OPEN PROBLEM SESSION: ARITHMETIC ASPECTS OF ALGEBRAIC GROUPS BANFF INTERNATIONAL RESEARCH STATION

NOTES BY ASHER AUEL
JUNE 2022

Problem 1 (Andrei Rapinchuk). *Groups with bounded generation.*

An abstract group Γ has *bounded generation* (*BG*) if there exist $\gamma_1, \ldots, \gamma_d \in \Gamma$ with $\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_d \rangle$. This means that $\Gamma = \{\, \gamma_1^{n_1} \gamma_2^{n_2} \cdots \gamma_d^{n_d} \mid n_1, n_2, \ldots, n_d \in \mathbb{Z} \,\}$.

What are some examples? Finitely generated nilpotent groups. What else? Carter and Keller showed that $\Gamma = \mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$ has BG. This fact can be rephrased in the terminology of elementary linear algebra. It is a basic fact that every invertible matrix can be reduced to the identity matrix by elementary row operations. This is over a field, but the same is true for matrices with integer entries. (Furthermore, for a matrix with determinant 1, the only necessary row operation is adding a multiple of one row to another row, so we see that the original matrix is a product the elementary matrices, which are unipotent.) What Carter and Keller proved is that every matrix in $\mathrm{SL}_n(\mathbb{Z})$ (with $n \geq 3$) can be reduced to the identity in a bounded number of steps.

For $\mathrm{SL}(n, \mathbb{Z})$, the $\gamma_1, \ldots, \gamma_d$ are elementary matrices, so are unipotent. For a long time, it was an open question whether such $\gamma_1, \ldots, \gamma_d \in \mathrm{SL}_n(\mathbb{Z})$ can be chosen to be semi-simple elements, but it was recently proved that this is impossible. More generally, the expectation is that if a group has no unipotent elements, then it usually should not have BG. As an example of this, it was recently shown that if Γ is boundedly generated by semisimple elements, then Γ is virtually solvable, i.e., has a solvable subgroup of finite index. Therefore, if $\Gamma \subset \mathrm{GL}_n(\mathbb{C})$ is an anisotropic group, i.e., if every element is semisimple, then Γ has BG if and only if Γ is finitely generated and virtually abelian, i.e., has an abelian subgroup of finite index.

A profinite group Δ has *bounded generation* (*BG*) if there exist elements $\gamma_1, \ldots, \gamma_d \in \Delta$ such that $\Delta = \overline{\langle \gamma_1 \rangle} \cdots \overline{\langle \gamma_d \rangle}$ where the overline means the topological closure.

There exist many S-arithmetic groups $\Gamma = G(\mathbb{Z})$ with the *congruence subgroup property* (*CSP*), which (roughly speaking) means that $\widehat{\Gamma} = \prod_p G(\mathbb{Z}_p)$, where the hat $\widehat{\ }$ means the profinite completion, and the product is over all primes. It is known that this implies that $\widehat{\Gamma}$ has BG as a profinite group. (On the other hand, if the original group Γ is anisotropic, then we know from above that Γ does not have BG.)

Question. Can one find $\gamma_1, \ldots, \gamma_d \in \Gamma$ such that $\widehat{\Gamma} = \overline{\langle \gamma_1 \rangle} \cdots \overline{\langle \gamma_d \rangle}$.

Date: June 17, 2022.

The latex file was edited by Dave Witte Morris, so he takes responsibility for any errors.

We know that there exist such $\gamma_1, \ldots, \gamma_d$ in $\widehat{\Gamma}$ (because $\widehat{\Gamma}$ has BG as a profinite group), but the question is whether these elements can be chosen to be in the original group Γ, instead of in the profinite completion.

The easiest case might be to take an integral quadratic form q. If q is indefinite over $\mathbb{R}$, then $\mathrm{SO}(q)(\mathbb{Z})$ often has the CSP. (If q is anisotropic over $\mathbb{R}$, consider $\mathrm{SO}(q)(\mathbb{Z}[\frac{1}{p}])$ instead.) This would be a good test case.

Reference. Pietro Corvaja, Andrei S. Rapinchuk, Jinbo Ren, and Umberto M. Zannier, Non-virtually abelian anisotropic linear groups are not boundedly generated, *Invent. Math.* 227 (2022) 1–26.

