Division Algebras and Algebraic Groups: structure and cohomology

Andrei S. Rapinchuk

Vavilov Memorial

September 18, 2024

Faddeev's sequence

FADDEEV (1951): Let k be a field of characteristic zero.

Brauer group of $K = k(x)$ is included in exact sequence

$$0 \to \mathrm{Br}(k) \longrightarrow \mathrm{Br}(K) \xrightarrow{\rho} \bigoplus_p H^1(k(p), \mathbb{Q}/\mathbb{Z}), \quad \rho = \oplus \rho_p, \qquad \text{(F)}$$

sum is over all monic irreducible $p \in k[x]$, $k(p) = k[x]/(p(x))$,

$\rho_p \colon \mathrm{Br}(K) \to H^1(k(p), \mathbb{Q}/\mathbb{Z})$ is *residue map*.

$a \in \mathrm{Br}(K)$ is *unramified* at p if $\rho_p(a) = 0$.

(F) $\Rightarrow$ *if* $a \in \mathrm{Br}(K)$ *is unramified at all* p *then* a *is* <u>*constant*</u>.

Recall that $a \in \mathrm{Br}(K)$ is unramified at p iff

$$a \in \mathrm{im}\left(\mathrm{Br}(\mathcal{O}_{K,p}) \to \mathrm{Br}(K)\right).$$

Thus,

$$\bigcap_p \mathrm{im}\left(\mathrm{Br}(\mathcal{O}_{K,p}) \to \mathrm{Br}(K)\right) \;=\; \mathrm{im}\left(\mathrm{Br}(k) \to \mathrm{Br}(K)\right).$$

By purity, LHS $= \mathrm{Br}(k[x])$, so

$$\mathrm{Br}(k[x]) \;=\; \mathrm{Br}(\mathbb{A}^1_k) \;=\; \mathrm{Br}(k). \qquad (*)$$

- isomorphism classes of degree n CSA over k

$$\leftrightarrow \quad H^1(k, \mathrm{PGL}_n)$$

- isomorphism classes of rank n Azumaya algebras over $X = \mathbb{A}^1_k$

$$\leftrightarrow \quad H^1_{\acute{e}t}(X, \mathrm{PGL}_n).$$

So, we would get $(*)$ **if** we knew that

$$H^1(k, \mathrm{PGL}_n) \longrightarrow H^1_{\acute{e}t}(X, \mathrm{PGL}_n)$$

is *surjective*.

Surjectivity question can be asked for *any* reductive k-group G.

Recall: $H^1(k, G)$ (resp., $H^1_{\acute{e}t}(X, G)$) parametrizes G-torsors over $\operatorname{Spec} k$ (resp., X).

Theorem 1 (Raghunathan-Ramanathan, 1984)

Let G be a connected reductive group over a field of characteristic zero. Every G-torsor $\pi\colon B \to \mathbb{A}^1_k$ is constant, i.e. is obtained from a G-torsor $\pi_0\colon B_0 \to \operatorname{Spec} k$ by base change.

Other proofs: Gille (2002), Chernousov - Gille - Pianzola (2012).

We found a new proof that uses buildings and Fixed-Point Theorem.

By standard procedures, argument is reduced to proving:

Let ℓ/k be a finite Galois extension. Then map

$$H^1(\ell/k, G(\ell)) \longrightarrow H^1(\ell/k, G(\ell[x]))$$

is surjective (hence bijective).

Sketch for $G = \mathrm{PGL}_2$

Here building associated to G over $\mathcal{L} := \ell((x^{-1}))$ is a *tree*.

Construction. (See J.-P. Serre, "Trees" for details.)

Set $\mathcal{O} = \ell[\![x^{-1}]\!]$, and let $\widetilde{\mathcal{V}}$ be set of all $\mathcal{O}$-lattices $A \subset \mathcal{L}^2$.

Define equivalence relation on $\widetilde{\mathcal{V}}$:

$$A_1 \sim A_2 \;\Leftrightarrow\; A_2 = \lambda A_1 \text{ for some } \lambda \in \mathcal{L}^\times.$$

$[A]$ = equivalence class of A; if v_1, v_2 is a basis of $\mathcal{L}^2$ then

$$[v_1, v_2] = \text{equivalence class of } \mathcal{O}v_1 + \mathcal{O}v_2.$$

$\mathcal{V} = \widetilde{\mathcal{V}}/\sim$ is *set of vertices* of tree.

