E_{k+2}^{DR} is given by the classical Eisenstein series, whose q-expansion is

$$E_{k+2}^{\mathrm{DR}} = 1 + \frac{2}{\zeta(-1-k)} \sum_{n=1}^{\infty} (\sum_{d|n} d^{k+1}) q^n.$$

Here it is clear that the denominator is the numerator of $\zeta(-1-k)/2$.

We have the same result for the denominator of the the Eisenstein class: Up to some irrelevant small factors we have $\Delta_{\mathrm{B}}(k) =$ numerator of $\zeta(-1-k)$. This has been proved in the Diploma thesis [4] of Christian Kaiser.

Both results have the same shape, but they are independent results in the following sense: Neither of the results is an easy or formal consequence of the other, they require independent proofs. Both results have a common consequence:

For any prime ℓ, which divides $\zeta(-1-k)$ we can find an extension $F/\mathbb{Q}$ with ring of integers $\mathcal{O}_F$, a prime $\mathfrak{l}$ lying above ℓ and eigenclasses $f_{\mathrm{DR}} \in H^0(S^\vee, \omega^{\otimes k} \otimes \omega^{\otimes 2}) \otimes F, f_{\mathrm{B}} \in H^1(S(\mathbb{C}), \tilde{\mathcal{M}}_k) \otimes F$ such that for the eigenvalues $T_p(f) = \lambda(p) f, \lambda(p) \in \mathcal{O}_F$, we have the congruences

$$\lambda(p) \equiv p^{k+1} + 1 \mod \mathfrak{l}.$$

It is well known that this result has important arithmetic consequences. (See [5])

Both approaches to produce such congruences generalize to other situations, but I strongly believe, that we have cases in which the approach via Betti-cohomology works but where it is not clear what it means to speak of denominators of de-Rham cohomology classes.

In my talk I discussed very briefly an example, where a conjectural assertion for a denominator of an Eisenstein class in the Betti-cohomology predicts congruences. (For more details see [2]). We consider the unique cusp form f of weight 22,

$$f(q) = q - 288q^2 - 128844q^3 - 2014208q^4 + 21640950q^5 + \ldots = \sum_{n=1}^{\infty} a_n q^n,$$

we find that the normalized L-value we get a divisibility $41 \mid \frac{\Lambda(f,14)}{\Omega_+}$, from the numbers $k+2 = 22$ and the critical argument 14 we new numbers $\nu = 22 - 14 = 8, \nu - 1 = 7, k + 2 - 2\nu - 2 = 4$, and this provides a highest weight $\lambda = 4\gamma_\beta + 7\gamma_\alpha$ for the symplectic group $\mathrm{GSp}_2/\mathrm{Spec}(\mathbb{Z})$ and hence a coefficient system $\tilde{\mathcal{M}}_\lambda$. Again we have a space $S(\mathbb{C}) = \mathrm{GSp}_2(\mathbb{Z}) \backslash \mathbb{H}_2$. The form f represents a class $[f]$ in the integral cohomology $H^3(\partial(S(\mathbb{C})), \tilde{\mathcal{M}}_\lambda)$, the resulting Eisenstein class $\mathrm{Eis}[f] \in H^3(S(\mathbb{C}), \tilde{\mathcal{M}}_\lambda) \otimes \mathbb{Q}$. I expect that the denominator of this class is divisible by $\ell = 41$. This would imply that we find a vector valued Siegel modular form E_f which is an eigenform with eigenvalues $\lambda^{(1)}(p)$ for a Hecke operator $T_p^{(1)}$ such that we have the congruences

$$\lambda^{(1)}(p) \equiv p^{13} + a_p + p^8 \mod 41 \text{ for all primes } p.$$

The existence of such a form follows from the work of C. Faber and G. van der Geer [1] and computer program in the background also provided me with a list of eigenvalues $\lambda^{(1)}(p)$ for $p \leq 37$. The congruences are true for these primes.

References

[1] C. Faber and G. van der Geer, *Sur la cohomologie des systemes locaux sur les espaces de modules des courbes de genre 2 et des surfaces abeliennes*, I. C. R. Math. Acad. Sci. Paris **338** (2004), 381–384.

[2] G. Harder, *A congruence between a Siegel and an elliptic modular form*, (Eisenstein/kolloquium.pdf), http://www.math.uni-bonn.de/people/harder/.

[3] G. Harder, *Cohomology of arithmetic groups*, (buch/chap. 2-6), http://www.math.uni-bonn.de/people/harder/.

[4] C. Kaiser, *Die Nenner von Eisensteinclassen zu gewissen Kongruenzuntergruppen*, Dipolmarbeit, Bonn 1990.

[5] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Inv. Math. **34** (1976), 151–162.

The congruence kernel of an arithmetic lattice in a rank one algebraic group over a local field

P. A. Zalesskii

(joint work with A. W. Mason, A. Premet and B. Sury.)

Let k be a global field and let $\mathbf{G}$ be a connected, simply-connected linear algebraic group over k, which is absolutely almost simple. For each non-empty, finite set S of places of k, containing all the archimedean places, let $\mathcal{O}(S)$ denote the corresponding *ring of S-integers in k.* The problem of determining whether or not a finite index subgroup of the arithmetic group, $\mathbf{G}(\mathcal{O}(S))$, contains a principal congruence subgroup (modulo some non-zero $\mathcal{O}(S)$-ideal), the so-called *congruence subgroup problem* or CSP, has attracted a great deal of attention since the 19th century. As a measure of the extent of those finite index subgroups of $\mathbf{G}(\mathcal{O}(S))$ which are not congruence, its so-called *non-congruence subgroups*, Serre [S1] has introduced a profinite group, $C(S, \mathbf{G})$, called the *(S-)congruence kernel* of $\mathbf{G}$. In his terminology [S1] the CSP for this group has an *affirmative* answer if this kernel is finite. Otherwise the CSP has an *essentially negative* answer. The principal result in [S1] is that, for the case $\mathbf{G} = \mathbf{SL}_2$, the congruence kernel $C(S, \mathbf{G})$ is *finite* if and only if card$S \geq 2$. Moreover Serre has formulated the famous *congruence subgroup conjecture* [PR, p. 556], which states that the answer to the CSP is determined entirely by the *S-rank* of $\mathbf{G}$, rank$_{\mathrm{S}}\mathbf{G}$. (See [Mar, p. 258].) It is known [Mar, (2.16) Theorem, p. 269] that $C(S, \mathbf{G})$ is finite (cyclic), when $\mathbf{G}$ is *k-isotropic* and rank$_S\mathbf{G} \geq 2$. It is also known that $C(S, \mathbf{G})$ is infinite for many "rank one" $\mathbf{G}$ (for example, $\mathbf{G} = \mathbf{SL}_2$). The conjecture however remains open for some of these cases. (See, for example, [L3].) The congruence kernel $C(S, H)$ can be defined in a similar way for every subgroup H of $\mathbf{G}(k)$ which is commensurable with $\mathbf{G}(\mathcal{O}(S))$. (From this definition it is clear that $C(S, H)$ is finite if and only if $C(S, \mathbf{G})$ is finite.)

The books of Margulis [Mar, p. 268] and Platonov/Rapinchuk [PR, Section 9.5] emphasise the importance of determining the *structure* of the congruence kernel. (Lubotzky refers to this as the *complete* solution of the CSP.) We are concerned with the structure of infinite congruence kernels. The first result of this type is due to Mel'nikov [Me], who shows that, for the case where $\mathbf{G} = \mathbf{SL}_2$, $k = \mathbb{Q}$ and $S = \{\infty\}$, (i.e. $\mathbf{G}(\mathcal{O}(S)) = \mathrm{SL}_2(\mathbb{Z})$, the classical *modular group*), the congruence kernel is isomorphic to $\hat{F}_\omega$, the *free profinite group on countably many generators.* Lubotzky [L1] has proved that, when $\mathbf{G} = \mathbf{SL}_2$ and card $S = 1$, the congruence kernel of $\mathrm{SL}_2(\mathcal{O}(S))$ has a closed subgroup isomorphic to $\hat{F}_\omega$, reproving Mel'nikov's result in the process. (When char $k = 0$ and card $S = 1$, it is known that $k = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$, with $S = \{\infty\}$, where d is a square-free positive rational integer.) In [Mas2] it is shown that, when $\mathbf{G} = \mathbf{SL}_2$ and card $S = 1$, the congruence kernel maps onto every free profinite group of finite rank.

We extend these results by determining the structure of the congruence kernel of an arithmetic lattice in a rank one algebraic group over a local field, providing a complete solution of the CSP for this case. With the above notation let V_k be the set of places of k and let (the local field) k_v be the completion of k with respect to v. In addition to the above hypotheses we assume that $\mathbf{G}$ has k_v-rank 1. We denote the set of k_v-rational points, $\mathbf{G}(k_v)$, by G. Let Γ be a *lattice* in G, i.e. a discrete subgroup of (the locally compact group) G for which $\mu(G/\Gamma)$ is *finite*, where μ is a Haar measure on G. As usual Γ is said to be *cocompact* (resp. *non-uniform*) if G/Γ is compact (resp. not compact). We assume further that Γ is $(S-)$*arithmetic*, i.e. Γ is commensurable with $\mathbf{G}(\mathcal{O})$, where $\mathcal{O} = \mathcal{O}(S)$ is as above. *Example.* When char$k > 0$, $S = \{v\}$ and $\mathbf{G} = \mathbf{SL}_2$, the group $\Gamma = \mathrm{SL}_2(\mathcal{O})$ is a (non-uniform) arithmetic lattice (in $\mathrm{SL}_2(k_v)$). This lattice, which plays a central role in the theory of Drinfeld modules, is the principal focus of attention in Chapter II of Serre's book [S2].

As in Margulis's book [Mar, Chapter I, 3.1, p.60] we assume that $\mathbf{G}$ is k-subgroup of $\mathbf{GL}_n$, for some n. We consider the standard representation for $\mathbf{GL}_n(k_v)$. For each $\mathcal{O}$-ideal $\mathfrak{q}$, we put

$$\mathbf{GL}_n(\mathfrak{q}) = \{X \in \mathbf{GL}_n(\mathcal{O}) \mid X \equiv I_n \pmod{\mathfrak{q}}\}.$$

We denote $\mathbf{G} \cap \mathbf{GL}_n(\mathfrak{q})$, the *principal S-congruence subgroup of* $\mathbf{G}$ *(of level* $\mathfrak{q}$*)*, by $\mathbf{G}(\mathfrak{q})$. If M is any subgroup of G we put $M(\mathfrak{q}) = M \cap \mathbf{G}(\mathfrak{q})$. It is clear that $M(\mathfrak{q})$ is of finite index in M when $\mathfrak{q} \neq \{0\}$.
The finite index subgroups of $\Gamma(\mathcal{O})$ define the *S-arithmetic* topology on Γ. The completion of Γ with respect to this topology is a profinite group denoted by $\hat{\Gamma}$. On the other hand the subgroups $\Gamma(\mathfrak{q})$, where $\mathfrak{q} \neq \{0\}$, define the *S-congruence* topology on Γ and the completion of Γ with respect to this topology is also a profinite group denoted by $\bar{\Gamma}$. Since every S-congruence subgroup is S-arithmetic, there is an exact sequence

$$1 \to C(\Gamma) \to \hat{\Gamma} \to \overline{\Gamma} \to 1.$$

The (profinite) group $C(\Gamma)(= C(S,\Gamma))$ is called the *(S-)congruence kernel* of Γ. It is known [Mar Chapter I, 3.1] that the definition of $C(\Gamma)$ does not depend on the

choice of k-representation. (The definition of congruence kernel extends to any S-arithmetic subgroup of G, including any finite index subgroup of Γ.)
Our principal results are the following.

Theorem A. *If* Γ *is cocompact, then* $C(\Gamma)$ is isomorphic to a free profinite group $\hat{F}_\omega$.

It is well-known that Γ is cocompact when, for example, char $k = 0$. For examples of this type see [S2, p. 84]. This result however is not a straightforward generalization of Mel'nikov's theorem [Me]. On the one hand $\mathrm{SL}_2(\mathbb{Z})$ is *not* a lattice in $\mathrm{SL}_2(\mathbb{Q}_p)$, where $\mathbb{Q}_p$ is the p-adic completion of $\mathbb{Q}$ with respect to any rational prime p; $\mathrm{SL}_2(\mathbb{Z})$ is a *non-uniform* lattice in $\mathrm{SL}_2(\mathbb{R})$. (See [Mar, p. 295].) Moreover it was proved in [Za2] that the congruence kernel of every arithmetic lattice in $\mathrm{SL}_2(\mathbb{R})$ is isomorphic to $\hat{F}_\omega$.

Theorem B. *If* Γ *is non-uniform and* $p =$ char k*, then*

$$C(\Gamma) \cong \hat{F}_\omega \amalg N(\Gamma),$$

the free profinite product of $\hat{F}_\omega$ *and* $N(\Gamma)$*, where* $N(\Gamma)$ *is a free profinite product of groups, each of which is isomorphic to the direct product of* $2^{\aleph_0}$ *copies of* $\mathbb{Z}/p\mathbb{Z}$.

