# ESI Workshop Profinite Groups December 2008 – Talks

December 19, 2008

**M. Abert** Profinite actions and dynamics

**J. Almeida** Tameness in pseudovarieties of groups

**Y. Barnea** Abstract commensurators of profinite groups

**L. Bary-Soroker** Quasifree subgroups of quasifree groups

**L. Bary-Soroker** Projective pairs of profinite groups

**G. Bergauer** 2-dimensional profinite complexes

**M. Boggi** The congruence subgroup property for the hyperelliptic modular group

**N. Boston** Random $p$-groups

**I. Efrat** On the descending $p$-central sequence of absolute Galois groups

**H. Koch** The Galois group of the maximal $p$-extension of an algebraic number field with given ramification points

**D. Kochloukova** Pro-$p$ limit groups

**P. Lochak** Automorphisms of profinite Teichmueller groups

**K. Lorensen** Good groups and pro-$p$ good groups

**A. Lubotzky** Discrete and profinite presentations of finite simple groups

**A. Lucchini** Profinite groups in which the subgroup zeta function and the probabilistic zeta function coincide

**A. Mann** Positively finitely generated groups and their zeta functions

**A. Pinto** Normal subgroups of profinite groups of non-negative deficiency

**P. Plaumann** Boolean loops

**L. Pyber** On groups of polynomial index growth

**A.S. Rapinchuk** $p$-adic techniques in the theory of Lie groups and differential geometry

**A.S. Rapinchuk** On almost 1-generation of the congruence kernel

**L. Ribes** Wreath products and classical subgroup theorems for abstract and profinite groups

**D. Segal** Which verbal subgroups are closed

**J-P. Serre** Variation with $p$ of the number of solutions mod $p$ of polynomial equations

**J-P. Serre** Independence of $l$-adic representations

**A. Shalev** Words, Ore's conjecture and random walks

**P. Shumyatsky** On pro-$p$ groups admitting a fixed-point-free automorphism

**B. Steinberg** Symbolic dynamics, projective profinite groups and free profinite monoids

**P. Symonds** On the Cohomology of a pro-$p$ Group considered as an Abstract Group

**Th. Weigel** Profinite groups acting on pro-p trees

**J.S. Wilson** Exchange Theorems

**E. Zelmanov** Infinite Groups

**A. Zuk** Automata groups

# M. Abert

## Profinite actions and dynamics

A profinite action is a projective limit of finite transitive group actions. We analyze these actions using dynamical tools. This leads to applications in seemingly unrelated fields, like graph theory or 3-manifold theory. The results are joint works with Nikolay Nikolov and Gabor Elek.

# J. Almeida

## Tameness in pseudovarieties of groups

Consider a finite system of equations whose variables are constrained to take values in fixed rational subsets of a certain free monoid. Given a pseudovariety V of groups, is it decidable whether, modulo each homomorphism into members of $\mathbf{V}$, such a system always has some solution? A standard compactness argument transfers this problem to the profinite world, whereupon the constraints become clopen subsets of a free profinite monoid and solutions are sought modulo the natural continuous homomorphism to the free pro-$\mathbf{V}$ group on the same set of free generators. But, does this really help in answering the decidability question, the number of candidates for solutions being in general uncountable?

Inspired by pioneering work of Ash, Steinberg and the author (2000) proposed a method to establish decidability that isolates a reducibility condition. It states that if there is a solution to the system then there is one of a restricted algebraic type. Once such a condition is established for a suitable algebraic type, which allows enumeration of terms, which can be effectively evaluated in finite semigroups, and whose word problem with respect to $\mathbf{V}$ is decidabe, one can show that the original problem is decidable.