Two vertices $[A_1], [A_2] \in \mathcal{V}$ define a (nonoriented) edge if one can find representatives $A_1' \in [A_1], A_2' \in [A_2]$ such that

$$A_2' \subset A_1' \quad \text{and} \quad A_1'/A_2' \simeq \ell \quad \text{as} \quad \mathcal{O}\text{-module}.$$

For example, if $\mathbf{e}_1, \mathbf{e}_2$ is standard basis of $\mathcal{L}^2$ then there is an edge between $[\mathbf{e}_1, \mathbf{e}_2]$ and $[\mathbf{e}_1, x^{-1}\mathbf{e}_2]$.

Let $\mathcal{E}$ be set of all such edges.

Then $\mathcal{T} = (\mathcal{V}, \mathcal{E})$ is a desired **tree** (which we will identify with its geometric realization).

Group $G(\mathcal{L})$ acts on $\mathcal{T}$, with subgroup $\Gamma = G(\ell[x])$ acting without inversions.

The following ray $\mathcal{R}$ is a fundamental domain for Γ:

$[\mathbf{e_1}, \mathbf{e_2}]$ $[\mathbf{e_1}, x^{-1}\mathbf{e_2}]$ $[\mathbf{e_1}, x^{-2}\mathbf{e_2}]$

(This follows from Birkhoff's decomposition for $\mathrm{GL}_n(\ell[x, x^{-1}])$ which also implies Grothendieck's theorem on vector bundles on $\mathbb{P}^1$.)

Galois group $\mathcal{G} = \mathrm{Gal}(\ell/k)$ acts on Γ and $\mathcal{T}$ in a compatible manner. Since all vertices in fundamental domain $\mathcal{R}$ are $\mathcal{G}$-fixed, $\mathcal{G}$ acts on $\mathcal{T}$ without inversion.

Thus, $\Delta = \Gamma \rtimes \mathcal{G}$ acts on $\mathcal{T}$ without inversions.

We also need information about stabilizers of vertices

$$p_n = [\mathbf{e}_1\,,\ x^{-n}\mathbf{e}_2] \quad (n = 0, 1, 2, \ldots) \quad \text{of} \quad \mathcal{R}.$$

By direct computation: $\mathrm{Stab}_\Gamma(p_0) = G(\ell)$, and for $n \geqslant 1$:

$$\mathrm{Stab}_\Gamma(p_n) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \;\middle|\; a\,,\ d \in \ell^\times,\ b \in \ell[x] \text{ with } \deg b \leqslant n \right\}.$$

It follows that $H^1(\ell/k\,,\ \mathrm{Stab}_\Gamma(p_0)) = H^1(\ell/k\,,\ G)$, and

$$H^1(\ell/k\,,\ \mathrm{Stab}_\Gamma(p_n)) = 1 \text{ for } n \geqslant 1.$$

Proof of Raghunathan-Ramanathan Theorem

Let $f\colon \mathcal{G} \to \Gamma$ be a 1-cocyle. Then

$$\tilde{f}\colon \mathcal{G} \to \Delta = \Gamma \rtimes \mathcal{G}, \quad \sigma \mapsto (f(\sigma), \sigma),$$

is group homomorphism.

$\tilde{f}$ defines an action of $\mathcal{G}$ on $\mathcal{T}$ without inversion.

By Fixed-Point Theorem, $\mathcal{G}$ fixes a vertex p of $\mathcal{T}$.

Since $\mathcal{R}$ is a fundamental domain,

$$p = \gamma \cdot p_n \quad \text{for some} \quad \gamma \in \Gamma \quad \text{and} \quad n = 0, 1, 2, \ldots.$$

Then $f'\colon \mathcal{G} \to \Gamma$, $f'(\sigma) = \gamma^{-1} \cdot f(\sigma) \cdot \sigma(\gamma)$, has values in $\mathrm{Stab}_\Gamma(p_n)$.

Required fact follows from above computation of stabilizers and their cohomology.

Similar application of Fixed-Point Theorem to building of a reductive k-group over $\mathcal{K} = k((x^{-1}))$ yields

Theorem 2

Let G be a reductive algebraic group over a field k of char 0. Then every finite subgroup of $G(k[x])$ is conjugate to a subgroup contained in $G(k)$.

- This was not known even for $G = \mathrm{SL}_n$.
- This is **false** in positive characteristic.