The most interesting consequence of Theorems A and B is that the structure of $C(\Gamma)$ depends *only* on the characteristic of k.
The proofs are based on the action of G, and hence Γ, on the associated Bruhat-Tits tree T. The theory of groups acting on trees shows how to derive the structure of Γ from that of the quotient graph $\Gamma\backslash T$. For the cocompact case it is well known that $\Gamma\backslash T$ is finite. Theorem A then follows from the theory of free profinite groups. For the non-uniform case the situation is much more complicated. Here Lubotzky [L2] has shown that $\Gamma\backslash T$ is the union of a finite graph together with a (finite) number of ends, each of which corresponds to $\mathbf{P}$, a minimal parabolic k_v-subgroup of $\mathbf{G}$. The proof that the torsion-free part of the decomposition of $C(\Gamma)$ is $\hat{F}_\omega$ involves substantially more effort than that of Theorem A. It can be shown that the torsion part $N(\Gamma)$ is a free profinite product of groups each isomorphic to $C(U) = C(\mathbf{U}(\mathcal{O}))$, the *S-congruence kernel* of $\mathbf{U}$, where $\mathbf{U}$ is the unipotent radical of some $\mathbf{P}$ of the above type. It is known [BT2] that such a $\mathbf{U}$, and hence $C(U)$, is nilpotent of class at most 2. In fact it can be shown that $C(U)$ is *abelian*, even when $\mathbf{U}$ is not. In the proofs the various types of $\mathbf{G}$, which arise from Tits Classification [T], are dealt with separately. A crucial ingredient (when dealing with non-abelian $\mathbf{U}$) is the following unexpected property of "rank one" unipotent radicals.

Theorem C. *Let* $\mathbf{U}$ *be the unipotent radical of a minimal parabolic* k_v*-parabolic subgroup of* $\mathbf{G}$ *of the above type. If* $\mathbf{U}(k)$ *is not abelian then* $\mathbf{U}$ *is defined over* k.

Theorem B extends a number of existing results. The fourth author [Za1, Theorem 4.3] has proved Theorem B for the special case $\mathbf{G} = \mathbf{SL}_2$ and $S = \{v\}$. (This case is rather more straightforward since here $\mathbf{U}$ is abelian, and so Theorem C, for example, is not required.) Lubotzky [L1] has proved that, for this case, $C(\Gamma)$ has a closed subgroup isomorphic to $\hat{F}_\omega$. Lubotzky has also shown [L2, Theorem 7.5] that $C(\Gamma)$ is *infinite* when Γ is non-uniform.

Acknowledgements. The author was partially supported by FINATEC. He also thanks the organizers of the meeting and the Mathematisches Forschunginstitut for providing the opportunity to exchange ideas with the colleagues.

References

[BT2] A. Borel and J. Tits, Homomorphismes "abstraits" de groupes algébriques simples, Ann. of Math. (2) 97 (1973), 499-571.

[L1] A. Lubotzky, Free quotients and the congruence kernel of SL_2, J. Algebra 77 (1982), 411-418.

[L2] A. Lubotzky, Lattices in rank one Lie groups over local fields, Geom. Funct. Anal. 1 (1991), 405-431.

[L3] A. Lubotzky, Eigenvalues of the Laplacian, the first Betti number and the congruence subgroup problem, Ann. of Math. 144 (1996), 441-452.

[Mar] G.A. Margulis, *Discrete Subgroups of Semisimple Lie Groups*, Springer, 1991.

[Mas2] A.W. Mason, Quotients of the congruence kernels of SL_2 over arithmetic Dedekind domain, Israel J. Math. 91 (1995), 77-91.

[Me] O. V. Mel'nikov, The congruence kernel of the group $\mathrm{SL}_2(\mathbb{Z})$, (Russian) Dokl. Akad. Nauk. 228 (1976), 1034-1036. (Translation) Soviet Math. Dokl. 17 (1976), 867-870.

[PR] V. P. Platonov and A. S. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1994.

[S1] J-P. Serre, Le problème des groupes de congruence pour $\mathbf{SL}_2$, Ann. of Math. 92 (1970), 489-527.

[S2] J-P. Serre, *Trees*, Springer, 1980.

[T] J. Tits, Classification of algebraic semi-simple groups, Proc. Symp. Pure Math. 33, part 1, American Math. Soc., Providence (1979), 29-69.

[Za1] P.A. Zalesskii, Normal subgroups of free constructions of profinite groups and the congruence kernel in the case of positive characteristic, (Russian) Izv. Ross. Akad. Nauk Ser. Mat. 59 (1995), 59-76. (Translation) Izv. Math. 59 (1995), 499-516.

[Za2] P. A. Zalesskii, Profinite surface groups and the congruence kernel of arithmetic lattices in $\mathrm{SL}_2(\mathbb{R})$. Israel Journal of Mathematics 146 (1995), 111-123.

Euler characteristics of p-torsion Iwasawa modules

S. Wadsley

Suppose k is a finite field of characteristic p and G is a p-adic analytic group without elements of order p. Write G_{reg} for the subset of G consisting of elements of finite order and kG for the completed group algebra of G over k.

Given a finitely generated kG-module we may define the Euler characteristic by taking the alternating product of the orders of the homology groups $H_i(G, M)$. A theorem of Serre says that the Euler characteristic is 1 for all kG-modules that are finite dimensional over k if and only if the centralisers of all elements in G_{reg} are infinite. The question arises as to how this theorem generalises to finitely generated kG-modules not finite dimensional over k.

A joint paper of Konstantin Ardakov and myself proved the following

Theorem 1. *The Euler characteristic is* 1 *for all finitely generated torsion kG-modules if and only if* $C_G(x)$ *is open in* G *for all* x *in* G_{reg}.

This follows from a stronger theorem we proved.

Theorem 2. *The rank of the natural map*

$$K_0(\textit{finitely generated torsion kG-modules}) \to K_0(\textit{finitely generated kG-modules})$$

is equal to the number of Galois orbits of conjugacy classes in G_{reg} *of dimension at most* $\dim G - 1$.

Now there is a natural dimension function on the category of all finitely generated kG-modules given by $\dim_G(M) = d - \min\{j \mid \mathrm{Ext}^j(M, kG) \neq 0\}$. This gives a filtration of the category of finite dimensional kG-modules:

$$F_t = \{\text{finitely generated kG-modules with } \dim_G(M) \leq t\}.$$

Now we may define natural maps θ_t from $K_0(F_t)$ to $K_0(F_d)$ and ask what the rank of these maps is. The following half answers this question.

Theorem 3. *The rank of* θ_t *is at most the number of Galois orbits of conjugacy classes in* G_{reg} *with centraliser of dimension at most* t.

It follows that if $\dim C_G(x) > t$ for all x in G_{reg} then the Euler characteristic is 1 for all M in F_t.

It is natural to ask whether one always gets equality in the theorem above. The answer is yes for $t = 0$, $t = \dim G - 1$ and $t = \dim G$ irrespective of the group and for all t if G has an open abelian subgroup. However it is not true in general.

For example if one takes the group $H = H_{2r+1}$, the pro-p completion of a discrete Heisenberg group of dimension $2r + 1$, one may find an automorphism g of finite order that only fixes the centre. Now if G is the semi-direct product of H and $\langle g \rangle$ then it provides a counter-example since every module of dimension at most r has Euler characteristic 1 and so the rank of θ_r is 0 but $C_G(g)$ has dimension 1 which may be chosen to be smaller than r.

This leaves the following two natural open questions

(1) Can the bound be improved?
(2) What happens if k is replaced by the p-adic integers?

On the $K(\pi,1)$-property for rings of integers

A. Schmidt

Let k be a number field, S a finite set of non-archimedean primes of k and p a prime number which, for simplicity, we assume to be *odd*. Let k_S denote the maximal extension of k unramified outside S and let $k_S(p)$ be the maximal pro-p subextension of k in k_S. We put $G_S = \mathrm{Gal}(k_S/k)$ and $G_S(p) = \mathrm{Gal}(k_S(p)/k)$.

The group $G_S(p)$ reflects arithmetic properties of k and is difficult to understand. A systematic study of this group had been started by Shafarevich and was continued by Koch, Kuzmin, Wingberg and many other people.

See [NSW], VIII, §7 for basic properties of $G_S(p)$. It is most interesting if it reflects the étale cohomology of the underlying scheme. We put $X = Spec(\mathcal{O}_k)$. Then $G_S(p)$ is the maximal pro-p-factor group of the étale fundamental group $G_S = \pi_1^{et}(X \smallsetminus S)$ of the complement $X \smallsetminus S$ of S in X. Therefore each discrete p-primary $G_S(p)$-module M defines a locally constant étale sheaf on X which we will also denote by M. For each M and all i the Hochschild-Serre spectral sequence for the universal pro-p-covering of $X \smallsetminus S$ induces natural homomorphisms

$$\phi_{M,i}\colon\ H^i(G_S(p), M) \longrightarrow H^i_{et}(X \smallsetminus S, M),$$

which are isomorphisms for $i = 0, 1$ for trivial reasons.

Definition 1. *We say that* $\boldsymbol{X \smallsetminus S}$ **is a** $\boldsymbol{K(\pi,1)}$ **for** $\boldsymbol{p}$ *(and the étale topology) if* $\phi_{M,i}$ *is an isomorphism for all* M *and* i.

Remarks: 1. The given condition is satisfied if and only if the natural morphism

$$(X \smallsetminus S)_{et}(p) \longrightarrow K(G_S(p), 1)$$

from the pro-p-completion of the étale homotopy type $(X \smallsetminus S)_{et}$ of $X \smallsetminus S$ (see [AM]) to the $K(\pi, 1)$-pro-space attached to the pro-p-group $G_S(p)$ is weak equivalence. This justifies the terminology.

2. If $X \smallsetminus S$ is a $K(\pi, 1)$ for p, then $cd\, G_S(p) \leq 3$. If S contains at least one non-archimedean prime then $cd\, G_S(p) \leq 2$.

We denote by S_p and S_∞ the set of primes of k dividing p and the set of archimedean primes of k, respectively.

Proposition 2. *If* S *contains* S_p*, then* $X \smallsetminus S$ *is a* $K(\pi, 1)$ *for* p.

Having dealt with the *wild case* $S \supset S_p$, two cases remain: The *tame case* where $S \cap S_p = \varnothing$ and the *mixed case*, where there are primes dividing p in S as well as outside S. We will not consider the mixed case here, as it is much harder and only little is known.

For the remainder of this paper, we will restrict to the tame case, i.e. we assume that $S \cap S_p = \varnothing$. Further, as p is odd, archimedean primes are not of interest and we assume $S \cap S_\infty = \varnothing$. Consider the subset

$$\begin{aligned} S^{\min} &= \{\mathfrak{p} \in S \mid N(\mathfrak{p}) \equiv 1 \bmod p\} \\ &= \{\mathfrak{p} \in S \mid \mu_p \subset k_{\mathfrak{p}}\}. \end{aligned}$$

Then $G_S(p) = G_{S^{\min}}(p)$ and also the étale cohomology does not change. Further, we will exclude the case $S = \varnothing$. Therefore we will assume in what follows:

S is a non-empty finite set of non-archimedean primes with $N(\mathfrak{p}) \equiv 1 \bmod p$.

Lemma 3. $X \smallsetminus S$ *is a* $K(\pi, 1)$ *for* p *if and only if the following conditions* (i) *and* (ii) *hold.*

(i) $H^2(G_S(p), \mathbb{Z}/p\mathbb{Z}) \hookrightarrow H^2(X \smallsetminus S, \mathbb{Z}/p\mathbb{Z})$ *is an isomorphism.*

(ii) $cd\, G_S(p) \leq 2$.

Example: Assume that either $k = \mathbb{Q}$ or k is an imaginary quadratic number field with $(h_k, p) = 1$ and $k \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$. Then condition (i) holds and condition (ii) holds if S is strictly circular, see [La], [Vo].

Proposition 4. *Assume that $X \smallsetminus S$ is a $K(\pi, 1)$ for p and that $G_S(p) \neq 1$. Then the following holds.*

(i) *$cd\, G_S(p) = 2$, $scd\, G_S(p) = 3$.*
(ii) *$G_S(p)$ is a duality group (of dimension 2).*

Remarks: 1. If $X \smallsetminus S$ is a $K(\pi, 1)$ for p and $G_S(p) = 1$, then $\#S = 1$, k is imaginary quadratic and $p = 2$ or 3. See [Sc] for a more precise statement.

2. In the wild case $S \supset S_p$, where $X \smallsetminus S$ is always a $K(\pi, 1)$ for p, $G_S(p)$ is not necessarily of cohomological dimension 2 (e.g. $k = \mathbb{Q}(\zeta_p)$, p regular, $S = S_p$). The strict cohomological dimension in the wild case is conjecturally equal to 2 (=Leopoldt's conjecture for each finite subextension of k in $k_S(p)$). In the wild case, $G_S(p)$ is "often" a duality group.

It is a natural question how far we get locally at the primes in S when going up to $k_S(p)$.

Proposition 5. *Assume that $X \smallsetminus S$ is a $K(\pi, 1)$ for p and that $G_S(p) \neq 1$. Then $k_S(p)$ realizes the maximal unramified p-extension of $k_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$, i.e.*

$$k_{\mathfrak{p}}^{nr}(p) \subset k_S(p)_{\mathfrak{p}} \quad \text{for all } \mathfrak{p} \in S.$$

If $\mathfrak{p} \in S$ ramifies in k_S, then $k_S(p)_{\mathfrak{p}} = k_{\mathfrak{p}}(p)$, i.e. $k_S(p)$ realizes the maximal p-extension of $k_{\mathfrak{p}}$.

The next result gives a sufficient criterion for a prime $\mathfrak{p} \in S$ to ramify in $k_S(p)$. For the definition of the group $V_S = V_S(k, \mathbb{Z}/p\mathbb{Z})$ see [NSW], VIII, §6.

