Mathematisches Forschungsinstitut Oberwolfach

Report No. 28/2008

Profinite and Asymptotic Group Theory

Organised by
Fritz Grunewald, Düsseldorf
Dan Segal, Oxford

June 22nd – June 28th, 2008

Abstract. This meeting was focused on asymptotic aspects of group theory. The resulting problems lead, in particular, to the study of infinite groups, with an emphasis on the asymptotic behaviour of their finite quotients. Properties of infinite families of finite groups are at the center of interest in the field. Our meeting also covered new results from the theory of profinite groups. The methods and results of this area find important applications in several other fields of mathematics. To give an example from number theory, the absolute Galois group of the rational numbers is a profinite group in a very natural way. We had several talks covering the applications.

Mathematics Subject Classification (2000): 20E-xx, 20F-xx, 22x-xx, 11R-xx.

Introduction by the Organisers

This meeting was focused on asymptotic aspects of group theory. The resulting problems lead, in particular, to the study of infinite groups, with an emphasis on the asymptotic behaviour of their finite quotients. Also, properties of infinite families of finite groups are at the center of interest in the field.

We had talks on the most important recent developments in the field of asymptotic and profinite group theory. We single out some of these new results.

The classification of finite simple groups has provided an impetus for the detailed investigation of properties of families of groups of Lie type and of alternating groups. This has produced many results of asymptotic or probabilistic nature, describing in a quantitative way properties that hold for all sufficiently large simple groups, or else that hold 'almost surely' as the orders of the groups are tending to infinity. Here we had a talk of Aner Shalev on his recent solution (with coauthors) of Ore's conjecture.

Recently there has been much activity in the study of infinite groups, with an emphasis on the asymptotic behaviour of their finite quotients, or their finite-index

subgroups. The theory of subgroup growth is now well established; the theory of the associated zeta functions is making good progress. More subtle variations of subgroup growth are also developing into significant theories in their own right: there are important new results on representation growth – of arithmetic groups, nilpotent groups and pro-p groups; and on maximal subgroup growth, with applications to probabilistic generation properties.

Profinite groups are 'asymptotic limits' of finite groups. The nature of verbal subgroups and verbal mappings, in both finite and profinite groups, has been the focus of much recent work. This has led among other things to the solution of Serre's problem on subgroups of finite index in finitely generated profinite groups; other significant results include the characterisation of closed verbal subgroups in pro-p groups and new characterisations of solubility in finite groups.

Branch groups, both discrete and profinite, are certain groups of automorphisms of rooted trees; introduced by Grigorchuk and others over 20 years ago, they have provided the solution to several outstanding problems, and their study continues to provide new results. Some of them were reported on in our meeting.

We also had talks from important fields of mathematics in which profinite and asymptotic group theory finds application. There is, for instance, the study of the absolute Galois group of the rationals and in particular its closed pro-p subgroups. Methods from pro-p group theory have successfully been applied in order to understand fundamental groups of (hyperbolic) 3-manifolds. The interplay between the topological fundamental group of a complex algebraic surface and its profinite completion which is the etale fundamental group of the surface is the subject of recent research.

We believe that the meeting was exciting and successful. The high quality lectures covered a lot of very recent results in the field. There were many intense discussions between mathematicians of different fields. Altogether there were over 50 participants from all over the world. The percentage of young researchers was very high.

The following extended abstracts were collected and edited by Dr. Evija Ribnere.

Workshop: Profinite and Asymptotic Group Theory

Table of Contents

Abstracts

Counting arithmetic lattices and arithmetic surfaces

Alex Lubotzky
(joint work with M. Belolipetsky, T. Gelander, A. Shalev)

Let G be a non-compact simple Lie group with Haar measure μ. A classical theorem of Wang asserts that if G is not isomorphic to $PSL_2(\mathbb{R})$ or $PSL_2(\mathbb{C})$ then for every $0 < x \in \mathbb{R}$, there exists only finitely many conjugacy classes of lattices Γ in G with $\mu(G/\Gamma) < x$. This is clearly not true for $PSL_2(\mathbb{R})$ and $PSL_2(\mathbb{C})$. (The former even have continuous families of such lattices and the latter countably many). Still Borel shows that if one restricts himself only to arithmetic lattices, the result is still true.

In recent years there have been a number of works giving quantitative estimates to Wang's Theorem. Here we give quantitative estimates on Borel's Theorem. So let $AL_G(x)$ denote the number of conjugacy classes of arithmetic lattices of covolume at most x in G. We prove:

Theorem A1. *There exists $0 < b \in \mathbb{R}$ such that for every $x \gg 0$,*

$$AL_G(x) \leq x^{bx}.$$

Theorem A2. *If $G = PSO(n,1)$ then there exists $0 < a = a(n) \in \mathbb{R}$ such that for every $x \gg 0$,*

$$x^{ax} \leq AL_G(x).$$

For $G = PSL_2(\mathbb{R})$, we have a very precise estimate:

Theorem B. *Let $G = PSL_2(\mathbb{R})$ and μ the Haar measure of G obtained from lifting the hyperbolic measure from $\mathbb{H}^2 = G/K$ - the upper half plane. Then*

$$\lim_{x\to\infty} \frac{\log AL_G(x)}{x \log x} = \frac{1}{2\pi}.$$

Theorem A1 and B are proved by first giving upper bounds on the number of maximal arithmetic lattices. As this number is "small" (bounded by $x^{c \log x}$) we can fix a maximal arithmetic lattice and count its finite index subgroups. For this we use the following Theorem which is of independent interest:

Theorem C. *Let G be a simple Lie group. Then there exists a constant c such that for every lattice Γ in G, $d(\Gamma) \leq c\mu(G/\Gamma)$ when $d(\Gamma)$ denotes the number of generators of Γ.*

By subgroup growth theory the number of subgroups of index n in Γ is bounded by $n^{d(\Gamma)n}$ and this proves Theorem A1. For Theorem B one needs a more delicate analysis. Here, the miracle which enables such a precise estimate is that the covolume of a lattice Γ is proportional to $X(\Gamma)$ - the Euler characteristic of Γ (by Gauss-Bonnet formula). At the same time the subgroup growth of a Fuchsian group Γ is approximately $n^{-x(\Gamma)n}$. (The proof of this last result is based on

estimates of the character values of the symmetric group!). A combination of these two facts gives the upper bound of Theorem B. The lower bound of Theorem B and Theorem A2 are proved using an analysis of how many subgroups of index n in Γ can be conjugate in G.

Cohomology and presentations

Robert M. Guralnick
(joint work with W.M.Kantor, M.Kassabov and A.Lubtozky)

Let G be a finite group. We are interested in giving a short and/or bounded presentations of G both as a discrete group and as a finite group. Write $G = F/R$ where F is a free group on d generations and R can be generated (as a normal subgroup) by r elements. We write $r(G)$ for the minimum number of relations required (this certainly depends on d and perhaps depende on the given presentation). We are also interested in the length of the presentation (we define the length to be the number of generators plus the sum of the lengths of each relator).

It is conjectured that every finite group has a presentation with length $O(\log |G|)^3)$ (and this is best possible). This problem has been reduced to the case of simple groups (if one can show every finite simple group has a presentation of length $O(\log |G|)$, then the general result follows.

Note that if G is cyclic of prime order p, then it has a presentation with 1 generator and 1 relation. However the length of this presentation is $p + 1$ – much bigger than $\log |G|$. Indeed, it is trivial to see that there can be no family of bounded presentations with length $O(\log p)$. On the other hand, one can write down presentations of length $O(\log p)$. In fact, very recently, Goldstein, Hales and Stong proved that $\lim_{p\to\infty} \ell(p)/3 \log p \to 1$, where $\ell(p)$ is the length of the shortest presentation of the cyclic group of prime order p. In the example, they construct, there are roughly $(1/2) \log p)$ generators with the length of the relations $(5/2) \log p$.

The $\log |G|$ bound was known for almost all families of finite simple groups, but in fact we prove much more ([1]):

Theorem A. Let G be a finite nonabelian simple group other than a sporadic group or ${}^2G_2(3^{2k+1})$. Then G has a presentation with at most C relations with total length $O(\log qn)$.

Here G is a Chevalley group defined over the field of q elements of rank 1 (A_{n+1} has $q = 1$ and $n = n$). This is an asymptotic result and so the sporadic groups are not relevant. This theorem does not depend on the classifciation of finite simple groups except for asserting there are no more (the theorem could just be stated for Chevalley groups and alternating groups). The $\log(qn)$ is essentially best possible. It is not known whether the Ree groups have either a bound presentation or short presentation ($O(\log |G|)$; let alone whether this can be done simultaneously.

If we do not worry too much about the length or use a different notion of length (eg, bit length), one can do better ([3]):

Theorem B. Let G be a finite nonabelian simple group other than ${}^2G_2(3^{2k+1})$. Then G has a presentation with 2 generators and at most 80 relations.

In many cases, one can do much better. For example, if $G = A_{p+2}$ with $p \equiv 11$ mod 12 prime, then $G \times T$ has a presentation with 2 generators and 3 relations where T is the subgroup of index 2 in $\mathrm{AGL}(1, p)$ (this is an example of an efficient presentation – the number of relations for this group has to be larger than the number of generators). Thus, G itself has a presentation with 2 generators and 4 relations (close to the optimal of 2 generators and 3 relations). This leads to ([3]):

Theorem C. If $G = A_n$ or S_n, then G has a presentation with 3 generators and at most 7 relations.

Suppose now we consider profinite presentations (so F is a free profinite group on d generators and R is a closed normal subgroup of F generated as a closed normal subgroup by $\hat{r}$ elements. Write $\hat{r}(G)$ for the minimal number of profinite relations. In fact, now $\hat{r}(G)$ only depends on d (indeed, $\hat{r}(G) - d$ is invariant).

Clearly, $r(G) \geq \hat{r}(G)$ and it is unknown whether this is an equality for all finite groups. In this case, there is a formula in terms of cohomology groups for $\hat{r}$.

If M is an $\mathbb{R}_p G$-module of finite dimension, define

$$\nu_2(M) = \lceil \frac{\dim H^2(G, M) - \dim H^1(G, M) + \dim H^0(G, M)}{\dim M} \rceil.$$

Then

$$\hat{r} - d = \max\{\nu_2(M) - 1\},$$

where p ranges over all primes and M ranges over all irreducible $\mathbb{F}_p G$-modules. This depends upon a theorem of Swan and was proved independently by Gruenberg-Kovács and Lubotzky. Using a combination of cohomology results and presentations, we show ([2]):

Theorem D. Let G be a finite simple group. Then G has a profinite presentation with 2 generators and at most 17 relations.

It is like that the right number of required relations (even in the disrete case as conjectured by John Wilson) is 2 plus the rank of the Schur multiplier (which is at most 2). This allows us to prove Holt's conjecture:

Corollary E. Let G be a finite group, k a field and M an irreducible faithful kG-module. Then $\dim H^2(G, M) \leq (18.5) \dim M$.

We conjecture that if G is a finite group, k a field and M ia an absolutely irreducible kG-module, then for any $j > 0$, there is a constant C_j such that

$\dim H^j(G,M) \leq C_j(\dim M)^{j-1}$. There are examples to show that one can do no better. This is a theorem for $j = 2$ but open in all other cases (for $j = 1$, this is a conjecture of the speaker from 1984).

ACKNOWLEDGEMENTS

I would like to acknowledge the major contributions of Karl Gruenberg both to the subject and to the author. It is altogether fitting that I gave this lecture in June 2008. I first met Karl 25 years ago in June 1983 in Oberwolfach, and Karl was a good friend and very supportive over the years.

The author also thanks Oberwolfach and the organizers for the opportunity to be here and present this work. He also thanks the Institute for Advanced Study, Princeton where some of this research was carried out. He also acknowledges the support of NSF grant DMS 0653873.

References

[1] R. Guralnick, W. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: a quantitative approach*, J. Amer. Math. Soc. **11** (2008), 711–774.

[2] R. Guralnick, W. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: profinite and cohomological approaches*, Groups Geom. Dyn. **1** (2007), 469–523.

[3] R. Guralnick, W. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: a computational approach*, submitted, arXiv:0804.1396

On the clique and chromatic numbers of the generating graphs of finite groups

Andrea Lucchini

(joint work with A. Maroti)

Define a graph $\Gamma(G)$ on the elements of a finite group G by connecting two vertices by an edge if and only if they generate G. Let the clique number (size of a largest complete subgraph) of $\Gamma(G)$ be $\omega(G)$, and let the chromatic number (least number of colors needed to color the vertices of the graph in such a way that for each edge in the graph the endpoints receive different colors) of $\Gamma(G)$ be $\chi(G)$. It is clear that $\omega(G) \leq \chi(G)$. A covering for a group G is a set of proper subgroups of G whose union is G. For a finite non-cyclic group G denote the minimal size of a covering for G by $\sigma(G)$. Clearly, $\chi(G) \leq \sigma(G)$ for a non-cyclic finite group G.

The functions $\omega(G)$ and $\sigma(G)$ were much investigated. For example Blackburn [1] showed that $\omega(G) = \sigma(G)$ for infinitely many symmetric and alternating groups G. He asked whether $\omega(G)/\sigma(G)$ tends to 1 as the size of the non-abelian finite simple group G tends to infinity. We have proved [3]:

Theorem 1. *There exists a constant $c \geq 1$ such that if G is a projective special linear group, a Suzuki group, a Ree group, an alternating group of degree not divisible by 4 and not a prime of the form $(q^k - 1)/(q - 1)$ where q is a prime power and k is a positive integer, then $(1 - c/m(G))\sigma(G) \leq \omega(G) \leq \sigma(G)$ where $m(G)$ is the minimal index of a proper subgroup in G.*

It is tempting to ask whether there exists a universal constant $c \geq 1$ such that for any finite simple group G the estimate $(1 - c/m(G))\sigma(G) \leq \omega(G)$ holds. The answer to this question is not known even for alternating groups.

The proof of the previous theorem together with a result of Liebeck and Shalev (saying that there exists a constant c such that $\omega(G) \geq cm(G)$ for any non-abelian simple group [2, Theorem 7.2]) implies:

Theorem 2. *Let α denote ω, χ, or σ. For a positive number x define $\alpha(x)$ to be the number of positive integers n at most x with the property that there exists a non-abelian finite simple group G so that $\alpha(G) = n$. Then $\alpha(x) = (2\sqrt{2} + o(1))(\sqrt{x}/\ln x)$.*

For simple groups the numbers $\omega(G)$, $\chi(G)$ and $\sigma(G)$ are conjectured to be not too different and coincide in many cases. One can ask whether something similar holds for any finite (non cyclic) 2-generated group. A negative answer to this question comes from the following result:

Theorem 3. *Let S be a non-abelian finite simple group, and let n be the largest positive integer such that $G = S^n$ is 2-generated. Then $\sigma(G) = \sigma(S)$ while $\omega(G) \leq (1 + o(1))m(S)$ (as $|S|$ tends to infinity).*

For example, if $m \equiv 2 \mod 4$ is large enough, then $\sigma(\mathrm{Alt}(m)^n) = \sigma(\mathrm{Alt}(m)) = 2^{m-2}$ (see [1]) while $\omega(\mathrm{Alt}(m)^n) \leq 2m$.

The previous result is strong enough to conclude that the quotient $\sigma(G)/\omega(G)$ can be arbitrarily large. However we don't know how sharp this lower bound is. In particular we don't know if there exists a non-abelian simple group S with $\omega(S^n) > 3$.

The situation could be different in the solvable case. No 2-generated solvable group G is known with $\sigma(G) \neq \omega(G)$ and for example the following have been proved:

Theorem 4. *If G is a non cyclic 2-generated solvable group of Fitting length at most 2, then $\omega(G) = \chi(G) = \sigma(G)$.*

References

[1] S. Blackburn, *Sets of permutations that generate the symmetric group pairwise*, J. Combin. Theory Ser. A **113** (2006), no. 7, 1572–1581.

[2] M. W. Liebeck, A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky*, J. Algebra **184** (1996), no. 1, 31–57.

[3] A. Lucchini, A. Maróti, *On the clique and covering numbers of finite groups*, In preparation.