Borel and Harish-Chandra (1962): *Every arithmetic subgroup has finitely many conjugacy classes of finite subgroups.*

Corollary

Let G be a reductive algebraic group over a finite extension k of p-adic field $\mathbb{Q}_p$. Then $G(k[t])$ has finitely many conjugacy classes of finite subgroups.

A similar question over coordinate rings of other p-adic curves has not been investigated.

Definition 1

An abstract group Γ has *bounded generation* (BG) if there exist $\gamma_1, \dots, \gamma_d \in \Gamma$ such that

$$\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_d \rangle, \qquad \text{(BG)}$$

where $\langle \gamma_i \rangle$ is cyclic subgroup generated by γ_i.

Profinite version:

Definition 2

A profinite group Γ has *bounded generation* $(\mathrm{BG})_{\mathrm{pr}}$ if there exist $\gamma_1, \dots, \gamma_d \in \Gamma$ such that

$$\Gamma = \overline{\langle \gamma_1 \rangle} \cdots \overline{\langle \gamma_d \rangle},$$

where $\overline{\langle \gamma_i \rangle}$ is closure of cyclic subgroup generated by γ_i.

- (BG) for $\Gamma \Rightarrow (\mathrm{BG})_{\mathrm{pr}}$ for $\widehat{\Gamma}$ (profinite completion).

- Question of whether the converse is true remained open for a long time.

- Our results show that $(\mathrm{BG})_{\mathrm{pr}} \not\Rightarrow$ (BG).

In fact, in some situations $(\mathrm{BG})_{\mathrm{pr}}$ may be more useful (and maybe even more natural) than (BG) itself.

We will return to (BG) vs. $(\mathrm{BG})_{\mathrm{pr}}$ later but for now will talk almost exclusively about (BG) for discrete groups.

Groups with (BG) and $(\mathrm{BG})_{\mathrm{pr}}$ have remarkable properties:

- If Γ has (BG) and satisfies

$(\mathrm{F}^{\mathrm{ab}})$ every finite index subgroup $\Gamma_1 \subset \Gamma$ has finite abelianization $\Gamma_1^{\mathrm{ab}} = \Gamma_1/[\Gamma_1, \Gamma_1]$,

then Γ is *SS-rigid*, i.e. it has only finitely many inequivalent completely reducible representations $\rho\colon \Gamma \to \mathrm{GL}_n(\mathbb{C})$ in each dimension.

- Let $\Gamma = G(\mathcal{O}(S))$ be an S-arithmetic subgroup of an absolutely almost simple simply connected algebraic group G over a number field K. If Γ has (BG) (and Margulis-Platonov conjecture holds) then Γ has *Congruence Subgroup Property*, i.e. congruence kernel $C^S(G)$ is finite.

- A pro-p group satisfies $(\mathrm{BG})_{\mathrm{pr}}$ if and only if it is *analytic*.

(BG) was used to prove some cases of Margulis-Zimmer conjecture (Shalom, Willis), to estimate Kazhdan constants (Kassabov), to analyze first order rigidity (Avni, Lubotzky, Meiri) etc.

At some point, we felt that (BG) should hold keys to understanding properties of higher rank lattices.

However, (BG) is **not** easy to establish, particular if there are no obvious candidates for elements γ_i in bounded factorization (BG).

Remarks and Examples

(BG) and $(\mathrm{BG})_{\mathrm{pr}}$ are *purely group-theoretic properties*, but both positive and negative results on (BG) have strong number-theoretic connections.

Let us begin with some remarks and examples.

- Every group with (BG) is finitely generated.

- Conversely, every finitely generated *abelian*, or more generally, *nilpotent* group has (BG).

- Every solvable subgroup of $\mathrm{GL}_n(\mathbb{Z})$ is polycyclic (Mal'cev) hence has (BG).

In other known cases, verification of (BG) is nontrivial.

First "semi-simple" examples (viz., $\mathrm{SL}_n(\mathbb{Z})$, $n \geqslant 3$) came about from investigation of a linear algebra question.

Every $A \in \mathrm{SL}_n(F)$ (F a field) can be reduced to I_n by a sequence of elementary row/column operations:

$$A \longrightarrow A_1 \longrightarrow \cdots \longrightarrow I_n \quad \Rightarrow$$

$$A = e_{i_1 j_1}(\alpha_1) \cdots e_{i_r j_r}(\alpha_r) \quad (\alpha_i \in F)$$

where $e_{ij}(\alpha) = \begin{pmatrix} 1 & & \alpha & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$. In fact,

$$\boxed{r \leqslant n^2 + (\text{const}) \cdot n}$$

(independent of A).

