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 $\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_d \rangle = \{ \gamma_1^{n_1} \gamma_2^{n_2} \cdots \gamma_d^{n_d} \mid n_1, n_2, \ldots, n_d \in \mathbb{Z} \}$.

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, see [7]. This fact can be rephrased in the terminology of elementary linear algebra. It is a basic fact that, over a field, every invertible matrix can be reduced to the identity matrix by elementary row operations. 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 $\mathrm{SL}_n(\mathbb{Z})$ (for fixed $n \geq 3$) 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, see [10]. 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. See the survey [14], and the references within, for more details on the CSP. 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. Given an abstract group Γ whose profinite completion $\widehat{\Gamma}$ has BG, 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: July 19, 2022.

Added to and 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 we assume $\widehat{\Gamma}$ 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 has Witt index ≥ 2 over $\mathbb{R}$, then $\mathrm{Spin}(q)(\mathbb{Z})$ is known to have CSP (this was proved by M. Kneser); otherwise, one can consider the group of points $\mathrm{Spin}(q)\big(\mathbb{Z}[1/s]\big)$ over a suitable localization. This would be a good test case.

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

Following P.M. Cohn [9], we call a (not necessarily commutative) ring R with 1 a GE_n *ring* (n a natural number > 1) if $\mathrm{GL}_n(R)$ is generated by elementary and invertible diagonal matrices, i.e., if $\mathrm{GL}_n(R) = \mathrm{GE}_n(R)$.

For commutative R this is equivalent to $\mathrm{SL}_n(R) = \mathrm{E}_n(R)$. We will restrict to (commutative) integral domains in the following. It is clear that fields and Euclidean domains are GE_n rings for all n. GE_n properties of S-arithmetic rings are also well known (but also not relevant to this problem). A. Suslin [16] studied the question of when GE_n properties of a base ring A carry over to (Laurent) polynomial rings over A. In particular, he obtained the following:

Theorem 1. *If A is a field or Euclidean domain, and ℓ, m and n are natural numbers with $\ell \leq m$, then $R = A[t_1, ..., t_m; 1/t_1, ..., 1/t_\ell]$ is a GE_n ring for all $n > 2$.*

This leaves the question when these rings are also GE_2. A general answer was given by H. Chu [8]. Among his results for integral domains S are the following:

Theorem 2. *If $R = S[t]$ is a GE_2 ring, then S is a field.*

Corollary. *If A is a field, $m > 1$, and $\ell < m$ or A is any integral domain that is not a field, m is any natural number and $\ell < m$, then $R = A[t_1, ..., t_m; 1/t_1, ..., 1/t_\ell]$ is not a GE_2 ring.*

Theorem 3. *If $R = S[t, 1/t]$ is a GE_2 ring, then S is a Bezout domain.*

Corollary. *If A is a field and $\ell = m > 2$ or A is any integral domain which is not a field and $\ell = m > 1$, then $R = A[t_1, ..., t_m; 1/t_1, ..., 1/t_m]$ is not a GE_2 ring.*

It is worth noting that for Laurent polynomial rings the situation is more complicated than for polynomial rings as described in Theorem 2. Namely, Chu also proved:

Theorem 4. *If S is a valuation domain (but not a field), then $R = S[t, 1/t]$ is still a GE_2 ring.*

So the most interesting questions in this context which (to the best of our knowledge) are still open after many decades are the following two:

Question 1. Is $\mathbb{Z}[t, 1/t]$ a GE_2 ring, i.e., is $\mathrm{SL}_2\big(\mathbb{Z}[t, 1/t]\big) = \mathrm{E}_2\big(\mathbb{Z}[t, 1/t]\big)$?

Obviously, the latter group is finitely generated. So a weaker variant of this question would be:

Question 1′. Is $\mathrm{SL}_2\big(\mathbb{Z}[t, 1/t]\big)$ finitely generated?

Question 2. Is it true for some/all/no fields F that $R = F[t_1, t_2, 1/t_1, 1/t_2]$ is a GE_2 ring?

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. For more details, see [13].

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 $\mathrm{PSL}(n, \mathbb{C})$.

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 $\mathrm{O}_n \to \mathrm{GL}_n$ 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. This is known to be true for small n, e.g., [4], and also when n is divisible by 4 (unpublished).

