Snapshots of modern mathematics
from Oberwolfach

№ 14/2016

Profinite groups

Laurent Bartholdi

Profinite objects are mathematical constructions used to collect, in a uniform manner, facts about infinitely many finite objects. We shall review recent progress in the theory of profinite groups, due to Nikolov and Segal, and its implications for finite groups.

1 Numbers

When children learn to compute, they learn that numbers are finite sequences of digits among $\{0,\dots,9\}$, with the usual rules to compute with them. Thus '12' represents twelve, and $12/3 = 4$. Quickly, however, they run into calculations that don't have an answer in this number system: how should they describe $1/3$? The traditional answer is to extend the number system by placing a '.' and possibly infinitely many subsequent digits on the right, to express tenths, hundredths, etc.; thus they learn to write

$$\frac{1}{3} = 0.3333333333333333\dots, \qquad \sqrt{41} = 6.40312423743284868\dots.$$

A child might come up with an altogether different extension of the number system, by allowing infinitely many digits on the *left*: consider the expressions

$$\frac{1}{3} = \dots 666666666666666667, \qquad \sqrt{41} = \dots 445932736758703821. \tag{1}$$

They seem "obviously wrong", but only to us adults: multiplying and squaring the expressions without the dots one gets

$$3\cdot\frac{1}{3} = 2000000000000000001, \qquad (\sqrt{41})^2 = 1988560057131074380000000000000000041.$$

If we had carried these calculations to infinite precision, then the non-zero digits different from 1 and 41 respectively would be infinitely far away on the left – this is why they have been represented smaller – so that (in some sense to be defined below) the expressions in (1) are valid descriptions of $\frac{1}{3}$ and $\sqrt{41}$, respectively.

Both ways of representing numbers made use of infinite expressions; but we cannot perform infinite calculations in finite time. Already when we wrote $\sqrt{41} = 6.403\ldots$, we meant that there is a sequence of rational numbers $6, 6.4, 6.40, 6.403, \ldots$ that approaches $\sqrt{41}$, in the sense that the difference can be made smaller than any $\epsilon > 0$ by going far enough in the sequence; we never compute with the *infinite* expansion of $\sqrt{41}$, but merely with some approximation that is "good enough", depending on how much precision is required.

Similarly, the sequence of numbers $21, 821, 3821, 703\,821, \ldots$ has the property that their squares $441, 674\,041, 14\,600\,041, 495\,364\,000\,041, \ldots$ are congruent to 41 modulo higher and higher powers of 10. We are in effect redefining the notion of "approaching", by saying that integers that agree on a large number of rightmost digits – are congruent modulo a high power of 10 – are close.

Thus the statement that $\sqrt{41}$ exists and may be written as $\ldots 3821$ is a compact manner of stating that the congruence $X^2 \equiv 41 \pmod{10^n}$ is solvable for all integers n, with a typical solution having the rightmost n digits equal to $\ldots 3821$. Note that, in this number system, some numbers do not have a square root. For example $X^2 \equiv 3 \pmod{10}$ is not solvable, since the last decimal digit of a square will always be in $\{0, 1, 4, 5, 6, 9\}$. On the other hand, if a positive integer s ending in 1 or 9 has an approximate square root x_0 with $x_0^2 \equiv s \pmod{10^3}$ then it *does* have an exact square root in this number system, obtained by iterating what is called the *Newton–Raphson method* $x_{i+1} = \frac{1}{2}(x_i + s/x_i)$ and taking the limit.[1]

1.1 Profinite integers

There is no reason to restrict ourselves to base 10 in expressing numbers. Any other basis may be chosen, or in fact a combination of all bases together: one may write numbers as

[1] As an example, take $s = 89$, starting with $x_0 = 33$. This is a valid example since $33^2 = 1089 \equiv 89 \pmod{10^3}$. To calculate the inverses $1/x_0$ in the Newton–Raphson method, we only consider the last four rightmost digits; hence we look for a number Y, such that $Y \cdot x_0 \equiv 1 \pmod{10^4}$. In this case we can calculate $1/x_0 = 9697$, since $9697 \cdot 33 = 320001 \equiv 1 \pmod{10^4}$. Then we obtain $x_1 = \frac{1}{2}(33 + 89 \cdot 9697) = 431533 \equiv 1533 \pmod{10^4}$.