Examples

Every $A \in \mathrm{SL}_n(\mathbb{Z})$ can also be reduced to I_n by integral elementary operations, resulting in a factorization

$$A = e_{i_1 j_1}(\alpha_1) \cdots e_{i_r j_r}(\alpha_r) \quad \text{with} \quad \alpha_i \in \mathbb{Z}.$$

Question. Can r be *bounded* by $c(n)$ *independent* of A?

"**No!**" for $n = 2$ b/c $\mathrm{SL}_2(\mathbb{Z})$ is v. free. What about $n \geqslant 3$?

This question was asked by Dennis and van der Kallen in 1979 over any ring $\mathcal{O}$ of algebraic integers.

Theorem (Carter, Keller, 1983)

Let $\mathcal{O} = \mathcal{O}_K$ be a ring of algebraic integers, and $n \geqslant 3$. Then every $A \in \mathrm{SL}_n(\mathcal{O})$ is a product of

$$\leqslant \tfrac{1}{2}(3n^2 - n) + 68 \cdot \Delta - 1$$

elementaries, $\Delta = \#$ of prime divisors of discriminant of K.

(BG) for $\mathrm{SL}_n(\mathbb{Z})$, $n \geqslant 3$

- Any $A \in \mathrm{SL}_n(\mathbb{Z})$ can be reduced to $\begin{pmatrix} a & b & & \\ c & d & & \\ & & I_{n-2} & \end{pmatrix}$ by $\leqslant 1/2 \cdot (3n^2 - n)$ elementary operations.

So, it is enough to show that any $\begin{pmatrix} a & b & \\ * & * & \\ & & 1 \end{pmatrix}$ can be reduced to I_3 inside $\mathrm{SL}_3(\mathbb{Z})$ by a bounded number of elementary operations.

- Bounded multiplicativity of Mennicke symbols: for $\ell > 0$

$$\begin{pmatrix} a & b & \\ * & * & \\ & & 1 \end{pmatrix}^{\ell} \Rightarrow \begin{pmatrix} a^{\ell} & b & \\ * & * & \\ & & 1 \end{pmatrix}$$ by 16 elementary operations.

One elementary operation: $\begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} a & b+ta & \\ c & d+tc & \\ & & 1 \end{pmatrix}$

So, using Dirichlet's Prime Number Theorem, we can assume that $b = p$ a prime.

Applying Dirichlet's Theorem twice, we can assume that

$A = \begin{pmatrix} u & p & \\ q & v & \\ & & 1 \end{pmatrix}$ with p, q odd primes and $\gcd(\frac{p-1}{2}, \frac{q-1}{2}) = 1$

Find $m, n > 0$ such that $m \cdot \frac{p-1}{2} - n \cdot \frac{q-1}{2} = \pm 1$ and set

$$s = m \cdot \frac{p-1}{2} \quad \text{and} \quad t = n \cdot \frac{q-1}{2}$$

.

We have $u^s \equiv \pm 1 (\mathrm{mod}\, p)$, so

$$A^s \overset{16}{\Rightarrow} \begin{pmatrix} u^s & p & \\ * & * & \\ & & 1 \end{pmatrix} \overset{1}{\Rightarrow} \begin{pmatrix} \pm 1 & p & \\ * & * & \\ & & 1 \end{pmatrix},$$

which is a bounded product of elementaries. So, A^s is a bounded product of elementaries.

Applying transpose and using same argument, we find that A^t is also a bounded product of elementaries.

Then $A^{\pm 1} = (A^s) \cdot (A^t)^{-1}$ is a bounded product of elementaries.

For $A = (a_{ij}) \in \mathrm{SL}_n(\mathbb{Z})$, set $\mathbf{m}(A) := \max_{i,j} |a_{ij}|$.

We saw: there exists $w = w(n)$ such that every $A \in \mathrm{SL}_n(\mathbb{Z})$ admits a factorization

$$A = e_{i_1 j_1}(\alpha_1) \cdots e_{i_r j_r}(\alpha_r) \qquad (*)$$

with $r \leqslant w$, **but** proof gives no estimate on α_i.