For instance, Ash's "Inevitable Graphs" Theorem (1991) essentially shows that the reducibility condition holds for the pseudovariety of all finite groups when we consider systems whose variables are the vertices and edges of a finite directed graph and whose equations describe multiplication as in a Cayley graph. The algebraic type in question is quite natural, adding a pseudoinversion to multiplication, which restricts to the usual algebraic language for groups. This result solved a long-standing conjecture of Rhodes, which was also proved independently by Ribes and Zaleskii (1993) using profinite group theory. It was rediscovered, in a model-theoretic disguise by Herwig and Lascar (1997).

The aim of the talk is to give an introduction to this topic and to call attention to some open problems in the area.

# Y. Barnea

## Abstract commensurators of profinite groups

Joint work with Mikhail Ershov and Thomas Weigel

In this talk we will discuss the use of the abstract commensurator to study profinite groups. Results on commensurators of profinite groups were obtained before, but they were not formulated in that language. Indeed, several celebrated rigidity theorems, like Pink's analogue of Mostow's strong rigidity theorem for simple algebraic groups defined over local fields, and the Neukirch-Uchida theorem, can be reformulated as structure theorems for the commensurators of certain profinite groups.

We will see the importance of commensurators in understanding the local-global relation in totally disconnected locally compact groups, and how computing commensurators can be useful in classifying profinite groups. We will demonstrate these applications in the case of the Nottingham group, i.e. the group of wild automorphisms of a local field of positive characteristic, for which Mikhail Ershov recently computed the commensurator.

# L. Bary-Soroker

## Semi-free groups and fields with free absolute Galois groups

Recently Harbater used the notion of quasi-free profinite groups to prove that if k is separably closed, then the maximal abelian extension of $k((x, y))$ has a free absolute Galois group. In this talk we introduce the condition of a profinite group being semi-free, which is more general than being free and more restrictive than being quasi-free. Then we discuss permanence properties of free groups that carry over to semi-free groups. We explain how this implies that many field extensions of $k((x, y))$ have free absolute Galois groups (when $k$ is separably closed). This work is joint with Dan Haran and David Harbater.

# L. Bary-Soroker

## Projective pairs of profinite groups

We will discuss the notion of projective pairs of a profinite group and a closed subgroup. Then we shall talk about Pseudo Algebraically Closed extensions and its connection with projective pairs.

## G. Bergauer

### 2-dimensional profinite complexes

2-dimensional complexes, based upon a concept of unoriented profinite graphs, are presented. Our theory intends to comprise certain results obtained by P.A.Zalessskii and O.V.Melnikov for profinite groups acting on trees and profinite fundamental groups of profinite graphs of profinite groups. We provide, as a special situation, a profinite version of the van Kampen theorem for 2-complexes and give an interpretation of the HNN-extension of torsionfree profinite groups.

## M. Boggi

### The congruence subgroup property for the hyperelliptic modular group

Let $\mathcal{M}_{g,n}$ and $\mathcal{H}_{g,n}$, for $2g-2+n>0$, be, respectively, the moduli stack of $n$-pointed, genus $g$ smooth curves and its closed substack consisting of hyperelliptic curves. Their topological fundamental groups can be identified, respectively, with $\Gamma_{g,n}$ and $H_{g,n}$, the so called *Teichmüller modular group* and *hyperelliptic modular group*. A choice of base point on $\mathcal{H}_{g,n}$ defines a monomorphism $H_{g,n} \hookrightarrow \Gamma_{g,n}$.

Let $S_{g,n}$ be a compact Riemann surface of genus $g$ with $n$ points removed. The Teichmüller group $\Gamma_{g,n}$ is the group of isotopy classes of diffeomorphisms of the surface $S_{g,n}$ which preserve the orientation and a given order of the punctures. As a subgroup of $\Gamma_{g,n}$, the hyperelliptic modular group then admits a natural faithful representation $H_{g,n} \hookrightarrow \mathrm{Out}(\pi_1(S_{g,n}))$.

