

groups, rings, logic

Dan Segal

June 2021

- *Vague question*: how much can we say about a group in first-order language?
- *For example*: which groups are completely determined by their first-order properties? Which groups are determined by a *single* first-order sentence?
- A group G is **FA** (finitely axiomatizable) in a class \mathcal{C} if there is a sentence σ such that G is the unique member of \mathcal{C} that satisfies σ .
- Andre Nies called a group G *QFA* if G is FA in the class of f. g. groups. He produced several examples; Oger and Sabbagh characterized the f.g. nilpotent groups that are QFA.

profinite groups

X a definable (e.g. finite) subset of a group G . Usually the subgroup $\langle X \rangle$ is not definable, let alone the closed subgroup $\overline{\langle X \rangle}$ if G is profinite.

For each n , the set

$$X^{*n} = X \cdot X \cdot \dots \cdot X \quad (n \text{ factors})$$

is definable.

If G is profinite and X is finite, then

$$\langle X \rangle = \overline{\langle X \rangle} \iff \langle X \rangle = X^{*n} \quad (\text{some } n)$$

i.e. $\langle X \rangle$ has *finite width* w.r.t. X .

Theorem

(Nikolov-Segal) Let G be a f.g. profinite group. Then for each m the subgroup G^m is closed, hence definable.

It follows that the finite quotients of G are first-order describable.

Theorem

(Lubotzky-Jarden) A f.g. profinite group is determined up to isomorphism (in the class of all profinite groups) by its first-order theory. (i.e. it is 'first-order rigid'.)

Are such group *finitely* axiomatizable? USUALLY NOT.

Theorem

(Oger-Sabbagh, Śmielew) Let G be a group such that $Z(G)G' / G'$ is not periodic. If ϕ is a sentence such that $G \models \phi$, then $G \times C_p \models \phi$ for almost all primes p .

Thus $\widehat{\mathbb{Z}}$ is not FA.

Similarly it follows that 'being generated by d elements' is not a first-order property (in profinite groups or in abstract groups).

But if G is a pro- p group, then

$$d(G) \leq d \iff |G/G^d| \leq p^d,$$

a first-order property.

If $d(H) \leq r$ for every closed subgroup H of G one says $\text{rk}(G) \leq r$.

Lemma

For each positive integer r , there is a sentence ρ_r such that for a pro- p group G ,

$$\text{rk}(G) \leq r \implies G \models \rho_r \implies \text{rk}(G) \leq r(2 + \log_2(r)).$$

A pro- p group of finite rank is *p -adic analytic*.

In a recent arXiv paper with Andre Nies and Katrin Tent we establish:

Theorem

A p -adic analytic pro- p group G is FA in the class of all pro- p groups, assuming either

- a G has a finite pro- p presentation using (finite) group words, or*
- b we allow symbols for p -adic powers in the first-order language.*

Theorem

*A f. g. nilpotent pro- p group G is FA in the class of all profinite groups if and only if $Z(G)G' / G'$ is finite, assuming either **a** or **b** as above.*

The extra assumptions are necessary, because there are uncountably many of these pro- p groups, but countably many sentences in the (ordinary) language of groups.

Similar results are proved for direct products of pro- p groups with finitely many different primes p .

They are definitely *false* if infinitely many primes occur, because of a general model-theoretic result known as the Feferman-Vaught Theorem, that characterizes first-order properties of products.

Combining these results, we can prove for example that groups like $SL_d(\mathbb{Z}_p)$ are FA in the class of all profinite groups.

As before, this is false for groups like $SL_d(\mathbb{Z}_\pi)$, where $\mathbb{Z}_\pi = \prod_{p \in \pi} \mathbb{Z}_p$ and π is an infinite set of primes.

This approach is basically group theory, using the fact that p -adic analytic groups have a finite dimension in a suitable sense.

A different approach: express *group-theoretic* properties of $SL_d(\mathbb{Z}_p)$ as *ring-theoretic* properties of \mathbb{Z}_p ;

then axiomatizability of the group can be deduced from axiomatizability - in ring language - of the ring, which may be easier to establish (for \mathbb{Z}_p it is).

The machinery for doing this is called **bi-interpretation**.