Note that only the rightmost $i + 4$ digits of the quotient s/x_i need to be computed. Calculating the next few x_k and their inverses in $\mathbb{Z}/10^{k+4}\mathbb{Z}$ we obtain the sequence $33, 1533, 26533, 26533, 1026533, 6026533, 156026533, 3656026533, 18656026533, \ldots$.

$$a = \cdots a_n \cdots a_2 a_1, \qquad \text{with } a_1 \in \{0,1\},\ a_2 \in \{0,1,2\},\ \ldots,\ a_n \in \{0,\ldots,n\},\ \ldots$$

representing the number $\cdots + a_n \cdot n! + \cdots + a_2 \cdot 2! + a_1 \cdot 1!$. Integers are as usual represented as numbers with only finitely many non-zero digits; thus for example the notation 321 represents the usual integer (in base 10)

$$3 \cdot 3! + 2 \cdot 2! + 1 \cdot 1! = 18 + 4 + 1 = 23.$$

The conditions on the digits $0 \leq a_n \leq n$ ensure that every number has only one representation. In this new system, called the *profinite integers* and written $\widehat{\mathbb{Z}}$, two numbers are close if they agree modulo $n!$ for some large n, or equivalently modulo m for every $m = 1, 2, \ldots, n$ and n large.

It turns out[2] that the only integers admitting a square root in $\widehat{\mathbb{Z}}$ are precisely the usual squares $0, 1, 4, 9, \ldots$. Thus there is a perfect agreement between computing $\sqrt{s}$ in integers and solving the congruences $X^2 \equiv s \pmod{n}$ for all n; or, in more mathematical terms, between solving $X^2 = s$ in the integers $\mathbb{Z}$ or in all finite rings $\mathbb{Z}/n\mathbb{Z}$.

Note that this does not hold for all equations: for example, the equation $3X^3 + 4Y^3 = 5$ admits a solution $\pmod{n}$ for all n, and thus in $\widehat{\mathbb{Z}}$, but not in $\mathbb{Z}$ itself, as Selmer showed in [9][3]. Selmer's article is long, and is not an easy read; a shorter and more specific treatment is in [3].

2 Completions

Let us make the discussion yet more mathematical. We have an object of interest X, say the integers $\mathbb{Z}$; and a family of quotients X_n of X, say the residue systems $\mathbb{Z}/n\mathbb{Z}$, or only the subfamily $\mathbb{Z}/10^n\mathbb{Z}$. We write $p_n \colon X \to X_n$ for the reduction map. There are also some natural maps between the various X_n, for example from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ when m divides n, or from $\mathbb{Z}/10^n\mathbb{Z}$ to $\mathbb{Z}/10^m\mathbb{Z}$ when $n \geq m$. We assume that we are given such maps $q_{n,m}$, which satisfy the condition $q_{n,m} \circ p_n = p_m$, see Figure 1.

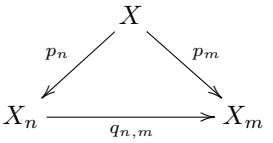

Figure 1: $q_{n,m} \circ p_n = p_m$

Out of this data, we construct a *completed object* $\widehat{X}$. It is simply defined as the set of tuples $(x_1, x_2, \ldots)$ with each $x_i \in X_i$, subject to the condition that $q_{n,m}(x_n) = x_m$ for all maps $q_{n,m}$.

[2] This is a deep result by Minkowski, known as the "Hasse principle"; see the first four chapters of [10].

[3] The inexistence of solutions in $\mathbb{Z}$ is a variant of Fermat's Last Theorem (proven by Euler in degree 3). Intuitively, the cubes are too sparse in $\mathbb{Z}$, but at least a third of the numbers are cubes $\pmod{n}$, so that $3X^3 + 4Y^3 \equiv 5 \pmod{n}$ is underdetermined.