The *congruence subgroup problem for* $H_{g,n}$ asks whether, for any given finite index subgroup $H^\lambda$ of $H_{g,n}$, there exists a finite index characteristic subgroup $K$ of $\pi_1(S_{g,n})$ such that the kernel of the induced representation $H_{g,n} \to \mathrm{Out}(\pi_1(S_{g,n})/K)$ is contained in $H^\lambda$. In the talk, I will explain why this question has an affirmative answer.

## N. Boston

### Random $p$-groups

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

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

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

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

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 $1 \pmod p$ 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 $\alpha \in Aut(F)$ 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 $\alpha$ 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.

## I. Efrat

### On the descending $p$-central sequence of absolute Galois groups

For a prime number $p$ and a profinite group $G$, the descending $p$-central sequence of $G$ is defined inductively by

$$G^{(1)} = G, \quad G^{(i+1)} = (G^{(i)})^p[G^{(i)}, G].$$

Thus $G^{(2)}$ is the intersection of all normal open subgroups $N$ of $G$ with $G/N \cong \mathbb{Z}/p$. When $p \neq 2$, and under a certain cohomological assumption on $G$, we give a similar characterization of $G^{(3)}$: it is the intersection of all closed normal subgroups $N$ of $G$ such that $G/N$ is isomorphic to $\mathbb{Z}/p^2$ or to the unique nonabelian group $M_{p^3}$ of order $p^3$ and exponent $p^2$.

The above-mentioned cohomological assumption holds, e.g., when $G$ is the absolute Galois group of a field $F$ containing a root of unity of order $p$. This gives a new restriction on the possible group-theoretic structure of absolute Galois groups.

This is a joint work with Ján Mináč (University of Western Ontario)

## H. Koch

### The Galois group of a maximal $p$ extension of an algebraic number field with given ramification points

Let $p$ be a prime number, let $K$ be an algebraic number field and let $S$ be a set of places of $K$ (= equivalence classes of valuations of $K$). The maximal $p$-extension $K_S$ of $K$ unramified outside $S$ is the union of all finite normal extensions of $K$ which have a degree being a power of $p$ and being unramified outside $S$. The Galois group of $G_S = \mathrm{Gal}(K_S/K)$ is a pro-$p$ group.

The subject of the talk is the study of the structure of $G_S$. We begin with some classical results of Shafarevich, Tate, Golod-Shafarevich and Koch and come then to recent results of Boston, Labute, A.Schmidt and Eick-Koch.

## D. Kochloukova

### Pro-$p$ limit groups

In a recent joint work with Pavel Zalesskii we define pro-$p$ limit groups and show that they satisfy some of the known properties of abstract limit groups i.e. finite cohomological dimension, non-positive Euler characteristic, are (free pro-$p$)-by-(torsion-free nilpotent), non-trivial finitely generated normal subgroups of a limit group always has finite index, 2 generated limit groups are either free pro-$p$ or abelian. Still there are many open questions: we do know know whether pro-$p$ limit groups are residually free pro-$p$ or whether the Euler characteristic is 0 only in the abelian case. The main method used in the proofs is the pro-$p$ version of Bass-Serre theory of groups acting on trees.

## P. Lochak

### Automorphisms of profinite Teichmueller groups

I will explain how, modulo a very plausible but still open geomtric conjecture, one can compute the automorphism groups of the profinite Teichmueller (alias mapping class) groups in term of the so-called Grothendieck-Teichmueller group. The result is 'universal' in that it applies to all (but a finite number of low-dimensional exceptions) Teichmueller groups and indeed also to all their open subgroups.

## K. Lorensen

### Good groups and pro-$p$ good groups

If $G$ is an abstract group, we denote the profinite completion of $G$ by $\hat{G}$ and the pro-$p$ completion by $\hat{G}^p$ for any prime $p$. The group $G$ is considered "good" if the canonical map $H^*(\hat{G}, A) \to H^*(G, A)$ is an isomorphism for any finite, discrete $\hat{G}$-module $A$; $G$ is "pro-$p$ good" if the canonical map $H^*(\hat{G}^p, A) \to H^*(G, A)$ is an isomorphism for any finite, discrete $\hat{G}^p$-module $A$ with order a power of $p$. Both "good" and "pro-$p$ good" groups are endowed with intriguing properties, and these notions have recently been applied fruitfully in geometry.

