BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 38, Number 4, Pages 475–479
S 0273-0979(01)00914-4
Article electronically published on June 12, 2001

Profinite groups, by J. S. Wilson, Clarendon Press, Oxford, 1998, ix+284 pp., $115.00, ISBN 0-19-850082-3

Profinite groups, by L. Ribes and P. Zalesskii, Springer, New York, 2000, xiv+ 435 pp., $109.00, ISBN 3-540-66986-8

Analytic pro-p groups, by J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, 2nd edition, Cambridge University Press, Cambridge, UK, 1999, xviii+ 368 pp., $59.95, ISBN 0-521-65011-9

New horizons in pro-p groups, by M. du Sautoy, D. Segal, and A. Shalen (eds.), Birkhäuser, Boston, 2000, xiii+423 pp., $79.00, ISBN 0-8176-4171-8

The theory of profinite groups is flourishing! This is the first immediate observation from looking at the four books on the subject which have come out in the last two years. The subject, which only two decades ago was somewhat remote, has made its way to mainstream mathematics in several different ways.

What is a profinite group? A profinite group G is a topological group which is Hausdorff, compact and totally disconnected. A more meaningful equivalent definition is that G is the inverse limit of finite groups. As such, much of the theory of finite groups can be carried over to profinite groups.

The origin of the subject lies in Galois theory: If E is an infinite algebraic Galois extension of a field F and $G = \mathrm{Gal}(E/F)$ is the group of the automorphisms of E fixing F, then the classical Galois theory does not hold anymore. Intermediate fields between F and E give rise to subgroups of G, but the fixed point sets of different subgroups of G can give the same intermediate subfield.

Now G has a natural topology called the Krull topology obtained by declaring, for every finite subextension $F \subseteq L \subseteq E$, the subgroup $G(E/L)$ to be open in G. The classical Galois theorem now holds in the following form: There is a one to one correspondence between intermediate field extensions and *closed* subgroups of G. So infinite Galois theory leads one naturally to profinite groups. Many questions of arithmetic interest are naturally formulated in this way. For example, the inverse Galois problem asking whether every finite group is a Galois group of some (finite) Galois extension of $\mathbf{Q}$ is actually the question whether every finite group is a quotient of the profinite group $G(\bar{\mathbf{Q}}/\mathbf{Q})$ when $\bar{\mathbf{Q}}$ is the field of all algebraic numbers. Indeed, the profinite group $G(\bar{\mathbf{Q}}/\mathbf{Q})$ has been the focus of a lot of research. More generally, "Field Arithmetic" (see [FJ]) is the area which studies these infinite field extensions, their Galois theory and model theoretic aspects.

Profinite groups have come up also from a different direction. The notion of a Lie group is fundamental in many areas of mathematics: This is a topological group which is at the same time an analytic manifold, i.e., locally homeomorphic to a ball in $\mathbf{R}^n$, so that the group operations are analytic functions in the local coordinates. One can replace $\mathbf{R}$ by any locally compact field over which "analytic functions" can be defined - in particular by $\mathbf{Q}_p$, the field of p-adic numbers - to get a "p-adic Lie group". It turns out that such a p-adic Lie group always has an open

2000 *Mathematics Subject Classification.* Primary 20E18; 20J05, 12G05, 20E05, 20E06; 20G25; 11R23, 11S15, 11S20, 20D15, 20E07, 20E08, 20F05, 20F10, 20F40, 20F50, 20M35, 22E20.

pro-p subgroup, where a pro-p group is a profinite group which is the inverse limit of finite p-groups.