There is a natural map $X \to \widehat{X}$, given by $x \mapsto (p_1(x), p_2(x), \ldots)$. Additionally, there is a notion of proximity in $\widehat{X}$: two tuples $(x_1, x_2, \ldots)$ and $(y_1, y_2, \ldots)$ are close if they agree in many coordinates.

If (X_n) is the family of *all* finite quotients of X, then $\widehat{X}$ is called the *profinite completion* of X. The object $\widehat{\mathbb{Z}}$ constructed in the previous section is the profinite completion of the integers $\mathbb{Z}$. The completion of $\mathbb{Z}$ with respect to the quotients $\mathbb{Z}/10^n\mathbb{Z}$ is written $\mathbb{Z}_{10}$, the *10-adics*.

Note that the object $\widehat{X}$ is constructed purely out of the objects X_n and the maps $q_{n,m}$; it may be defined independently of the object X, and even if no such object X preexists.

3 Topology

The notion of proximity given above is nicely expressed as a *topology* on $\widehat{X}$. In a topology on a set X, we are given a collection $\mathcal{O}$ of subsets of X called *open subsets*, and some axioms that $\mathcal{O}$ must satisfy:

- The empty set and X are contained in $\mathcal{O}$.
- Finite intersections of elements in $\mathcal{O}$ are again contained in $\mathcal{O}$.
- Arbitrary unions of elements in $\mathcal{O}$ are again contained in $\mathcal{O}$.

A subset $A \subset X$ is called *closed* if its complement $X \setminus A$ is open. Note that a subset $A \subset X$ can be closed or open, but can also have both or neither property.

The idea behind the terminology is that a set A is open if every element of A has a small neighborhood around it and entirely contained in A; the closer two points are, the more open sets contain both or none of these points. Closed sets get their name from being "closed under taking limits": A is closed if whenever a sequence of elements in A approaches an element $x \in X$, then x is also contained in A. Solution sets of equations are typical examples of closed sets: if a sequence of solutions has a limit, then the limit is also a solution.

Let us define directly what the closed and open sets of our profinite object $\widehat{X}$ are: for a subset $A \subseteq \widehat{X}$, we say that A is

open if, for every $a = (a_1, a_2, \ldots) \in A$, there are finitely many coordinates $i_1 < \cdots < i_k$ such that, if $b = (b_1, b_2, \ldots) \in \widehat{X}$ agrees with a on $i_1, \ldots, i_k$, then $b \in A$;

closed if, whenever $x = (x_1, x_2, \ldots) \in \widehat{X}$ is such that, for all n, *some* element of A starts with $(x_1, \ldots, x_n, *, *, \ldots)$, then $x \in A$.

For example, $\mathbb{Z}$ is neither open nor closed in $\widehat{\mathbb{Z}}$: it is impossible to know, from finitely many digits of a profinite integer, whether it is an actual integer, so $\mathbb{Z}$ is

not open, and as we saw above $x = \sqrt{41}$ admits arbitrarily good approximations $(x_1, \ldots, x_n, 0, \ldots)$ in $\mathbb{Z}$ yet $x \notin \mathbb{Z}$.

The set of odd numbers $2\mathbb{Z}_{10} + 1$ is open and closed in $\mathbb{Z}_{10}$: to determine whether a number is odd, it suffices to look at its last digit, and the same applies to the complement set of even numbers. More generally, arithmetic progressions $a\widehat{\mathbb{Z}} + b$ are closed and open in $\widehat{\mathbb{Z}}$. Finite subsets are closed but not open in $\widehat{\mathbb{Z}}$; it suffices to check this for sets containing only one element. No profinite integer is determined by finitely many of its digits, but conversely a sequence of digits determines uniquely a profinite integer.