In this talk we discuss some of the properties of “good groups” and “pro-$p$ good groups” and mention several new examples of groups that belong to these classes. In conclusion, we look at ascending HNN extensions of polycyclic groups, presenting compelling evidence that such groups might be “good.”

# A. Lubotzky

### Discrete and profinite presentations of finite simple groups

Finding ‘nice & compact’ presentations of various groups has been a subject of great interest for groups theorists for more than a century. Well known presentations are the Coxeter presentation of the finite symmetric groups and Steinberg presentation of groups of Lie type. In response to conjectures of Babai and Szemeredi on one hand (motivated by questions in computational group theory) and of Mann on the other hand (motivated by questions on subgroup growth) we show that all non-abelian finite simple groups (with the possible exception of Ree groups) have presentations which are small (bounded number of relations) and short (w.r.t the length of the relations). This is very surprizing as the simple abelian groups- the cyclic groups of prime order- do not have such presentations! We will describe the motivations and results, a cohomological application (proving a conjecture of Holt) and some connections with discrete subgroups of Lie groups. We will also discuss the connection with profinite presentations and we will recall some old problems in new form.

Based on joint works with Bob Guralnick, Bill Kantor and Martin Kassabov ( J. of the AMS 2007, Groups, Geomerty and Dynamics 2007 and J. of the European Math. Soc., to appear).

# A. Lucchini

### Profinite groups in which the subgroup zeta function and the probabilistic zeta function coincide

To a finitely generated profinite group $G$ one may associate two numerical sequences, considering

- $a_n(G)$ the number of the open subgroups of index $n$;
- $b_n(G) = \sum_{|G:H|=n} \mu_G(H)$, where $\mu_G$ is the Möbius function associated to the lattice of open subgroups of $G$.

The two Dirichlet series $\zeta_G(s) = \sum_n a_n(G)/n^s$ and $p_G(s) = \sum_n b_n(G)/n^s$ are called the subgroup zeta function and the probabilistic zeta function of $G$. If $G = \hat{\mathbb{Z}}$ then $\zeta_G(s)$ is the Riemann zeta function and $p_G(s)$ is its multiplicative inverse. We investigate the groups $G$ which satisfy the property $\zeta_G(s)p_G(s) = 1$. Partial results and several related open questions are presented.

## A. Mann

### Positively finitely generated groups and their zeta functions

A profinite group $G$ is *positively finitely generated* (PFG) if for some $k$, the probability that $k$ random elements generate $G$ is positive. E.g. a finitely generated prosoluble group is PFG, a free non-abelian group is not PFG, etc. PFG groups were characterized by A.Mann-A.Shalev as groups in which the number of maximal subgroups grows (at most) polynomially with the index. More structural characterizations were given recently by L.Pyber and A.Jaikin-Zapirain. Their results have applications to counting finite groups. I'll survey these results, discuss the "probabilistic zeta function" that can be associated to some PFG groups (conjecturally to all of them), and mention several open problems.

## A. Pinto

### Normal subgroups of profinite groups of non-negative deficiency

In a joint work with Fritz Grunewald, Andrei Jaikin-Zapirain and Pavel Zalesski, we initiate the study of profinite groups of non-negative deficiency. We show that the existence of a finitely generated normal subgroup of infinite index in a profinite group $G$ of non-negative deficiency gives rather strong consequences for the structure of $G$. To make this precise we introduce the notion of $p$-deficiency ($p$ a prime) for a profinite group $G$. This concept is more useful in the study of profinite groups then the notion of deficiency. We prove that if the $p$-deficiency of $G$ is positive and $N$ is a finitely generated normal subgroup such that the $p$-Sylow subgroup of $G/N$ is infinite and $p$ divides the order of $N$ then we have $\mathrm{cd}_p(G) = 2$, $\mathrm{cd}_p(N) = 1$ and $\mathrm{vcd}_p(G/N) = 1$ for the cohomological $p$-dimensions; moreover either the $p$-Sylow subgroup of $G/N$ is virtually cyclic or the $p$-Sylow subgroup of $N$ is cyclic.