Proposition 6. *Let $\mathfrak{p} \in S$ be a prime and let $S' = S \smallsetminus \{\mathfrak{p}\}$. Assume that the natural inclusion $V_S \hookrightarrow V_{S'}$ is an isomorphism. Then $\mathfrak{p}$ ramifies in $k_S(p)$.*

Corollary 7. *Assume that either $k = \mathbb{Q}$ or k is an imaginary quadratic number field with $(h_k, p) = 1$, and $p \neq 3$ if $k = \mathbb{Q}(\sqrt{-3})$. Then every prime $\mathfrak{p} \in S$ ramifies in $k_S(p)$. If, addition, $X \smallsetminus S$ is a $K(\pi, 1)$ for p, then $k_S(p)_{\mathfrak{p}} = k_{\mathfrak{p}}(p)$ for all $\mathfrak{p} \in S$.*

The fact that all primes in S ramify in $k_S(p)$ can be reformulated as an assertion on universal norms of global units.

Proposition 8. *Assume that $X \smallsetminus S$ is a $K(\pi, 1)$ for p. Then the following conditions are equivalent.*

(i) *all primes $\mathfrak{p} \in S$ ramify in $k_S(p)$.*
(ii)

$$\varprojlim_{K \subset k_S(p)} \mathcal{O}_K^\times / p = 0,$$

where K runs through all finite subextensions of k in $k_S(p)$.

Question:[1] *Can it ever happen that some $\mathfrak{p} \in S$ does not ramify in $k_S(p)$?*

Next we consider the problem of extending the set S.

Proposition 9. *Assume that $X \smallsetminus S$ is a $K(\pi,1)$ for p, and let $S' \supset S$ be a finite set of primes of norm $\equiv 1 \bmod p$. Assume that each $\mathfrak{q} \in S' \smallsetminus S$ does not split completely in $k_S(p)$. Then the following holds.*

(i) *$X \smallsetminus S'$ is a $K(\pi,1)$ for p.*
(ii) *$k_{S'}(p)_{\mathfrak{q}} = k_{\mathfrak{q}}(p)$ for all $\mathfrak{q} \in S' \smallsetminus S$.*

Furthermore, the arithmetic form of Riemann's existence theorem holds, i.e. the natural homomorphism

$$\mathop{*}_{\mathfrak{p} \in S' \backslash S(k_S(p))} T_{\mathfrak{p}}(k_{S'}(p)/k_S(p)) \longrightarrow Gal(k_{S'}(p)/k_S(p))$$

is an isomorphism. Here $T_{\mathfrak{p}}$ is the inertia group and $*$ denotes the free pro-p-product of a bundle of pro-p-groups, cf. [NSW], *Ch. IV, §3.*

Finally, we calculate the dualizing module.

Proposition 10. *Assume that $X \smallsetminus S$ is a $K(\pi,1)$ for p and that all $\mathfrak{p} \in S$ ramify in $k_S(p)$. Then the dualizing module D of $G_S(p)$ is given by*

$$D = tor_p C_S(k_S(p)),$$

where $tor_p C_S(k_S(p))$ is the subgroup of p-torsion elements in the S-idèle class group $C_S(k_S(p))$ of $k_S(p)$.

Proofs can be found in [Sc].

References

[AM] M. Artin and B. Mazur *Étale homotopy.* Lecture Notes in Math. No. 100 Springer-Verlag, Berlin-New York 1969

[La] J. P. Labute *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, to appear in J. Reine und angew. Math. 2006

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grundlehren der math. Wiss. Bd. 323, Springer-Verlag 2000.

[Sc] A. Schmidt *On the $K(\pi,1)$-property for rings of integers*, Preprint 2006.

[Vo] D. Vogel, *Circular sets of primes of imaginary quadratic number fields*, Preprints der Forschergruppe *Algebraische Zykel und L-Funktionen* Regensburg/Leipzig Nr. 5, 2006. http://www.mathematik.uni-regensburg.de/FGAlgZyk

Tree representations of discrete and profinite groups

M. Abert

Reporter's Note: *The following summary is based on the speaker's handwritten entry in the Vortragsbuch.*

Let Γ be a residually finite group and let $(H_i)_i$ be a chain of subgroups of Γ with $\bigcap_i H_i = 1$. If all the H_i have finite index in Γ, then Γ acts naturally on a

[1] We proved shortly after the conference that each $\mathfrak{p} \in S$ ramifies. See [Sc].

rooted tree whose vertices correspond to the cosets of the H_i. We analyze these actions on rooted trees for various classes of discrete groups.

Circular sets of primes of imaginary quadratic number fields

D. Vogel

Let K be a number field, p an odd prime number and S a finite set of primes of K not containing any primes diving p. Let $K_S(p)$ denote the maximal pro-p extension of K unramified outside S. Until recently, not much has been known on the structure of the Galois group $G_S(K)(p) = G(K_S(p)/K)$. In [1], Labute introduced the class of mild pro-p-groups and showed that mild pro-p-groups are of cohomological dimension 2. Additionally, he could show that if S satisfies a certain technical condition, namely if S is strictly circular, then $G_S(\mathbb{Q})(p)$ is a mild pro-p-group and hence of cohomological dimension 2. In [2], Schmidt extended Labute's results by arithmetical methods and obtained a criterion for S such that $G_S(\mathbb{Q})(p)$ is of cohomological dimension 2, although it is not necessarily a mild group. It is a natural question if one can find examples such that $G_S(K)(p)$ is a mild pro-p-group if the base field K is different from $\mathbb{Q}$.

In order to be able to apply the results of Labute on mild pro-p-groups, we have to make sure that $G_S(K)(p)$ has a minimal presentation with the same number of generators and relations. It turns out that if K is an imaginary quadratic number field whose class number is not divisible by p and which is different from $\mathbb{Q}(\sqrt{-3})$ if $p = 3$, then $G_S(K)(p)$ has a minimal presentation by $\#S$ generators and relations. We define linking numbers between the primes of $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ as follows. For each $i = 1, \dots, n$ we fix an extension $\mathfrak{Q}_i$ of $\mathfrak{q}_{\mathrm{i}}$ to $K_S(p)$, a generator τ_i of the inertia group of $\mathfrak{Q}_i$ in $K_S(p)/K$, and a Frobenius σ_i of $\mathfrak{Q}_i$ in $K_S(p)/K$. The linking number $\ell_{ij} \in \mathbb{Z}/p\mathbb{Z}$ between $\mathfrak{q}_i$ and $\mathfrak{q}_j$ is given by the image of σ_i under the projection map from $G_S(K)(p)$ to the Galois group of the maximal elementary abelian p-extension of K unramified outside of $\mathfrak{q}_j$, which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, a generator being induced by τ_j. Making use of the linking numbers we associate a directed graph $\Gamma_S(p)$ to S in the same way as Labute does in the case $K = \mathbb{Q}$. If $\Gamma_S(p)$ is a non-singular circuit, we call S strictly circular with respect to p. If S is strictly circular with respect to p, then $G_S(K)(p)$ is a mild pro-p-group and hence of cohomological dimension 2.

In view of Schmidt's results on the $K(\pi, 1)$-property of rings of integers, see [3], $\mathrm{Spec}(\mathcal{O}_K) - S$ is then a $K(\pi, 1)$ for the étale topology and p. Therefore, if S is strictly circular with respect to p, the strict cohomological dimension of $G_S(K)(p)$ equals 3, $G_S(K)(p)$ is a duality group and the dualizing module can be calculated. In addition, if $l \notin S$ is a prime of K whose norm is $\equiv 1$ modulo p, and which does not split completely in $K_S(p)/K$, then the cohomological dimension of the Galois group of $K_{S\cup\{l\}}(p)/K$ equals 2.

References

[1] J. Labute, *Mild pro-p groups and Galois groups of p-extensions of* $\mathbb{Q}$, to appear in J. Reine Angew. Math.

[2] A. Schmidt, *Circular sets of prime numbers and p-extensions of the rationals*, to appear in J. Reine Angew. Math.

[3] A. Schmidt, *On the* $K(\pi,1)$*-property for rings of integers*, this volume

[4] D. Vogel, *Circular sets of primes of imaginary quadratic number fields*, preprint

On global and local fundamental groups of algebraic varieties

F. Catanese

1. Motivation

The absolute Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on the set $\mathfrak{N}$ of irreducible components of moduli spaces, e.g., of $\mathfrak{M}_{x,y} := \{$ isomorphism classes of minimal surfaces S of general type with $\chi(\mathcal{O}_S) = x, K_S^2 = y\}$, since $\mathfrak{M}_{x,y}$ is defined over $\mathbb{Z}$.

In particular, $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on the set of 0-dimensional components, which correspond to the *rigid* varieties.

In this talk our preferred prime is $p = \infty$, and thus Frobenius is given by complex conjugation: $\sigma(z) = \bar{z}$ which acts on a moduli space by $[X] \mapsto [\bar{X}]$. An obvious but important fact is that the complex conjugate variety $\bar{X}$ is diffeomorphic to X.

Example 1. *Assume we have a class* $\mathfrak{M}$ *of complex algebraic varieties such that if* $X \in \mathfrak{M}$*, and* X*,* X'*, have the same characteristic numbers and isomorphic fundamental groups* $\pi_1(X) \cong \pi_1(X')$*, then* X' *and* X *or* X' *and* $\bar{X}$ *are deformation equivalent. Then* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *acts (factoring through* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})/\langle\langle\sigma\rangle\rangle$*) on the set of fundamental groups* $\{\pi_1(X) | [X] \in \mathfrak{M}\}$*.*

In the talk I explained the geometric results underlying a joint project with I. Bauer and F. Grunewald, but did not discuss local fundamental groups.

2. Fundamental groups and fibrations onto a curve

We recall some classical and some new results (see [3] and [6] for more references)

Theorem 1 (Castelnuovo-de Franchis)**.** *Let* X *be a compact Kähler manifold and* $U \subset H^0(X, \Omega^1_X)$ *be an isotropic subspace (for the wedge product) of dimension* ≥ 2*. Then there exists a fibration* $f : X \to B$*, where* B *is a curve, such that* $U \subset f^*(H^0(B, \Omega^1_B))$ *(in particular, the genus* $g(B)$ *of* B *is at least* 2*).*

Definition 1. *Such a fibration* f *as above is called an* irrational pencil.

Using Hodge theory and the Künneth formula, the Castelnuovo-de Franchis theorem implies (see [3]) the following

Theorem 2 (Isotropic subspace theorem)**.** 1) *Let* X *be a compact Kähler manifold and* $U \subset H^1(X, \mathbb{C})$ *be an isotropic subspace of dimension* ≥ 2*. Then there exists an irrational pencil* $f : X \to B$*, such that* $U \subset f^*(H^1(B, \mathbb{C}))$*.*

2) *There is a 1-1 correspondence between irrational pencils* $f : X \to B$*,* $g(B) = b \geq 2$*, and subspaces* $V = U \oplus \bar{U}$*, where* U *is maximal isotropic of dimension* b*.*

Proof. The correspondence is given by $f \mapsto f^*(H^1(B, \mathbb{C}))$ (cf. [3]). □

The following result due to Gromov follows then as a simple consequence.

Corollary 1. *Let X be a compact Kähler manifold and assume we have a surjective morphism $\pi_1(X) \to \Gamma$, where Γ has a presentation with n generators, m relations, $n - m \geq 2$. Then there is an irrational pencil $f : X \to B$, such that $2g(B) \geq n - m$ and $H^1(\Gamma, \mathbb{C}) \subset f^*(H^1(B, \mathbb{C})$.*

Proof. $H^1(\Gamma, \mathbb{C})$ injects into $H^1(X, \mathbb{C})$ and each vector in $H^1(\Gamma, \mathbb{C})$ is contained in an isotropic subspace. The corresponding subspaces V are defined over $\mathbb{Q}$. $H^1(\Gamma, \mathbb{C})$ is contained in their union, whence, by Baire's theorem, in one of them. □

The genus of the target curve B can also be detected from the fundamental group.

Definition 2. *Let X be a compact Kähler manifold and assume we have a pencil $f : X \to B$. Assume that $t_1, \ldots, t_r$ are the points of B whose fibres $F_i := f^{-1}(t_i)$ are the multiple fibres of f. Denote by m_i the multiplicity of F_i. Then the* **orbifold fundamental group** *$\pi_1(f) := \pi_1(b, m_1, \ldots, m_r)$ is defined as the quotient of $\pi_1(B \setminus \{t_1, \ldots, t_r\})$ by the subgroup normally generated by the $\gamma_i^{m_i}$'s, where γ_i is a geometric loop around t_i.*

The orbifold fundamental group is said to be of hyperbolic type if the corresponding universal ramified covering of B is the upper half plane.

Remark 1. *In the above situation we have the orbifold fundamental group exact sequence $\pi_1(F) \to \pi_1(X) \to \pi_1(b, m_1, \ldots, m_r) \to 0$, where F is a smooth fibre.*

The following result can be easily deduced from the arguments given in [6].

Theorem 3. *Let X be a compact Kähler manifold and let $(b, m_1, \ldots, m_r)$ be a hyperbolic type. Then there is a bijection between pencils $f : X \to B$ of type $(b, m_1, \ldots, m_r)$ and epimorphisms $\pi_1(X) \to \pi_1(b, m_1, \ldots, m_r)$ with finitely generated kernel.*

3. Varieties isogenous to a product

Definition 3. *A complex algebraic variety X of dimension n is said to be* **isogenous to a higher product** *if and only if there is a finite étale cover $C_1 \times \ldots \times C_n \to X$, where $C_1, \ldots, C_n$ are compact Riemann surfaces of respective genera $g_i := g(C_i) \geq 2$.*

In fact, X is isogenous to a higher product if and only if there is a finite étale Galois cover of X isomorphic to a product of curves of genera at least two, ie., $X \cong (C_1 \times \ldots \times C_n)/G$, where G is a finite group acting freely on $C_1 \times \ldots \times C_n$.