It is easy to see that, in our definition, a set A is open if and only if its complement $\widehat{X} \setminus A$ is closed: for example consider A open and $x \in \widehat{X}$. To show that $\widehat{X} \setminus A$ is closed, it suffices to show that either $x \in \widehat{X} \setminus A$ or that there exists n such that every element of $\widehat{X} \setminus A$ differs from x in one of its first n coordinates. Assuming $x \in A$ and A open, there are finitely many coordinates $i_1 < \cdots < i_t$ such that ass $(*, \ldots, x_{i_1}, *, \ldots, *, x_{i_t}, *, \ldots)$ belong to A. One may then take $n = i_t$.

Intuitively, a set A is closed if solving an equation in A is equivalent to solving it in the image $p_n(A)$ for all n; and a set A is open if "being an element of A" can be checked by examining finitely many coordinates (though "not being an element of A" need not be certifiable).

At this point, we cannot resist giving a topological proof of the well-known fact that there are infinitely many primes, due to Fürstenberg [4]. Arithmetic progressions in $\widehat{\mathbb{Z}}$ are closed; so the union of a finite number of arithmetic progressions is closed. Consider now the set $A = \bigcup_p p\widehat{\mathbb{Z}}$, where p runs through the set of primes. The only numbers not in A are $\{-1, 1\}$, which is not open, so A is not closed. Thus A is not a finite union, and there are infinitely many primes. For more details see [2, p. 5]

Here is some more vocabulary. The *closure* of a subset A is the smallest closed set that contains A. A set A is *dense* if its closure equals $\widehat{X}$. For example, $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$, and more generally X is dense in $\widehat{X}$.

4 Groups

We now turn to groups: mathematical structures that capture symmetries of objects. They are sets endowed with a composition operation, such that left- and right-composition by an element is invertible. Rather than going into the formalism[4], here is a basic example: the group G of invertible self-maps of a rooted tree $\mathcal{T}$, displayed in Figure 2, that preserve its root vertex.

[4] For more on groups see Snapshot 5/2016 *Symmetry and characters of finite groups* by Eugenio Giannelli and Jay Taylor as well as Snapshot 7/2014 *Swallowtail on the shore* by Ragnar-Olaf Buchweitz and Eleonore Faber.

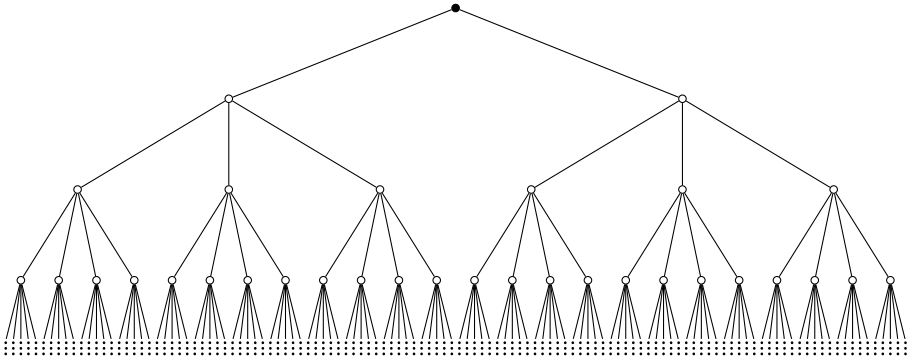

Figure 2: The infinite rooted tree $\mathcal{T}$.

We can compose two of these invertible self-maps to obtain a new invertible self-map. An invertible self-map of the tree from Figure 2 may be described as follows: the root vertex maps to itself. Consider then the two neighbors of the root; they may be fixed or exchanged. Consider next the vertices at distance 2 from the the root. They come in two blocks of 3; where the blocks map is already determined, but within each block they may be permuted arbitrarily. More generally, there are $n!$ vertices at distance $n-1$ from the root, and each of these vertices has $n+1$ direct descendants, which can be permuted arbitrarily.