A profinite Poincaré duality group $G$ of dimension 3 at a prime $p$ ($PD^3$-group) has $p$-deficiency 0. In this case we show that for $N$ and $p$ as above (i.e. $N$ is a finitely generated normal subgroup such that the $p$-Sylow subgroup of $G/N$ is infinite and $p$ divides the order of $N$) either $N$ is $PD^1$ at $p$ and $G/N$ is virtually $PD^2$ at $p$ or $N$ is $PD^2$ at $p$ and $G/N$ is virtually $PD^1$ at $p$. In particular if $G$ is pro-$p$ then either $N$ is infinite cyclic and $G/N$ is virtually Demushkin or $N$ is Demushkin and $G/N$ is virtually infinite cyclic.

We apply this results to deduce structure information on the profinite completions of ascending HNN-extensions of free groups.

## P. Plaumann

### Boolean loops

A boolean space is a compact, totally disconnected topological Hausdorff space on which the group of homeomorphisms acts transitively.
We call a loop $(L, \cdot, /, \backslash, 1)$ a *boolean loop* if $L$ is a boolean space and the operations $\cdot, /$ and $\backslash$ are continuous.
*Profinite loops* can be defined without any difficulty. One sees immediately that

(B) *Every profinite loop is a boolean loop.*

For groups it is well known that the converse of (B) is true. The situation for loops, however, is not immediately clear to us. So we discuss the question

(Q) *Is it true that every boolean loop is profinite?*

For this we use an approach to describe loops completely in the language of transformation groups which goes back to Reinhold Baer. A *loop folder* $\xi = (G, H, T)$ is a triple consisting of a group $G$ with a subgroup $H$ and a subset $T$ of $G$ such that $1 \in T$ and $T$ is a transversal for all conjugates $H^g, g \in G$. Given a loop folder $\xi = (G, H, T)$ and $x, y \in T$, one defines $x \star y$ by the condition $(Hx)(Hy) = H(x \star y)$. Then $(T, \star)$ is a loop which we denote by $\mathsf{L}(\xi)$.

Let $\mathcal{L}$ be the category of loops and homomorphisms, and let $\mathcal{T}$ the class of all loop folders. There is a natural way to define morphisms between elements of $\mathcal{T}$ such that $\Lambda$ becomes a functor from $\mathcal{T}$ to $\mathcal{L}$.

Similar constructions exist in various classes of groups and loops. Here we are interested in boolean groups and loops. One considers continuous homomorphisms only and assumes that decompositions $G = H^g T$ which belong to a given loop folder $(G, H, T)$ are topological products. We consider the resulting categories $\mathcal{L}_{\text{boolean}}$ and $\mathcal{T}_{\text{boolean}}$.

**Proposition 1** *For every loop $L$ in $\mathcal{L}_{\text{boolean}}$ there is a loop folder $\xi$ in $\mathcal{T}_{\text{boolean}}$ satisfying $L = \Lambda(\xi)$.*

Both categories $\mathcal{L}_{\text{boolean}}$ and $\mathcal{T}_{\text{boolean}}$ have projective limits.

**Proposition 2** *Let $\xi = (G, H, T)$ be a loop folder in $\mathcal{T}_{\text{boolean}}$ such that $H$ is finite and set $L = \Lambda(\xi)$. Then one has $\xi = \varprojlim_{\alpha} \xi_\alpha$ for finite loop folders $\xi_\alpha$. In particular, the loop $L$ is profinite.*

For the general case however, the answer to question $(\mathsf{Q})$ is negative.