These are the "Analytic Pro-p Groups" which are the focus of interest of the book of Dixon, du Sautoy, Mann and Segal. Such p-adic Lie groups and some products of them, i.e. "Adelic groups", have become important objects in representation theory, algebraic groups, arithmetical number theory, etc. For example, if E is an elliptic curve defined over $\mathbf{Q}$, it has a structure of a group where ∞ serves as the zero element and $E(\mathbf{C}) \simeq S^1 \times S^1$. Hence for every n, $E[n] := \{P \in E(\mathbf{C}) \mid nP = \infty\} \simeq \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. The Galois group $G(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on $E(\bar{\mathbf{Q}})$ and hence on $E(n)$, giving a representation $\rho_n : G(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{Z}/n\mathbf{Z})$. Accumulating these representations together when $n = p^r$ and $r \to \infty$, one gets a p-adic representation $\tilde{\rho} : G(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{Z}_p)$ where $\mathbf{Z}_p$ is the ring of p-adic integers. So $\tilde{\rho}$ is nothing but a homomorphism between two profinite groups - one a Galois group and the other a p-adic Lie group. These representations have played a crucial role in Andrew Wiles' proof of the Taniyama-Shimura conjecture and therefore also in Fermat's last theorem. Some of this is described in Nigel Boston's survey article "p-adic Galois Representations and pro-p Galois Groups" in *New Horizons in Pro-p Groups*.

But maybe the new boom in profinite groups is due mainly to the discovery that they can act as a bridge between finite and infinite groups. To explain this, let Γ be a discrete group. Make Γ a topological group by declaring all finite index normal subgroups N of Γ to serve as a basis of neighborhoods of the identity of Γ. This is called the profinite topology of Γ. For example, if $\Gamma = \mathbf{Z}$ is the infinite cyclic group, then one can see that a subset A of $\mathbf{Z}$ is open in the profinite topology if for every $a \in A$ there exists $0 \neq t \in \mathbf{Z}$ such that $a + t\mathbf{Z} \subseteq A$; i.e., the arithmetic progressions serve as a basis for the open sets of $\mathbf{Z}$.

Before continuing to non-commutative groups, let us mention the amusing use of this topology, due to Furstenberg [F] (then an undergraduate), to prove that there are infinitely many primes. Indeed, every arithmetic progression is open but also closed, as its complement is a union of arithmetic progressions. Now, if there are only finitely many primes p, then $\bigcup_p p\mathbf{Z}$ is closed and hence its complement $\mathbf{Z} \setminus \bigcup_p p\mathbf{Z} = \{\pm 1\}$ is open. But the finite set $\{\pm 1\}$ is not open.

Going back to the general case of Γ, we note that usually Γ is not complete with respect to the profinite completion, but one can complete it to get $\hat{\Gamma}$, which is actually isomorphic to $\varprojlim \Gamma/N$, the inverse limit over all the finite quotients of Γ. For example, for $\Gamma = \mathbf{Z}$ one gets $\hat{\mathbf{Z}}$ which is actually isomorphic to $\prod_p \mathbf{Z}_p$ (this last statement is just a reformulation of the Chinese remainder theorem). The group $\hat{\mathbf{Z}}$ is actually a ring. Another amusing observation is that $\hat{\mathbf{Z}}^\times$, the set of invertible elements of $\hat{\mathbf{Z}}$ (invertible with respect to the multiplication), is equal to $\bar{\mathcal{P}} \setminus \mathcal{P}$, where $\mathcal{P}$ is the set of all primes in $\mathbf{Z}$ and $\bar{\mathcal{P}}$ denotes its closure in $\hat{\mathbf{Z}}$. This last observation is equivalent to the Dirichlet Theorem on the existence of infinitely many primes in arithmetic progression. (Can this lead to a new proof of the Dirichlet Theorem?)