The group G is naturally a *profinite group*, namely the completion $\widehat{G}$ of a family (G_n) of finite groups. Indeed, when we describe an invertible self-map of $\mathcal{T}$, we automatically describe invertible self-maps of finite subtrees, namely the subtrees obtained by truncating $\mathcal{T}$ at level n for all values of $n \in \mathbb{N}$. The finite group G_n is the group of self-maps of the finite tree consisting of the first n levels of $\mathcal{T}$, and is finite because its elements are specified by finitely many permutations.

In fact, all choices of permutations lead to valid tree self-maps, so every element of G_n is uniquely determined by one element in $\mathfrak{S}_2$, the symmetric group on 2 symbols, two elements in $\mathfrak{S}_3$ and so on until finally $n!$ elements in $\mathfrak{S}_{n+1}$. It follows that G_n has precisely $2!(3!)^{2!}\cdots((n+1)!)^{n!}$ elements.

The 2-adic integers $\mathbb{Z}_2$, namely the completion of $\mathbb{Z}$ with respect to its quotients $\mathbb{Z}/2^n\mathbb{Z}$, is another example of a group, with the operation being addition. In fact, it is related to the tree example as follows. Consider on the one hand the *binary rooted tree* from Figure 3, and its group G of self-isometries, as described in the previous paragraphs. On the other hand, consider the set of all arithmetic progressions $\{2^n\mathbb{Z} + a \,:\, 0 \leq a < 2^n\}$, and order them by

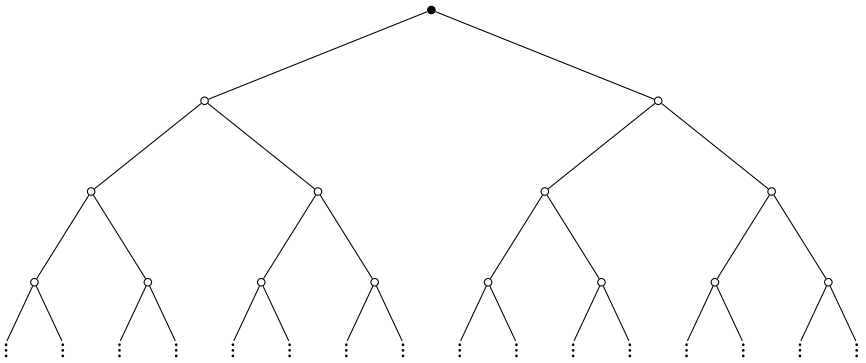

Figure 3: The binary rooted tree $\mathcal{T}_2$.

inclusion[5]. These may be assembled into a tree, by putting an edge between $2^n\mathbb{Z}+a$ and $2^{n+1}\mathbb{Z}+b$ whenever $2^n\mathbb{Z}+a \subset 2^{n+1}\mathbb{Z}+b$, see Figure 4. This tree is again the binary rooted tree! Given an element $x = \dots x_n \dots x_1 x_0$ of $\mathbb{Z}_2$, we can define an invertible self-map of this binary rooted tree by adding x to arithmetic progressions:

$$2^n\mathbb{Z}+a \mapsto 2^n\mathbb{Z}+a+\sum_{k=1}^{n-1} 2^k x_k.$$

[5] One may equivalently consider arithmetic progressions $2^n\mathbb{Z}_2+a$ and obtain the same tree.

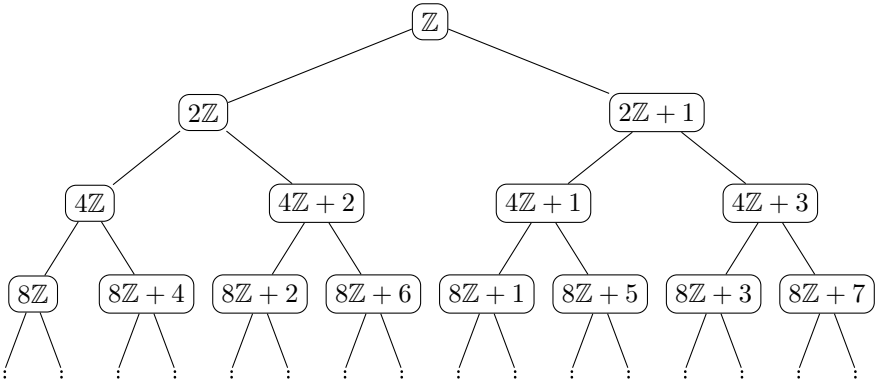

Figure 4: The binary tree of arithmetic progressions.