The Abstract Commensurators of Profinite Groups

Yiftach Barnea
(joint work with M. Ershov and T. Weigel)

It is well know that the Nottingham group J_p shares many properties with $\mathrm{SL}_d^1(\mathbb{F}_p[[t]])$ the first congruence subgroup of $\mathrm{SL}_d(\mathbb{F}_p[[t]])$, where $\mathbb{F}_p[[t]]$ are formal power series over a field of p elements. The latter group can be embedded as an open subgroup in a topologically simple group, namely $\mathrm{PSL}_d(\mathbb{F}_p[[t]])$. During the conference Groups St. Andrews 2005 Thomas Weigel asked me the following question: is it possible to embed J_p as an open subgroup in a topologically simple group?

I had no idea what is the answer to this question. However, the following evening Claas Röver described to me his work [5] in which he was able to embed the (discrete) Grigorchuk group into a finitely presented simple group. His main tool was the abstract commensurator of the Grigorchuk group. This stroke me also as the right tool to approach Weigel's question.

Let L be a group and let G be a subgroup of L. The *(relative) commensurator of G in L*, denoted $\mathrm{Comm}_L(G)$, is defined as the set of all $h \in L$ such that the group $hGh^{-1} \cap G$ has finite index in both G and hGh^{-1}. A particularly interesting case is when L is a totally disconnected locally compact group and G is an open compact subgroup. In this case G is a profinite group with the induced topology from L and $\mathrm{Comm}_L(G) = L$.

We recall that two groups U and V are *commensurable* if they contain subgroups of finite index which are isomorphic. In the case when U and V are profinite groups we require that the isomorphism is continuous and replace finite index by open.

A *virtual automorphism* of a group G is defined to be an isomorphism between two finite index subgroups of G; two virtual automorphisms are said to be equivalent if they coincide on some finite index subgroup of G. As before if G is profinite, then we require the isomorphism to be continuous and replace finite index by open. Equivalence classes of virtual automorphisms are easily seen to form a group, called the abstract commensurator (or just *the commensurator* of G) and denoted $\mathrm{Comm}(G)$.

Several celebrated rigidity theorems, like Pink's analogue of Mostow's strong rigidity theorem for simple algebraic groups defined over local fields, see [4], and the Neukirch-Uchida theorem, see [2], [3] and [6], can be reformulated as structure theorems for the commensurators of certain profinite groups. Recently, Mikhail Ershov [1] was able to show that $\mathrm{Comm}(J_p) = \mathrm{Aut}(J_p) = \mathrm{Aut}(\mathbb{F}_p((t)))$ for $p > 3$.

If G is a subgroup of a larger group L, then conjugation induces a natural map $\mathrm{Comm}_L(G) \to \mathrm{Comm}(G)$ which is injective under some natural conditions. So $\mathrm{Comm}(G)$ often contains information about all relative commensurators. For instance, one can use Ershov's result to give a negative answer to Weigel's question: the Nottingham group for $p > 3$ cannot be embedded as an open subgroup of a topologically simple group. Moreover, Ershov's result implies that if G is commensurable to the Nottingham group ($p > 3$) and G satisfies some mild conditions, it

must be an open subgroup of $\mathrm{Aut}(\mathbb{F}_p((t)))$. (We must have some conditions on G, otherwise for instance one can take direct sum of any group commensurable with J_p with any finite group.) Thus, the commensurators play an important role in classifying profinite groups up to commensurability.

As we have seen in the case of the Nottingham group it is interesting to understand the connection between the local structure of a locally compact group and its global structure. George Willis [7] proved that a profinite soluble group cannot be embedded as an open subgroup of a compactly generated topologically simple group. We are able to prove similar result that if G is a profinite group with a non-trivial nilpotent Fitting radical and G has no element with centralizer which is open in G, then G cannot be embedded as an open subgroup of a compactly generated topologically simple group. For example, a parabolic subgroup of $\mathrm{SL}_n(R)$ for some infinite profinite ring R cannot be embedded as an open subgroup of a compactly generated topologically simple group.

We also have a positive result in that direction. Using Röver's result we were able to construct a new compactly generated simple topologically group which contains the pro-2 completion of the Grigorchuk group as an open subgroup. As a corollary one obtains that there exists a compactly generated topologically simple group which contains every countably based pro-2 group as a closed subgroup.

I would like to mention briefly that in addition to the results above, we studied more structural properties of $\mathrm{Comm}(G)$ when G is a profinite group. For instance, we found two natural ways to turn $\mathrm{Comm}(G)$ into a topological group and we studied the connection between the algebraic properties of G and properties of these topologies. A particularly important case in which we have general results is when G is a hereditarily just infinite profinite group.

References

[1] M. Ershov, *On the commensurator of the Nottingham group*, preprint (2006).

[2] J. Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 296–314.

[3] J. Neukirch, *Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen*, J. Reine Angew. Math. **238** (1969), 135–147.

[4] R. Pink, *Compact subgroups of linear algebraic groups*, J. Algebra **206** (1998), no. 2, 438–504.

[5] C. E. Röver, *Abstract commensurators of groups acting on rooted trees*, Proceedings of the Conference on Geometric and Combinatorial Group Theory, Part I (Haifa, 2000), vol. 94, 2002, 45–61.

[6] K. Uchida, *Isomorphisms of Galois groups*, J. Math. Soc. Japan **28** (1976), no. 4, 617–620.

[7] G. A. Willis, *Compact open subgroups in simple totally disconnected groups*, J. Algebra **312** (2007), no. 1, 405–417.

A proof of Ore's Conjecture

Aner Shalev

1. Prehistory

In 1951 Ore [7] proposed the following:

Conjecture. Every element of a (nonabelian) finite simple group is a commutator.

At the time this was a rather daring conjecture; first, the classification, and even the construction, of all finite simple groups was far from completed yet; and secondly, even for known families of simple group very little was known.

Ore himself proved his conjecture for alternating groups A_n (but in fact this was established much earlier by G.A. Miller). Versions for certain Lie groups and algebraic groups were obtained in 1949-1963 by Goto, Ree and others.

In a series of papers [9, 10, 11] from 1961-1962, R.C. Thompson proved Ore's conjecture for special linear groups $\mathrm{PSL}_n(q)$. The case where $q = 2, 3$ is more difficult and required special treatment. This will be typical also in later investigations of the conjecture, where groups over tiny fields present the biggest challenge.

2. History

More progress was obtained on Ore's conjecture in the 80s and the 90s. In 1984, using methods of computational group theory, Neubüser, Pahlings and Cleuvers proved Ore's conjecture for the 26 sporadic simple groups [6].

Some symplectic groups where handled by Gow [3], and Bonten proved the conjecture for exceptional groups of rank at most 4. Bonten also showed that, for every fixed simple Lie type X, there exists a number q_0, such that Ore's conjecture holds for simple groups $X(q)$ if $q > q_0$.

This was greatly improved by Ellers and Gordeev [1] in 1998. They showed that the conjecture holds for all simple groups $X(q)$ where q is any prime power greater than 8. Their precise result is more detailed and gives better bounds on q for certain families of Lie type groups.

3. Commutators and probability

In 1984 J.S. Wilson showed, using tools from model theory, that there exists an absolute constant c such that every element of a finite simple group is a product of c commutators [12]. Using a probabilistic approach and character theory we showed the following.

Theorem 1. (Shalev [8])

(i) *The probability that a randomly chosen element of finite simple group G is a commutator tends to* 1 *as* $|G| \to \infty$.

(ii) *Every element in a large enough finite simple group is a product of* 2 *commutators.*

Note that part (ii) easily follows from part (i): once the number of commutators in $|G|$ exceeds $|G|/2$ every element of G is a product of 2 commutators. Further probabilistic properties of the commutator map on finite simple groups are given below.

Theorem 2. (Garion-Shalev [2]) *Let G be a finite simple group and let $\alpha : G\times G \to G$ be the commutator map $\alpha(x,y) = [x,y]$.*

(i) *α is almost measure preserving, in the sense that there exists $\epsilon(G)$ which tends to 0 as $|G| \to \infty$, such that for every subset $Y \subseteq G$ we have $|\alpha^{-1}(Y)|/|G|^2 - |Y|/|G|| \leq \epsilon(G)$.*

(ii) *The probability that a randomly chosen element $g \in G$ is a commutator $g = [x,y]$ where x, y generate G tends to 1 as $|G| \to \infty$.*

Part (ii) follows from part (i) and the well known result that almost all pairs of elements in a finite simple groups are generating pairs (see [4]). Note that assertion (ii) above is novel even for groups for which Ore's Conjecture was established; it is intriguing that this assertion can be applied to prove a conjecture of Guralnick and Pak on the Product Replacement Algorithm (see [2] for details).

4. Proving Ore's Conjecture

The results of the previous section already show that most elements in a finite simple group are commutators, and the challenge is to replace most by all. Recently, in joint work with Liebeck, O'Brien and Tiep, we achieved this.

Theorem 3. (Liebeck-O'Brien-Shalev-Tiep [5]) *Ore's Conjecture holds in general.*

The strategy of the proof is to combine three ingredients: character theory, induction on dimension, and computational group theory. Let us now describe it in some more detail.

The connection with character theory is based on the classical result of Frobenius that an element g of a finite group G is a commutator if and only if $0 \neq \sum_\chi \chi(g)/\chi(1)$, where the sum is over all irreducible characters of G. Using character theory of groups of Lie type we estimate the sum above. We show that if g is an element with a small centralizer, then the numbers $|\chi(g)|/\chi(1)$ are small for $\chi \neq 1$, and the main contribution to the sum $\sum_\chi \chi(g)/\chi(1)$ comes from the trivial character $\chi = 1$. This enables us to deduce that this sum is positive, so elements with small centralizer are commutators.

For elements whose centralizers are not small, our strategy is to reduce to groups of Lie type of lower dimension and use induction. In our proof for symplectic or orthogonal groups, this is usually possible since such elements have a Jordan decomposition into several Jordan blocks, and hence lie in a corresponding product of smaller symplectic or orthogonal groups; if we can (inductively) express each block as a commutator in the smaller classical group, then clearly the original element is itself a commutator. However, various technical difficulties have to be overcome to make this idea work, and for unitary groups our proof is somewhat different.

Since the proofs are inductive, we need to establish various base cases. This is done using computational methods. We note that our proof of Ore's Conjecture seems to be a rare case where the difficulty lies not just in the inductive argument, but also in establishing the induction base; indeed quite large groups had to be conisdered, and altogether this required about 3 years of CPU time.

References

[1] E.W. Ellers and N. Gordeev, *On the conjectures of J. Thompson and O. Ore*, Trans. Amer. Math. Soc. **350** (1998), 3657–3671.

[2] S. Garion and A. Shalev, *Commutator maps, measure preservation, and T-systems*, to appear in Trans. Amer. Math. Soc.

[3] R. Gow, *Commutators in the symplectic group*, Arch. Math. **50** (1988), 204–209.

[4] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Ded. **56** (1995), 103–113.

[5] M.W. Liebeck, E. O'Brien, A. Shalev and P. Tiep, *A proof of Ore's Conjecture*, Preprint, 2008.

[6] J. Neubüser, H. Pahlings and E. Cleuvers, *Each sporadic finasig G has a class C such that* $CC = G$, Abstracts AMS **34** (1984), 6.

[7] O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307–314.

[8] A. Shalev, *Word maps, conjugacy classes, and a non-commutative Waring-type theorem*, to appear in Annals of Math.

[9] R.C. Thompson, *Commutators in the special and general linear groups*, Trans. Amer. Math. Soc. **101** (1961), 16–33.

[10] R.C. Thompson, *On matrix commutators*, Portugal. Math. **21** (1962), 143–153.

[11] R.C. Thompson, *Commutators of matrices with coefficients from the field of two elements*, Duke Math. J. **29** (1962), 367–373.

[12] J.S. Wilson, *First-order group theory*, in Infinite Groups 1994, de Gruyter, Berlin, 1996, pp. 301–314.

Profinite properties and property Tau

Martin Kassabov

(joint work with N. Nikolov)

A property P defined for residually finite finitely generated groups is called *profinite* if for any two groups Γ_1 and Γ_2 with isomorphic profinite competitions $\widehat{\Gamma_1} \simeq \widehat{\Gamma_2}$ either both have property P or neither one has it.

There are many (almost trivial) examples of profinite properties: any property P which is defined using only the pro-finite completion of the group is trivially profinte, e.g. subgroup growth, being virtually abelain, etc.

Alex Lubotzky possed the question weather property Tau is a profinite property. There are reasons to expect that it is – in "some sense" a group Γ has property Tau "if" the profinite completion $\widehat{\Gamma}$ has property T.

On the other side the examples of families of finite groups which admit both expanding and no-expanding generating sets suggest that property Tau may not be a profinite one.

The main result combines results from [1] and [2] to show:

Theorem: There exists two finitely generated groups Γ_1 and Γ_2 with

$$\widehat{\Gamma_1} \simeq \widehat{\Gamma_2} \simeq \prod_{n>3} \mathrm{Alt}(n),$$

such that Γ_1 does not have property Tau but Γ_2 has property Tau.

As a result of this theorem one immediately obtains that property Tau is not a profinite property.

References

[1] M. Kassabov, *Symmetric groups and expander graphs*, Inventiones 2008
[2] M. Kassabov, N. Nikolov, *Cartesions Products as profinite completions*, IMRN 2006???

On the dynamics of profinite group actions

Miklos Abert
(joint work with G. Elek)

Let Γ be a finitely generated group. A *chain* in Γ is a sequence $\Gamma = \Gamma_0 \geq \Gamma_1 \geq \ldots$ of subgroups of finite index in Γ. We say that the chain is *normal* if it consists of normal subgroups. Let $T = T(\Gamma, (\Gamma_n))$ denote the coset tree of Γ with respect to (Γ_n) and let ∂T denote the boundary of T. Then Γ acts on ∂T by measure-preserving homeomorphisms; we call this action the *boundary representation* of Γ with respect to (Γ_n). An especially nice case is when the chain is normal with trivial intersection. Here ∂T is simply the profinite completion of Γ with respect to (Γ_n), endowed with the normalized Haar measure.

Let f and g be measure preserving actions of Γ on the probability spaces (X, μ) and (Y, ν), respectively. We say that f *weakly contains* g ($f \succeq g$) if for all measurable subsets $A_1, \ldots, A_n \subseteq Y$, finite sets $F \subseteq \Gamma$ and $\varepsilon > 0$ there exist measurable subsets $B_1, \ldots, B_n \subseteq X$ such that

$$|\mu(B_i^\gamma \cap B_j) - \nu(A_i^\gamma \cap A_j)| < \varepsilon \quad (1 \leq i, j \leq n, \gamma \in F).$$

This means that we can 'copy' the action g into X with arbitrarily small error. We call f and g *weakly equivalent* ($f \approx g$) if $f \succeq g$ and $g \succeq f$.

Theorem 1. *Let f and g be boundary representations of Γ such that f is strongly ergodic. If f and g are weakly equivalent then they are isomorphic.*

In terms of chains, this means that all elements in one of the chains contains a conjugate of an element of the other chain and vice versa. The representation f is strongly ergodic e.g. when the corresponding chain has Luboztky's property (τ).

This leads to a new result on the edit distance of expanders from bipartite graphs. By a covering tower of graphs, we mean a sequence G_n of graphs such that for all $n \geq 1$ there is a covering map from G_{n+1} to G_n.

Theorem 2. *Let G_n be an expanding covering tower of k-regular graphs. Then one of the following holds:*
1) all but finitely many of the G_n are bipartite;
2) there exists $r > 0$ such that for all n one needs to delete at least $r\,|G_n|$ edges of G_n to make it bipartite.

Equivalently, the so-called independence ratio of G_n (the maximal size of an independent subset divided by the size of the graph) is bounded away from 1/2.

On spectral language, Theorem 2 takes the following equivalent form. For a k-regular graph G on v points, let $\lambda_1(G) \geq \lambda_2(G) \geq \ldots \geq \lambda_v(G) = \lambda_-(G)$ denote the eigenvalues of the adjacency matrix of G. Then $\lambda_1(G) = k$ and $\lambda_-(G) \geq -k$. Assuming that G is connected, equality holds if and only if G is bipartite.

Corollary. *Let G_n be a covering tower of non-bipartite k-regular graphs. If $\lambda_2(G_n)$ is bounded away from k then $\lambda_-(G_n)$ is bounded away from $-k$.*

Trivially, all these results are far from being true for an arbitrary expander sequence of k-regular graphs.

We demonstrate the use of this rigidity result by answering a question of Lubotzky and Zuk. They asked whether if H_n is a family of finite index subgroups in Γ with property (τ), then the set

$$\left\{ \bigcap_{j=1}^{k} H_{n_j}^{g_j} \mid n_j \in \mathbb{N},\, g_j \in \Gamma \right\}$$

also has property (τ). The answer is negative.