For simplicity, assume in the following $X = S$ to be a surface: we have then

Theorem 4 (see [4]). a) *A projective smooth surface is isogenous to a product if and only if the following two conditions are satisfied:*

1) *there is an exact sequence*

$$1 \to \Pi_{g_1} \times \Pi_{g_2} \to \pi = \pi_1(S) \to G \to 1,$$

where G is a finite group and where π_{g_i} denotes the fundamental group of a Riemann surface of genus $g_i \geq 2$;

2) $e(S)(= c_2(S)) = 4(g_1 - 1)(g_2 - 1)$.

b) *Any surface X with the same topological Euler number and the same fundamental group as S is diffeomorphic to S. The corresponding subset of the moduli space $\mathfrak{M}_S^{top} = \mathfrak{M}_S^{diff}$, corresponding to surfaces homeomorphic, resp., diffeomorphic to S, is either irreducible and connected or it contains two connected components which are exchanged by complex conjugation.*

In particular, if X is orientedly diffeomorphic to S, then X is deformation equivalent to S or to $\bar{S}$.

Remark 2. *A similar result holds in higher dimension, but the Zeuthen-Segre theorem allows an easier formulation in dimension two.*

Definition 4. *A surface S isogenous to a higher product is called a* Beauville surface *if and only if S is rigid.*

The following question is not yet completely answered.

Question 1. *Which groups G can occur?*

Beauville surfaces were extensively studied in [1] and the action of complex conjugation $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ was completely described. The datum of a Beauville surface amounts to a purely group theoretical datum, of two systems of generators $\{a, c\}$ and $\{a', c'\}$ for a finite group G (some condition must be satisfied, assuring that the diagonal action on the product of the two corresponding triangle curves is free). We prove in [1]:

Theorem 5. *There are Beauville surfaces S not biholomorphic to $\bar{S}$ (i.e., σ acts non trivially on S) with group*

1) *the symmetric group $\mathfrak{S}_n$ for $n \geq 7$,*
2) *the alternating group $\mathfrak{A}_n$ for $n \geq 16$ and $n \equiv 0$ mod 4, $n \equiv 1$ mod 3, $n \not\equiv 3, 4$ mod 7.*

We get also examples of real points in the moduli space which do not correspond to real surfaces:

Theorem 6. *Let $p > 5$ be a prime with $p \equiv 1$ mod 4, $p \not\equiv 2, 4$ mod 5, $p \not\equiv 5$ mod 13 and $p \not\equiv 4$ mod 11. Set $n := 3p + 1$. Then there is a Beauville surface S with group $\mathfrak{A}_n$ which is biholomorphic to its conjugate $\bar{S}$, but is not real.*

References

[1] I. Bauer, F. Catanese, F. Grunewald, F., *Beauville surfaces without real structures.* In: Geometric methods in algebra and number theory, Progr. Math., **235**, Birkhäuser (2005), 1–42.

[2] I. Bauer, F. Catanese, F. Grunewald, F., *Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory.* Mediterranean J. Math.**3**, no.2, (2006) 119–143.

[3] F. Catanese, *Moduli and classification of irregular Kähler manifolds (and algebraic varieties) with Albanese general type fibrations.* Invent. math. **104**, (1991), 263-289.

[4] F. Catanese, *Fibred surfaces, varieties isogenous to a product and related moduli spaces.*, Amer. J. Math. **122**, no.1 (2000), 1–44.

[5] F. Catanese, *Moduli Spaces of Surfaces and Real Structures.* Ann. Math. **158**, no.2, (2003) 577–592.

[6] F. Catanese, *Fibred Kähler and quasi projective groups*, Advances in Geometry, suppl. , Special Issue dedicated to A. Barlotti's 80-th birthday (2003), Adv. Geom. suppl., (2003) S13–S27.

Characteristic Elements for p-torsion Iwasawa modules

K. Ardakov

(joint work with S. J. Wadsley)

Notation. *G will be a compact p-adic analytic group with no elements of order p. The notation will conform with that of Ken Brown's talk* [3]*; in particular $\Lambda_G = \mathbb{Z}_p[[G]]$ and $\Omega_G = \mathbb{F}_p[[G]]$ will denote the Iwasawa algebras of G with coefficients in $\mathbb{Z}_p$ and $\mathbb{F}_p$ respectively. All modules are right modules.*

1. Background

Suppose $G \cong \mathbb{Z}_p^d$ so that $\Lambda_G \cong \mathbb{Z}_p[[T_1, \dots, T_d]]$.

Definition. *A finitely generated Λ_G-module M is* pseudonull *if*

$$\mathrm{Cdim}_{\Lambda_G}(M) \leq \mathrm{gld}(\Lambda_G) - 2 = d - 1.$$

A classical result of Bourbaki reads as follows:

Theorem (Structure Theorem)**.** *Let M be a finitely generated torsion Λ_G-module. Then there exists a short exact sequence of finitely generated Λ_G-modules*

$$0 \to \bigoplus_{i=1}^{t} \frac{\Lambda_G}{L_i} \to \frac{M}{M_0} \to C \to 0$$

where M_0 is the maximal pseudonull submodule of M, C is pseudonull and $L_i = f_i\Lambda_G$ for some elements $f_i \in \Lambda_G$.

Definition. *A* characteristic power series *for M is*

$$\xi_M = \prod_{i=1}^{t} f_i.$$

Remarks.

(1) ξ_M is only defined up to a unit in Λ_G,
(2) $\xi_M = 1$ if and only if M is pseudonull,
(3) The 'Main Conjecture' of classical Iwasawa Theory is phrased using these characteristic power series.

What if G is non-commutative?

Keep the same definition of pseudonull. Coates, Schneider and Sujatha [5] proved a very similar structure theorem for arbitrary G (assuming G is p-valued). The only difference was that the L_i's are no longer two-sided principal ideals in Λ_G and are in general just reflexive right ideals. Since there exist non-principal reflexive right ideals, it is unclear how to define a characteristic element in this setting. It is still an open question as to whether or not it is possible to choose possibly different L_i's which *are* principal.

How does one define a characteristic element in general?

2. K-theory

The main idea (due to Venjakob [7]) is to use the following localisation long exact sequence from K-theory:

Theorem. *Let R be a Noetherian ring with $\mathrm{gld}(R) < \infty$ and let $S \subset R$ be an Ore set consisting of regular elements. Let $\mathcal{C}_S$ be the abelian category of all finitely generated S-torsion R-modules. Then there exists a long exact sequence of abelian groups:*

$$\cdots \to K_1(R) \to K_1(R_S) \xrightarrow{\partial} K_0(\mathcal{C}_S) \xrightarrow{\alpha} K_0(R) \to K_0(R_S) \to 0$$

where

- $\alpha([M]) = \sum_{j=0}^{n}(-1)^j[X_j]$ *if* $0 \to X_n \to \cdots \to X_0 \to M \to 0$ *is a finite projective resolution of M, and*
- $\partial(\theta(x)) = [R/xR] \in \mathcal{C}$ *for all* $x \in R \cap R_S^\times$.

Here $\theta : R_S^\times \to K_1(R_S) = \mathrm{GL}(R_S)^{\mathrm{ab}}$ *is the natural map.*

Definition. *If M is a finitely generated S-torsion R-module, a* characteristic element *for M is any $\xi_M \in K_1(R_S)$ such that*

$$\partial(\xi_M) = [M].$$

Examples.

(1) Suppose there exists a closed normal subgroup H of G such that $G/H \cong \mathbb{Z}_p$ - Galois groups G often occur in arithmetic having this property. Set $R = \Lambda_G$. Then there exists an Ore set S^* such that $\mathcal{C}_{S^*}$ consists precisely of those finitely generated Λ_G-modules M such that $M/M(p)$ is finitely generated over Λ_H. Here $M(p)$ denotes the largest p-torsion submodule of M; see [4] for more details.

(2) Relaxing the assumption on G, set $R = \Lambda_G$ and $T = \{1, p, p^2, \cdots\}$, so that $\mathcal{C}_T$ consists of the finitely generated p-torsion Λ_G-modules and $R_T \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda_G$. This is the situation that we concentrate primarily on in [2].

Remarks.

(1) If G is commutative and $M = \bigoplus_{i=1}^{t} \Lambda_G/f_i\Lambda_G$, then

$$\partial\left(\theta\left(\prod_{i=1}^{t} f_i\right)\right) = [M]$$

(for a suitable Ore set S) so we can take $\xi_M = \theta(\prod_{i=1}^{t} f_i)$. We thus have agreement with the classical definition.

(2) In both of the above examples one can show that $\alpha = 0$, which forces ∂ to be surjective. Thus characteristic elements always exist in these cases.

(3) The two examples are compatible: since $T \subseteq S^*$ always, there exists a commuting diagram of K-groups:

$$\begin{tikzcd} K_1((\Lambda_G)_T) \arrow[r, "\partial"] \arrow[d] & K_0(\mathcal{C}_T) \arrow[d] \\ K_1((\Lambda_G)_{S^*}) \arrow[r, "\partial"] & K_0(\mathcal{C}_{S^*}). \end{tikzcd}$$

3. Results

Because Λ_G is semilocal, Λ_G has only finitely many simple modules up to isomorphism - $V_1, \ldots, V_s$ say. Since p lies in the Jacobson radical J of Λ_G, each V_i is killed by p.

By lifting idempotents modulo J, we can find some idempotents $e_1, \ldots, e_s \in \Lambda_G$ such that $V_i \cong e_i\Lambda_G/e_iJ$ for each $i = 1, \ldots, s$.

Definition.

Let M be a finitely generated p-torsion Λ_G-module.

(1) The *Euler Characteristic* of M is defined as follows:

$$\chi(G, M) = \prod_{n\geq 0} |\mathrm{Tor}_n^{\Lambda_G}(M, \mathbb{Z}_p)|^{(-1)^n},$$

see S. Wadsley's talk [9] for a more detailed discussion.

(2) The *$i-th$ twisted $\mu-$invariant* of M is

$$\mu_i(M) = \frac{\log_p \chi(G, (\mathrm{gr}_p M) \otimes_{\mathbb{F}_p} V_i^*)}{\dim_{\mathbb{F}_p} \mathrm{End}_{\Omega_G}(V_i)}.$$

where $\mathrm{gr}_p M = \bigoplus_{k=0}^{\infty} Mp^k/Mp^{k+1}$ is the graded module of M with respect to p-adic filtration. Because M is p-torsion, this is a finitely generated Ω_G-module. Note that $\mu_i(M)$ is *a priori* just an element of $\mathbb{Q}$.

We can now state our main results.

Theorem A. *Let M be a finitely generated p-torsion Λ_G-module. Then*

(a) $\mu_i(M) \in \mathbb{Z}$ for all $i = 1, \dots, s$.

(b) The characteristic element of M is

$$\xi_M = \theta\left(\prod_{i=1}^{s}(1+(p-1)e_i)^{\mu_i(M)}\right).$$

In the case when G is pro-p, the above formula for ξ_M simplifies considerably. Because G is assumed to have no elements of order p, G is torsionfree so Ω_G is a Noetherian domain [1, Theorem C]. Following Venjakob [8] and Howson [6], we can define the *μ-invariant* $\mu(M)$ of a finitely generated p-torsion Λ_G-module M to be the Ω_G-rank of $\mathrm{gr}_p(M)$; we can then show that $\mu(M) = \mu_1(M)$ (note that $s = 1$ in this case because Λ_G is local). Applying Theorem A we hence obtain the formula

$$\xi_M = \theta(p^{\mu(M)}).$$

Recall that in the commutative case, a desirable property of the characteristic element is that $\xi_M = 1$ if and only if M is pseudonull. Unfortunately, this is not true in general; however:

Theorem B. *Let M be a finitely generated p-torsion Λ_G-module such that $\xi_M = 1$. Then M is pseudonull.*

Part (5) of the next result was used by S. Wadsley as a starting point of his research into Euler characteristics [9].

Theorem C. *The following are equivalent:*

(1) $\xi_M = 1$ for all finitely generated p-torsion pseudonull Λ_G-modules M,

(2) $\chi(G, M) = 1$ for all finitely generated p-torsion pseudonull Λ_G-modules M,

(3) (Integrality) *$\chi(G, M) \in \mathbb{Z}$ for all finitely generated p-torsion Λ_G-modules M,*

*(4) G is $p-$*nilpotent*, that is, $G \cong F \rtimes P$ where F is a finite normal p'-subgroup of G and P is a Sylow pro-p subgroup of G,*

(5) $\dim C_G(x) = \dim G$ for all $x \in G_{\mathrm{reg}}$.

References

[1] K. Ardakov and K. A. Brown, *Primeness, semiprimeness and localisation in Iwasawa algebras*, Transactions of the Amer. Math. Soc., to appear.

[2] K. Ardakov and S. J. Wadsley, *Characteristic elements for p-torsion Iwasawa modules*, Journal of Algebraic Geometry, **15** (2006), 339-377.

[3] K. A. Brown, *Properties of Iwasawa algebras*, talk given at Oberwolfach in May 2006.

[4] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163-208.