Since addition preserves arithmetic progressions, the tree structure is preserved by action of $\mathbb{Z}_2$.

A *subgroup* of a group is simply a subset that is preserved by the group operation. Our identification of both binary rooted trees lets us view $\mathbb{Z}_2$ as a subgroup of the full group G of binary tree invertible self-maps. (It is a *closed* subgroup; we leave this as an exercise.)

4.1 More profinite groups

For those readers familiar with the basics of group theory, we provide some more examples of profinite groups.

Our choice of the group of invertible self-maps of a rooted tree to exemplify profinite groups is in fact quite generic. Let indeed G be a profinite group, given by a collection of finite groups (G_n) and maps $q_{n,m}$; denote by $p_n \colon G \to G_n$ the projection maps. Construct the following rooted tree $\mathcal{T}_G$. The set of vertices at distance n from the root is $G_1 \times \cdots \times G_n$. The root is the empty product, and there is an edge between $(g_1, \dots, g_n)$ and $(g_1, \dots, g_n, g_{n+1})$ for all $g_i \in G_i$. The group G naturally acts on $\mathcal{T}_G$, the action of g sending $(g_1, \dots, g_n)$ to $(p_1(g)g_1, \dots, p_n(g)g_n)$. Thus all profinite groups may be seen as groups of self-maps of rooted trees.

There are numerous other examples of profinite groups. For example, the group of invertible $n \times n$ matrices with coefficients in $\widehat{\mathbb{Z}}$ is a profinite group; the corresponding finite groups are matrix groups with coefficients in $\mathbb{Z}/n\mathbb{Z}$.

Here is another important example of profinite group. Let us call *generating set* for a group G a subset $S \subset G$ such that every element of G may be written as a composition of elements of S. A group G is called *k-generated* if it admits a generating set of size k, and *finitely generated* if it admits a finite generating set.

Fix once and for all an integer k, and let (F_n) be an enumeration of all k-generated finite groups, with for each F_n a fixed generating set $S_n = \{s_{n,1}, \dots, s_{n,k}\}$ of cardinality k. Consider this family of groups, with maps $q_{n,m}$ between them whenever the identification $s_{n,i} \mapsto s_{m,i}$ extends by the rule $q_{n,m}(xy) = q_{n,m}(x)q_{n,m}(y)$ to a well-defined map $F_n \to F_m$. The resulting profinite group is called the *free profinite group on k generators* $\widehat{F}$. Note that, for all $i = 1, \dots, k$, the sequence $(s_{n,i})_{n \geq 1}$ defines an element $\widehat{s}_i$ of $\widehat{F}$; and that the subgroup of $\widehat{F}$ generated by $\{\widehat{s}_1, \dots, \widehat{s}_k\}$ is dense. Every statement about $\widehat{F}$ amounts to a uniform statement about all finite k-generated groups.

If $k = 1$, the enumeration (F_n) can be taken as $(\mathbb{Z}/n\mathbb{Z})$. It follows, in this case, that $\widehat{F}$ is isomorphic to $\widehat{\mathbb{Z}}$.

5 Verbal subgroups

We will need one last notion from group theory. Consider a group G and a subgroup H. For $t \in G$, we denote by Ht the set of products $\{ht : h \in H\}$, and call it a *coset* of H. It is easy to see that two cosets are either equal or disjoint. The *index* of H is defined as the number of distinct cosets of H, and H is called a *finite-index subgroup* if it has finitely many cosets.

The following question has remained open for more than 30 years, before being finally settled. Let G be a finitely generated profinite group, and let H be a subgroup of G. If H is open in G, then it has finite index in G.[6] Does the converse hold?