Theorem 3. *There exists a family of finite index subgroups $H_n \leq F_4$, such that H_n has property (τ), but the chain $\Gamma_n = \cap_{k=1}^{n} H_k$ does not.*

Our subgroups H_n are explicitely constructed.

Using amaneble groups, we can say something about free groups.

Proposition 1. *Let p be a prime and let Γ be a finitely generated free group. Then the action of Γ on its pro-p completion is weakly equivalent to the action on its pro-(finite solvable) completion.*

Functional equations for zeta functions of groups and rings

Christopher Voll

Let Λ be a torsion-free ring of finite rank, i.e. a torsion-free abelian group of rank n, say, with a bi-additive (not necessarily associative or commutative) multiplication. The subring zeta function $\zeta_\Lambda(s)$ of Λ is the Dirichlet generating function enumerating finite index subrings in Λ:

$$\zeta_\Lambda(s) := \sum_{H \leq \Lambda} |\Lambda : H|^{-s},$$

where s is a complex variable. It is well-known that $\zeta_\Lambda(s)$ satisfies an Euler product decomposition into local factors $\zeta_{\Lambda,p}(s)$, indexed by the primes, enumerating subrings of p-power index. We mainly discussed the following result.

Theorem 1. [1, Theorem A] *For almost all primes p, the local factors satisfy the functional equation*

$$\zeta_{\Lambda,p}(s)|_{p\to p^{-1}} = (-1)^n p^{\binom{n}{2}-ns}\zeta_{\Lambda,p}(s).$$

In general, formulae for the local factors involve the cardinalities of smooth projective algebraic varieties over $GF(p)$. By the Weil conjectures, these cardinalities can be expressed as alternating sums of Frobenius eigenvalues. The definition of the operation $p \to p^{-1}$ involves the inversion of these complex numbers.

The proof of this result proceeds by expressing the local factors in terms of p-adic integrals over flag varieties, and analysing them using techniques from algebraic geometry (principalization of ideals) and combinatorics (generating functions associated to rational polyhedral cones).

An immediate corollary of this theorem is an analogous result on local zeta functions of finitely generated groups. I also discussed some variants, including the ideal zeta functions of torsion-free nilpotent Lie rings, where the phenomenon of local functional equations breaks down, in general.

References

[1] C. Voll, *Functional equations for zeta functions of groups and rings*, Ann. of Math., to appear.

Reduced zeta functions of Lie algebras

Anton Evseev

This is a brief exposition of some of the results of [3]. Let L be a finite-dimensional Lie algebra over $\mathbb{Z}$, torsion-free as an abelian group. If $m \in \mathbb{N}$, let $a_m^{\lhd}$ be the number of ideals of index m in L and $a_m^{\leq}$ be the number of subalgebras of index m in L. The following zeta functions have been studied in some detail (see [2, 4], for example):

$$\zeta_L^*(s) := \sum_{m=1}^{\infty} a_m^* m^{-s},$$

where $*$ stands for one of $\lhd$ and $\leq$ here and in the sequel and s is a complex variable. Corresponding local zeta functions can also be defined for each prime p:

$$\zeta_{L,p}^*(s) = \sum_{n=0}^{\infty} a_{p^n}^* T^n.$$

In fact, an Euler product formula holds:

$$\zeta_L^*(s) = \prod_p \zeta_{L,p}^*(s).$$

It is more convenient for us to view p^{-s} as a single formal variable. Therefore, we modify the definition:

$$\tilde{\zeta}^*_{L,p}(T) := \sum_{n=0}^{\infty} a^*_{p^n} T^n \in \mathbb{Z}[[T]].$$

In some cases (though by no means always) there is a rational function $f(X,Y)$ such that $\tilde{\zeta}^*_{L,p}(T) = f(p,T)$ for almost all primes p. In this work we consider, loosely speaking, the reduced zeta function $R^*_L(T) := f(1,T)$. This function encodes a lot less information than the usual local zeta function, but is often a lot easier to calculate and to analyse and possesses certain multiplicativity properties that $\zeta^*_{L,p}(s)$ lacks.

In order to give a general definition of reduced zeta functions, we use motivic zeta functions developed by du Sautoy and Loeser [1]. These are defined as follows. Let L be a finite-dimensional Lie algebra over $\mathbb{C}[[t]]$. Let $X_n = \mathrm{Gr}_n(L/t^nL)$ be the Grassmannian which consists of all subspaces of L/t^nL of codimension L. Let $A^*_n \subseteq X_n$ be the constructible set of all ideals (if $* = \lhd$) or subalgebras (if $* = \leq$) of codimension n in L (or, equivalently, in L/t^nL). Let $\mathcal{M}$ be the Grothendieck ring of varieties. The *motivic zeta function* is defined by

$$P^*_L(T) = \sum_{n=0}^{\infty} [A^*_n] T^n \in \mathcal{M}[[T]],$$

where $[A^*_n]$ is the element of $\mathcal{M}$ corresponding to the constructible set A^*_n (see [1] for more detail). We define the reduced zeta function by

$$R^*_L(T) = \sum_{n=0}^{\infty} \chi(A^*_n) T^n,$$

where χ is the Euler characteristic. It is proved in [1] that $P^*_L(T)$ is rational in a certain sense, and it follows that $R^*_L(T) \in \mathbb{Q}(T)$. If L is a Lie algebra over a subring S of $\mathbb{C}[[T]]$ then we define $R^*_L(T) = R^*_{L \otimes_S \mathbb{C}[[t]]}(T)$.

From now on, assume that L is a Lie algebra over $\mathbb{C}[[t]]$, torsion-free as a module. Let $\mathcal{B} = \{x_1, \ldots, x_d\}$ be a basis for L. Call $\mathcal{B}$ *simple* if for all i, j, either $[x_i, x_j] = 0$ or $[x_i, x_j] = a x_k$ for some k and some invertible element $a \in \mathbb{C}[[t]]$. Call a pair (i,j) *removable* (with respect to $\mathcal{B}$) if there exist integers $l_1, \ldots, l_d$ such that

(1) for all $z \in \mathbb{C} \setminus \{0\}$, the map given by $x_r \mapsto z^{l_r} x_r$ is an automorphism of L;
(2) $l_i \neq l_j$.

Call $\mathcal{B}$ *nice* if all pairs $1 \leq i < j \leq d$ are removable. If $\mathcal{B}$ is simple, define polyhedral cones:

$$C^{\lhd}_{\mathcal{B}} = \{\mathbf{y} \in \mathbb{R}^d_{\geq 0} : y_i \geq y_k \text{ and } y_j \geq y_k \text{ whenever } [x_i, x_j] = a x_k,\ a \neq 0\} \quad \text{and}$$
$$C^{\leq}_{\mathcal{B}} = \{\mathbf{y} \in \mathbb{R}^d_{\geq 0} : y_i + y_j \geq y_k \text{ whenever } [x_i, x_j] = a x_k,\ a \neq 0\}.$$

If $C \subseteq \mathbb{R}^d_{\geq 0}$, define the power series

$$S_C(T) = \sum_{\mathbf{n} \in C \cap \mathbb{Z}^d} T^{n_1 + \cdots + n_d}.$$

Theorem 1. *Suppose $\mathcal{B}$ is a nice and simple basis of L. Then*

$$R_L^*(T) = S_{C_{\mathcal{B}}^*}(T).$$

This result allows one to calculate zeta functions in many cases (e.g. free nilpotent Lie algebras of class 2, Lie algebras of maximal class), though the hypotheses are not satisfied by a 'random' Lie algebra.

As indicated above, reduced zeta functions are multiplicative with respect to direct sums under certain conditions.

Theorem 2. *Let L and N be finite-dimensional torsion-free Lie algebras over $\mathbb{C}[[t]]$. Then*

$$R_{L\oplus N}^{\triangleleft}(T) = R_L^{\triangleleft}(T) R_N^{\triangleleft}(T).$$

Suppose further that there is a basis $\{x_1, \ldots, x_d\}$ of L such that, for all $j \in [1, d]$, there exist integers $l_{j1}, \ldots, l_{jd}$ with the properties that $l_{jj} \neq 0$ and, for all $z \in \mathbb{C} \setminus \{0\}$, the map $x_r \mapsto z^{l_{jr}} x_r$ induces an automorphism of L. Then

$$R_{L\oplus N}^{\leq}(T) = R_L^{\leq}(T) R_N^{\leq}(T).$$

It has been observed that in many cases there is a functional equation

$$\tilde{\zeta}_{L,p}^*(T^{-1})|_{p\to p^{-1}} = (-1)^{\epsilon} p^a T^b \tilde{\zeta}_{L,p}^*(T).$$

for some integers ϵ, a and b. The existence of such a functional equation has been recently established by C. Voll [6] for zeta functions counting ideals in nilpotent Lie algebras of class 2 and for zeta functions counting subalgebras in arbitrary Lie algebras. (There are examples of zeta functions counting ideals with no functional equation: see [2].) Using Theorem 1 and a combinatorial result of Stanley [5], one can easily find conditions for a reduced zeta function to possess a functional equation as long as the Lie algebra in question has a nice and simple basis.

Proposition 1. *Under the hypotheses of Theorem 1,*

$$R_L^{\leq}(T^{-1}) = (-1)^d T^d R_L^{\leq}(T),$$

where $d = \dim L$ as before.

In the case of zeta functions counting ideals, we assume that L is nilpotent and has a nice and simple basis $\{x_1, \ldots, x_d\}$. Let h_i be the smallest number such that $x_i \in Z_{h_i}$, where

$$0 = Z_0 \leq Z_1 \leq \cdots \leq Z_c = L$$

is the upper central series of L. Write $x_l \prec x_i$ if there exists j such that $[x_i, x_j] = a x_l$, $a \neq 0$ and extend this relation by transitivity.

Proposition 2. *In addition to the statements in the preceding paragraph, assume that whenever $x_l \prec x_i$ and $h_i > h_l + 1$, there exists r such that $x_l \prec x_r \prec x_i$. Then*

$$R_L^{\triangleleft}(T^{-1}) = (-1)^d T^{\sum_{i=1}^d h_i} R_L^{\triangleleft}(T).$$

References

[1] M.P.F. du Sautoy and F. Loeser, *Motivic zeta functions of infinite dimensional lie algebras* Sel. math., New series **10** (2004), 253–303.

[2] M.P.F. du Sautoy and L. Woodward, *Zeta functions of groups and rings. Lecture Notes in Mathematics*, no. 1925, Springer Verlag (2008).

[3] A. Evseev, *Reduced zeta functions of Lie algebras*, to appear in J. reine angew. Math.

[4] F.J. Grunewald, D. Segal, and G.C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[5] R. Stanley, *Linear homogeneous diophantine equations and magic labelings of graphs*, Duke Math. J. **40** (1973), 607–632.

[6] C. Voll, *Functional equations for zeta functions of groups and rings*, to appear in Ann. of Math.

Representation zeta functions of compact p-adic analytic groups

Benjamin Klopsch

(joint work with C. Voll)

This is a report on joint work with Christopher Voll. Full proofs of the results described will be made available in form of a preprint later this year.

Let G be a profinite group. For $n \in \mathbb{N}$ we denote by $r_n(G)$ the number of (isomorphism classes of) continuous irreducible n-dimensional complex representations of G. These numbers are finite if and only if G is FAb, i.e. if and only if every open subgroup of G has finite abelianisation. If G is a compact p-adic analytic group, then G is FAb if and only if the $\mathbb{Q}_p$-Lie algebra associated to G is perfect. Consequently, a promising field for investigation is the representation growth of open compact subgroups of semisimple p-adic Lie groups, e.g. groups like $\mathrm{SL}_n(\mathbb{Z}_p)$ and its principal congruence subgroups.

The representation zeta function of a FAb profinite group G is defined as

$$\zeta_G^{\mathrm{irr}}(s) := \sum_{n=1}^{\infty} r_n(G) n^{-s}.$$

The zeta functions of prominent compact p-adic analytic groups, e.g. $\mathrm{SL}_n(\mathbb{Z}_p)$, can also be interpreted as local Euler factors of the representation zeta functions of corresponding arithmetic groups, if the latter satisfy the Congruence Subgroup Property, e.g. $\mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$; cf. [5, 1]. Using the Kirillov orbit method and model theoretic arguments, Jaikin-Zapirain [4] showed that the representation zeta function $\zeta_G^{\mathrm{irr}}(s)$ of a FAb p-adic analytic pro-p group G is a rational function over $\mathbb{Q}$ in p^{-s}, for p odd.[1] In fact, he proved a more general theorem which applies to compact p-adic analytic groups.

Three central themes of our investigation are: 'functional equations', 'uniformity' and 'poles'. For specific families of groups one may also try to find explicit formulae for the corresponding representation zeta functions. As Jaikin-Zapirain,

[1] The same assertion is expected to be true for $p = 2$, and it is known to hold if one further assumes that G is uniform.

we use the Kirillov orbit method, but an additional key step of our approach consists in expressing the zeta functions under consideration in terms of generalised Igusa local zeta functions, in the same spirit as in [7].

Regarding the topic of functional equations, we give a positive result in a general global setting, which applies in particular to open pro-p subgroups of semisimple p-adic Lie groups. For this we consider families of p-adic Lie groups whose associated Lie algebras share a common $\mathbb{Z}$-Lie sublattice. Denote by $\mathbf{P}$ the set of all primes. Let L be a Lie lattice over $\mathbb{Z}$, and for $p \in \mathbf{P}$ let $L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ denote the localisation of L at p. Then for all $p \in \mathbf{P}$ and all $k \in \mathbb{N}$, with $k \geq 2$ if $p = 2$, the $\mathbb{Z}_p$-Lie lattice $p^k L_p$ is powerful and thus corresponds to a uniform pro-p group $G_{p,k}$ by p-adic Lie theory; cf. [3].

Theorem A. *Let L be a Lie lattice over $\mathbb{Z}$ such that $\mathbb{Q} \otimes_{\mathbb{Z}} L$ is a perfect $\mathbb{Q}$-Lie algebra of dimension d. For $p \in \mathbf{P}$ consider the family of FAb uniform pro-p groups $G_{p,k}$ corresponding to the family of powerful $\mathbb{Z}_p$-Lie lattices $p^k L_p$, $k \in \mathbb{N}$ where $k \geq 2$ if $p = 2$.*

Then for almost all $p \in \mathbf{P}$ the representation zeta functions associated to the groups $G_{p,k}$, $k \in \mathbb{N}$, satisfy the functional equations

$$\zeta^{\mathrm{irr}}_{G_{p,k}}(s)|_{p \to p^{-1}} = p^{(1-2k)d} \zeta^{\mathrm{irr}}_{G_{p,k}}(s).$$

The functional equation is to be interpreted as follows. The zeta function $\zeta^{\mathrm{irr}}_{G_{p,k}}(s)$ is a rational function in p^{-s} whose coefficients can be expressed as polynomials in p and in the numbers of $\mathbb{F}_p$-points of certain smooth projective $\mathbb{F}_p$-defined varieties V. In case of the latter, the operation $p \to p^{-1}$ is performed by inverting certain Frobenius eigenvalues associated to V.