Problem 2 (Peter Abramenko). *Generation by elementary matrices.*

Let R be an integral domain. Let

$$E_2(R) = \left\langle \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} \;\middle|\; a, b \in R \right\} \right\rangle \subset \mathrm{SL}_2(R)$$

be the subgroup generated by elementary matrices.

Question. Is $E_2(R) = \mathrm{SL}_2(R)$?

There is a positive answer when R is a Euclidean domain and a negative answer for $R = \mathbb{Z}[t]$. One remaining open case seems to be $R = \mathbb{Z}[t, t^{-1}]$. (This has been an open problem for a long time.)

In a similar spirit, the question has a negative answer for $R = \mathbb{F}_q[t_1, t_1^{-1}, t_2]$ but is still open for $R = \mathbb{F}_q[t_1, t_1^{-1}, t_2, t_2^{-1}]$.

Reference for $\mathbb{F}_q[t_1, t_1^{-1}]$. Boris Kunyavskii, Eugene Plotkin, and Nikolai Vavilov, Bounded generation and commutator width of Chevalley groups: function case, preprint, https://arxiv.org/abs/2204.10951

Problem 3 (Eugene Plotkin and Boris Kunyavskii). *Matrix word maps.*

Let $w(x, y) \in F_2$ be a nontrivial word in the free group on x, y. Let $G = \mathrm{PSL}_2(\mathbb{C})$. Then w defines a map $w : G \times G \to G : (g_1, g_2) \mapsto w(g_1, g_2)$.

Question. Is w always surjective? In other words, for any $a \in \mathrm{PSL}_2(\mathbb{C})$, does the equation $w(x, y) = a$ always have a solution?

The answer is believed to be "yes". This has been checked by computer for "short words" and it's also true if w is a commutator or belongs to the second commutant subgroup in the derived series. However, nobody knows what happens if the word lies deeper in the derived series.

On the other hand, the answer is "no" for $G = \mathrm{SL}_2(\mathbb{C})$. (A counterexample can be obtained by taking $w(x) = x^n$, where n is even. In general, if G is a connected, semisimple algebraic group over $\mathbb{C}$, then the power map $x \mapsto x^n$ cannot be surjective on $G(\mathbb{C})$ unless n is relatively prime to the order of the center of G.)

One might want to generalize to any adjoint algebraic group G, but there are counterexamples in general, which requires a slight modification of the question. The only group which might possess exactly the same property is $\mathrm{PSL}(n, \mathbb{C})$.

Reference. Nikolai Gordeev, Boris Kunyavskiĭ, and Eugene Plotkin, Word maps on perfect algebraic groups. *Internat. J. Algebra Comput.* 28 (2018) 1487–1515.

Problem 4 (Uriya First). *Extensions of torsors.*

Let F be a field, e.g., $F = \mathbb{C}$. Let G, H_1, H_2 algebraic groups over F and consider morphisms $H_1 \to G$ and $H_2 \to G$.

Question. Is there a G-torsor $T \to X$ over an F-variety X that is extended from H_1 but not from H_2?

As an example, for $\mathrm{SO}_n \to \mathrm{GL}_n$ and $\mathrm{Sp}_n \to \mathrm{GL}_n$, the question is equivalent to the existence of a locally free module E on X such that E has a regular quadratic form but not a regular symplectic form.

Of course, if there is a morphism $H_1 \to H_2$ compatible with the morphisms to G, then every G-torsor extended from H_1 is also extended from H_2. The general expectation is that, if there is no such morphism, then the question has a positive answer for some F-variety X.

If one bounds the complexity of the possible X, then this becomes harder. For example, for $PGL_p \to \mathrm{PGL}_p$ the identity map and $\mathbb{Z}/p\mathbb{Z} \rtimes \mu_p \to \mathrm{PGL}_p$ and taking $X = \mathrm{Spec}(F)$, then this question is equivalent to whether there exists a noncyclic p-algebra. Similarly, for $G \to G$ the identity map and $\{1\} \to G$ the inclusion of the trivial subgroup, the question has a positive answer over $X = \mathrm{Spec}(F)$ if and only if G is not a special group.

At the extreme case, the question should be easiest to answer if one takes "$X = BG$."

Reference for some special cases. Asher Auel, Uriya A. First, and Ben Williams, Azumaya algebras without involution, *J. Eur. Math. Soc.* 21 (2019) 897–921.

Problem 5 (Chen Meiri). *Local-global property for commutators.*

Let $\mathcal{O}$ be a ring of S-integers with infinitely many units and consider $\mathrm{SL}_2(\mathcal{O})$.