We report in this section on the positive solution to this long-standing problem, and on byproducts of its solution. For references, see the excellent texts [5, 6, 7].

Consider a word $w(X_1, \ldots, X_n)$ in unknowns $X_1, \ldots, X_n$ and their inverses[7] Given a group G, we denote by $w\{G, \ldots, G\}$ the set of values obtained by substituting elements of G for the unknowns, and we denote by $w(G)$ the subgroup of G generated by $w\{G, \ldots, G\}$:

$$w\{G, \ldots, G\} = \{w(g_1, \ldots, g_n) \,:\, g_i \in G\}, \qquad w(G) = \langle w\{G, \ldots, G\} \rangle.$$

For example, take $w = X_1 X_2 X_1^{-1} X_2^{-1}$. In a group G with $ab = ba$ for all elements $a, b \in G$, we have $w(a, b) = aba^{-1}b^{-1} = baa^{-1}b^{-1} = bb^{-1} = 1$ and therefore $w(G) = \{1\}$, the trivial group consisting only of the unit element.

A word w is called *locally finite* if, whenever H is a finitely generated group satisfying $w(H) = 1$, the group H must be finite. In progressive order of difficulty, it can be shown that $w = X_1^2$, X_1^3, X_1^4 and X_1^6 are locally finite words, but that X_1^{665} is not [1]; see [8] for a more modern treatment. This answers partly the "Burnside problem" from 1902, which asks to determine the exponents $k \in \mathbb{N}$ such that every finitely generated group in which $g^k = 1$ holds for all elements g is finite.

---

[6] Indeed, let $p_n \colon G \to G_n$ be the given maps from G to finite quotients. If H is open then there exist $i_1 < \cdots < i_t$ such that $p_n(H) = G_n$ for all $n \notin \{i_1, \ldots, i_t\}$, and therefore the index of H is at most $|G_{i_1}| \cdots |G_{i_t}|$.

[7] A *word* is defined to be a finite sequence of letters from an alphabet, in this case the set $\{X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}\}$. Examples are $X_1 X_7^{-1} X_3^{-1} X_3 X_5^{-1}$, $X_4^{-1} X_2 X_2$ and $X_1 X_1 X_1 X_1$. Here and in similar cases we abbreviate $X_1 X_1 X_1 X_1$ to X_1^4 and consider $X_1 X_7^{-1} X_3^{-1} X_3 X_5^{-1}$ and $X_1 X_7^{-1} X_5^{-1}$ to be the same.

In the following statements, the group G is a finitely generated profinite group and $w = w(X_1, \ldots, X_n)$ is a word in unknowns $X_1, \ldots, X_n$.

Theorem 1 *If w is locally finite, then $w(G)$ is open in G.*

Every closed, finite-index subgroup is open (since its complement is the union of finitely many (also closed) cosets), so Theorem 1 follows from the following, more quantitative result:

Theorem 2 *If w is locally finite and $k \geq 1$, then there exists a constant f depending only on k and w such that, whenever G is a k-generated group, every element of $w(G)$ is the product of at most f elements of $w\{G, \ldots, G\}$.*

If w is the "commutator word" $X_1X_2X_1^{-1}X_2^{-1}$, the same conclusion holds. In fact, more generally, for every k-generated group G and every subgroup $H \subseteq G$ such that $gHg^{-1} = H$ for all $g \in G$, the following holds: Every product of elements of $w\{H, G\}$ may be rewritten as a product of length at most f.

In particular, the subgroup generated by $w\{H, G\}$ is closed as soon as H is closed.

The statements really are uniform statements about finite groups: for example, if W is a locally finite word, the assertion is that, in *every* finite group Q, every element of $w(Q)$ is a product of at most f values of w.
These considerations enable Nikolay Nikolov and Dan Segal to prove the following statement:

Theorem 3 *Let G be a finitely generated profinite group, and let H be a finite-index subgroup of G. Then H is open in G.*

As a consequence, the topology on G (see Section 3) is uniquely determined by the algebraic structure of G.