A second central problem concerning the local zeta functions associated to an arithmetic group (or a Lie ring defined globally over $\mathbb{Z}$) is suggested by the phenomenon of 'uniformity'. In our context it is natural to pose the concrete

Question. Let L be a Lie lattice over $\mathbb{Z}$ such that $\mathbb{Q} \otimes_{\mathbb{Z}} L$ is a semisimple $\mathbb{Q}$-Lie algebra of dimension d. For $p \in \mathbf{P}$ and $k \in \mathbb{N}$ let $G_{p,k}$ be defined as in Theorem A. Is there a rational function $W_L(X, Y) \in \mathbb{Q}(X, Y)$ such that for almost all $p \in \mathbf{P}$,

$$\zeta^{\mathrm{irr}}_{G_{p,k}}(s) = p^{dk} W_L(p, p^{-s}) \quad \text{for all } k \in \mathbb{N}?$$

Our approach towards answering this question is based upon a geometric interpretation of the generalised Igusa local zeta functions which play a central role in the proof of Theorem A. A sketch of the ideas involved is as follows. Let L be a Lie lattice over $\mathbb{Z}$ such that $\mathcal{L} := \mathbb{C} \otimes_{\mathbb{Z}} L$ is a semisimple Lie algebra of dimension d. Recall that the rank $\mathrm{rk}(\mathcal{L})$ of $\mathcal{L}$ is equal to the dimension of any Cartan subalgebra of $\mathcal{L}$. We define an invariant ρ of $\mathcal{L}$ so that $2\rho = d - \mathrm{rk}(\mathcal{L}) = |\Phi|$ where Φ denotes the root system associated to $\mathcal{L}$. It is well known that for every element $x \in \mathcal{L}$ the difference between the dimension of its centraliser $\mathrm{C}_{\mathcal{L}}(x)$ and $\mathrm{rk}(\mathcal{L})$ is a non-negative even number. We consider the stratification

$$\mathcal{L} = \mathcal{V}_0 \supseteq \mathcal{V}_1 \supseteq \ldots \supseteq \mathcal{V}_\rho = \{0\},$$

where

$$\mathcal{V}_i = \{x \in \mathcal{L} \mid \dim \mathrm{C}_{\mathcal{L}}(x) \geq \mathrm{rk}(\mathcal{L}) + 2i\}.$$

The elements of $\mathcal{L}$ which lie outside $\mathcal{V}_1$ are known as the regular elements of $\mathcal{L}$. We show that computing the representation zeta function of the groups $G_{p,k}$ associated to the $\mathbb{Z}$-lattice L via $p^k L_p$ at the prime p is as difficult as working out the Igusa type integral

$$\mathcal{Z}_p(r,t) = \int_{(x,\mathbf{y}) \in p\mathbb{Z}_p \times (L_p \setminus pL_p)} |x|_p^t \prod_{1 \leq j \leq \rho} \frac{\|F_j(\mathbf{y}) \cup F_{j-1}(\mathbf{y}) x^2\|_p^r}{\|F_{j-1}(\mathbf{y})\|_p^r} \, d\mu(x,\mathbf{y}),$$

where $F_j(\mathbf{Y})$ denotes a finite set of integer polynomials defining the algebraic variety $\mathcal{V}_{\rho+1-j}$, $\|F\|_p = \max\{|f|_p \mid f \in F\}$ and the Haar measure μ is normalised so that $\mu(\mathbb{Z}_p \times L_p) = 1$. In theory such an integral can be evaluated by taking a principalisation of the chain of ideals corresponding to the stratification $\mathcal{V}_i$, $0 \leq i \leq \rho$; cf. [6]. If such a principalisation could be carried out more effectively, one would probably be able to answer the above question about uniformity.

Let $\mathcal{G}$ denote the adjoint group of the semisimple Lie algebra $\mathcal{L}$. The theory of sheets associated to the adjoint action of $\mathcal{G}$ on $\mathcal{L}$ provides a useful tool for studying the stratification $\mathcal{V}_i$, $i \in \{0, \ldots, \rho\}$; cf. [2]. Indeed, a sheet of $\mathcal{L}$ is a maximal irreducible subset of $\mathcal{L}$ consisting of $\mathcal{G}$-orbits of a fixed dimension. Thus $\mathcal{V}_i \setminus \mathcal{V}_{i+1}$ is a (finite) union of sheets for each $i \in \{0, \ldots, \rho - 1\}$. In particular, this point of view allows us to compute explicit formulae for the representation zeta functions of principal congruence subgroups of $\mathrm{SL}_2(\mathbb{Z}_p)$ and $\mathrm{SL}_3(\mathbb{Z}_p)$.

Proposition B. *Let $p \in \mathbf{P}$ and $k \in \mathbb{N}$. Then*

$$\zeta^{\mathrm{irr}}_{\mathrm{SL}_2^k(\mathbb{Z}_p)}(s) = \begin{cases} p^{3k}(1 - p^{-2-s})(1 - p^{1-s})^{-1} & \text{for } p > 2, \\ 2^{3k}(2^2 - 2^{-s})(1 - 2^{1-s})^{-1} & \text{for } p = 2 \text{ and } k \geq 2. \end{cases}$$

From these formulae one can derive the representation zeta functions of the compact groups $\mathrm{SL}_2(\mathbb{Z}_p)$, which for $p > 2$ were computed by Jaikin-Zapirain [4] by a careful study of the characters of finite congruence quotients.

Proposition C. *Let $p \in \mathbf{P}$ with $p \neq 3$, and let $k \in \mathbb{N}$ with $k \geq 2$ if $p = 2$. Then*

$$\zeta^{\mathrm{irr}}_{\mathrm{SL}_3^k(\mathbb{Z}_p)}(s) = \frac{p^{8k-5}(p^5 + p^5 u(p^{-1}) p^{-2s} + u(p) p^{-3s} + p^{-5s})}{(1 - p^{1-2s})(1 - p^{2-3s})}$$

where $u(X) = 1 + X - X^2 - X^3 - X^4$.

We are in the process of computing from this result the representation zeta functions of the groups $\mathrm{SL}_3(\mathbb{Z}_p)$, $p \neq 3$, which can be interpreted as local factors of the representation zeta function associated to the arithmetic group $\mathrm{SL}_3(\mathbb{Z})$. Note that Propositions B and C yield positive answers to the above question about 'uniformity' in the two special cases under consideration and that they illustrate the more general Theorem A.

Larsen and Lubotzky [5] determined the precise abscissae of convergence of the representation zeta functions associated to norm-1 groups $\mathrm{SL}_1(\mathbb{D}_p)$ of central division algebras $\mathbb{D}_p$ over $\mathbb{Q}_p$. Our approach allows us to regain relatively easily

their result in the special case where the index of $\mathbb{D}_p$ over $\mathbb{Q}_p$ is a prime number. Moreover we can provide a set-up for computing an explicit formula for $\zeta^{\mathrm{irr}}_{\mathrm{SL}_1(\mathbb{D}_p)}(s)$ in this case. Thus far, we have carried out the calculation fully for norm-1 groups in non-split quaternion algebras.

Proposition D. *Let $p \in \mathbf{P}$ with $p > 3$. Let $\mathbb{D}_p$ denote a non-split quaternion algebra over $\mathbb{Q}_p$ with maximal order Δ_p. Then the representation zeta functions of $\mathrm{SL}_1(\mathbb{D}_p)$ and its principal congruence subgroups $\mathrm{SL}_1^k(\Delta_p)$, $k \in \mathbb{N}$, are*

$$\zeta^{\mathrm{irr}}_{\mathrm{SL}_1(\mathbb{D}_p)}(s) = \frac{(p+1)(1-p^{-s}) + 4(p-1)((p+1)/2)^{-s}}{1-p^{-s+1}},$$

$$\zeta^{\mathrm{irr}}_{\mathrm{SL}_1^k(\Delta_p)}(s) = p^{3(k-1)}\,\frac{p^2-p^{-s}}{1-p^{-s+1}}.$$

Similar formulae for higher principal congruence subgroups are also valid for $p \in \{2,3\}$, namely as soon as the Kirillov orbit method can be applied.

References

[1] N. Avni, *Arithmetic groups have rational representation growth*, preprint arXiv:math.GR/0803.1331v1 (2008).

[2] W. Borho, *Über Schichten halbeinfacher Lie-Algebren*, Invent. Math. **65** (1981/82), 283–317.

[3] J. Dixon, M. du Sautoy, A. Mann, D. Segal, Analytic pro-p groups, 2nd ed., Cambridge University Press, Cambridge, 1999.

[4] A. Jaikin-Zapirain, *Zeta functions of representations of compact p-adic analytic groups*, J. Amer. Math. Soc. **19** (2006), 91–118.

[5] M. Larsen, A. Lubotzky, *Representation growth of linear groups*, *J. Eur. Math. Soc. (JEMS)* **10** (2008), 351–390.

[6] W. Veys, W.A. Zúñiga-Galindo, *Zeta functions for analytic mappings, log-principalization of ideals, and Newton polyhedra*, Trans. Amer. Math. Soc. **360** (2008), 2205–2227.

[7] C. Voll, *Functional equations for zeta functions of groups and rings*, to appear in Ann. of Math., preprint arXiv:math.GR/0612511.

The fake degree conjecture for odd prime numbers p

Thomas Weigel

(joint work with A. Previtali)

For a given finite p-group P there are four basic questions concerning its character theory:

(i) How can one parametrize the P-conjugacy classes?
(ii) How can one compute the class number h_P of P (the number of P-conjugacy classes)?
(iii) How can one describe the irreducible characters $\mathrm{Irr}(P)$?
(iv) How can one compute the number of irreducible characters of P of degree p^k?

Generalized Cayley maps - as introduced by T. A. Springer in [6] - provide a rather elegant solution of problem (i) for certain classes of p-groups. However, at the moment it is not clear for which class of finite p-groups this approach will apply.

Let $f\colon P \to \mathfrak{L}$ be the logarithmic generalized Cayley map given by Lazard correspondence. In this case the orbit method of A. A. Kirillov (see [4]) turns out to produce irreducible characters of P, and thus provides a solution to problem (iii). This result goes back to D. Kazhdan (see [3]). However, this approach is limited to p-groups of nilpotency class less or equal to p. For powerful p-central p-groups a similar result has been proved recently by J. Gonzàlez-Sànchez.

Together with A. Previtali, we investigated recently question (ii) and (iv) for the class of *algebra groups*. A finite p-group P is called an algebra group, is there exists a finite nilpotent associative $\mathbb{Z}_p$-algebra A such that $P = 1 + A$. I. M. Isaacs introduced this notion in [1] for answering a question of J. Thompson on the character degrees of the finite p-groups $U_n(q)$, the upper uni-triangular matrices over the finite field with q-elements.

Let $f\colon P \to \mathfrak{L}$ be a generalized Cayley map of a finite p-group P onto a finite $\mathbb{Z}_p$-Lie algebra $\mathfrak{L}$. Then P is acting on $\mathfrak{L}^\vee$ - the Pontrjagin dual of $\mathfrak{L}$ - and the set of P-orbits $\mathcal{O}$ is called the set of *co-adjoint orbits* of P. The following question arises: Under which conditions is it true that

$$\{\, \chi \in \mathrm{Irr}(P) \mid \chi(1) = p^k \,\} = \{\, \Omega \in \mathcal{O} \mid |\Omega| = 2k \,\}$$

for all $k \geq 0$? For algebra group with its classical Cayley map this question was also called the *fake degree conjecture*. In [2], A. Jaikin-Zapirain showed that this conjecture is wrong for $p = 2$. It is somehow surprising that for odd primes the situation is quite different. In fact we showed that if P is an algebra group for a on odd prime number p, then the fake degree conjecture holds for P.

In [5], A. A. Kirillov asked whether one can compute the class number of the finite p-group $U = U_n(q)$, $q = p^f$, from a certain sum involving the strictly upper triangular matrices and the strictly lower triangular matrices. We were able to answer his question for odd primes p in a broader context. As a consequence we were able to show the following: Let $f\colon P \to \mathfrak{L}$ be a generalized Cayley map of a finite p-group P onto a finite $\mathbb{F}_q$-Lie algebra $\mathfrak{L}$ satisfying two additional properties. Then

$$h_P = \frac{|\mathfrak{L}_0|}{|\mathfrak{L}|},$$

where $\mathfrak{L}_0 = \{\, (x, y) \in \mathfrak{L} \times \mathfrak{L} \mid [x, y] = 0 \,\}$.

This result is related to another question of J. Thompson which has attracted much attention in recent years. Does there a exist e a polynomial $t \in \mathbb{Z}[T]$ such that

$$h_{U_n(q)} = t(q)?$$

Obviously there is an affine algebraic variety $\mathcal{V}$ defined over $\mathbb{Z}$ such that

$$\mathcal{V}(q) = \frac{|\mathfrak{L}_0(U_n(q))|}{|\mathfrak{L}(U_n(q))|}.$$

The variety $\mathcal{V}$ is just given by the vanishing of the Lie bracket on the wedge square of $\mathfrak{L}$. Therefore, we have reformulated J. Thompson's question as follows: Is $|\mathcal{V}(\mathbb{F}_q)|$ a polynomial function in q? Although this might be likely there is some experimental evidence that the geometric complexity of the varieties $\mathcal{V}$ increases with the rank n. Further investigations using more machinery from algebraic geometry seem to be necessary for answering this question.

References

[1] I. M. Isaacs, *Characters of groups associated with finite algebras*, J. Algebra **177** (1995), 708–730.

[2] A. Jaikin-Zapirain, *A counterexample to the fake degree conjecture*, Chebyshevskiĭ Sb. **5** (2004), 188–192.

[3] D. Kazhdan, *Proof of Springer's hypothesis*, Israel J. Math. **28** (1977), 272–286.

[4] A. A. Kirillov, *Merits and demerits of the orbit method*, Bull. Amer. Math. Soc. (N.S.) **36** (1999), 433–488.

[5] ———, *The orbit method and finite groups*, Surveys in modern mathematics, London Math. Soc. Lecture Note Ser. **321**, 34–69, Cambridge Univ. Press, Cambridge, 2005.

[6] T. A. Springer, *The unipotent variety of a semi-simple group*, Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), 373–391, Oxford Univ. Press, London, 1969.

A new construction in (geometric) group theory

Thomas W. Müller

(joint work with I. M. Chiswell)

My talk described a new and powerful construction associating with each (discrete) group G a group $\mathcal{RF}(G)$ together with a canonical action by isometries of $\mathcal{RF}(G)$ on some $\mathbb{R}$-tree $\mathbf{X}_G$. To some extent these groups $\mathcal{RF}(G)$ may be viewed as continuous analogues of free groups. Results, as presented in the talk, include

(1) functoriality of $\mathcal{RF}(-)$ on the category of groups and monomorphisms,

(2) a characterisation of bounded subgroups,

(3) the construction of a non-trivial generalised exponent sum $e_x : \mathcal{RF}(G) \to \mathbb{R}$ for each non-involution $x \in G$ via Lebesgue measure theory; leading to the conclusion that $\mathcal{RF}(G)$ is not generated by its elliptic elements, provided G is not an elementary abelian 2-group,

(4) an analogue of cyclic reduction,

(5) an algebraic characterisation of elliptic and hyperbolic elements,

(6) an analog of the transformation law for free groups (conjugacy of hyperbolic elements),

(7) a detailed analysis of the centralizers of hyperbolic elements,

(8) the absence of bounded and soluble normal subgroups,

(9) a stability theorem. Let

$$\mathrm{Inv}(G) = \left\{x \in G : \, x^2 = 1_G\right\}$$

be the set of involutions in G, and denote by $E(G)$ the subgroup generated by the elliptic elements of $\mathcal{RF}(G)$. Then our theorem states: if G and H are groups such that

$$|G| = |H|$$

and

$$|\mathrm{Inv}(G)| = |\mathrm{Inv}(H)|,$$

then we have

$$|\mathcal{RF}(G)| = |\mathcal{RF}(H)|$$

and

$$\mathcal{RF}(G)/E(G) \cong \mathcal{RF}(H)/E(H);$$

(that is, both the cardinality of $\mathcal{RF}(G)$ as well as the isomorphism type of the quotient $\mathcal{RF}(G)/E(G)$ depend only on two cardinal numbers, namely the order of G, and the number of its involutions).

I also discussed a number of open problems related to this construction.

References

[1] I. M. Chiswell and T. W. Müller, *A class of groups with canonical $\mathbb{R}$-tree action*, to appear.
[2] T. W. Müller and J.-C. Schlage-Puchta, *On a new construction in group theory*, in preparation.
[3] T. W. Müller and T. Weigel, *On a new construction in group theory II*, in preparation.
[4] T. W. Müller, *Free Groups And Their Continuous Relatives*, Monograph, in preparation.

Invariant and stationary measures for groups of toral automorphisms

Shahar Mozes

The growth of free products

Avinoam Mann

Let the group G be generated by the finite set S. Each element $x \in G$ can be written as a product of elements from S and their inverses, and the minimal length of such a product is termed the *length* $l(x)$ of x. Write $s_G(n)$ (or just $s(n)$) for the number of elements of length at most n. G is said the have *exponential growth*, if there exist numbers $A > 0$ and $c > 1$, such that $s(n) \geq AC^n$. It is easy to see that this notion is independent of the set of generators. Write $\omega(G, S) = \lim s(n)^{1/n}$ (this limit always exists). Then G has exponential growth iff $\omega(G, S) > 1$. Write $\Omega(G) = \inf \omega(G, S)$, the infimum taken over all finite generating sets of G. G has *uniform exponential growth*, if $\Omega(G) > 1$. Groups of non-uniform exponential growth exist, but there are many classes of groups in which all groups of exponential growth are of uniform exponential growth. E.g. soluble groups, elementarily amenable groups, linear groups, hyperbolic and

relatively hyperbolic groups,...M.Bucher, P.de la Harpe, and R.I.Grigorchuk have shown that amalgamated free products, HNN-extensions, and 1-relator groups are, with explicitely known exceptions, of uniform exponential growth, and indeed $\Omega(G) \geq \sqrt[4]{2}$. We improve the constant for all three classes. E.g. if G is an HNN-extension, then $\Omega(G) \geq \frac{1+\sqrt{5}}{2}$ (the golden ratio).