One should note, however, that in general Γ does not inject into its profinite completion. This happens if and only if Γ is residually-finite; i.e., the intersection of its finite index subgroups is trivial. But, if Γ injects into $\hat{\Gamma}$, the latter can be a powerful tool to study Γ. On the face of it, $\hat{\Gamma}$ is a more complicated group (uncountable even if Γ is countable), but many of the techniques of finite group

theory can be applied to $\hat{\Gamma}$, and then later to Γ. Here is an example to illustrate it: A group has rank r if every finitely generated subgroup of it is generated by (at most) r elements. It has been a long-standing open problem whether every finitely generated group Γ of finite rank is virtually solvable, i.e., contains a finite index solvable subgroup. This was shown not to be the case in general by Ol'shanskii and Rips, who constructed the "Tarski monster", an infinite simple group Γ which is generated by two elements and with all its proper subgroups cyclic (in particular Γ has rank 2). In fact, this Tarski monster is a counter-example to various questions of this sort which ask whether some "finiteness assumptions" imply finiteness or solvability of the group Γ. In [LM] it was shown that the answer is yes if Γ is in addition residually finite. So a finitely generated, residually finite group of finite rank is virtually solvable. The proof runs like this: Replace Γ by $\hat{\Gamma}$; then using a theorem of Tate on finite groups and the Feit-Thompson theorem on the solvability of finite groups of odd order (both results carried by standard inverse limit arguments from finite to profinite groups), it is deduced that (after going to a finite index subgroup) all finite quotients of $\hat{\Gamma}$ are solvable. Further arguments enable one to replace $\hat{\Gamma}$ by an appropriate pro-p group G in which Γ sits as a dense subgroup. The fact that Γ is of finite rank implies that G is a pro-p group of finite rank. Now, the theory of analytic pro-p groups implies that G is a p-adic Lie group and can be embedded in $GL_n(\mathbf{Q}_p)$ for some n. This implies that Γ (being a subgroup of G and $\mathbf{Q}_p$ a subfield of $\mathbf{C}$ when one forgets the topology) is linear over $\mathbf{C}$. For such a linear group, Tits' well known alternative asserts that either Γ contains a non-abelian free group or it is virtually solvable. As Γ has finite rank, it must be virtually solvable.

Two points should be emphasized in the above description of the proof: we have used results on finite groups (and in particular a theorem on finite groups of odd order) when our group under study, Γ, is an infinite group and possibly without any element of finite order. This illustrates how profinite groups can serve as a bridge to use finite group theory (and sometimes also the classification of finite simple groups and its applications) in the world of infinite groups. Another crucial ingredient in the proof is the use of p-adic analytic pro-p groups as a machinery to "linearize" groups. Once the group is linear (i.e., a matrix group over a field) a wealth of methods from algebraic and arithmetic group theory are available.

As frequently happens, the theory of profinite groups, which has first been studied for its applications to other fields, turns out also to have a beauty all its own. The four books under review describe much of this theory and its applications in various directions.

The books of Wilson and of Ribes-Zalesskii carry out a systematic study of the general theory of profinite groups. Both start with generalities on profinite groups, for example, the definition of the order of a profinite group as a supernatural number. This definition enables one to talk about p-Sylow subgroups and Sylow theory (in spite of the fact that in general G has no elements of order p). Much of the theory of finite groups, when interpreted in the proper way, can be carried out to profinite groups. But at the same time, the category of profinite groups has free objects - the free profinite groups. This presents a new challenge: how the combinatorial group theory - for example, the part of it which describes subgroups of discrete free groups (or free products, etc.) - can be extended to the category of profinite groups where combinatorial methods are not available anymore. Indeed, some of the results hold and some do not: for example a closed subgroup H of

a free profinite group F is not necessarily free, not even if H is normal. But a surprising result says that if H is normal, then any *proper* finite index subgroup of H is free. So the area of "combinatorial" group theory of profinite groups is still far from being understood.

Both books also treat in detail the cohomology theory of profinite groups. This subject has also been treated in the two previously written monographs on profinite groups: the classical *Cohomologie Galoisienne* by J.-P. Serre from 1964 [S] and *Profinite Groups and Galois Cohomology* by L. Ribes from 1970 [R]. The old books were written with number theoretic applications in mind and contain a wealth of such applications. The current books focus on the profinite groups and their applications within group theory. An important point of novelty in the current books is that they develop the cohomological theory when the module can also be profinite and not necessarily discrete. This was an aspect well needed which has not been systematically covered in the literature so far, and the authors should be thanked for taking the effort of developing and putting in print a complete theory.