Definition

A group Γ is *bi-interpretable* with a ring R if

- 1 Γ is interpretable in R , i.e. a copy of Γ sits definably in some R^n (in ring language)
- 2 R is interpretable in Γ , i.e. a copy of R sits definably in some Γ^m (in group language)
- 3 The resulting map from Γ into Γ^{mn} is definable (in group language).

(Also a condition 3_{bis} swapping Γ and R ; in practice (for us) this drops out with no effort.)

In this situation, first-order properties of the group Γ correspond to first-order properties of the ring R . In particular, if R is FA in a certain class of rings, then Γ is FA in a corresponding class of groups.

To illustrate the definition, consider $\Gamma = \mathrm{SL}_d(R)$.

For **1.**, Γ is identified with $d \times d$ matrices with determinant 1 over R (so $n = d^2$), and the group operation is defined by matrix multiplication.

For **2.**, R is identified with a root subgroup $U_{12} = 1 + Re_{12} < \Gamma$ (so $m = 1$).

Addition in R is given by group multiplication in U_{12} ; defining ring multiplication is more complicated, using the commutator map $U_{12} \times U_{23} \rightarrow U_{13}$ and identifying these three subgroups via conjugation in Γ .

The subtlest part is **3.** For this, one has to show for each pair (i, j) that for $g \in \Gamma$, the element of U_{12} that represents the matrix entry g_{ij} can be defined *group-theoretically* inside Γ .

Chevalley groups

The rest is joint work with Katrin Tent.

Theorem

Let G be an adjoint simple Chevalley-Demazure group scheme of rank at least 2, and let R be a commutative integral domain. Then $G(R)$ is bi-interpretable with R (almost always).

For an integral domain R we can think of $G(R)$ simply as $G(k) \cap \mathrm{SL}_d(R)$, where k is the field of fractions of R and $G(k) \leq \mathrm{SL}_d(k)$ is a usual Chevalley group. However, the scheme approach is really helpful for the proof.

"Almost always" means we can't quite prove it when G is one of the exceptional groups (apart from G_2) and R has no nontrivial units. In particular if $\mathrm{char}(R) \neq 2$ the result holds without exception.

Sketch of the proof

The first step is

Theorem

Let G be as above, and let U_α be a root subgroup. Then (usually) for $1 \neq u \in U_\alpha(R)$ we have

$$U_\alpha(R) = Z(C_{G(R)}(u)).$$

(The result is slightly different if G is symplectic and $|R^*| \leq 2$, contradicting 'folklore'!)

This shows that $U_\alpha(R)$ is a definable subgroup of $G(R)$, and can be used to interpret R inside $G(R)$.

The Chevalley commutator relations can then be used to define the ring multiplication.

As before, we can define $G(R)$ as a group of matrices.

The interesting challenge is point **3**.

Elementary width

We have identified R with (a chosen root subgroup) $U := U_\alpha(R)$ via

$$r \longmapsto r' = x_\alpha(r).$$

This gives a map

$$\begin{aligned} \theta : G(R) &\rightarrow \mathrm{SL}_d(R) \rightarrow \mathrm{M}_d(U) \\ (g\theta)_{ij} &= (g'_{ij}). \end{aligned}$$

We need to show that each component of θ is definable in group language.

For each root β the matrix entries of $x_\beta(r)$ are given by certain \mathbb{Z} -polynomials in r .

Also, *either* $x_\beta(r)$ is conjugate to $x_\alpha(r)$, *or* can be obtained from $x_\alpha(r)$ using both conjugation and commutation with a suitable other root element.

This means that we can define θ group-theoretically on each 'elementary root element' $x_\beta(r)$.

For a natural number N let

$$E^N(R)$$

denote the set of all products of N elementary root elements. The restriction of θ to $E^N(R)$ is definable.

In many cases, we have $G(R) = E^N(R)$ for some N ; one says ' $G(R)$ has finite elementary width'.

So far we have established

Theorem

If $G(R)$ has finite elementary width then $G(R)$ is bi-interpretable with R .

Examples:

- R is a field
- R is a local ring (G simply connected) (E. Abe)
- R is a ring of S -integers in a number field (G simply connected). (O. Tavgen)

The generic element

Assume now that G is *adjoint*. In that case,

$$\bigcap_{\beta \in \Phi} C_G(x_\beta(1)) = Z(G) = 1$$

where Φ is the set of roots.