Random p-groups

Nigel Boston

Suppose that G is a pro-p group with $d(G) = g$ generators and $r(G) = r$ relators. Let F denote the free pro-p group on g generators. We wish to compute the probability for a fixed p, g, r that if r elements are picked randomly with respect to the Haar measure on the Frattini subgroup of F, then the group presented is isomorphic to G. Call this probability $pr(G)$.

If G is finite, then

$$(*) \quad pr(G) = \phi_p(g)\phi_p(r)p^{gr-g(g+1)/2-r(r+1)/2}|G|^{g-r}/|\mathrm{Aut}(G)|$$

where $\phi_g(n) = (p^n - 1)(p^{n-1} - 1)...(p - 1)$.

If $g = r = 2$ and p is fixed, then the probability that the group presented is finite is $> 99\%$ and $< 100\%$. The lower bound follows by using $(*)$ and summing $pr(G)$ over many explicit 2-generator 2-relator finite p-groups. The upper bound follows by a refinement of the theorem of Golod and Shafarevich, indicating that 2 relations at a certain fixed depth inside the free pro-p group on 2 generators necessarily present an infinite group.

There are also relative versions of $(*)$. In particular, the theorem reads the same if we take G to be of p-class $\leq c$ and consider presentations qua p-class $\leq c$. This yields a version of $(*)$ for infinite groups, namely that if we denote the maximal p-class c quotient of G by G_c, then

$$(*') \quad pr(G) = \phi_p(g)\phi_p(r)p^{gr-g(g+1)/2-r(r+1)/2} \lim_{c\to\infty} |G_c|^{g-r}/|\mathrm{Aut}(G_c)|$$

What is maybe surprising is that there exist infinite groups G satisfying $pr(G) > 0$. This family includes the free pro-p groups (for which $pr(G) = 1$, i.e. if you pick 0 relations, then with certainty the group presented is the free group) and metaprocyclic pro-p groups. In this latter case, picking 1 relator from the free pro-p group on 2 generators presents a metaprocyclic group with probability $(p-1)/p$. Apparently, a relator chosen from the remaining $1/p$ presents a group G with $pr(G) = 0$.

There are, however, other infinite groups G with $pr(G) > 0$. One such example is the 3-generator 1-relator pro-2 group $G =< x, y, z \mid x^y = x^3z^2 >$. For this group $pr(G) = 21/64$. There are many other such 1-relator groups. The method of proof will be elaborated upon in joint work with Charles Leedham-Green - the idea is to show that if a p-group has only one immediate descendant that could be a p-quotient of a 1-relator group, then the same is true of this descendant.

Note that for the limit in $(*')$ to be nonzero, $g > r$. In other words, any infinite group G with $d(G) \leq r(G)$ has $pr(G) = 0$. This observation is behind the following result that the tame Fontaine-Mazur conjecture is true with probability 100% for such groups.

Namely, fix a prime p and an integer $g \geq 1$. Let S be a set of g primes that are 1 (mod p) and G_S denote the Galois group of the maximal pro-p extension of $\mathbf{Q}$ unramified outside S. It is known that $d(G_S) = r(G_S) = g$, but not much else is known about G_S, in particular when infinite. Fontaine and Mazur did, however, conjecture that every continuous homomorphism $G_S \to GL_n(\mathbf{Z}_p)$ has finite image (since algebraic geometry produces no others).

They were hesitant about this conjecture but in fact the above methods show that if G is a randomly presented g-generator r-relator pro-p group where $g \leq r$, then with 100% probability every continuous homomorphism $G \to GL_n(\mathbf{Z}_p)$ has finite image.

One can also consider the probability that, as S varies through sets of g primes, G_S is isomorphic to a given g-generator g-relator pro-p group G. This probability $pr'(G)$ is given as a Dirichlet density. Comparing $pr(G)$ and $pr'(G)$ is analogous to the work of Dunfield and Thurston comparing fundamental groups of random 3-manifolds with a genus g Heegaard splitting and random g-generator g-relator discrete groups.

For example, if p is odd and G is the 2-generator 2-relator p-group of order p^3, then $pr(G) = (1 - 1/p)^3(1 + 1/p)^2$ whereas $pr'(G) = (1 - 1/p)^3(1 + 1/p)$. I have a conjecture in joint work with Jordan Ellenberg that predicts that if $\alpha \in \mathrm{Aut}(F)$ and we set $G_\alpha =< x_1, ..., x_g \mid \alpha(x_1) = x_1, ..., \alpha(x_g) = x_g >$, then $pr'(G)$ is the probability that as α varies through the pro-p braid group, $G_\alpha \cong G$. There is an explicit formula for this and it may be considered as a nonabelian Cohen-Lenstra heuristic.

Representation growth of arithmetic groups

Alex Lubotzky
(joint work with M. Larsen)

Let k be a number field, say $k = Q$ for simplicity of notations, G a simple k-algebraic group, $G \hookrightarrow GL_r$. Let $\Gamma = G(k) \cap GL_r(\theta)$ an arithmetic group, e.g. $\Gamma = SL_d(\mathbb{Z})$. We say that Γ has the congruence subgroup property (CSP, for short) if $\mathrm{Ker}(\hat{\Gamma} \to GL_r(\hat{\theta}))$ is finite. Lubotzky and Martin showed that Γ has CSP iff it has polynomial representation growth, i.e., $r_n \leq n^c$ for some constant c, where r_n denotes the number of degree n irreducible representations of Γ.

Assume now Γ has CSP. Larsen and Lubotzky defined $\xi_\Gamma(s) = \sum_n r_n n^{-s}$ and studied its properties.

Proposition. $\xi_\Gamma(s) = \xi_{G(\mathbb{C})}(s) \times \prod_p \zeta_{G(\mathbb{Z}_p)}(s)$.

This enables one to reduce the study of $\xi_\Gamma(s)$ to local cases: at infinity - i.e., studying the representation of the simple algebraic group $G(\mathbb{C})$, and finite primes: studying the representations of the p-adic analytic compact group $G(\mathbb{Z}_p)$.

We were mainly interested in the abscissa of convergence:

$$\alpha(\Gamma) = \limsup_n \frac{\log R_n(\Gamma)}{\log n}$$

when $R_n(\Gamma) = \sum_{i=1}^{n} r_i(\Gamma)$.

In a paper (JEMS 2008), we proved an absolute lower bound on $\alpha(\Gamma)$ for all Γ! In fact $\alpha(\Gamma) \geq \frac{1}{15}$. We are now working on proving an absolute upper bound. But the big mystery is what is the value of $\alpha(\Gamma)$. Nir Avni proved that this is a rational number. We believe (based on some results on subgroup growth of lattices) that if Γ is a lattice in a simple Lie group H, $\alpha(\Gamma)$ depends only on H and not on Γ. But we do not have any idea (nor even a guess) what the value of $\alpha(\Gamma)$ is even for, say, $\alpha(SL_d(\mathbb{Z}))$

Applications of the Gowers trick

László Pyber
(joint work with N. Nikolov and in part with L. Babai)

Answering an 1985 question of Babai and Sós [BS] Gowers [Gow] shoved that the group $\Gamma = \mathrm{PSL}(2, p)$ has no product-free subsets of size $\geq c|\Gamma|^{\frac{8}{9}}$ for some $c > 0$. He obtained this as a consequence of the following general result.

Theorem: *Let G be a group of order n, such that the minimal degree of a nontrivial representation is k. If A, B, C are three subsets of G such that $|A||B||C| > \frac{n^3}{k}$, then there is a triple $(a, b, c) \in A \times B \times C$ such that $ab = c$.*

The starting point of [NP] is the following surprising consequence.

Corollary 1. [NP]. *Let G be a group of order n, such that the minimal degree of a nontrivial representation is k. If A, B, C are three subsets of G such that $|A||B||C| > \frac{n^3}{k}$, then we have $A \cdot B \cdot C = G$. In particular, if, say, $|B| > \frac{n}{k^{\frac{1}{3}}}$, then we have $B^3 = G$.*

Corollary 1 apart from its intrinsic interest, seems to be an extremely useful tool.

For groups of Lie type rather strong lower bounds on the minimal degree of a representation are known [LS].

Combining these bounds with Corollary 1 e.g. for $L = \mathrm{PSL}(n, q)$ we obtain the following.

Proposition 1. *Let B be a subset of size at least $2|L|/q^{\frac{n-1}{3}}$. Then we have $B^3 = L$.*

A slightly weaker result in the case of $\Gamma = \mathrm{PSL}(2,p), p$ prime was obtained earlier by Helfgott [He1]. The result proved in [He1] plays an important role in proving the main result of [He1]; namely that the diameter of any Cayley graph of Γ is bounded by $(\log p)^c$ for some constant c.

Recently Helfgott [He2] (resp. Dinai [Di]) has obtained similar polylogarithmic bounds for the diameters of Cayley graphs of $\mathrm{PSL}(3,p)$ (resp. $\mathrm{PSL}(2,p^\alpha)$) using (among many other tools) Proposition 1.

In [BNP] several extensions of Corollary 1 are obtained. For example we prove the following

Theorem 1. [BNP] *Let G be a finite group of order n, such that the minimal degree of a nontrivial representation is k. Let X and Y be two probability distributions over G. Then*

$$\|X * Y - U\| \leq \sqrt{n/k}\|X - U\|\|Y - U\|$$

(where U is the uniform distribution over G and $\|\ \|$ the ℓ_2 norm.)

This can be used to prove the following results.

Theorem 2. [BNP] *Let G be a nonabelian finite simple group. For a group word w let $W = w(G)$ denote the set of values of w in G.*

Then the probability that for three random elements y_1, y_2, y_3 of W we have $y_1, y_2, y_3 = g$ is $(1 + o(1))|G|^{-1}$ for all $g \in G$.

This implies a deep result of Shalev [Sh]; if G is a large enough simple group than we have $W^3 = G$.

The proof of Theorem 1 rests on estimates for $|w(G)|$ obtained in [LSh] and [LP].

Theorem 3. [BNP]

Let G be finite simple group in Lie(p). Then G is a product of 5 Sylow p-subgroups.

Earlier Liebeck and Pyber [LP] have proved that 25 Sylow p-subgroups suffice.

Finally we mention an application of the argument of Gowers to constructing graphs which imitate random graphs.

Theorem 4. [Py] *Let Γ_n be a sequence of graphs of order n and density $\geq p$ (for some $p > 0$). Assume that the groups $G_n = Aut(\Gamma_n)$ are primitive and the index of the largest abelian normal subgroup of G_n goes to ∞. Then for λ_n, the second largest eigenvalue of the adjacency matrix of Γ_n we have $\lambda_n = o(n)$ i.e. Γ_n is quasirandom.*

(See [Gow] for motivation and terminology).

References

[BNP] L. Babai, N. Nikolov, L. Pyber *Product growth and Mixing in finite groups*, in preparation

[BS] L. Babai and V. T. Sós, *Sidon sets in groups and induced subgraphs of Cayley graphs*, Europ. J. Comb. **6** (1985), 101 – 114.

[Di] O. Dinai, manuscript
[Gow] W. T. Gowers, Quasirandom groups, Combinatorics, Probability and Computing **17** (2008), 363 – 387.
[He1] H. A. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$* Ann. Math **167** (2008), 601 – 623.
[He2] H. A. Helfgott, manuscript
[LP] M. W. Liebeck, L. Pyber, *Finite linear groups and bounded generation*, Duke Math J. **107** (2001), 159 – 171.
[LS] V. Landazuri and G. M. Seitz, *On the minimal degree of projective representations of the finite Chevalley groups,* J. Algebra **32** (1974), 418–443.
[LSh] M. Larsen and A. Shalev, *Word maps and Waring type problems*, preprint
[NP] N. Nikolov and L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem*, preprint
[Py] L. Pyber, in preparation
[Sh] A. Shalev, *Word maps, conjugacy classes, and a non-commutative Waring-type theorem*, Annals of Math., to appear

Zeta functions of nilpotent groups, uniformity

Marcus du Sautoy

Random walks on finite permutation groups

Jan-Christoph Schlage-Puchta

Let G be a finite group, S a generating set of G. Define a random walk on G by putting $g_0 = 1$, $g_{n+1} = s_n g_n$, where the random elements s_n are chosen from S independently and subject to the uniform distribution. Let δ_n be the distribution function of g_n. The question whether δ_n converges to the unifom distribution, and if it does converge, how fast the speed of convergence is has become an important area of research. In this talk I describe a strategy to obtain bounds for the mixing time for groups acting in a well-understood way on some finite set. The idea is to start a random walk and define t to be the least integer, such that δ_t resembles the uniform distribution in some aspect, e.g. the expected number of fixed points or orbits. If one can show that with high probability the element g_t lies in large conjugacy classes, one can obtain upper bounds for $|\chi(g_t)|$ for a complex irreducible character χ of G. One can then apply the upper bound lemma to obtain estimates for the mixing time of the random walk.

If $G = S_n$ the symmetric group on n letters, and S is a conjugacy class, one can put for t the least integer such that the expected number of fixed points of g_n is less than $\log n$. One then obtains a cut-off phenomenon for the symmetric group, that is, the distance of δ_n to he uniform distribution stays close to the maximal value for some time, and then declines over a much shorter time to 0. Similarly, one can show that for a conjugacy class with $o(\sqrt{n})$ fixed points the mixing time is at most 3.

If $G = \mathrm{PSL}_n(\mathbb{F}_q)$, and S is a conjugacy class, one can take the number of fixed points of the induced action on the $n-1$-dimensional projective space. In this way one obtains the correct order of the mixing time for such walks.

The same method can be applied to estimate the Fourier-coefficients of words over S_n. Let w be an arbitrary word in $\{x_1^{\pm 1}, \ldots, x_k^{\pm 1}\}$. Then the representation function

$$R(\pi) = \#\{\sigma_1, \ldots, \sigma_k \in S_n : w(\sigma_1, \ldots, \sigma_k) = \pi\}$$

is a class function and can be expanded in terms of characters as

$$R(\pi) = n!^{k-1} \sum_{\chi} \alpha_w(\chi)\chi(\pi).$$

Using this approach one obtains upper bounds for $|\alpha_w(\chi)|$ in comparison to $\chi(1)$, which allows to estimate $|\mathrm{Hom}(\Gamma, S_n)|$, where Γ is the one-relator group $\Gamma = \langle x_1, \ldots, x_k | w \rangle$. As application we prove that for $\Gamma^+ = \langle x_1, \ldots, x_k, y_1, y_2 | w[y_1, y_2] \rangle$ we have $s_n(\Gamma^+) \sim \delta n n!^k$, where s_n denotes the number of subgroup of index n. This asymptotic equivalence can further be refined to an asymptotic series in n^{-1}. The coefficients of this series are algorithmically computable, more precisely, they can be expressed in terms of character polynomials and the expected number of short cycles of $w(\sigma_1, \ldots, \sigma_k)$, where $\sigma_1, \ldots, \sigma_k \in S_n$ are chosen at random. Unfortunatelly, the effort to do so grows exponentially with the length of the word.

The asymptotics of Dehn functions and algorithmic problems

Alexander Yu. Olshanskiy

On subgroup structure of a 3-generated 2-group of intermediate growth

Rostislav Grigorchuk
(joint work with T. Nagnibeda)

1. Introduction

A group is *branch* if it acts faithfully on a spherically homogeneous rooted tree and has the lattice of subnormal subgroups similar to the structure of the tree, [6]. A group G is *self-similar* if it has a faithful action on a d-regular rooted tree, $d \geq 2$, such that the section of any element $g \in G$ is again an element of the group modulo the canonical identification of the subtree and the original tree. Equivalently, it is generated by states of non-initial invertible Mealy type automaton, [11]. Precise definitions, more details, and relevant references can be found in [2, 11, 13].