Up to now we have talked about the similarities. There are also differences which are naturally based on personal taste and the authors' background. Ribes-Zalesskii's book puts an emphasis on much of the combinatorial group theory of profinite groups; free construction such as amalgamated free product, HNN construction, automorphism groups, etc. Wilson on the other hand elaborates on the "small" profinite groups such as those of finite rank, solvable groups and finitely presented pro-p groups. The book of Ribes-Zalesskii is of more an encyclopedic nature with detailed theory, while Wilson's book is based on a graduate course the author gave and therefore is perhaps easier to digest for newcomers to the area.

The other two books under review are very different. *Analytic Pro-p Groups* by Dixon, du Sautoy, Mann and Segal is a revised and expanded version of a book with the same title which came out in 1991. That book was a landmark in the development of profinite and pro-p group theory: it presented in a self-contained and beautiful way the theory of analytic pro-p groups - the pro-p groups which have the structure of p-adic Lie groups. The theory of p-adic analytic pro-p groups was developed mainly by Lazard in his seminal paper [La] in 1965, where he showed, among other things, that they have finite rank. Only since the late 80's have these groups become popular among group theorists as it was realized that they can serve as a vehicle for "linearization" of discrete groups. The treatment of Dixon, du Sautoy, Mann and Segal overturned the historical development, starting with the study of the pro-p groups of finite rank and showing that they are exactly the analytic pro-p groups. Along the way they present the internal beauty of this class of groups, making them into an interesting object of study, independent of their applications. The current version is, as said, an expanded one, adding topics such as pro-p groups of finite class, dimension subgroups and analytic pro-p groups over other pro-p rings (such as $\mathbf{F}_p[[t]]$, the formal power series over the finite field $\mathbf{F}_p$; here the theory of Lie groups of characteristic p is needed and many problems are still open).

The last book, *New Horizons in Pro-p Groups*, gives a panoramic view of current pro-p group theory. This is a collection of 12 articles by the world's experts on the subject who describe the various directions the theory takes these days. Some of the articles are dedicated to the study of pro-p groups for their own sake, for example, their classification and their cohomology. Others deal with special subclasses, e.g., branch pro-p groups, the Nottingham group, Golod-Shafarevich groups and more.

Other papers deal with subgroup growth and the associated zeta functions. Two papers deals with the connection between the abstract theory of pro-p groups and number theory (e.g., via p-adic Galois representations mentioned above). The diversity and richness of these papers prove our claim at the beginning of this review: the theory of profinite groups is indeed flourishing in quantity and quality.

References

[FJ] M.D. Fried, M. Jarden, *Field Arithmetic,* Springer, Berlin, 1986. MR **89b:**12010

[F] H. Furstenberg, *On the infinitude of primes,* Amer. Math. Monthly **62** (1955), 353. MR **16:**904e

[La] M. Lazard, *Groupes analytiques p-adiques,* Publ. Math. I.H.E.S. **26** (1965), 389-603. MR **35:**188

[LM] A. Lubotzky, A. Mann, *Residually finite groups of finite rank,* Math. Proc. Cambridge Philos. Soc. **106** (1989), 385-388. MR **91a:**20028

[R] L. Ribes, *Profinite Groups and Galois Cohomology,* Queen's Papers Pure Appl. Math. **24** (1970), Kingston, ON, Canada. MR **41:**5495

[S] J.-P. Serre, *Cohomologie Galoisienne,* Lect. Notes Math. **5**, third ed., Springer-Verlag, Berlin, 1965. MR **34:**1328

Alexander Lubotzky

Hebrew University

E-mail address: alexlub@math.huji.ac.il