Question. If $g \in \mathrm{SL}_2(\mathcal{O})$ is locally a commutator, then is g a commutator?

Here, "locally" means in the profinite completion. For carefully chosen p, there are counterexamples when $\mathcal{O} = \mathbb{Z}[\frac{1}{p}]$. Are there any counterexamples when $\mathcal{O} \subset \mathbb{Q}(\sqrt{p})$ is the ring of integers?

Since $\mathcal{O}$ has infinitely many units, we know that $\mathrm{SL}_2(\mathcal{O})$ has the congruence subgroup property, so "locally" is equivalent to checking modulo all congruence subgroups.

One can ask the same question for $\mathrm{SL}_2(\mathbb{Z})$, or the free subgroup $F_2 \subset \mathrm{SL}_2(\mathbb{Z})$. Khalif proved that the answer is "yes" for the free group though here the congruence subgroup property does not hold), and the same methods apply to $\mathrm{SL}_2(\mathbb{Z})$. However, for a general free product of finite cyclic groups $C_n * C_m$, the question is open.

Reference. Amit Ghosh, Chen Meiri, and Peter Sarnak, Commutators in SL_2 and Markoff surfaces I, preprint, https://arxiv.org/abs/2110.11030

Problem 6 (Dave Morris). *Normal subsemigroups.*

Let G be a simple algebraic group over a field K of characteristic 0. A subset $N \subset G(K)$ is a normal subgroup if and only if N is nonempty, closed under multiplication, closed under inverses, and closed under conjugation. We have general classification results for all normal subgroups.

Question. Classify the normal subsemigroups (so not assumed to be closed under inverses).

In fact, this classification should reduce to the classical one.

Conjecture. Every normal subsemigroup is a subgroup.

Maybe one expects the conjecture to also hold for arithmetic groups such as $\mathrm{SL}_n(\mathbb{Z})$?

The question can be rephrased in different ways, because the following are equivalent:

- every normal subsemigroup is a subgroup,
- for every $x \in G(K)$ there exist $y_1, \ldots, y_n$ such that $x^{-1} = x^{y_1} \cdots x^{y_n}$ (where $x^y = y^{-1}xy$ is the conjugate of x by y),
- for every $x \in G(K)$, there exist $y_1, \ldots, y_n$ such that $1 = x^{y_1} \cdots x^{y_n}$,
- there does not exist a nontrivial bi-invariant partial order on $G(K)$, i.e., $x < y \Rightarrow gx < gy$ and $xg < yg$ for all $g \in G(K)$ (and "nontrivial" means there exist some x and y such that $x < y$).

The conjecture was verified when K is algebraically closed or a local field, and when G is a split classical group. But it is open for $K = \mathbb{Q}$.

Reference. Dave Witte, Products of similar matrices, *Proc. Amer. Math. Soc.* 126 (1998) 1005–1015.

Problem 7 (Andrei Rapinchuk). *How to classify algebraic groups?*

Let K be an arbitrary field and L/K a fixed quadratic extension. Can one classify all simple groups over K that are split over L?

Specifically, say that G is L/K-*admissible* if G has a maximal K-torus T that is anisotropic over K but splits over L. (For example, for $\mathbb{C}/\mathbb{R}$, then T is compact.) Can we classify these groups?

It would be especcially interesting to do E_6, E_7, E_8.

Something is special about $\mathbb{C}/\mathbb{R}$, which is that there is a unique nonsplit central simple algebra, which makes the classification nice.

This notion of L/K-admissible groups was introduced by Boris Weisfeiler, and there is a theory of the admissible tori in G, including elementary moves that allow one to move from one admissible torus to another.

References.

Mikhail Borovoi and Dmitry A. Timashev, Galois cohomology of real semisimple groups via Kac labelings, preprint, https://arxiv.org/abs/2008.11763

Mikhail Borovoi and Dmitry A. Timashev, Galois cohomology and component group of a real reductive group, preprint, https://arxiv.org/abs/2110.13062

B. Weisfeiler (or Veĭsfeĭler), Semisimple algebraic groups which are split over a quadratic extension, *Math. USSR Izvestiya*, 5 (1971) 57–72. https://doi.org/10.1070/IM1971v005n01ABEH001007

B. Weisfeiler, Monomorphisms between subgroups of groups of type G_2, *J. Algebra* 68 (1981) 306–334.