[5] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2**, (2003) 73-108.

[6] S. Howson, Euler characteristics as invariants of Iwasawa modules, Proc. London Math. Soc. (3) **85** (2002) 634-658.

[7] O. Venjakob, *Characteristic elements in non-commutative Iwasawa theory*, Habilitationsschrift, Heidelberg University (2003).

[8] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. (3) **4** (2002) 271-311.

[9] S. J. Wadsley, *Euler Characteristics for p-torsion Iwasawa modules*, talk given at Oberwolfach in May 2006.

On a weak form of Greenberg's conjecture

T. Nguyen Quang Do

Abstract. Let p be an odd prime. For any CM number field K containing a primitive p^{th} root of unity, class field theory and Kummer theory put together yield the well known reflection inequality ("Spiegelung") $\lambda^+ \leq \lambda^-$ between the "plus" and "minus" part of the Iwasawa λ-invariant attached to K. Greenberg's classical conjecture predicts the vanishing of λ^+. We propose a weak form of this conjecture: $\lambda^+ = \lambda^-$ if and only if $\lambda^+ = \lambda^- = 0$. Note that the two forms (weak and strong) are equivalent if the usual Iwasawa series is irreducible. We prove the weak conjecture when K^+ is abelian, p is totally split in K^+, and certain (mild) conditions on the cohomology of circular units are satisfied.

1. Vandiver and Greenberg

For $K = \mathbb{Q}(\mu_p)$, Vandiver's conjecture predicts that $p \nmid h(K^+)$ (with obvious notations). Greenberg's conjecture may be considered as a reasonable generalization of Vandiver's:

Conjecture 1.1 (Greenberg's conjecture (G)).
Let p be an odd prime. For any totally real number field F, the Iwasawa invariants attached to F are trivial: $\lambda = \mu = 0$.

The vanishing of μ has been proved by Ferrero and Washington for any abelian number field. Here we'll concentrate on λ. For $p = 3$, thanks to various criteria due to many authors, (G) has been checked for all quadratic number fields $\mathbb{Q}(\sqrt{d})$ s.t. $0 < d < 10^4$. But practically no general result (e.g. when p varies) is known. We propose the following:

Conjecture 1.2 (Greenberg's weak conjecture (WG)).
For any CM field containing μ_p, we have $\lambda^- > \lambda^+$, unless $\lambda^- = \lambda^+ = 0$.

Remark 1.3.
If the usual Iwasawa series attached to K (the one which is related to p-adic L functions via the Main Conjecture) is irreducible, it is easy to show that $(G) \Leftrightarrow (WG)$. Hence a proof of (WG) would be a first (small but general) step towards (G).

2. Translation

From now on, we are in the setting of (WG), unless otherwise specified. We put $F = K^+$ to simplify notations. Let $F = \cup F_n$ the cyclotomic $\mathbb{Z}_p$-extension of F, $\Gamma = \mathrm{Gal}(F_\infty/F)$, $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$, A_n the p-class group of F_n, $A_\infty = \varinjlim A_n$, $X_\infty = \varprojlim A_n$. The following is well known:

Lemma 2.1 (see [3])**.**
(G) for $F \Leftrightarrow X_\infty$ is finite $\Leftrightarrow A_\infty$ is trivial.

Concerning (WG) we have the following:

Lemma 2.2 (see [2], 1.4)**.**
$\lambda^+ = \lambda^-$ if and only if the following conditions are satisfied:
(i) $X_\infty^\Gamma = (0)$ and (ii) $\dfrac{R(F)}{\sqrt{D(F)}} w(K) p^{-f} h(F) \overset{p}{\sim} (X_\infty)_\Gamma$

Here $R(F)$ denotes the p-adic regulator, $D(F)$ the discriminant, $h(F)$ the class number, $f = \sum_{v|p} f_v$ the absolute inertia index of F at p, $w(K)$ is the number of roots of unity in K, and the sign $\overset{p}{\sim}$ means p-adic equivalence.

Remarks 2.3.
1) *Assuming Leopoldt's conjecture for F, we know that X_∞^Γ is finite. Hence, denoting by X_∞^0 the maximal finite submodule of X_∞, condition (i) is equivalent to the vanishing of X_∞^0. Note that X_∞^0 is a capitulation kernel, more precisely $X_\infty^0 \simeq Ker\,(A_n \to A_\infty^{\Gamma_n})$ for $n >> 0$ so that the condition (i) is an asymptotic one.*
2) *The analytic flavor of condition (ii) comes from the Main Conjecture. In its algebraic formulation, it is automatically verified when p is totally split in F, by a lemma of Ozaki and Taya (*[5]*, lemma 2.2).*

3. Results

We first obtain character-wise results in the following setting:

Let k be a totally real field, $\chi \in \mathrm{Hom}(G_k, \overline{\mathbb{Q}_p}^\times)$. Suppose that χ is even, i.e. the field k^χ cut out by χ is totally real, and take $K = k^\chi(\mu_p)$. Let $\chi^* = \chi^{-1}\omega$ the mirror character, where ω is the Teichmüller character. Suppose for simplification that p does not divide the order of χ. Then the invariants $\lambda(\chi)$ and $\lambda(\chi^*)$ are defined in an obvious manner. Let $s(\chi^*) = \#\{$ p-places v of K_∞ s.t. the restriction of χ^* to the v-decomposition subgroup of $\mathrm{Gal}(K_\infty/k_\infty)$ is trivial $\}$. Define $s(\chi)$ similarly. Then:

Proposition 3.1 ([2], 4.6)**.**
i) If $s(\chi^*) \neq 0$, $\lambda(\chi^*) > \lambda(\chi)$.
ii) If $s(\chi^*) = s(\chi) = 0$, then $\lambda(\chi^*) - \lambda(\chi) = \dim_p \mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)(\chi^*)$, where N_∞ is the extension of K_∞ obtained by taking all p^n roots of units of K_∞, and $\dim_p M := \dim_{\mathbb{F}_p}(M/pM)$.

Idea of proof: These are refined "Spiegelung" results, using the capitulation cokernels $\mathrm{Coker}\,(A_n \to A_\infty^{\Gamma_n})$ studied in [4]. □

Remark 3.2.
The non triviality of $\dim_p \mathrm{Gal}(L_\infty \cap N_\infty/K_\infty)(\chi^*)$ can be checked at finite level, by constructing unramified Kummer extensions obtained by taking p^{th} roots of units. For examples, see [5]*, Â§5; see also* [1] *for the connection with Leopoldt's conjecture.*

It remains to study the case $s(\chi) \neq 0$. This is considered usually as the difficult case for Iwasawa descent, because of p-decomposition. But here we have:

Key lemma 3.3 ([5]), 5.5).
If F is a totally real abelian number field s.t. $p \nmid [F : \mathbb{Q}]$ and p is totally split in F, then $X^0_\infty = (0)$ if and only if $X_\infty = (0)$.

Idea of proof: compute the cohomology of circular units (in the sense of Sinnott) along the cyclotomic tower (see [6]) and use universal norms. □

The key lemma obviously implies:

Theorem 3.4 ([5], 5.6).
For F as in the key lemma, conjecture (WG) holds true.

Note that the semi-simplicity hypothesis $p \nmid [F : \mathbb{Q}]$ is not quite necessary. We also have:

Theorem 3.5 ([5], 5.7).
If F is a totally real abelian number field such that $p \nmid h(F)$ and p is totally split in F, then conjecture (WG) holds true.

References

[1] J. Assim and T. Nguyen Quang Do: *Sur la constante de Kummer-Leopoldt d'un corps de nombres*, Manuscripta Math., **115** (2004), 55-72.

[2] R. Badino and T. Nguyen Quang Do: *Sur les égalités du miroir et certaines formes faibles de la conjecture de Greenberg*, Manuscripta Math., **116** (2005), 323-340.

[3] R. Greenberg: *On the Iwasawa invariants of totally real number fields*, Amer. J. Math., **98**, 1 (1976), 263-284.

[4] M. Le Floc'h, A. Movahhedi and T. Nguyen Quang Do: *On capitulation cokernels in Iwasawa theory*, Amer. J. Math., **127** (2005), 851-877.

[5] T. Nguyen Quang Do: *Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé*, Int. J. Number Theory, **2**, 1, (2006), 1-16.

[6] T. Nguyen Quang Do and M. Lescop: *Iwasawa descent and co-descent for units modulo circulat units*, Pure Appl. Math. Quarterly, **2**, 2 (2006), 199-229.

Galois groups with restricted ramification

F. Hajir

In this talk, I gave some background, history, and motivation for the study of Galois groups of number fields with restricted ramification, highlighting certain properties (known as well as conjectured) of particular interest to group theorists.

Let p be a prime, K a number field, and S a finite set of places of K. Let K_S be the maximal pro-p extension of K unramified outside S. Concretely, the field K_S is the compositum of all finite p-extensions of K unramified outside S. The groups $G_{K,S} := \mathrm{Gal}(K_S/K)$ form a rich class of finitely generated groups, and they play a very critical role in number theory. In particular, they mediate the subtle and fruitful interaction between algebraic geometry and automorphic forms, an interaction that has been at the forefront of recent advances in number theory.

In particular, given a smooth projective variety $X_{/K}$, étale cohomology of X provides finite dimensional p-adic representations of $G_{K,S}$ where $S = \mathrm{Bad}(X_{/K}) \cup S_p$ is a finite set; here $\mathrm{Bad}(X_{/K})$ is the set of primes of K at which X has bad reduction and S_p is the set of primes of K of residue characteristic p. A recent conjecture of Fontaine and Mazur [4] gives criteria (one "local" and the other "global") for determining whether a given finite-dimensional representation comes from étale cohomology. Standard conjectures in arithmetic geometry (which include, for instance, the Tate conjecture on algebraic cycles) when combined with the vast "modularity" conjecture of Fontaine and Mazur mentioned above then predict:

Conjecture 1 (The Tame Fontaine-Mazur Conjecture (TFMC))**.** *If $S \cap S_p = \emptyset$, then every continuous homomorphism $G_{K,S} \to \mathrm{GL}_n(\mathbb{Z}_p)$, $n \geq 1$ has finite image. Equivalently, if $S \cap S_p = \emptyset$, then $G_{K,S}$ has no infinite p-adic analytic quotients.*

Class field theory yields immediately that every continuous homomorphism $G_{K,S} \to \mathrm{GL}_1(\mathbb{Z}_p)$ has finite image — this is the only dimension in which we know TFMC.

Problem 2. Let $\mathrm{SL}_2^1(\mathbb{Z}_p)$ be the principal congruence subgroup. Show that if K is a number field and L/K is a Galois extension with $\mathrm{Gal}(L/K) \approx \mathrm{SL}_2^1(\mathbb{Z}_p)$, then either

- there exists $\mathfrak{p} \subset \mathcal{O}_K$ dividing p such that $\mathfrak{p}$ ramifies deeply in L/K, or
- there exist infinitely many primes of K that ramify in L.

We note that extensions of both types exist, thanks to results of Khare-Larsen-Ramakrishna [7].

We next note that Boston [2] has proposed that one extend TFMC by replacing $\mathbb{Z}_p$ with an arbitrary complete local Noetherian ring with residue characteristic p.

Definition 3. If K is a number field, and L/K is an infinite algebraic extension, we say that L/K is asymptotically good if there exists $M \in \mathbb{R}$ such that for all finite degree intermediate fields $K \subseteq K' \subset L$, we have $rd_{K'} \leq M$, where for a number field F of degree m and discriminant d_F, we put $rd_F := |d_F|^{1/m}$ for its root discriminant.

Using a theorem of Coates-Greenberg [3] (which relies on a deep theorem of Sen [8]), Maire and I showed ([5]) that every shallowly ramified representation is potentially semistable. As a consequence, we obtained

Theorem 4. *The Tame Fontaine-Mazur Conjecture holds for all number fields if and only if every infinite p-adic analytic extension of every number field is asymptotically bad.*

Remark. The theorem can be interpreted as pointing toward a need for a "horizontal Sen's theorem" with which to attack Fontaine-Mazur.

Lubotzky [6] has shown that the fundamental group of a hyperbolic 3-manifold is virtually Golod-Shafarevich (GS), meaning $r(G) \leq d(G)^2/4$. At the Oberwolfach meeting, Boston conjectured the following analogue.

Conjecture 5 (Boston). *If $S \cap S_p = \emptyset$, and $G_{K,S}$ is infinite, then $G_{K,S}$ is virtually GS.*

To introduce a perhaps more precise version of this conjecture, let us define the growth exponent of G. For $s \in [0,1]$, let

$$a_G(s) = \limsup_{H \subset_o G} \frac{d(H)}{[G:H]^s}, \qquad \gamma(G) = \sup\{s \in [0,1] \mid a_G(s) > 0\}.$$

We call $\gamma(G)$ the rank growth exponent of G. Then we conjecture

Conjecture 6. *If $S \cap S_p = \emptyset$, and $G_{K,S}$ is infinite, then $\gamma(G_{K,S}) \geq \frac{1}{2}$.*

Can one show using group theory that these two conjectures are equivalent?

For questions regarding actions of finitely ramified Galois groups on rooted trees via iterated monodromy, see the abstract for the talk by Rafe Jones at this Oberwolfach meeting, as well as the work of Aitken-Hajir-Maire [1].