**Proposition 3** *There is a boolean loop* $W = \Lambda(\xi), \xi = (G, H, T) \in \mathcal{T}_{\text{boolean}}$ *such that the profinite group* $G$ *does not possess a normal subgroup* $N$ *of finite index for which the triple* $\xi/N = (G/N, HN/N, TN/N)$ *is a loop folder and the loop* $\Lambda(\xi/N)$ *is a proper loop.*

This is joint work with Wolfgang Herfort

## L. Pyber

### On groups of polynomial index growth[1]

A group $G$ is said to have polynomial index growth (PIG) if there is a constant $c$ such that for every finite quotient $G/N$ we have $|G/N| < (\exp(G/N)^c)$ (where $\exp(G)$ denotes the exponent of the group $G$). This holds for example if $G$ is an arithmetic group with the congruence subgroup property or if $G$ is boundedly generated (a product of finitely many cyclic groups). We investigate profinite completions of finitely generated PIG groups and profinite PIG groups in general.

## A.S. Rapinchuk

### $p$-adic techniques in the theory of Lie groups and differential geometry

This talk is based on a series of joint papers with Gopal Prasad. First, I will discuss the existence of special elements, called generic, in any finitely generated Zariski-dense subgroup of the group of rational points of a semisimple algebraic group over a field of characteristic zero. This result has the following interesting implication: any dense subgroup of a compact semisimple Lie group contains an element which generates a dense subgroup of the corresponding maximal torus (notice that this fact is false for (even finitely generated) subgroups of compact tori!). Even though this result refers to properties of (compact real) Lie groups, the only proof available at the moment uses $p$-adic techniques. More precisely, the crucial fact for our argument is that a finitely generated integral domain of characteristic zero can be embedded in the ring of $p$-adic integers $\mathbb{Z}_p$ for infinitely many $p$. Furthermore, I will discuss an extension of the above result to not necessarily compact semisimple Lie groups where it asserts the existence of generic $\mathbb{R}$-regular elements. These elements were used in rigidity problems, in analysis of the Auslander conjecture, and in other situations.

[1]The author regrets not be able to attend the meeting

In the second half of the talk, I will discuss our recent work where generic elements were used to analyze length-commensurable and isospectral locally symmetric spaces. From the algebraic perspective, these results hinge on the notion of weakly commensurable Zariski-dense subgroups. We have been able to obtain rather definite results regarding weakly commensurable $S$-arithmetic groups: it turns out that in many situations, weak commensurability of $S$-arithmetic subgroups implies their commensurability , and in all cases, the $S$-arithmetic subgroups weakly commensurable to a given $S$-arithmetic subgroup split into finitely many commensurability classes. These algebraic results have a number of important applications to locally symmetric spaces, in particular, we used these to answer Marc Kac's famous question "Can one hear the shape of a drum?" for compact arithmetically defined locally symmetric spaces.