Branch groups constitute one of three classes of just infinite groups [7]. Self-similar groups appear naturally in holomorphic dynamics [13]. Although quite different, these two classes of groups have large intersection, and many self-similar groups are also branch. In the class of finitely generated branch self-similar groups there are torsion groups and torsion free groups; groups of intermediate growth and groups of exponential growth; amenable and nonamenable groups. Branch self-similar groups have very interesting subgroup structure.

Among popular examples of branch self-similar groups is the 3-generated 2-group G of intermediate growth [5]. See [12] for an introduction to this group and [8] for detailed information and a list of open problems about it. Much is known about such subgroups of G as the stabilizers of vertices of the rooted binary tree (on which G acts) and of points on the boundary of the tree; the rigid stabilizers; the centralizers ; certain normal subgroups [4]). The group G has the congruence subgroup property (that is, every subgroup of finite index contains a stabilizer $st_G(n)$ of some level n), which allows to investigate its profinite completion $\hat{G}$ [10].

2. On closed subgroups of G. The result.

The main goal of this research is to understand subgroups of G closed in profinite topology (the group G is residually finite). One class of such subgroups consists of finitely generated subgroups, as proven in [9]. It is shown there that every finitely generated subgroup of G is (abstractly) commensurable with G. This unusual property relies on the fundamental result of Pervova [14] that every maximal subgroup of G has finite (hence = 2) index. For just infinite groups the property to have all maximal subgroups of finite index is preserved when passing to commensurable groups, and thus weakly maximal subgroups in G are closed in profinite topology (a subgroup is *weakly maximal* if it has infinite index and is maximal with respect to this property). For a branch group G, the stabilizers of points in the boundary of the tree are examples of weakly maximal subgroups. It would be interesting to describe all weakly maximal subgroups in G .

Torsion p-groups are of special interest in connection with the Kaplansky conjecture on Jacobson radical, which states that, in the case of a field of characteristic p, the Jacobson radical $JK[G]$ coincides with the augmentation radical $AK[G]$ if and only if the group is locally finite p-group. It is known that if $JK[G] = AK[G]$, any maximal subgroup of G is normal of finite index p . Therefore counterexamples (if they exist) to Kaplansky conjecture should lie in the class of p-groups with all maximal subgroups of finite index. If the group has as a homomorphic image onto a group which has maximal subgroup of infinite index then the group itself has a maximal subgroup of infinite index. Therefore it is natural to investigate which just infinite groups have this unusual property. In view of the trichotomy for just infinite groups mentioned above, and as finitely generated simple groups obviously are primitive, one should concentrate on the following two questions. Is it true that a finitely generated branch group has maximal subgroups only of finite index? Is it true that every finitely generated hereditary just infinite group has a maximal subgroup of infinite index?

The property of a group to have finitely generated subgroups closed in profinite topology is quite rare. It holds for free groups by a celebrated result of Marshall Hall Jr., as well as for a few other classes of groups. In [15] it is proven that a subset of a free group which is a product of finitely many finitely generated subgroups is closed in profinite topology. This remarkable property is known (in finitely generated case) only for free groups and their trivial generalizations. We believe that every subset of G which is a product of finitely many finitely generated

groups is closed in profinite topology. Our results may be considered as positive evidence towards this statement.

Let $V(T)$ be a set of vertices of the rooted binary tree. The group G is regularly branch over the subgroup $K =< [a,b] >^G$. This implies that for any vertex $u \in V(T)$, the copy K_u of K acting on the subtree T_u with the root u and acting trivially outside T_u is a subgroup of K. We shall say that two vertices u, v are *orthogonal* if the subtrees T_u, T_v do not intersect. A subset $U \subset V(T)$ is called *orthogonal* if it consist of pairwise orthogonal vertices. It is called *a section* if every infinite geodesic ray from the root of the tree intersects U in exactly one point. It is clear that a section is a finite set. Two subsets $U, V \subset V(T)$ are *orthogonal* if every vertex of one set is orthogonal to every vertex of the other set. We consider the lexicographic order on $V(T)$.

Let $U = (u_1, \dots, u_k)$ be an ordered orthogonal set of cardinality ≥ 2. Let $\Phi = (\phi_2, \dots, \phi_k)$ be a set of isomorphisms $\phi_i : K_{u_1} \to K_{u_i}, i = 2, \dots, k$. Then the pair (U, Φ) determines a *diagonal subgroup* D (abstractly isomorphic to K), consisting of elements g acting as $g \in K$ on the subtree T_{u_1}; as $\phi_i(g)$ on the subtree $T_{u_i}, i = 2, \dots, k$; and trivially on the rest of the tree T.

Next we define a *block subgroup*. Let $(U_0, \{U_i\}_{i\in I})$ be a finite family of orthogonal, pairwise orthogonal subsets of $V(T)$ with $|U_i| \geq 2$. Let $\{\Phi_i\}_{i\in I}$ be a collection of isomorphisms corresponding to $\{U_i\}_{i\in I}$ and $\{D_i\}_{i\in I}$ be the set of corresponding diagonal subgroups . The union of sets $(U_0, \{U_i\}_{i\in I})$ can be extended to a section S of the tree. These data determine a *block subgroup*

$$B = \prod_{u\in U_0} K_u \times \prod_{i\in I} D_i \times \prod_{v\in S\setminus(U_0\cup\bigcup_{i\in I} U_i)} \{1\}$$

Theorem 1. *Let $H \leq G$ be a finitely generated subgroup of G. Then there is block subgroup H_1 of H of finite index.*

This subgroup can be found algorithmically, given generators of H.

In addition to techniques developed in [9], the proof of Theorem 1 uses the following new results.

Theorem 2. *Let $H \leq G$ be a subgroup of finite index in G, and suppose that $H \simeq K^m$ for some $m \leq 1$. Then there is a section S, $|S| = m$ such that $H = \prod_{v\in S} K_v$. In particular if a subgroup of finite index in G is isomorphic to K then it is equal to K.*

Theorem 3. *The group G has no proper subgroups of finite index isomorphic to the group.*

Note that as G is self-similar, it has many proper subgroups isomorphic to it, but, by Theorem 3, all of them are of infinite index. This last result relates to investigation of a strong version of co-hopfianity called scale-invariance which asks for a group to have proper subgroups of finite index isomorphic to the group, with an additional condition that intersections of nested sequences of such subgroups should be finite [3].

References

[1] L. Bartholdi, R.I. Grigorchuk, *On parabolic subgroups and Hecke algebras of some fractal groups*, Serdica Math. J. **28** (2002), 47–90.
[2] L. Bartholdi, R. Grigorchuk, Z. Sunik, *Branch groups*, in: Handbook of Algebra **3** (2002), 989–1112.
[3] I. Benjamini, *A problem regarding scale-invariant groups*, http://www.wisdom.weizmann.ac.il/ itai
[4] T. Ceccherini-Silberstein, F. Scarabotti, F. Tolli, *The top of the lattice of normal subgroups of the Grigorchuk group*, J. Algebra **246** (2001), 292–310.
[5] R.I. Grigorchuk, *On the Milnor problem of group growth*, Dokl. Akad. Nauk SSSR **271** (1983), 30–33.
[6] R. Grigorchuk, *Branch groups*, Mat. Zametki **67** (2000), 852–858.
[7] R.I. Grigorchuk, *Just infinite branch groups*, in: "New horizons in pro-p groups", Birkhäuser, 2000.
[8] R. Grigorchuk, *Solved and unsolved problems around one group*, in: "Infinite Groups: Combinatorial, Geometric and Dynamical Aspects" in the Series "Progress in Mathematics" **248**, Bartholdi, L.; Ceccherini-Silberstein, T.; Smirnova-Nagnibeda, T.; Zuk, A. (Eds.), Birkhäuser (2005), 117–218.
[9] R.I. Grigorchuk, J.S. Wilson, *A structural property concerning abstract commensurability of subgroups*, J. London Math. Soc. **68** (2003), 671–682.
[10] R.I. Grigorchuk, W.N. Herfort, P.A. Zalesskii, *The profinite completion of certain torsion p-groups*, in: "Algebra (Moscow, 1998)", de Gruyter, Berlin (2000), 113–123.
[11] R.I. Grigorchuk, V. Nekrashvych, V.I. Sushchansky, *Automata, dynamical systems and groups*, Proceedings of the Steklov Institute of Mathematics **231** (2000), 128–203.
[12] P. de la Harpe, *Geometric Group Theory*, University of Chicago Press, 2000.
[13] V. Nekrashvych, *Self-similar groups*, Mathematical Surveys and Monographs **117** Amer. Math. Soc., Providence, RI, 2005.
[14] E.L. Pervova, *Everywhere dense subgroups of one group of tree automorphisms*, Trudy Mat. Inst. Steklov **231** (2000), 356–367.
[15] Luis Ribes, Pavel A. Zalesskii, *On the profinite topology on a free group*, Bull. London Math. Soc. **25** (1993), 37–43.

On Grigorchuk's Evil Twin

Laurent Bartholdi
(joint work with O. Siegenthaler)

We report on a malicious mutation of the Grigorchuk group; these results will form part of the second author's PhD.

1. The Good Guy

Recall Grigorchuk's remarkable example [2] of a group G: it

is generated by four involutions: yet three involutions suffice;
is residually-2: the intersection of its subgroups of index a power of 2 is trivial;
is just infinite: it is infinite but all of its proper quotients are finite;
is a torsion 2-group: every element has order a power of 2;

has intermediate word-growth: the number $\gamma(n)$ of group elements expressible as a product of at most n generators is asymptotically larger than any polynomial, but smaller than any exponential;

is commensurable with its square: G and $G \times G$ have isomorphic finite-index subgroups;

has finite width but infinite obliquity: the sections $\gamma_n(G)/\gamma_{n+1}(G)$ along the lower central series have bounded rank (actually, 1 or 2); there does not exist a bound O such that that every normal subgroup is sandwiched between $\gamma_n(G)$ and $\gamma_{n+O}(G)$;

is recursively presented: define the endomorphism σ of $\{a, b, c, d\}^*$ by $\sigma(a) = aca$, $\sigma(b) = d$, $\sigma(c) = b$, $\sigma(d) = c$; then

$$G = \langle a, b, c, d | \sigma | a^2, bcd, [d, d^a], [d, d^{acaca}] \rangle,$$

meaning that it is the largest group satisfying the given relations and on which σ induces an endomorphism.

The Schur multiplier $H^2(G, \mathbb{F}_2)$, qua $\mathbb{F}_2[\sigma]$-module, is generated by the last three relators, subject to the relation $(\sigma - 1) \cdot (bcd) = 0$.

Much that can be said about G comes from its action on the binary rooted tree. Recall that the automorphism group W of the binary rooted tree is a profinite group $W = \operatorname{proj\,lim} \wr^n C_2$, and that restriction of W to the link of the root gives an isomorphism $\psi : W \to W \wr C_2$.

G is naturally a subgroup of W, possessing important other properties: it is *self-similar*, in the sense that ψ restricts to an embedding $G \to G \wr C_2$; this embedding contracts the word metric on each coördinate. All elements $g \in G$ satisfy the following condition: there is a finite number of rays in the binary tree, such that g acts non-rigidly only on vertices neighbouring these rays.

G may actually be defined by ψ: one has

$$\psi(a) = (1, 1)\varepsilon, \quad \psi(b) = (a, c), \quad \psi(c) = (a, d), \quad \psi(d) = (1, b),$$

with ε the non-trivial permutation of the link of the root, and the condition that ψ be an embedding specifies G uniquely. Note that σ as above is a partial splitting of ψ, in the sense that $\psi(\sigma(g)) = (*, g)$. The commensurability of G with $G \times G$ takes the following concrete form: consider the subgroup $K = \langle [a, b] \rangle^G$. Then K has finite index (16) in G, and $\psi(K)$ contains $K \times K$.

The closure $\overline{G}$ of G in W can be described by finitely many polynomial equations, and their replicas on subtrees; this was already reported in Oberwolfach [1]. The natural map from G's profinite completion $\widehat{G}$ to $\overline{G}$ is an isomorphism.

2. The Evil Twin

Consider now the following sly variation: the group H is again as generated by four involutions, subject to

$$\psi(a) = (1, 1)\varepsilon, \quad \psi(b) = (c, a), \quad \psi(c) = (a, d), \quad \psi(d) = (1, b).$$

H shares many properties in common with G: it is also generated by four involutions, residually-2, just infinite, and 2-torsion; it is commensurable with its square,

and similarly if one defines $K = \langle [a,b],[b,c],[c,d],[b,d],bcd\rangle^H$ then $\psi(K)$ contains $K \times K$; it has finite width (actually, 4) but infinite obliquity; it is recursively presented: letting τ denote the endomorphism of $\{a,b,c,d\}^*$ defined by $\tau(a) = aca$, $\tau(b) = d$, $\tau(c) = aba$, $\tau(d) = c$, and setting $x = c^a b$ we have

$$H = \langle a,b,c,d|\tau|a^2,[d,d^a],[d,x],[d,x^c],[x,x^a]\rangle.$$

The Schur multiplier $H^2(H,\mathbb{F}_2)$ is a free $\mathbb{F}_2[\tau]$-module generated by the last four relators.

Yet H has mischievous differences with G. Its growth is unknown, but could very well be exponential. It is certainly not isomorphic to G, since H's abelianization has rank 4 and not 3.

Worse, H's closure in W equals $\overline{G}$, so $\widehat{H} \neq \overline{H}$. There is a natural map $H^2(G,\mathbb{F}_2) \to H^2(H,\mathbb{F}_2)$, whose nature is a bit mysterious.

Rephrasing, there exist finite-index subgroups of H which for no $n \in \mathbb{N}$ ever contain $H \cap \ker(W \to \wr^n C_2)$; the simplest example is $H' = [H,H]$. However, every finite-index subgroup of H contains $H \cap \ker(W \to \wr^n C_2)'$ for some $n \in \mathbb{N}$; it follows that the "congruence kernel" $C = \ker(\widehat{H} \to \overline{H} = \overline{G})$ is abelian.

To describe C more precisely, set $Q = K/(\langle a\rangle^G \cap K)$; then Q is a cyclic group of order 4, generated by bcd. We have

$$C = \operatorname{proj\,lim} \cdots \to Q^{2^2} \to Q^2 \to Q \to 1,$$

where the maps $Q^{2^n} \to Q^{2^{n-1}}$ are given by

$$(\dots, q_{2i-1}, q_{2i}, \dots) \mapsto (\dots, q_{2i-1} + q_{2i}, \dots).$$

References

[1] Laurent Bartholdi, *Profinite groups generated by automata*, in *Pro-p extensions of global fields and pro-p groups*, Oberwolfach Rep. **3** (2006), no. 2, 1463–1535, Abstracts from the workshop held May 21–27, 2006, Organized by Nigel Boston, John Coates and Fritz Grunewald.

[2] Rostislav I. Grigorchuk, *On Burnside's problem on periodic groups*, Funktsional. Anal. i Prilozhen. **14** (1980), no. 1, 53–54, English translation: Functional Anal. Appl. **14** (1980), 41–43.

On the solvable radical of a finite group

Eugene Plotkin

(joint work with N. Gordeev, F. Grunewald, B. Kunyavskii)

In the talk we discuss new results about descriptions of the solvable radical of a finite group. In particular, we will focus on the results below:

Theorem 1. *The solvable radical of a finite group G coincides with the collection of $g \in G$ satisfying the property: for any 3 elements $a,b,c \in G$ the subgroup generated by the conjugates $g, aga^{-1}, bgb^{-1}, cgc^{-1}$ is solvable.*

This statement may be viewed as a theorem of Baer–Suzuki type with respect to the solvability property, in light of

Theorem 2. *(Baer–Suzuki) The nilpotent radical of a finite group G coincides with the collection of $g \in G$ satisfying the property: for any $a \in G$ the subgroup generated by g, aga^{-1} is nilpotent.*

The result from Theorem 1 is the best possible: in the symmetric groups S_n ($n \geq 5$) any triple of transpositions generates a solvable subgroup. However, as mentioned by Flavell, one can expect a precise analogue of the Baer–Suzuki theorem to hold for elements of prime order greater than 3 in $R(G)$. We prove that indeed:

Theorem 3. *Let G be a finite group. An element x of prime order $p > 3$ belongs to the solvable radical $R(G)$ if and only if for any $y \in G$ the subgroup $\langle x, yxy^{-1} \rangle$ is solvable.*

Theorem 3 implies

Corollary. *A finite group G is solvable if and only if in each conjugacy class of G every two elements generate a solvable subgroup.*

We discuss also recent results by Flavell, Guralnick-Guest-Flavell, Shalev, J. Wilson and others related to the solvable radical and solvability of a finite group. In particular, Guralnick-Guest-Flavell announced the results coinciding with ones presented in the talk.