References

[1] W. Aitken, F. Hajir and C. Maire, Finitely ramified iterated extensions, IMRN 2005, no. 14, 855-880. (2006c:11125)

[2] N. Boston, p-adic Galois representations and pro-p Galois groups. in "New horizons in pro-p groups," 329–348, Progr. Math., 184, Birkhäuser, Boston 2000. (2001h:11073)

[3] J. Coates and R. Greenberg, Kummer theory for abelian varieties over local fields. Invent. Math. 124 (1996), no. 1-3, 129–174. MR1369413 (97b:11079)

[4] J.-M. Fontaine and B. Mazur, Geometric Galois representations. Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995. MR1363495 (96h:11049)

[5] F. Hajir and C. Maire, Extensions of number fields with wild ramification of bounded depth. Int. Math. Res. Not. 2002, no. 13, 667–696. MR1890847 (2002m:11096)

[6] A. Lubotzky, Group presentation, p-adic analytic Groups and lattices in $\mathrm{SL}_2(C)$. Ann. of Math. (2) 118 (1983), no. 1, 115–130. (85i:22017)

[7] C. Khare, M. Larsen, R. Ramakrishna, Constructing semi-simple p-adic Galois representations with prescribed properties, Amer. J. Math. 127 (2005), no. 4, 709–734. (2006f:11056)

[8] S. Sen, Ramification in p-adic Lie extensions. Invent. Math. 17 (1972), 44–50. MR0319949 (47 #8490)

Ideals in Iwasawa Algebras

C. J. B. Brookes

The aim of this talk was to provide some additional background and speculation about one of the questions discussed by Ken Brown in his introductory talk about Iwasawa algebras. For more details see his survey with Konstantin Ardakov [2].

Let G be a compact p-adic analytic group and U be an open normal uniform pro-p subgroup. Write Ω_G for the Iwasawa algebra $\mathbb{F}_p[[G]]$. This has the structure of a crossed product $\Omega_U * G/U$; both Ω_G and Ω_U are Noetherian. Let J be the unique maximal ideal in Ω_U, the kernel of the canonical map to $\mathbb{F}_p$. Ω_U is filtered by the powers of J and the associated graded ring $R = \mathrm{gr}\Omega_U$ is a commutative polynomial ring in d variables where $d = \dim U$.

Ken's question concerned the ideals in these Iwasawa algebras. What are they? At the end of Ken's talk Dan Segal asked whether methods used in the study of ideals in discrete group algebras might be adapted to these completed group algebras, especially in the case where G is soluble. This talk was prompted by this query and looked briefly at two techniques appearing in Roseblade's seminal work [8] on prime ideals in polycyclic group algebras, also examples of Noetherian algebras, and discussed whether these techniques might be applicable to Iwasawa algebras.

Let H be a group with normal subgroup A and k be a field. The intersection of an ideal of the group algebra kH with the subalgebra kA is an ideal of kA invariant under the conjugation action of H. In Roseblade's work a key case was when A is free abelian of rank n; he generalised a theorem of Bergman [3] about invariant ideals.in such group algebras kA using valuation theory. There is also a later, alternative proof due to Bieri and Groves [4] which is closer to Bergman's original geometric approach.

To each ideal I of kA one associates a subset Δ of $A^* = \mathrm{Hom}(A, \mathbb{R})$. This subset Δ may be defined in various ways but one method is to observe that each character χ in A^* induces a filtration of kA by k-subspaces $kA_{\chi \geq r}$ where $A_{\chi \geq r} = \{a \in A; \chi(a) \geq r\}$; then $\chi \in \Delta$ if this filtration induces a proper filtration on kA/I. Bieri and Groves showed that Δ is a closed rationally defined polyhedral cone, or fan, in the n-dimensional real vector space A^* and Sturmfels has pointed out that it is related to the Groebner fan studied in computational algebraic geometry; see Chapter 9 of [9]. Associated with the fan there are finitely many vector subspaces of A^*, the carrier space of the faces. Each carrier space is in fact the annihilator of an (isolated) subgroup of A, and hence associated to I we have a finite set of subgroups. The conjugation action of H on A induces a linear action of H on A^*. If our ideal I of kA is invariant under H then Δ is invariant under this linear action and the finitely many carrier spaces, and their corresponding subgroups, are permuted by H. If, for example, the only isolated subgroups with only finitely many H-conjugates are trivial and we can deduce that our invariant ideal has to be zero or kA/I is finite dimensional as a k-vector space. See [6] for further discussion and references.

Given that trees were prevalent at this Oberwolfach meeting it may be worth pointing out that there is an alternative way of looking at Δ is in terms of tree actions – see [5] and [7]. The character $\chi \in A^*$ defines a translation action of A on the real line. When $\chi \in \Delta$ the existence of a proper filtration induced on kA/I allows one to lift this translation action to an $\mathbb{R}$-tree action of a larger group, the split extension of the additive group of kA/I by A, in a non-trivial fashion.

To try and carry this technique over to Iwasawa algebras one would need to look for a good space of filtrations of the algebra and then associate a subset of this space with each (possibly one-sided) ideal I. (One might also hope for an interpretation in terms of tree actions.) It is tempting to think that associated to I there should be a canonical finite set of subgroups of G. This would give an approach to Ardakov's conjecture about the Krull dimension of Iwasawa algebras [1].

Of course we do know one very well behaved filtration of Ω_U, the J-adic one, with a polynomial algebra as associated graded ring. In this case we can associate a Groebner fan with the associated graded ideal gr$I$ of an ideal I of Ω_U. What information does this give us? In the discrete case outlined above, the fan of the graded ideal gr$I$ of the graded ring associated to the filtration defined by χ is just the tangent cone of Δ at the point χ.

The basis of the second technique used in the discrete theory is the simple observation that ideals I are closed under inner derivations of the algebra; if $x \in I$ then $xy - yx \in I$ for any y. In the Iwasawa algebra context we have a filtration yielding a commutative graded ring, much as we do for Weyl algebras and enveloping algebras of Lie algebras, so it is reasonable to suppose that it might prove helpful to define a Poisson bracket $\{-,-\}$ on $R = \mathrm{gr}\Omega_U$ to describe the infinitesimal failure of commutativity in the original algebra Ω_U, and then to observe that the graded ideal gr$I$ of R is necessarily closed under this Poisson bracket. (Recall that for a Poisson bracket $\{-,y\}$ defines a derivation on the algebra R.) We might then hope to use the bracket to define a skew-symmetric form on the tangent space of the (characteristic) variety associated with gr$I$ and do some symplectic geometry. The snag is that the characteristic of R is p, not zero, and so it is difficult to transfer information to the variety; gr$I$ can be closed under the bracket without its radical being so.

So let's consider a slightly different approach to derivations. Let L be the Lie algebra of all inner derivations of Ω_U. The J-adic filtration of Ω_U induces a filtration of L by the subalgebras $L_k = \{\delta \in L : \delta(J^i) \subset J^{i+k} \mathrm{foralli}\}$. Note that in general any inner derivation sends an ideal to itself and the commutativity of R ensures all inner derivations lie in L_1. Form the associated graded Lie algebra gr$L$. This acts on R via graded derivations; an element of L_k/L_{k+1} maps J^i/J^{i+1} to J^{i+k}/J^{i+k+1}. The graded ideal gr$I$ is invariant under this action of gr$L$. Derivations of a commutative algebra R in characteristic p are R^p-endomorphisms vanishing on pth powers. Other R^p-endomorphisms arise from multiplication by elements of R. Let D be the subring of R^p-endomorphisms of R generated by all these multiplications and the image of gr$L$ under the action described above. In this way R and gr$I$ are both D-modules. If D is large, close to being the whole of the full R^p-endomorphism ring of R, a matrix ring, then this restricts the D-submodules of R and so the options for gr$I$ are limited. The snag here is that this is not going to tell us anything about ideals I for which gr$I$ is generated by elements of R^p. As with the first technique it seems that we are led to consider other filtrations, not just the J-adic one.

References

[1] K. Ardakov, *Krull dimension of Iwasawa algebras*, J. Algebra **280** (2004), 190–206.

[2] K. Ardakov and K. A. Brown, *Ring-theoretic properties of Iwasawa algebras; a survey*, math.RA/0511345.

[3] G. M. Bergman, *The logarithmic limit set of an algebraic variety*, Trans. Amer. Math. Soc. **157** (1971), 459–469.

[4] R. Bieri and J. R. J. Groves, *The geometry of the set of characters induced by valuations*, J. Reine Angew. Math. **347** (1984), 168–195.

[5] R. Bieri, W. D. Neumann and R. Strebel, *A geometric invariant of discrete groups*, Invent. Math. **90** (1987), 451–477.

[6] C. J. B.Brookes, *Group-theoretic applications of non-commutative toric geometry*, Groups St Andrews 1997 in Bath, I, 176–194, London Math. Soc. Lecture Note Ser. **260**, Cambridge Univ. Press, Cambridge, 1999.

[7] K. S. Brown, *Trees, valuations and the Bieri-Neumann-Strebel invariant*, Invent. Math. **90** (1987), 479–504.

[8] J. E. Roseblade, *Prime ideals in group rings of polycyclic groups*, Proc. London Math. Soc. **36** (1978), 385–447.

[9] B. Sturmfels, *Solving systems of polynomial equations*, CBMS Regional Conference Series in Mathematics **97**, Amer. Math. Soc, Providence, 2002.

Maximal unramified 3-extensions of imaginary quadratic fields and $\mathbf{SL}_2(\mathbb{Z}_3)$

M. R. Bush

(joint work with L. Bartholdi)

Let k be a number field and let p be a prime. The *p-class tower of k* is the chain of fields

$$k = k_0 \subseteq k_1 \subseteq \ldots \subseteq k_n \subseteq \ldots$$

where k_{n+1} is the maximal unramified abelian p-extension of k_n for each $n \geq 0$. If we let $k^{ur,p} = \cup_{n\geq 0} k_n$ and $G = \mathrm{Gal}(k^{ur,p}/k)$ then G is a pro-p group whose structure incorporates a lot of arithmetic information about the field k and its unramified p-extensions. For instance, if H is an open subgroup of G and L is the associated fixed field then by class field theory $H/[H,H] \cong Cl_p(L)$ where $[H,H]$ is the commutator subgroup of H and $Cl_p(L)$ is the p-Sylow subgroup of the class group of L. One consequence of this is that the length of the p-class tower is the same as the length of the derived series of G.

In general determining the structure of G is difficult. We know that G can be infinite for certain choices of k and p due to work of Golod and Shafarevich [7]. We also know many examples where G is finite. One observes, however, that the finite examples usually have very small derived length ≤ 3 and so one is lead to ask whether or not there is a bound on the derived length when G is finite, and if not, how one can find examples where the length is large?

If k is an imaginary quadratic field and p is an odd prime then a result of Koch and Venkov [8] shows that G can be finite only if $d(G) \leq 2$ where $d(G)$ is the smallest number of generators for G as a pro-p group. Their proof exploits the fact that G has the structure of a Schur σ-group. By definition this is a finitely presented pro-p group G in which $d(G) = r(G)$ where $r(G)$ is the relation rank, $G/[G,G]$ is finite and there exists an automorphism $\sigma : G \to G$ such that $\sigma^2 = 1$ and the automorphism induced by σ on $G/[G,G]$ is the inversion map $x \mapsto x^{-1}$.

An obvious question that one might now ask is whether or not there exist finite Schur σ-groups with arbitrarily large derived length for some fixed prime p? The answer is yes and we give a family of examples below demonstrating this.

Let F be the free pro-3 group on two generators x and y. Let G_n be defined by the pro-3 presentation

$$G_n = \langle x, y \mid r_n^{-1}\sigma(r_n),\, t^{-1}\sigma(t)\rangle$$

where $r_n = x^3 y^{-3^n}$, $t = yxyx^{-1}y$ and $\sigma : F \to F$ is the automorphism defined by $x \mapsto x^{-1}$ and $y \mapsto y^{-1}$. The group G_n is a Schur σ-group with respect to the automorphism induced by σ.

Theorem. *For $n \geq 1$ the following hold:*

(i) *G_n is a finite 3-group of order 3^{3n+2};*

(ii) *G_n is nilpotent of class $2n+1$;*

(iii) *G_n has derived length $\lfloor \log_2(3n+3) \rfloor$.*

Each group G_n is a central extension of a finite quotient of the pro-3 group $H = \langle x, y \mid x^3,\, t^{-1}\sigma(t)\rangle$. The key step in the proof of the theorem is the following lemma which exhibits an explicit matrix representation for H.

Lemma. *Let $\alpha \in \mathbb{Z}_3$ satisfy $\alpha^2 = -2$. The map $\rho : H \to \mathrm{SL}_2(\mathbb{Z}_3)$, given by*

$$x \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad y \mapsto \alpha \begin{pmatrix} 0 & 1/2 \\ 1 & -1 \end{pmatrix},$$

is an isomorphism between H and a pro-3 Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$.

See [1] for a proof of the lemma and theorem as well as several examples of imaginary quadratic fields $k = \mathbb{Q}(\sqrt{d})$ in which the Galois group of the 3-class tower is G_1. The first three discriminants for which this occurs are $d = -4027$, -8751 and -19651. These and other examples were found by applying a computational method first used by Boston and Leedham-Green [3] to compute the Galois groups of certain maximal tamely ramified extensions of $\mathbb{Q}$. The method makes use of the p-group generation algorithm [9] to systematically enumerate all d-generated finite p-groups. Information about the Galois group one is seeking is used to eliminate some of these groups. In some cases the process terminates leaving a finite number of groups as candidates for the desired Galois group. The computations for the examples above were carried out using Magma [2]. (We note that the 3-class tower of the first field $d = -4027$ has previously been investigated in [10] using other methods). For other applications of the method (including the first examples of 2-class towers of length 3) see [5], [4] and [6].