## A.S. Rapinchuk

### On almost 1-generation of the congruence kernel

Let $G$ be an absolutely simple simply connected algebraic group defined over a global field $K$, and let $S$ be a nonempty (but not necessarily finite) set of places of $K$ containing all archimedean ones. We let $\widehat{G}$ (resp., $\overline{G}$) denote the $S$-arithmetic (resp., $S$-congruence) completion of the group $G(K)$ of $K$-rational points, and let $C^S(G)$ be the corresponding congruence kernel, i.e. the kernel of the canonical projection $\widehat{G} \xrightarrow{\pi} \overline{G}$. I will first discuss some general results on the centrality (in $\widehat{G}$) of $C^S(G)$. For example, $C^S(G)$ is central (hence trivial) if $S$ almost contains a generalized arithmetic progression (this result is based on the analysis of strong approximation in tori with respect to such $S$); in particular, $C^S(G)$ is central if $S$ contains almost all places (i.e. the corresponding ring $\mathcal{O}(S)$ of $S$-integers is semi-local). Using the semi-local case, we prove that $C^S(G)$ is central for general $S$ if the groups $G(K_v)$ over the completions $K_v$ for $v \notin S$ considered as subgroups of $\overline{G}$ (which coincides with the group of $S$-adeles $G(\mathbb{A}(S))$) admit pairwise commuting lifts in $\widehat{G}$ under $\pi$. This criterion yields very short proofs for the classical results that $C^S(G)$ is central if $G = \mathrm{SL}_n$ with $n \geqslant 3$, or $G = \mathrm{SL}_2$ and $|S| > 1$. Another consequence is that if $G$ is $K$-isotropic and $K$ is a number field then there is $g \in C^S(G)$ such that if $N$ is the normal subgroup of $\widehat{G}$ (topologically) generated by $g$ then $C^S(G)/N$ is a quotient of the metaplectic kernel $M(G, S)$ (in particular, $C^S(G)/N$ is a quotient of the finite cyclic group $\mu(K)$ of all roots of unity in $K$, and is in fact trivial if $K$ is not totally imaginary). These results are from the forthcoming joint paper with Gopal Prasad.

## L. Ribes

### Wreath products and classical subgroup theorems for abstract and profinite groups

We provide a conceptual framework using wreath products for simple proofs of the Nielsen-Schreier and Kurosh theorems that work simultaneously for abstract and profinite groups. We also provide, using the same technique, a straightforward proof of a recent theorem of Ribes-Stevenson-Zalesskii about open subgroups of quasifree profinite groups.

This is joint work with B. Steinberg.

## D. Segal

### Which verbal subgroups are closed

I suppose it was Serre who introduced the idea that the topology on a profinite group $G$ can be recovered from its algebraic structure if there are enough algebraically defined subgroups that are guaranteed to be open. Specifically, he showed that if $G$ is a finitely generated pro-$p$ group then the verbal subgroup $[G, G]G^p$ is open; iterating this we get a neighbourhood base of 1 in $G$ and so can reconstruct the topology. Now $[G, G]G^p$ is open because it is closed, and it is closed because the word $w = [x, y]z^p$ has finite width in $G$ (every product of $w$-values is equal to such a product of bounded length). Moreover, the width of $w$ in $G$ is the supremum of the width of $w$ in all finite continuous quotients of $G$. So Serre's theorem about pro-$p$ groups follows from (in fact it's equivalent to) the statement: given $d$, there exists $f = f(w, d)$ such that $w$ has width at most $f$ in every $d$-generator finite $p$-group.

In order to generalize Serre's theorem to all finitely generated profinite groups, Nikolay Nikolov and I had to consider different words; again we ended up proving a bounded-width result, about so-called $d$-locally finite words. We also proved the analogous result for commutators (of arbitrary length). The outcome is that the verbal subgroup $w(G)$ is closed in a finitely generated profinite group $G$ if the word $w$ is either locally finite or a left-normed commutator. On the other hand, $G''$ (the second derived group) is not closed in, say, the 2-generator free profinite group.

Can we characterize the words $w$ such that $w(G)$ is closed in $G$ for every finitely generated profinite group $G$? This is equivalent to asking: which words $w$ have bounded width (depending on $d$) in all $d$-generator finite groups, for each $d$? If we restrict to pro-$p$ groups, the complete answer has been given by Andrei Jaikin; I don't know the answer in general, but will discuss partial answers that extend Jaikin's result in various directions.

A kind of orthogonal question is: which finitely generated profinite groups have the property $C$: "every verbal subgroup is closed"? Again, Jaikin has made an important contribution by showing that all $p$-adic analytic profinite groups have $C$. Laci Pyber has suggested a big generalization of Jaikin's theorem, namely that all adelic groups have $C$; I will discuss a special case where this is true (the so-called FAb groups), and indicate why I think it is not true in general.