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 $\mathrm{PGL}_p \to \mathrm{PGL}_p$ 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 opposite extreme, the question should be easiest to answer if one takes "$X = BG$," and the question is open even in the topological category.

If we restrict to affine X, then, by taking Levi subgroups of H_1, H_2 and replacing G with $G/\mathrm{rad}_u(G)$, we can reduce to the case where G, H_1, H_2 are reductive (at least if F is perfect).

Past work has addressed special cases of this problem using topological methods, by choosing X to be an appropriate finite dimensional algebraic approximation of the classifying space $BG(\mathbb{C})$ of the complex Lie group $G(\mathbb{C})$. While the first use of such approximations is Raynaud's [15] study of stably free modules, this technique has been developed in the past decade by Antieau and Williams [1, 2, 3] with dramatic results on the purity problem for torsors. The results in [4] and [17] use similar techniques to address the above question. These methods usually require careful analysis of topological obstruction invariants tailored to the specific choice of the groups H_1, H_2, G. Also, they are oblivious to unipotent radicals, e.g., if $H_1 = B_2$, $H_2 = T_2$, $G = GL_2$, then we cannot use such methods. Is there a way to address this problem in general (rather than treating special cases separately), and more generally, in the presence of unipotent radicals?

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 $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\sqrt{D})$ where D is a square-free positive integer?

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 $F_2 \subset \mathrm{SL}_2(\mathbb{Z})$. Khelif [12] 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 $\mathrm{SL}_2(\mathbb{Z})$, see [11]. However, for a general free product of finite cyclic groups $C_n * C_m$, the question is open.

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 from G. 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, as conjectured in [20]:

Conjecture. Every normal subsemigroup is a subgroup.

Maybe one expects the conjecture to also hold for arithmetic groups such as $\mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$?

The question can be rephrased in different ways, as 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 $K = \mathbb{Q}$.

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, $\mathbb{C}/\mathbb{R}$-admissible tori are compact.) Can we classify these groups?

It would be especially interesting to work out the case of types 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, see [5, 6].

This notion of L/K-admissible groups was introduced by Boris Weisfeiler (or Veĭsfeĭler) [18], [19], 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

[1] Benjamin Antieau and Ben Williams, *The topological period-index problem over 6-complexes*, J. Top. **7** (2014), 617–640.

[2] Benjamin Antieau and Ben Williams, *Unramified division algebras do not always contain Azumaya maximal orders*, Invent. math. **197** (2014), no. 1, 47–56.

[3] Benjamin Antieau and Ben Williams, *Topology and purity for torsors*, Doc. Math. **20** (2015), 333–355.

[4] Asher Auel, Uriya A. First, and Ben Williams, *Azumaya algebras without involution*, J. Eur. Math. Soc. **21** (2019), 897–921.

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

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

[7] David Carter and Gordon Keller, *Bounded Elementary Generation of* $\mathrm{SL}_n(\mathcal{O})$, Am. J. Math. **105** (1983), no. 3, 673–687.

[8] H. Chu, *On the* GE_2 *of graded rings*, Journal of Algebra **90** (1984), 208–216.

[9] Paul M. Cohn, *On the structure of the* GL_2 *of a ring*, Publ. Math. IHÉS **30** (1966), 5–53.

[10] 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.

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

[12] A. Khelif, *Finite approximation and commutators in free groups*, J. Algebra **281** (2004), no. 2, 407–412.

[13] E. Klimenko, B. Kunyavskii, J. Morita, and E. Plotkin, *Word maps in Kac-Moody settings*, Toyama Mathematical Journal **37** (2015), 25–53. https://u.cs.biu.ac.il/~plotkin/papers/wordmaps.pdf

[14] M.S. Raghunathan, *The congruence subgroup problem*, Proc. Indian Acad. Sci. (Math. Sci.) **114** (2004), no. 4, 299–308.

[15] Michèle Raynaud, *Modules projectifs universels*, Invent. math. **6** (1968), 1–26.

[16] A. Suslin, *On the structure of the special linear group over polynomial rings*, Math. USSR Izvestija **11** (1977), no. 2, 221–238.

[17] Uriya First and Ben Williams, *Involutions of Azumaya algebras*, Doc. Math. **25** (2020) 527–633.

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

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

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