For $n \geq 2$ there is a limited amount of numerical evidence suggesting that the groups G_n may arise as Galois groups of 3-class towers. Whether or not this is actually the case is still open.

References

[1] L. Bartholdi, M. R. Bush, *Maximal unramified* 3*-extensions of imaginary quadratic fields and* $\mathrm{SL}_2(\mathbb{Z}_3)$, preprint, arXiv: math.NT/0602364.

[2] W. Bosma, J. J. Cannon, *Handbook of Magma functions*, School of Mathematics and Statistics, University of Sydney (1996).

[3] N. Boston, C. R. Leedham-Green, *Explicit computation of Galois p-groups unramified at p*, J. Algebra **256** (2002), 402–413.

[4] N. Boston, H. Nover, *Computing pro-p Galois groups*, preprint, 2006.

[5] M. R. Bush, *Computation of the Galois groups associated to the* 2*-class towers of some quadratic fields*, J. Number Theory **100** (2003), 313–325.

[6] B. Eick, H. Koch, *On the maximal* 2*-extensions of* $\mathbb{Q}$ *with given ramification*, to appear in Proc. St. Petersburg Math. Soc. (Russian); English transl.: to appear in Amer. Math. Soc. Trans..

[7] E. Golod, I. Shafarevich, *On class field towers*, Izv. Akad. Nauk SSSR **28** (1964), 261–272 (Russian); English transl.: Amer. Math. Soc. Trans. **48** (1965), 91–102.

[8] H. Koch, B. B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Astérisque **24-25** (1975), 57–67.

[9] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Computation **9** (1990), no. 5–6, 677–698.

[10] A. Scholz, O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm*, J. Reine Angew. Math. **171** (1934), 19–41.

Regular realizations of p-projective quotients and modular curve-like towers

M. D. Fried

Abstract. This exposition on Modular Towers (**MT** s) shows how the Regular Inverse Galois Problem (RIGP) generalizes modular curves by considering all Frattini extensions of a given p-perfect finite group G. The result is towers of spaces generalizing modular curve towers — minus their cusps : $\{Y_1(p^{k+1})\}_{k=0}^{\infty}$ is a case with $G = D_p$ (p odd).

The Main Conjecture on **MT** s is that there are no rational points at high levels [LUM]. If true the difficulty in the RIGP is because the context generalizes the Mazur-Merel results. More so, A. Cadoret has shown the Strong Torsion Conjecture (STC) implies the Main Conjecture [STMT]. Though the STC is known only for dim. 1, there has been serious progress on the Main Conjecture. Ingredients include a theory of cusp types on a **MT**. We understand those projective systems of tower components that have properties resembling modular curves through two tools:

- The Fried-Serre lifting invariant generalizing an invariant for the spin covers of alternating groups [AGLI]; and
- a result of T. Weigel that explains towers levels through a group extension problem applied to a p-Poincaré duality group [We].

Here is a list of the sections.

1. Use of conjugacy classes
2. Is the RIGP really so hard?
3. The RIGP realm using virtually pro-p groups
4. Cusps on curve components ($r = 4$)

5. Compare modular curve cusps with **MT** cusps
6. Where is the Main Conjecture with $r = 4$?

The following were not in the talk, but are an addition to the pdf talk file [WS].
7. What happens in real **MT** levels!
8. Generalizing Serre's OIT and the g-p' conjecture
App. A: Fried-Serre Formula for Spin-Lift Invariant
App. B: **sh**-incidence Matrix for $(A_4, \mathbf{C}_{\pm 3^2})$

The I(nverse)G(alois)P(roblem) for G: Is finite group G the Galois group of an extension of every number field?

The R(egular)IGP for G: Is there one Galois extension $L_G/\mathbb{Q}(z)$ with group G containing only $\mathbb{Q}$ for constants? From Hilbert's irreducibility Theorem, RIGP (for G) $\implies$ IGP (for G). Further, beyond the solvable case, the RIGP has provided most all the successes through the *braid monodromy method.*

1. Use of conjugacy classes

We say $\boldsymbol{g} \overset{\text{def}}{=} (g_1, \dots, g_r) \in G^r$ *generates* with product-one if

$$\langle g_1, \dots, g_r \rangle = G \text{ and } \prod g_1 \cdots g_r \overset{\text{def}}{=} \Pi(\boldsymbol{g}) = 1.$$

Also, $\boldsymbol{g}$ defines a set $\mathbf{C}$ of conjugacy classes in G. Given $\mathbf{C}$, $\boldsymbol{g} \in \mathbf{C}$ means $\boldsymbol{g}$ defines $\mathbf{C}$. Such $\boldsymbol{g}$ form the Nielsen class $\text{Ni}(G, \mathbf{C})$ of $(G, \mathbf{C})$.

In $\mathbf{C} = \{\text{C}_1, \dots, \text{C}_r\}$ some classes may appear several times: multiplicity counts; order does not.

1.1. R(iemann's)E(xistence)T(hm).

A regular realization $L_G/\mathbb{Q}(z)$ has $r \geq 2$ branch points $= \{z_1, \dots, z_r\}$ (z over which are less than $[L_G : \mathbb{Q}(z)]$ places): $z_i \mapsto$ conjugacy class C_i of inertia gen. from a clockwise small circle around z_i.

RET: $G(L_G/\mathbb{Q}(z)) = G \implies$ some $\boldsymbol{g} \in \mathbf{C}$ generates G with product-one.

Since the realization is over $\mathbb{Q}$, $\mathbf{C}$ is a rational union (its union is closed under putting all elements in it to powers prime to orders of elements in $\mathbf{C}$).

1.2. An addition to [FrV, Main Thm.]

Theorem 1.1 (Branch-Generation Thm.). *Assume G is centerless and $\mathbf{C}^*$ is a distinct set of (nonidentity) classes in G. An infinite set $I_{G,\mathbf{C}^*}$ indexes distinct absolutely irreducible $\mathbb{Q}$ varieties $\mathcal{R}_{G,\mathbf{C}^*} \overset{\text{def}}{=} \mathcal{R}_{G,\mathbf{C}^*,\mathbb{Q}} = \{\mathcal{H}_i\}_{i \in I_{G,\mathbf{C}^*}}$ with:*

- *$i \in I_{G,\mathbf{C}^*} \mapsto {}_i\mathbf{C}$, a rational union of r_i conjugacy classes in G with support in $\mathbf{C}^*$.*
- *The RIGP holds for G with conjugacy classes $\mathbf{C}$ supported in $\mathbf{C}^* \Leftrightarrow i \in I_{G,\mathbf{C}^*}$ with $\mathbf{C} = {}_i\mathbf{C}$ and $\mathcal{H}_i$ has a $\mathbb{Q}$ point.*

1.3. Using Nielsen classes.

Realizations come from augmenting existence of $\mathcal{R}_{G,\mathbf{C}^*}$ with info on $\mathcal{H}_i$, $i \in I_{G,\mathbf{C}^*}$.

The reduced space $\mathcal{H}_i^{\text{rd}}$: Equivalence field extensions under change of variables $z \mapsto \alpha(z)$, $\alpha \in \text{PGL}_2(\mathbb{C})$. Dimension of $\mathcal{H}_i^{\text{rd}}$ is $r_i - 3$.

1.4. D_p **and** A_n **cases.** $G = D_{p^{k+1}}$, p odd, $\mathbf{C}^* = \{\mathrm{C}_2\}$ (class of involution): Then $i \mapsto \mathbf{C}_{2^{r_i}}$ is one-one and onto $r_i \geq 4$ even. Also, H_i^{rd} identifies with the space of cyclic p^{k+1} covers of hyperelliptic jacobians of genus $\frac{r_i-2}{2}$.

(Fried-Serre) $G = A_n$ with $\mathbf{C}^* = \{\mathrm{C}_3\}$, class of 3-cycles: Then $i \mapsto \mathbf{C}_{3^{r_i}}$ with $r_i \geq n$ is two-one. Denote indices mapping to r by $i_r^{\pm}$. Covers in $\mathcal{H}_{i_r^{\pm}}$ are Galois closures of degree n covers $\phi : X \to \mathbb{P}_z^1$ with 3-cycles for local monodromy. Write divisor $(d\phi)$ of differential of ϕ as $2D_\phi$. Then, $\phi \in \mathcal{H}_{i_r^+}$ (resp. $\mathcal{H}_{i_r^-}$) if the linear system of D_ϕ has even (resp. odd) dim.; even (resp. odd) θ characteristic. For $r_i = n-1$, $i \mapsto \mathbf{C}_{3^{r_i}}$ is one-one.

2. Is the RIGP really so hard?

Dividing RIGP techniques into three cases shows how $i \in I_{G,\mathbf{C}^*}$ on ${}_i\mathbf{C}$ affects complexity of computation. Yet, it is diophantine reasons more than group theory complexity that makes the RIGP hard.

1. When $r_i = 3$, $\mathcal{H}_i^{\mathrm{rd}}$ is a finite collection of ($\mathbb{Q}$) points.
2. When $r_i = 4$, $\mathcal{H}_i^{\mathrm{rd}}$ is naturally an upper half-plane quotient and a cover of the j-line, with meaningful cusp types.
3. No matter what is r_i, $\mathcal{H}_i$ is a cover of U_{r_i}, projective r_i space minus its discriminant locus; can compare this with the (Galois) Noether cover $U^{r_i} \to U_{r_i}$ (with group S_{r_i}).

2.1. **Using #1.** *Rigidity* is an effective sufficiency test for finding $i \in I$ with $r_i = 3$. It requires only the character table of G to conclude the RIGP for G.

Problem: Rarely does this hold. Even for Chevalley groups, the method achieved only special rank 1 groups over prime finite fields (Belyi) and some other special simple groups by Matzat and Thompson.

2.2. **Using #3.** For many families of simple groups Thompson and Völklein found $\mathbf{C}^*$ and used specific $i \in I_{G,\mathbf{C}^*}$ (Thompson-tuples). Their $\mathcal{H}_i \to U_{r_i}$ covers were *almost* subcovers of $U^{r_i} \to U_{r_i}$. This gave many examples of simple G satisfying RIGP.

Problem: This required much luck and great expertise on simple group series.

2.3. **Virtues of using #2.**

- $\mathcal{H}_i^{\mathrm{rd}}$ is a curve with *useful cusps* from the moduli problem to compactify it. Gives precise statements about these spaces.
- More groups (like all simple groups and all their Frattini covers) have conjugacy classes producing this case than holds for #1.
- Combinatorial techniques allow computing the genus of these spaces, and to *identify the part of the Nielsen class they come from.*

3. The RIGP realm using virtually pro-p groups

We use the virtually pro-p *universal p-Frattini* cover ${}_p\tilde{G}$ of G, for any prime $p||G|$ to see how the RIGP generalizes classical results for modular curves. If G is centerless and *p-perfect* (no surjective $G \to \mathbb{Z}/p$), then ${}_p\tilde{G} = \lim_{\infty \leftarrow k} G_k$, with:

- G_k also p-perfect and centerless; and
- $G_k \to G$ versal for all extensions $\psi : H \to G$ with $\ker(\psi)$ a p-group of exponent at most p^k.

3.1. **Add a restriction on Ramification.** From Schur-Zassenhaus, if a conjugacy class is p', then it has a unique lifts to a p' class in G_k. So, if $\mathbf{C}$ consists of p' classes, denote those lifted classes to G_k by the same notation. Here is a *restrict ramification condition* depending on $r_0 \geq 3$:

Ram_{r_0}: For $k \geq 0$, use covers in $\mathrm{Ni}(G_k, \mathbf{C}_k)$ with at most r_0 classes in $\mathbf{C}_k$.

Question 3.1 (RIGP(G,p,r_0) Question)**.** Is there an r_0 so all G_k s satisfy the RIGP from covers in Ram_{r_0}?

3.2. **How the Main Conjecture Arises.**

Theorem 3.2 (Fried-Kopeliovic, 1997)**.** *If the conclusion of Quest. 3.1 is affirmative (for (G, p, r_0)), then there are p' conjugacy classes $\mathbf{C}$ (no more than r_0) in G, and a projective system $\{\mathcal{H}'_k \in \mathcal{R}_{G_k,\mathbf{C}}\}_{k=0}^{\infty}$ each having a $\mathbb{Q}$ point.*

We call $\{\mathcal{H}'_k\}_{k=0}^{\infty}$ a *M(odular) T(ower) component branch* (over $\mathbb{Q}$).

Conjecture 3.3 (Main Conjecture)**.** Given any **MT** component branch, and any number field K, for $k >> 0$, $\mathcal{H}'^{\mathrm{rd}}_k(K) = \emptyset$.

4. Cusps on curve components $(r = 4)$

Twist action of $H_4 = \langle q_1, q_2, q_3 \rangle$ generators on $\boldsymbol{g} \in \mathrm{Ni}(G_k, \mathbf{C})/G \overset{\text{def}}{=} \mathrm{Ni}(G_k, \mathbf{C})^{\mathrm{in}}$. Ex.: $q_2 : \boldsymbol{g} \mapsto (g_1, g_2 g_3 g_2^{-1}, g_2, g_4)$.

Level k Cusps: $\mathrm{Cu}_4 \overset{\text{def}}{=} \langle q_1 q_3^{-1}, (q_1 q_2 q_3)^2, q_2 \rangle$ orbits on $\mathrm{Ni}(G_k, \mathbf{C})^{\mathrm{in}}$. Denote $\langle q_1 q_3^{-1}, (q_1 q_2 q_3)^2 \rangle$ by $\mathcal{Q}''$.