It would be presumptuous to give any sketch of a proof of these statements. One element of the proof brings us back to the first section of this snapshot, namely an adaptation of the Newton–Raphson method, enabling the authors to lift approximate solutions $w(X_1, \ldots, X_n) \in K$ for a small subgroup K to exact solutions $w(X'_1, \ldots, X'_n) = 1$ of equations in groups.

These theorems seem, on the surface, to be quite abstract results about profinite groups. They are, actually, very concrete *uniform* statements about finite groups; indeed every statement about a profinite group G translates to an infinite family of statements about G's finite quotients. Considering for G a free profinite group amounts to considering a statement valid in *all* finite groups with specified number of generators.

Here is a concrete consequence of the theorems, stated for the word X^6 which is known to be locally finite. Consider a finite group G, and in G the subgroup H which is generated by sixth powers of elements in G, namely $H = \{g_1^6 g_2^6 \cdots g_f^6 \ : \ f \geq 1, g_1, \ldots, g_f \in G\}$. The number f of factors can be

bounded, at worst by the cardinality of G. What Nikolay Nikolov and Dan Segal prove is that f can be bounded by a function depending only on the number of generators of G.

To make this even more concrete, consider the family of finite symmetric groups: the family of groups $\mathfrak{S}_n$ of all permutations of $\{1, \dots, n\}$. The group $\mathfrak{S}_n$ is well-known to be 2-generated, for example by the transposition $(1, 2)$ and the long cycle $(1, 2, \dots, n)$. Theorem 2 implies that every product of sixth powers in $\mathfrak{S}_n$ can be rewritten as product of a bounded number (say 1000, but crucially independent of n) of sixth powers. Can you prove it directly?

References

[1] Sergei I. Adyan, Проблема Бернсайда и тождества в группах. *[The Burnside problem and identities in groups.]*, Nauka, Moscow, 1975.

[2] Martin Aigner and Günter M. Ziegler, *Proofs from THE BOOK*, 4th ed., Springer, 2009.

[3] Keith Conrad, *Selmer's example*, 2013, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/selmerexample.pdf, visited on September 15, 2016.

[4] Harry Fürstenberg, *On the infinitude of primes*, The American Mathematical Monthly **62** (1955), 353.

[5] Nikolay Nikolov and Dan Segal, *Finite index subgroups in profinite groups*, Comptes Rendus Mathématique. Académie des Sciences. Paris **337** (2003), no. 5, 303–308.

[6] ———, *On finitely generated profinite groups. I. Strong completeness and uniform bounds*, Annals of Mathematics. Second Series **165** (2007), no. 1, 171–238.

[7] ———, *On finitely generated profinite groups. II. Products in quasisimple groups*, Annals of Mathematics. Second Series **165** (2007), no. 1, 239–273.

[8] Mark V. Sapir, *Combinatorial algebra: syntax and semantics*, Springer Monographs in Mathematics, Springer, 2014, With contributions by Victor S. Guba and Mikhail V. Volkov.

[9] Ernst S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Mathematica **85** (1951), 203–362.

[10] Jean-Pierre Serre, *A course in arithmetic*, Springer, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

Laurent Bartholdi *is professor for pure mathematics at the Georg-August University, Göttingen.*

Mathematical subjects
Algebra and Number Theory, Geometry and Topology

DOI
10.14760/SNAP-2016-014-EN

Snapshots of modern mathematics from Oberwolfach are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the general public worldwide. It started as part of the project "Oberwolfach meets IMAGINARY" in 2013 with a grant by the Klaus Tschira Foundation. The project has also been supported by the Oberwolfach Foundation and the MFO. All snapshots can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

Junior Editors
Moritz Firsching and Johannes Niediek
junior-editors@mfo.de

Senior Editor
Carla Cederbaum
senior-editor@mfo.de

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9–11
77709 Oberwolfach
Germany

Director
Gerhard Huisken