A Cantor set of groups

Volodymyr Nekrashevych

The talk is an exposition of the papers [8] and [9].

For a finite alphabet X denote by X^* the free monoid generated by X, i.e., the set of finite words over X. Let $X = \{0, 1\}$. Define permutations of X^* labeled by infinite sequences $w \in X^\infty$ inductively by the rule

$$\begin{gathered}\alpha_w(0v) = 1v, \quad \alpha_w(1v) = 0v,\\ \beta_w(0v) = 0\alpha_{s(w)}(v), \quad \beta_w(1v) = 1\gamma_{s(w)}(v),\\ \gamma_w(0v) = 0\beta_{s(w)}(v), \quad \gamma_w(1v) = 1v,\end{gathered}$$

if the first letter of w is 0, and

$$\gamma_w(0v) = 0v, \quad \gamma_w(1v) = 1\beta_{s(w)}(v),$$

if the first letter of w is 1, where $s(x_1x_2\ldots) = x_2x_3\ldots$. The defined transformations are elements of the profinite group $\mathrm{Aut}(X^*)$ of automorphisms of the naturally defined rooted tree X^*, in which two vertices are adjacent if they are of the form v, vx for $v \in X^*$ and $x \in X$.

Denote by $\mathcal{D}_w$ the discrete subgroup of $\mathrm{Aut}(X^*)$ generated by $\alpha_w, \beta_w, \gamma_w$. The groups $\mathcal{D}_w$ appear naturally in the study of iterations of the rational mapping

$$f(z, p) = \left(\left(1 - \frac{2z}{p}\right)^2, \left(1 - \frac{2}{p}\right)^2\right).$$

We have the following characterization of the transformations $\alpha_w, \beta_w, \gamma_w$.

Proposition 1. *The conjugacy classes in* $\mathrm{Aut}(X^*)$ *of* $\alpha_w, \beta_w, \gamma_w$ *do not depend on* w.

If g_0, g_1, g_2 *are (independently) conjugate in* $\mathrm{Aut}(X^*)$ *to* $\alpha_w, \beta_w, \gamma_w$, *respectively, then there exists a unique sequence* $w_1 \in X^\infty$ *for which there exists* $h \in \mathrm{Aut}(X^*)$ *such that* $g_0^h = \alpha_{w_1}, g_1^h = \beta_{w_1}, g_2^h = \gamma_{w_1}$.

As a corollary we get that for any $w \in X^\infty$ the set of words $w_1 \in X^\infty$ such that $\mathcal{D}_w$ is conjugate in $\mathrm{Aut}(X^*)$ to $\mathcal{D}_{w_1}$, is countable.

Using rigidity theorems of [7] we prove that two groups $\mathcal{D}_{w_1}$ and $\mathcal{D}_{w_2}$ are isomorphic as abstract groups if and only if they are conjugate subgroups of $\mathrm{Aut}(X^*)$.

The following properties of the family of groups $\{\mathcal{D}_w\}_{w\in X^\infty}$ are proved in [8].

Theorem 1. *Two groups* $\mathcal{D}_{w_1}$ *and* $\mathcal{D}_{w_2}$ *are isomorphic if and only if the sequences* w_1, w_2 *are cofinal, i.e., are of the form* $w_1 = v_1 w$ *and* $w_2 = v_2 w$ *for* $w \in X^\infty$ *and* $v_1, v_2 \in X^*$ *of equal length.*

The closure of $\mathcal{D}_w$ *in* $\mathrm{Aut}(X^*)$ *does not depend (up to conjugacy in* $\mathrm{Aut}(X^*)$*) on the sequence* w.

The family $\{\mathcal{D}_w\}_{w\in X^\infty}$ contains two known groups. The group $\mathcal{D}_{000\ldots}$ is the iterated monodromy group of the polynomial $z^2 + i$ (see [2, 3]). It was proved by K.-U. Bux and R. Perez that this group is of intermediate growth. The group $\mathcal{D}_{111\ldots}$ coincides with one of the Grigorchuk groups, defined in [5]. This group was also studied by A. Erschler in [4], where estimates on its growth were given.

Let $\mathcal{G}_3$ be the space of marked 3-generated groups with natural topology (see [5]).

Theorem 2. *Let* $\Omega \subset \{0,1\}^\infty$ *be the set of sequences containing infinitely many zeros. Then the map* $w \mapsto (\mathcal{D}_w, \alpha_w, \beta_w, \gamma_w)$ *from* Ω *to* $\mathcal{G}_3$ *is a homeomorphic embedding.*

Denote by G_w the limit of the groups $\mathcal{D}_{w'}$ in $\mathcal{G}_3$ as w' approaches w staying inside Ω. Then $G_w = \mathcal{D}_w$ for $w \in \Omega$, while the group $G_{111\ldots}$ is an extension of C_4^∞ by $\mathcal{D}_{111\ldots}$. The same description of the isomorphism classes for the family G_w is true as for the family $\mathcal{D}_w$.

Theorem 3. *The group* $G_{111\ldots}$ *has non-uniform exponential growth, i.e., it has exponential growth, but the exponent of growth can be made arbitrarily close to 1 by changing the generating set.*

The question of existence of groups of non-uniform exponential growth was asked by M. Gromov in [6]. The first examples of groups of non-uniform exponential growth were constructed by J. Wilson in [11, 10]. See also an example due to L. Bartholdi [1].

References

[1] Laurent Bartholdi, *A Wilson group of non-uniformly exponential growth*, C. R. Acad. Sci. Paris. Sér. I Math. **336** (2003), No. 7, 549–554.

[2] Laurent Bartholdi, Rostislav Grigorchuk, and Volodymyr Nekrashevych, *From fractal groups to fractal sets*, In Peter Grabner and Wolfgang Woess, editors, *Fractals in Graz 2001. Analysis – Dynamics – Geometry – Stochastics*, pages 25–118. Birkhäuser Verlag, Basel, Boston, Berlin, 2003.

[3] Laurent Bartholdi, and Volodymyr Nekrashevych, *Iterated monodromy groups of quadratic polynomials I*, Groups, Geometry, and Dynamics **2** (2008), 309–336.
[4] Anna Erschler, *Boundary behaviour for groups of subexponential growth*, Annals of Mathematics **160** (2004), 1183–1210.
[5] Rostislav I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Math. USSR Izv. **25** (1985) No. 2, 259–300.
[6] Mikhael Gromov, *Structures métriques pour les variétés riemanniennes. Redige par J. LaFontaine et P. Pansu*, volume 1 of *Textes Mathematiques*. Paris: Cedic/Fernand Nathan, 1981.
[7] Yaroslav V. Lavreniuk and Volodymyr V. Nekrashevych, *Rigidity of branch groups acting on rooted trees*, Geom. Dedicata **89** (2002) No. 1, 155–175.
[8] Volodymyr Nekrashevych, *A minimal Cantor set in the space of 3-generated groups*, Geometriae Dedicata, **124** (2007) No. 2, 153–190.
[9] Volodymyr Nekrashevych, *A group of non-uniform exponential growth locally isomorphic to $IMG(z^2+i)$*, (to appear in Transactions of AMS.)
[10] John S. Wilson, *Further groups that do not have uniformly exponential growth*, Journal of Algebra, **279** (2004), 292–301.
[11] John S. Wilson, *On exponential growth and uniform exponential growth for groups*, Inventiones Mathematicae, **155** (2004), 287–303.

Finite presentability for subdirect products

Martin R. Bridson

Arithmetic Dynamics and the Characterization of Finite Solvable Groups

Tatiana M. Bandman
(joint work with F. Grunewald, B. Kunyavskii)

There are two theorems, characterizing solvable groups in the class of finite groups by identities in two variables ([1], [2]).

Theorems. Define two sequences u_n and s_n in the following way:

$$u_1(x,y) := x^{-2}y^{-1}x, \qquad s_1(x,y) := x,$$

and, inductively,

$$u_{n+1}(x,y) := [\, x\, u_n(x,y)\, x^{-1},\ y\, u_n(x,y)\, y^{-1}\,],$$
$$s_{n+1}(x,y) := [\, y^{-1}\, s_n(x,y)\, y,\ s_n(x,y)^{-1}\,].$$

A finite group G is solvable iff

- for any $(x,y) \in G \times G \quad \exists n : u_n(x,y) = 1$ ([1]);
- for any $(x,y) \in G \times G \quad \exists n : s_n(x,y) = 1$ ([2]).

Our **Question** is: what should be the properties of a sequence which may be used for characterization of finite solvable groups?

It appears that our **Question** has an interpretation as a problem in Arithmetic Dynamics on Affine Varieties. For both sequences the proof may be reduced to finding a periodic set of an endomorphism of an affine variety, connected to a group $PSL(2,\mathbb{F}_p)$ or $Sz(2^n)$.

For example, sequence s_n defines a map $\varphi : G \times G \to G$

$$\varphi(x,y) = [y^{-1}xy, x^{-1}] \tag{1}$$

and an endomorphism $\tilde{\varphi} : G \times G \to G \times G$,

$$\tilde{\varphi}(x,y) = (\varphi(x,y), y). \tag{2}$$

We want this map to have periodic points $x \neq 1, y \neq 1$ for every p.

In order to understand dynamical properties of such endomorphism, we consider the corresponding trace map. In $\tilde{G} = SL(2,\mathbb{Z})$ the trace of any word in two letters (x,y) can be written as a polynomial in $s = tr(x), u = tr(xy), t = tr(t)$. Denote by $\mathbb{A}^3_{s,u,t}$ the three-dimensional affine space with coordinates s,u,t. Let

$$f_1(s,u,t) = tr(\phi(x,y)), f_2(s,u,t) = tr(\phi(x,y)y),$$

$$\psi_{\tilde{\phi}}(s,u,t) = (f_1(s,u,t), f_2(s,u,t), t).$$

$$\pi(x,y) = (tr(x), tr(xy), tr(y)).$$

The commutative diagram (factorization) follows:

Diagram 1

$$\begin{array}{ccc} \tilde{G}\times\tilde{G} & \xrightarrow{\tilde{\phi}} & \tilde{G}\times\tilde{G} \\ \pi\downarrow & & \downarrow\pi \\ \mathbb{A}^3_{s,u,t} & \xrightarrow{\psi_{\tilde{\phi}}} & \mathbb{A}^3_{s,u,t} \end{array}$$

The set

$$\Sigma = \{f_1(s,u,t) = s, f_2(s,u,t) = u\}$$

of fixed points of $\psi_{\tilde{\phi}}$ has positive dimension.

Now the **Question** has arithmetic dynamics flavour: when the reduction of the map $\psi_{\tilde{\phi}} : \mathbb{A}^3(\mathbb{F}_p) \to \mathbb{A}^3(\mathbb{F}_p)$ has periodic point for every p?

For example, for the map (2) for p big enough the corresponding fixed point set Σ is defined over $\mathbb{F}_p$ and has irreducible components over $\overline{\mathbb{F}}_p$, thus $\Sigma(\mathbb{F}_p) \neq \emptyset$.

Using Arithmetic Dynamics methods we provide some necessary and sufficient conditions on a sequence to be appropriate for characterizing solvable groups.

References

[1] T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavskii, G. Pfister, Eu. Plotkin, *Identities for finite solvable groups and equations in finite simple groups*, Compositio Math. **142** (2006), 734–764.

[2] J. N. Bray, J. S. Wilson, R. A. Wilson, *Characterization of finite soluble groups by laws in two variables*, Bull. of London Math. Soc. **37** (2005), 179–186 .

Meromorphic Continuation of Euler Products

Gautami Bhowmik

(joint work with J. C. Schlage-Puchta, F. Grunewald)

1. Introduction and results

The Euler-product of a Dirichlet series is one of the most effective ways to access the series. Among important applications of Dirichlet-series is the asymptotic estimation of the sum of its coefficients where the question of continuation of Dirichlet-series beyond their domain of absolute convergence is a central issue.

In general, we would be interested in the series

$$D(s_1, s_2, \cdots, s_r) = \prod_p W(p^{-s_1}, \cdots, p^{-s_r})$$

where W is an integral polynomial in r variables. For the one-variable case Estermann[3] in 1928 showed that for an integral polynomial $W(x)$ with $W(0) = 1$ the Dirichlet-series $D(s) = \prod_p W(p^{-s})$ is either a finite product of Riemann ζ-functions, and therefore meromorphically continuable to the whole complex plane, or it is continuable to the half-plane $\Re\, s > 0$, and the line $\Re\, s = 0$ is the natural boundary of this function. The strategy of his proof was to show that every point on the line $\Re\, s = 0$ is an accumulation point of poles or zeros of D. This method of proof was extended to much greater generality and it was recently shown that [1] Estermann's theorem can be extended to r variables. Much interest has been generated by ζ-functions of nilpotent groups introduced by Grunewald, Segal and Smith[6] as well as height zetafunctions [2] where the Euler products are often of the form $D(s) = \prod W(p, p^{-s})$ for an integral polynomial W and where, in general, the known results on natural boundaries do not apply. Du Sautoy and Grunewald[4] gave a criterion for such a function to have a natural boundary, which, in a probabilistic sense, applies to almost all polynomials. Again, it is shown that all points on the presumed boundary is an accumulation point of zeros or poles. The following conjecture [5] is believed to be true.

Conjecture 1. *Let $W(x, y) = \sum_{n,m} a_{n,m} x^n y^m$ be an integral polynomial with $W(x, 0) = 1$. Then $D(s) = \prod_p W(p, p^{-s})$ is meromorphically continuable to the whole complex plane if and if only if it is a finite product of Riemann ζ-functions. Moreover, in the latter case if $\beta = \max\{\frac{n+1}{m} : a_{n,m} \neq 0\}$, then $\Re\, s = \beta$ is the natural boundary of D.*

Here we show that any refinement of Estermann's method is bound to fail to prove this conjecture. Define an obstructing point z to be a complex number with $\Re\, z = \beta$, such that there exists a sequence of complex numbers z_i, $\Re\, z_i > \beta$, $z_i \to z$, such that D has a pole or a zero in z_i for all i. Obviously, each obstructing point is an essential singularity for D, the converse not being true in general.

Initially, $D(s)$ may not be convergent on the half-plane $\Re\, s > \beta$. To continue it meromorphically to this half-plane, one writes D as a product of Riemann ζ-functions and a function $R(s)$ holomorphic, zero-free, and bounded on every half-plane $\Re\, s > \beta + \epsilon$. More precisely, there exists integers $c_{n,m}$, such that

$$D(s) = \prod_{n,m} \zeta(ns+m)^{c_{n,m}} \times R(s)$$

When approximating $D(s)$ by a product of Riemann *zeta*-functions, the main contribution comes from monomials $a_{n,m}x^n y^m$ with $\frac{n+1}{m} = \beta$. We collect these monomials into the monomial $\tilde{W}$, that is, we have

$$W(x,y) = \tilde{W}(x,y) + \sum\nolimits^*_{n,m} a_{n,m}x^n y^m,$$

where $\sum^*$ means summation over all pairs n, m with $\frac{n+1}{m} < \beta$.

Our main result is the following.

Theorem 1. *Let W be a polynomial, and define $\beta, \tilde{W}$ as above. Then precisely one of the following holds true.*

1. *$W = \tilde{W}$, and W is cyclotomic; in this case, D is a finite product of Riemann ζ-functions;*
2. *$\tilde{W}$ is not cyclotomic; in this case, every point of the line $\Re\, s = \beta$ is an obstruction point;*
3. *$W \neq \tilde{W}$, $\tilde{W}$ is cyclotomic, and there are infinitely many pairs n, m with $a_{n,m} \neq 0$ and $\frac{n}{m} < \beta < \frac{n+1}{m}$; in this case, β is an obstruction point;*
4. *$W \neq \tilde{W}$, $\tilde{W}$ is cyclotomic, there are only finitely many pairs n, m with $a_{n,m} \neq 0$ and $\frac{n}{m} < \beta < \frac{n+1}{m}$, but there are infinitely many primes p such that the equation $W(p, p^{-s}) = 0$ has a solution s_0 with $\Re\, s_0 > \beta$; in this case every point of the line $\Re\, s = \beta$ is an obstruction point;*
5. *None of the above; in this case, no point on the line $\Re\, s = \beta$ is an obstruction point.*

We give examples of each of these cases and show that there are Euler-products like

$$g(s) = \prod_p \left(1 - p^{-s} + p^{2-s}\right)$$

for which Estermann's approach cannot work.