Since θ is a group isomorphism from $G(R)$ to its image, to determine $g\theta$ it suffices to define θ on each element of the form

$$x_\beta(1)^g.$$

Here is a great observation due to A. Stepanov:

Lemma

There exists N (depending only on Φ) such that

$$x_\beta(1)^g \in E^N(R) \text{ for all } g \in G(R) \text{ and each } \beta \in \Phi.$$

Thus when G is an adjoint group we can argue as before that θ is definable on $G(R)$. The main theorem follows.

Sketch proof of the lemma:

The group scheme G is defined by

$$G(R) = \text{Hom}(A, R)$$

for each ring R , where $A = \mathbb{Z}[G]$ is the co-ordinate ring of G .

The **generic element** of G is

$$\gamma = \text{Id}_A \in G(A) = \text{Hom}(A, A).$$

Of course, G is a functor.

In particular each $g \in G(R) = \text{Hom}(A, R)$ induces a homomorphism $\widehat{g} : G(A) \rightarrow G(R)$, and

$$\widehat{g}(\gamma) = g.$$

For any ring S , the 'elementary group' $E(S)$ generated by all root elements $x_\beta(s)$ is a *normal* subgroup of $G(S)$ (a theorem of G. Taddei). In particular, for each root β

$$x_\beta(1)^\gamma \in E(A).$$

Say

$$x_\beta(1)^\gamma = \prod_{j=1}^N x_{\beta_j}(s_j)$$

Apply \widehat{g} to this equation to get

$$x_\beta(1_R)^g = \prod_{j=1}^N x_{\beta_j}(s_j g) \in E^N(R).$$

qed

Axiomatizability, again

Some examples of finitely axiomatizable rings:

- *Each finitely generated ring* is FA in the class of all f.g. rings (Aschenbrenner, Khélif, Naziazeno and Scanlon)
- *A regular, unramified complete local ring with finite residue field* is FA in the class of all profinite rings (Nies, Tent and Segal) (these are the rings $\mathbb{F}_q[[T]]$, $\mathfrak{o}_q[[T]]$, $T = \{t_1, \dots, t_n\}$, \mathfrak{o}_q a finite unramified extn. of \mathbb{Z}_p)
- *A locally compact field* is FA in the class of all locally compact rings (Aschenbrenner)

Theorem

Let $\Gamma = G(R)$, G as above, R an integral domain.

- If Γ is finitely generated then Γ is FA among f.g. groups.
- If R is one of $\mathbb{F}_q[[T]]$, $\mathfrak{o}_q[[T]]$ then Γ is FA among profinite groups.
- If R is a local field then Γ is FA among locally compact groups.

refs

A. Nies, D. Segal and K. Tent: Finite axiomatizability for profinite groups, arXiv:1907.02262
(to appear in *PLMS*)

D. Segal and K. Tent: Defining R and $G(R)$, arXiv:2004.13407
(to appear in *JEMS*)

- **1.** The bi-interpretability of $G(R)$ with R may hold more generally for commutative rings R that are not integral domains; provided the root subgroups are definable, the rest of the argument is OK.

In particular R can be a direct product of domains, or an adèle ring.

Back to profinite groups.

- **2.** *Isomorphisms* are supposed to be *continuous*. This is not first-order expressible, but where needed is established directly. We prove for example that the affine group

$$\Gamma = \mathbb{F}_p[[t]] \rtimes \mathbb{F}_p[[t]]^*$$

is FA among profinite groups. This *implies* that any profinite group abstractly isomorphic to Γ is topologically isomorphic. But note that Γ is *not* ‘strongly complete’ (because it has an open pro- p subgroup that is not f.g.)

Open problems.

3. Characterize the **soluble** pro- p groups of finite rank that are FA among profinite groups.

A soluble pro- p group of finite rank is poly-procyclic; for abstract group we have

Theorem

(C. Lasserre) A virtually polycyclic group G is FA among f.g. groups iff $Z(H)H'/H'$ is finite for every $H \leq_f G$.

Perhaps one could prove the analogous result for pro- p groups.

4. We have no results about pro- p groups of infinite rank.

Question. Is a f.g. free pro- p group FA among pro- p groups?