## J-P. Serre

### Variation with $p$ of the number of solutions mod $p$ of polynomial equations

## J-P. Serre

### Independence of $l$-adic representations

It is an unpublished theorem on systems of l-adic representations; it generalizes the one I once made for elliptic curves, and later for abelian varieties.

## P. Symonds

### On the Cohomology of a pro-$p$ Group considered as an Abstract Group

We compare the discrete and the continuous cohomologies of a pro-$p$ group. In particular we ask when they are equal. We present some positive and some negative results.

## A. Shalev

### Words, Ore's conjecture and random walks

I will describe our recent proof of Ore's conjecture as well as new probabilistic results on general word maps.

## P. Shumyatsky

### On pro-$p$ groups admitting a fixed-point-free automorphism

An automorphism $\phi$ of a group $G$ is called fixed-point-free if it has no nontrivial fixed points in $G$. We study pro-$p$ groups admitting such an automorphism. One of the results that we intend to discuss is the following theorem.

THEOREM. *Let $G$ be a compact torsion group having an abelian subgroup $A$ such that $C_G(A)$ is finite. Then $G$ has finite exponent.*

## B. Steinberg

### Symbolic dynamics, projective profinite groups and free profinite monoids

Symbolic dynamics takes place in the realm of infinite words. The space of infinite words can be viewed as the boundary of a regular rooted tree, or equivalent the boundary of a certain profinite completion of the free monoid. Hence the boundary of the free profinite monoid maps onto the space of infinite words and so symbolic dynamics can be "lifted" to the free profinite monoid. Via this lifting, Almeida assigned to each minimal (or more generally irreducible) symbolic dynamical system a profinite group, which is a conjugacy invariant of the system. These groups are certain maximal subgroups of the free profinite monoid. Almeida showed that the groups associated to Sturmian systems are free profinite groups of rank 2. On the other hand, the group associated to the Thue-Morse word was shown by Almeida and Costa not to be free profinite.

Margolis asked in 1998 whether all maximal subgroups of a free profinite monoid are projective. In joint work with Rhodes, we answer this question in the affirmative: the class of projective profinite groups is exactly the class of closed subgroups of free profinite monoids. This implies that every finite order element of a free profinite monoid is an idempotent. The speaker has also proven that the maximal subgroup of the minimal ideal of a finitely generated free profinite monoid is a free profinite group of countable rank. Since the minimal ideal has the structure of a "principal bundle" over its space of idempotents with fibre the maximal subgroup, this describes to a large extent the minimal ideal. The technique is via wreath products.

## Th. Weigel

### Profinite groups acting on pro-p trees

Some times ago L. Ribes and P. Zalesskii introduced the notion of a pro-$p$ tree and studied pro-$p$ groups acting on such a profinite space. There is some analogy to Bass-Serre theory, but some phenomena are also quite different. Every finitely generated virtual pro-$p$ group $G$ with cohomological $p$-dimension 1 has an action on a locally-finite pro-$p$ tree with finite stabilizers and without inversion of edges. However, there are profinite groups of this type which must have infinitely many orbits on vertices for any such action.

## J.S. Wilson

### Exchange Theorems

If $G$ is a finitely presented (abstract or pro-$p$) group with $n$ generators and $m$ relators, where $m < n$, then *any* generating set for $G$ contains $n - m$ elements that freely generate a free subgroup of $G$. I shall discuss the proof of this result and mention recent extensions of it.

## E. Zelmanov

### Infinite Groups

We will discuss basic problems and ideas in the theory of infinite groups, such as
(i) The Burnside Problem
(ii) Groups as geometric objects
  (a) growth of a group,
  (b) expander families and group theory
(iii) Algorithmic problems and complexity.

## A. Zuk

### Automata groups

We present recent developments in the theory of groups generated by finite automata. In particular we discuss problems related to amenability and growth.