We then give an application by establishing a bijection between right cosets of $2t \times 2t$ symplectic matrices and submodules of finite index of $\mathbb{Z}^{2t}$ which are equal to their duals and which we call polarised. The counting function obtained

corresponds to the p-adic zeta function [7] of algebraic groups $\mathcal{G}$ with respect to their normalised Haar measure μ.

$$Z(s) = \int_{\mathcal{G}_p^+} |\det(\rho(g)|_p^s \mu_{\mathcal{G}}(g)$$

where $\mathcal{G}_p^+ = \rho^{-1}(\rho(G(\mathbb{Q}_p)) \cap M_n(\mathbb{Z}_p))$.

In [4] it was proved that $\Re\ s = \frac{4}{3}$ is the natural boundary when $\mathcal{G} = GSp_6$. Using this information we can study the average order of the number of polarised submodules.

References

[1] G. Bhowmik, D. Essouabri, B. Lichtin, *Meromorphic Continuation of Multivariable Euler Products*, Forum Math. **19** (2007), 1111–1139.

[2] R. de la Bretèche, Sir P. Swinnerton-Dyer, *Fonction zêta des hauteurs associée à une certaine surface cubique*, Bulletin de la SMF **135** (2007), 65–92.

[3] T. Estermann, *On certain functions represented by Dirichlet series*, Proc. London Math. Soc. **27** (1928), 435–448.

[4] M. du Sautoy, F. Grunewald, *Zeta functions of groups: zeros and friendly ghosts*, Amer. J. Math. **124** (2002), 1–48.

[5] M. du Sautoy, L. Woodward, *Zeta functions of groups and rings*, Lecture Notes in Mathematics, 1925. Springer-Verlag, Berlin, 2008.

[6] F. J. Grunewald, D. Segal, and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[7] J.-I. Igusa, *Universal p-adic zeta functions and their functional equations*, Amer. J. Math. **111** (1989), 671–716.

The conjugacy problem for some extensions of groups and a presentation of Mihailova's subgroup

Oleg Bogopolski

Let F be an arbitrary group and F_n be a free group of rank n. If two elements $u, v \in F$ are conjugate we write $u \sim v$. Below we define a generalization of the conjugacy problem $\mathrm{CP}(F)$.

Let $\varphi \in \mathrm{Aut}(F)$. We say that $u, v \in F$ are *twisted conjugate with respect to* φ and write $u \underset{\varphi}{\sim} v$ if there exists an $f \in F$ such that $\varphi(f)uf^{-1} = v$. This relation was introduced by K. Reidemeister in [11].

The *twisted conjugacy problem for* F, denoted $\mathrm{TCP}(F)$ is the following: Given $u, v \in F$ and $\varphi \in \mathrm{Aut}(F)$, decide whether $u \underset{\varphi}{\sim} v$. If we fix φ, we get the *φ-twisted conjugacy problem* for F, denoted $\mathrm{TCP}_\varphi(F)$. Clearly $\mathrm{TCP}_{id}(F)$ coincides with $\mathrm{CP}(F)$. The following theorem was proven by O. Bogopolski, A. Martino, O. Maslakova and E. Ventura in [1].

Theorem A [1]. 1) *The twisted conjugacy problem for F_n is solvable.*

2) *The conjugacy problem for any extension $F_n \rtimes \mathbb{Z}$ is solvable.*

The second statement can be deduced also by combining the recent results of A. Olshanski and M. Sapir [10] (if G is a finitely presented group with at most quadratic Dehn function, then $\mathrm{CP}(G)$ is solvable) and M.R. Bridson and D. Groves [4] (any extension $F_n \rtimes \mathbb{Z}$ has at most quadratic Dehn function).

Definition. A subgroup $A \leqslant \mathrm{Aut}(F)$ is called *orbit decidable* if, given $u, v \in F$, one can decide whether there exists an $\alpha \in A$ such that $\alpha(u) \sim v$.

J.H.C. Whitehead [12] proved that the whole group $\mathrm{Aut}(F_n)$ is orbit decidable in $\mathrm{Aut}(F_n)$ and P. Brinkmann [5] proved that any cyclic subgroup in $\mathrm{Aut}(F_n)$ is orbit decidable.

Let F be a normal subgroup of a group G. Then G acts by conjugation on F and so induces automorphisms on F. The group of all induced automorphisms is denoted by A_G. The following theorem says that under certain assumptions the solvability of the conjugacy problem for G is equivalent to the orbit decidability of the subgroup $A_G \leqslant \mathrm{Aut}(F)$.

Theorem B [2]**.** *Let $1 \to F \to G \to H \to 1$ be a short exact sequence, such that the following three conditions are satisfied:*

1) $\mathrm{TCP}(F)$ *is solvable;*

2) $\mathrm{CP}(H)$ *is solvable;*

3) *for any nontrivial $h \in H$ holds $|C_H(h) : \langle h \rangle| < \infty$ and one can compute a set of coset representatives of $\langle h \rangle$ in the centralizer $C_H(h)$.*

Then $\mathrm{CP}(G)$ is solvable if and only if $A_G \leqslant \mathrm{Aut}(F)$ is orbit decidable.

Note, that the condition 1) is satisfied for polycyclic groups, finitely generated free groups and fundamental groups of compact surfaces. The condition 2) is satisfied for torsion free hyperbolic groups.

From this theorem and from a result of J. McCool, we deduce the following corollary.

Corollary 1 [2]**.** *The conjugacy problem is solvable for any extension of the form $F_2 \rtimes F_m$ and of the form $\mathbb{Z}^2 \rtimes F_m$.*

Now we describe a method to construct an orbit undecidable subgroup $A \leqslant \mathrm{Aut}(F)$. In view of Theorem B, this will enable us to construct some simple examples of groups with unsolvable conjugacy proplem (but with solvable word problem), see Theorem D.

For $f \in F$ we denote $\mathrm{Stab}^*(f) = \{\varphi \in \mathrm{Aut}(F) \,|\, \varphi(f) \sim f\}$.

Theorem C [2]**.** *Let $A \leqslant B \leqslant \mathrm{Aut}(F)$ be such that the following two conditions are satisfied:*

1) *the membership problem $\mathrm{MP}(A, B)$ is unsolvable;*

2) *there exists $f \in F$ such that $B \cap \mathrm{Stab}^*(f) = 1$.*

Then $A \leqslant \mathrm{Aut}(F)$ is orbit undecidable.

In [8], K.A. Mihailova showed how to construct a finitely generated subgroup A of $B = F_n \times F_n$, $n \geqslant 2$, with unsolvable membership problem $\mathrm{MP}(A, B)$. Thus we get

Corollary 2 [2]**.** *Let F be a group such that the following two conditions are satisfied:*

1) $\mathrm{Aut}(F)$ *contains a subgroup* $B \cong F_n \times F_n$*, where* $n \geqslant 2$*;*

2) *there exists an element* $v \in F$ *such that* $B \cap \mathrm{Stab}^*(v) = 1$*.*

Then $\mathrm{Aut}(F)$ *contains a finitely generated orbit undecidable subgroup* A*.*

Note that the groups $\mathrm{Aut}(\mathbb{Z}^4)$ and $\mathrm{Aut}(F_3)$ contain subgroups isomorphic to $F_2 \times F_2$. Using this, Corollary 2 and Theorem B, we deduce

Theorem D [2]**.** *There exist extensions of the form* $\mathbb{Z}^4 \rtimes F_{14}$ *and of the form* $F_3 \rtimes F_{14}$ *with unsolvable conjugacy problem.*

The statement about unsolvability of the conjugacy problem for some extensions of the form $F_n \rtimes F_m$ was proven ealier by C.F. Miller III (see [9]).

Questions. 1) Does there exists a finitely presented subgroup $A \leqslant \mathrm{Aut}(F_n)$, which is orbit undecidable?

2) Is $\mathrm{CP}(\mathbb{Z}^3 \rtimes F_m)$ solvable?

In [7] F. Grunewald proved that the Mikhailova subgroup is not finitely presented. The aim of this paragraph is to give an explicit presentation of Mihailova's subgroup of $F_n \times F_n$, where F_n is a free group with basis $x_1, \ldots, x_n$, and $n \geqslant 2$. Let H be a group which admits a finite Peiffer aspherical presentation $\langle x_1, x_2, \ldots, x_n \,|\, R_1, \ldots, R_m \rangle$ (see [6] for the definition of asphericity). By definition, Mihailova's subgroup $A(H) \leqslant F_n \times F_n$ is generated by pairs $d_i = (x_i, x_i)$ and $t_j = (1, R_j)$, $i = 1, \ldots, n$; $j = 1, \ldots, m$.

For any free group F and a nontrivial element $f \in F$, let $\mathrm{root}(f)$ denote the element $g \in F$ such that $f = g^{k(g)}$ and $k(g)$ is maximal.

Theorem E. *The Mihailova group $A(H)$ has the following presentation:*

$$\langle d_1, \ldots, d_n, t_1, \ldots, t_m \,|\, [t_j, z^{-1} t_i^{-1} R_i(d) z], \\ [t_i,\ \mathrm{root}(R_i(d))]\ \ (1 \leqslant i, j \leqslant m;\ z \in D_n) \rangle,$$

where D_n denotes the free group generated by $d_1, \ldots, d_n$, and $R_i(d)$ denotes the word in D_n obtained from R_i by replacing each x_k by d_k.

References

[1] O. Bogopolski, A. Martino, O. Maslakova and E. Ventura, *Free-by-cyclic groups have solvable conjugacy problem*, Bulletin of the London Math. Soc. v. **3**8, part 5 (2006), 787-794.

[2] O. Bogopolski, A. Martino and E. Ventura, *Orbit decidability and the conjugacy problem for some extensions of groups*, Available at http://arxiv.org/abs/0712.3104
Accepted to Transactions of AMS.

[3] O. Bogopolski and E. Ventura, *A presentaition of Mihailova's subgroup*, in progress.

[4] M.R. Bridson and D. Groves, *The quadratic isoperimetric inequality for mapping tori of free-group automorphisms.* To be a memoir of the AMS. Available at http://arxiv.org/abs/0802.1323

[5] P. Brinkmann, *Detecting automorphic orbits in free groups*, preprint. Available at http://math.sci.ccny.cuny.edu/people?name=Peter_Brinkmann

[6] M. Chiswell, D.J. Collins and J. Huebschmann, *Aspherical group presentations*, Math. Z. **178** (1981), 1–36.
[7] F.J. Grunewald, *On some groups which cannot be finitely presented*, J. London Math. Soc. **17** (2) (1978), 427–436.
[8] K. A. Mihailova, *The occurrence problem for direct products of groups*, Dokl. Acad. Nauk SSRR **119** (1958), 1103-1105.
[9] C.F. Miller III, *On group-theoretic decision problems and their classification*, Annals of Math. Studies **68**, 1971.
[10] A. Olshanski and M. Sapir, *Groups with small Dehn functions and bipartitute chard diagrams*. Available at http://arxiv.org/abs/math/0411174
[11] K. Reidemeister, *Automorphismen von homotopiekettenringen*, Math. Ann. **112** (1936), 586-593.
[12] J.H.C. Whitehead, *On equivalent sets of elements in a free group*, Ann. of Math. **37** (1936), 782-800.

Reporter: Evija Ribnere

Participants

Prof. Dr. Miklos Abert
Department of Mathematics
The University of Chicago
5734 South University Avenue
Chicago, IL 60637-1514
USA

Prof. Dr. Tatiana Bandman
Dept. of Mathematics
Bar-Ilan University
52 900 Ramat-Gan
ISRAEL

Prof. Dr. Yiftach Barnea
Department of Mathematics
Royal Holloway College
University of London
Egham
GB-Surrey TW 20 0EX

Prof. Dr. Laurent Bartholdi
Ecole Polytechnique Federale de Lausanne
SB IMB MAD - MA C3 605
Station 8
CH-1015 Lausanne

Prof. Dr. Ingrid Bauer-Catanese
Lehrstuhl für Mathematik VIII
Universität Bayreuth
NW - II
95440 Bayreuth

Dr. Gautami Bhowmik
Universite Lille I
Laboratoire Paul Painleve
UFR de Mathematiques
F-59655 Villeneuve d'Ascq Cedex

Prof. Dr. Oleg Bogopolski
Fakultät für Mathematik
Technische Universität Dortmund
Vogelpothsweg 87
44221 Dortmund

Prof. Dr. Nigel Boston
University of Wisconsin-Madison
Van Vleck Hall
480 Lincoln Drive
Madison WI 53706
USA

Prof. Dr. Martin R. Bridson
Mathematical Institute
Oxford University
24-29 St. Giles
GB-Oxford OX1 3LB

Dr. ChristopherJ.B. Brookes
Corpus Christi College
GB-Cambridge, CB2 1RH

Dr. Rachel Camina
Dept. of Pure Mathematics and Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 0WB

Prof. Dr. Fabrizio Catanese
Lehrstuhl für Mathematik VIII
Universität Bayreuth
NW - II
95440 Bayreuth

Erika Damian
Dept. of Mathematics
Ben-Gurion University of the Negev
Beer Sheva 84 105
ISRAEL

Dr. Eloisa Detomi
Dipartimento di Matematica Pura
e Applicata
Universita di Padova
Via Trieste, 63
I-35121 Padova

Dr. Anton Evseev
Selwyn College
GB-Cambridge CB3 9DQ

Prof. Dr. Ivan B. Fesenko
Dept. of Mathematics
The University of Nottingham
University Park
GB-Nottingham, NG7 2RD

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. Robert M. Guralnick
Department of Mathematics
KAP 108
University of Southern California
3620 S. Vermont Avenue
Los Angeles CA 90089-2532
USA

Prof. Dr. Martin Kassabov
Department of Mathematics
Cornell University
310 Malott Hall
Ithaca NY 14853-4201
USA

Prof. Dr. Elena Klimenko
Mathematisches Institut
Heinrich-Heine-Universität Düsseldorf
Universitätsstr. 1
40225 Düsseldorf

Dr. Benjamin Klopsch
Department of Mathematics
Royal Holloway College
University of London
Egham
GB-Surrey TW 20 0EX

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

Prof. Dr. Boris Kunyavski
Department of Mathematics
Bar-Ilan University
52900 Ramat Gan
ISRAEL

Prof. Dr. Alex Lubotzky
Department of Mathematics
The Hebrew University
Givat Ram
Jerusalem 91904
ISRAEL

Dr. Andrea Lucchini
Dipartimento di Matematica Pura
e Applicata
Universita di Padova
Via Trieste, 63
I-35121 Padova

Dr. Keivan Mallahi-Karai
School of Engineering and Science
Jacobs University Bremen
Postfach 750561
28725 Bremen

Prof. Dr. Avinoam Mann
Institute of Mathematics
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

Prof. Dr. Shahar Mozes
Institute of Mathematics
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

Prof. Dr. Thomas W. Müller
School of Mathematical Sciences
Queen Mary College
Mile End Road
GB-London E1 4NS

Prof. Dr.
Volodymyr V. Nekrashevych
Department of Mathematics
Texas A & M University
College Station, TX 77843-3368
USA

Dr. Nikolay Nikolov
Department of Pure Mathematics
Imperial College London
South Kensington Campus
GB-London SW7 2AZ

Prof. Dr.
Alexander Yu. Olshanskiy
Department of Mathematics
Vanderbilt University
1326 Stevenson Center
Nashville, TN 37240
USA

Dr. Eugene Plotkin
Dept.of Mathematics & Comp. Science
Bar-Ilan University
52900 Ramat-Gan
ISRAEL

Dr. Laszlo Pyber
Alfred Renyi Mathematical Institute
of the Hungarian Academy of Science
Realtanoda u. 13-15
H-1053 Budapest

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

Dr. Evija Ribnere
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

Prof. Marcus du Sautoy
Department of Mathematics
University of Oxford
24-29 St Giles
GB-Oxford OX1 3LB

Prof. Jan Saxl
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 0WB

Dr. Jan-Christoph Schlage-Puchta
Mathematisches Institut
Universität Freiburg
Eckerstr. 1
79104 Freiburg

Prof. Dr. Dan Segal
All Souls College
GB-Oxford OX1 4AL

Prof. Dr. Aner Shalev
Institute of Mathematics
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

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

Dr. Christopher Voll
School of Mathematics
University of Southampton
Highfield Campus
GB-Southampton SO17 1BJ

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