4.1. **Why $\bar{M}_4 \overset{\text{def}}{=} H_4/\mathcal{Q}''$ is** $\mathrm{PSL}_2(\mathbb{Z})$**.**

- $q_2 \mapsto \gamma_\infty$;
- $q_1 q_2 q_3$ (shift) $\mapsto \gamma_1$ (order 2).
- $q_1 q_2 \mapsto \gamma_0$ has order 3, from braid relation $q_1 q_2 q_1 = q_2 q_1 q_2 \mod \mathrm{Cu}_4$ and Hurwitz relation $1 = q_1 q_2 q_3 q_3 q_2 q_1$:

$$= q_1 q_2 q_1 q_1 q_2 q_1 = q_1 q_2 q_1 q_2 q_1 q_2 = (q_1 q_2)^3.$$

4.2. **From a component branch, what to compute.**

- Nature of cusps and their widths (length of $\mathrm{Cu}_4 \mod \mathcal{Q}''$ orbits).
- How they fall in $\bar{M}_4$ orbits and of what genera (Riemann-Hurwitz).

5. Compare modular curve cusps with **MT** cusps

When $r = 4$, **MT** levels ($k \geq 0$) are j-line covers, but rarely modular curves. The following description of cusps is from [LUM, §3.2].

With $r = 4$, $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$, denote:

$$\langle g_2, g_3\rangle = H_{2,3}(\boldsymbol{g}) \text{ and } \langle g_1, g_4\rangle = H_{1,4}(\boldsymbol{g}).$$

$(\boldsymbol{g})\mathrm{Cu}_4$ is a *g-p' cusp*: $H_{2,3}(\boldsymbol{g})$ and $H_{1,4}(\boldsymbol{g})$ are p' groups. Ex: H(arbater)-M(umford) cusps have $g_2 = g_1^{-1}$.

p cusps: Those with $p|\mathrm{ord}(g_2g_3)$.

o(nly)-p': Cusps neither p nor g-p'.

Modular curve $X_1(p^{k+1})$ has H-M cusps, many p cusps of different cusps widths, all growing in width by p as k increases, but no o-p' cusps.

5.1. **Apply R-H to MT components.**

Ni' is a $\bar{M}_4$ orbit on a reduced Nielsen class $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}/\mathcal{Q}''$ (or $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}/\mathcal{Q}''$). Denote action of $(\gamma_0, \gamma_1, \gamma_\infty)$ (§4.1) on Ni' by $(\gamma'_0, \gamma'_1, \gamma'_\infty)$: Branch cycles for a cover $\overline{\mathcal{H}}' \to \mathbb{P}^1_j$,

R-H gives genus, $g_{\overline{\mathcal{H}}'}$: $2(\deg(\overline{\mathcal{H}}'/\mathbb{P}^1_j)+g'-1) = \mathrm{ind}(\gamma'_0) + \mathrm{ind}(\gamma'_1) + \mathrm{ind}(\gamma'_\infty)$.

5.2. **Answer these questions to compute genera of MT components.**

- What are the components $\overline{\mathcal{H}}'_k$ of $\overline{\mathcal{H}}_k$ ($\bar{M}_4$ orbits Ni'_k on $\mathrm{Ni}^{\mathrm{rd}}_k$)?
- What are ram. orders over ∞ (orbit lengths of γ'_∞ on Ni'_k)?
- What points ramify in each component over elliptic points $j = 0$ or 1; length 3 (resp. 2) orbits of γ'_0 (resp. γ'_1) on Ni'_k?

6. Where is the Main Conjecture with $r = 4$?

[LUM] has three Frattini Principles. We use here Frattini Princ. 1: If $g \in G_k$ is exactly divisible by p^u, $u > 0$, it has above it in G_{k+1} only elements of order exactly divisible by p^{u+1}. [LUM, Prop. 3.3] shows Main Conj. 3.3 for G a general p-perfect group reduces to the case the p part of the center is trivial. This allows the following conclusion: A level $k+1$ cusp over a p cusp at level k is ramified (of order p).

6.1. **Reductions from** [LUM].

Let $B' = \{\mathcal{H}'_k\}_{k=0}^\infty$ be an infinite component branch. Main Conj. contradictions:

(6.1a) $g_{\overline{\mathcal{H}}'_k} = 0$ for all $0 \leq k < \infty$ (B' has genus 0; $g_{B'}$ consists of 0's); or

(6.1b) For k large, $g_{\overline{\mathcal{H}}'_k} = 1$ (B' has genus 1; almost all of $g_{B'}$ is 1's).

Usage: From R-H, for $k >> 0$, (6.1b) implies $\overline{\mathcal{H}}'_{k+1} \to \overline{\mathcal{H}}'_k$ doesn't ramify. So, FP1 says: For no k does $\overline{\mathcal{H}}'_k$ have a p cusp or a Main Conj. exception satisfies (6.1a).

6.2. **Possible exceptional cases! [LUM, §5].** Assume $\boldsymbol{p}'_k \in \overline{\mathcal{H}}'_k$ is a p cusp (some k). Denote: $\deg(\overline{\mathcal{H}}'_{k+1}/\overline{\mathcal{H}}'_k) = \nu_k$ and $|\boldsymbol{p}_{k+1} \in \overline{\mathcal{H}}'_{k+1}$ over $\boldsymbol{p}'_k| = u_k$.

Theorem 6.1. *Then, the Main Conj. is true unless for $k >> 0$, $\nu_k = p$, $u_k = 1$ and $\overline{\mathcal{H}}'_{k+1}/\overline{\mathcal{H}}'_k$ is equivalent (as a cover over K) to either:*

- ($\mathrm{P}^{\mathrm{oly}}$ M) *a degree p polynomial map; or*
- ($\mathrm{R}^{\mathrm{edi}}$M) *a degree p rational function p order ramification over two points.*

Corollary 6.2. *If neither* ($\mathrm{P}^{\mathrm{oly}}$M) *nor* ($\mathrm{R}^{\mathrm{edi}}$M) *hold for the component branch B', then high levels of B' have no K points.*

For B' with full elliptic ramification (includes when B' has fine reduced moduli) for $k >> 0$, the Main Conj. holds unless ($\mathrm{R}^{\mathrm{edi}}$ M) *holds.*

References

[STMT] A. Cadoret, *Modular Towers and Torsion on Abelian Varieties*, preprint May, 2006.

[FrV] Michael D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), no. 4, 771–800.

[AGLI] Alternating groups and lifting invariants, Out for refereeing (2006), 1–36.

[LUM] M.D. Fried, *The Main Conjecture of Modular Towers and its higher rank generalization*, in Groupes de Galois arithmetiques et differentiels (Luminy 2004; eds. D. Bertrand and P. Dèbes), Seminaires et Congres, **13**, 2006.

[WS] M.D. Fried, *Regular realizations of p-projective quotients and modular curve-like towers*, this is the talk I gave on May 26 at Oberwolfach, augmented by other topics. Access at www.math.uci.edu/conffiles_rims/exp-profgeom.html in the list in the scientific part of the homepage of the conference "Profinite Arithmetic Geometry and Their Associated Moduli Spaces," at RIMS, Kyoto October 23 - 29, 2006.

[We] T. Weigel, *Maximal l-Frattini quotients of l-Poincaré duality groups of dimension* 2, Arch. Math. (Basel) **85** (2005), no. 1, 55–69.

Reporter: Benjamin Klopsch (Düsseldorf)

Participants

Prof. Dr. Miklos Abert
Department of Mathematics
The University of Chicago
5734 South University Avenue
Chicago, IL 60637-1514
USA

Prof. Dr. Victor Abrashkin
Dept. of Mathematical Sciences
The University of Durham
Science Laboratories
South Road
GB-Durham, DH1 3LE

Prof. Dr. Konstantin Ardakov
Christ's College
GB-Cambridge CB2 3BU

Dr. Laurent Bartholdi
IMB, Batiment MA, Station 8
Ecole Polytechnique Federale
CH-1015 Lausanne

Prof. Dr. Ingrid Bauer-Catanese
Lehrstuhl für Mathematik VIII
Universität Bayreuth
NW - II
95440 Bayreuth

Inga Blomer
Mathematisches Institut
Georg-August-Universität
Bunsenstr. 3-5
37073 Göttingen

Prof. Dr. Nigel Boston
University of Wisconsin-Madison
Van Vleck Hall
480 Lincoln Drive
Madison WI 53706
USA

Dr. ChristopherJ.B. Brookes
Corpus Christi College
GB-Cambridge, CB2 1RH

Prof. Dr. Ken A. Brown
Department of Mathematics
University of Glasgow
University Gardens
GB-Glasgow, G12 8QW

Prof. Dr. Michael Bush
Dept. of Mathematics
University of Massachusetts
Amherst, MA 01003-9305
USA

Prof. Dr. Fabrizio Catanese
Lehrstuhl für Mathematik VIII
Universität Bayreuth
NW - II
95440 Bayreuth

Prof. Dr. John H. Coates
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

Prof. Dr. Jordan S. Ellenberg
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706-1388
USA

Tobias Finis
Mathematisches Institut
Universität Leipzig
Augustusplatz 10/11
04109 Leipzig

Prof. Dr. Michael David Fried
Department of Mathematics
University of California at Irvine
Irvine, CA 92697-3875
USA

Prof. Dr. Rostislav Ivan. Grigorchuk
Department of Mathematics
Texas A & M University
College Station, TX 77843-3368
USA

Prof. Dr. Fritz Grunewald
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

Prof. Dr. Farshid Hajir
Department of Mathematics
University of Massachussets
Lederle graduate res. tower
710 North Pleasant Street
Amherst MA 01003
USA

Prof. Dr. Günter Harder
MPI für Mathematik
Vivatsgasse 7
53111 Bonn

Prof. Dr. Andrei Jaikin-Zapirain
Departamento de Matematicas
Facultad de Ciencias, C-XV
Universidad Autonoma de Madrid
ctra.de Colmenar Viejo, Km. 15
E-28049 Madrid

Prof. Dr. Rafe Jones
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706-1388
USA

Dr. Benjamin Klopsch
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

Dr. Jürgen Klüners
FB 17 - Mathematik/Informatik -
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel

Prof. Dr. Helmut Koch
Institut für Mathematik
Humboldt-Universität
10099 Berlin

Prof. Dr. John Labute
Dept. of Mathematics and Statistics
McGill University
805, Sherbrooke Street West
Montreal, P.Q. H3A 2K6
CANADA

Prof. Dr. Charles R. Leedham-Green
School of Mathematical Sciences
Queen Mary College
University of London
Mile End Road
GB-London, E1 4NS

Dr. Franz Lemmermeyer
Department of Mathematics
Faculty of Science
Bilkent University Lojmanlari
Bilkent
06800 Ankara
TURKEY

Prof. Dr. Hiren Maharaj
Dept. of Mathematical Sciences
Clemson University
Martin Hall
Clemson, SC 29634-0975
USA

Prof. Dr. Christian Maire
GRIMM, UFR S.E.S.
Universite Toulouse II
5, Allee Antonio Machado
F-31058 Toulouse Cedex 9

Kathrin Maurischat
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg

Prof. Dr. Jan Minac
Department of Mathematics
Middlesex College
University of Western Ontario
London, Ontario N6A 5B7
CANADA

Prof. Dr. Thong Nguyen Quang Do
Dept. de Mathematiques
Universite de Franche-Comte
16 route de Grey
F-25030 Besancon cedex

Harris Nover
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706-1388
USA

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

Evija Ribnere
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

Prof. Dr. Alexander Schmidt
Naturwissenschaftliche Fakultät I
Mathematik
Universität Regensburg
93040 Regensburg

Prof. Dr. Rene Schoof
Dipartimento di Matematica
Universita degli Studi di Roma II
Tor Vergata
Via della Ricerca Scientifica
I-00133 Roma

Prof. Dr. Dan Segal
All Souls College
GB-Oxford OX1 4AL

Prof. Dr. Romyar Sharifi
Department of Mathematics and
Statistics
McMaster University
1280 Main Street West
Hamilton, Ont. L8S 4K1
CANADA

Marc Siegmund
Mathematisches Institut
Heinrich-Heine-Universität
Universitätsstr. 1
40225 Düsseldorf

Prof. Dr. Michael Stoll
School of Engineering and Science
International University Bremen
Postfach 750561
28725 Bremen

Prof. Dr. Otmar Venjakob
Mathematisches Institut
Universität Bonn
Beringstr. 1
53115 Bonn

Dr. Denis Vogel
NWF-I Mathematik
Universität Regensburg
93040 Regensburg

Dr. Christopher Voll
IMB, Batiment MA, Station 8
Ecole Polytechnique Federale
CH-1015 Lausanne

Dr. Simon Wadsley
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

Dr. Thomas Weigel
Dip. di Matematica e Applicazioni
Universita di Milano-Bicocca
Edificio U5
via Roberto Cozzi 53
I-20125 Milano

Prof. Dr. John S. Wilson
Mathematical Institute
Oxford University
24-29 St. Giles
GB-Oxford OX1 3LB

Prof. Dr. Kay Wingberg
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg

Prof. Dr. Christian Wuthrich
Departement de Mathematiques
Ecole Polytechnique Federale
de Lausanne
CH-1015 Lausanne

Gergely Zabradi
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

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

Prof. Dr. Andrzej Zuk
Inst. de Mathematiques de Jussieu
Universite Paris VI
175 rue du chevaleret
F-75013 Paris