Question. Are there constants w, C and d such that every $A \in \mathrm{SL}_n(\mathbb{Z})$ has a factorization $(*)$ with

$$r \leqslant w \quad \text{AND} \quad |\alpha_i| \leqslant C \cdot \mathbf{m}(A)^d ?$$

w **must** depend on n.

Whether (and how) C and/or d should depend on n is unclear.

Proof of BG involves Dirichlet's Theorem on Primes in Arithmetic Progressions.

An effective version of Dirichlet's Theorem was given by Linnik (1944):

if $(a,m)=1$ *and* $a<m$ *then minimal prime in progression* $a+mk$ *is* $\leqslant D\cdot m^L$ *for some constants* D *and* L.

Best known unconditional value for L is 5 (Xylouris, 2011), and D can be effectively computed (Heath-Brown).

But our proof requires raising A to a "large" power, hence Linnik's Theorem does not automatically give a polynomial estimate on magnitude of elementaries.

One takeaway from our discussion of Carter–Keller result is that (BG) for $\mathrm{SL}_n(\mathcal{O})$, where $\mathcal{O}$ is a ring of algebraic integers, follows from *bounded elementary generation*.

It results in a bounded factorization (BG) where **all** γ_i are *unipotent*.

TAVGEN (1990) generalized result of Carter–Keller concerning bounded elementary generation for all untwisted Chevalley groups and some twisted groups.

This yields (BG) of such groups over rings of algebraic integers (and also S-integers).

The case $\Gamma = \mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O} = \mathcal{O}_{K,S}$ is ring of S-integers in a number field K, was completely resolved only recently.

When $\mathcal{O}$ is $\mathbb{Z}$ or ring of integers of imaginary quadratic field, Γ fails to have (BG). All other cases are covered in

Theorem (Morgan, R., Sury, 2018)

Assume that $\mathcal{O}^\times$ is infinite. Then every $A \in \mathrm{SL}_2(\mathcal{O})$ is a product of $\leqslant 9$ elementaries.

The case $\Gamma = \mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O} = \mathcal{O}_{K,S}$ is ring of S-integers in a number field K, was completely resolved only recently.

When $\mathcal{O}$ is $\mathbb{Z}$ or ring of integers of imaginary quadratic field, Γ fails to have (BG). All other cases are covered in

Theorem (+ Morris, 2023)

Assume that $\mathcal{O}^\times$ is infinite. Then every $A \in \mathrm{SL}_2(\mathcal{O})$ is a product of $\leqslant 7$ elementaries.

This results in a bounded factorization (BG) of $\Gamma = \mathrm{SL}_2(\mathcal{O})$ where some γ_i are *unipotent* and some *semi-simple* with unipotent elements necessarily present.

Some history

- Cooke and Weinberger (1975): assertion can be derived from results on Artin's Primitive Root Conjecture, for which one needs GRH (still unproven!).

- Morris (Witte) reworked (2007) preprint of Carter, Keller and Paige to prove existence of a bound using model theory – no explicit bound can be obtained!

- Vsemirnov (2014) proved assertion for $\mathcal{O} = \mathbb{Z}[1/p]$ using results of Heath-Brown.

Our proof relies only on traditional ANT.

(BG) is known for many other S-arithmetic subgroups of isotropic simple algebraic groups over number fields:

- Erovenko, R. (2006) considered isotropic, but not necessarily split or quasi-split, orthogonal groups.
- Heald (2013) considered some isotropic unitary groups.

Conjecturally, all higher rank S-arithmetic subgroups of isotropic simple algebraic groups over number fields should have (BG).

However, in 30 years of efforts not a single example of an *anisotropic* S-arithmetic subgroup with (BG) have been found! (Recall: G is anisotropic over a field K of char 0 if $G(K)$ does not contain unipotents $\neq e$.)

Question A. *Can* (BG) *possibly hold for an infinite S-arithmetic subgroup of an anisotropic simple algebraic group?*

In all known examples of S-arithmetic subgroups with (BG), the corresponding factorizations (BG) always involve non-semi- simple elements.

Question B. *Which linear groups are boundedly generated by semi-simple elements?*

Theorem (Corvaja, R., Ren, Zannier, 2020)

Let $\Gamma \subset \mathrm{GL}_n(K)$ *be a linear group,* $\operatorname{char} K = 0$, *which is* **not** *virtually solvable. Then any possible presentation* (BG) *for* Γ *involves at least* **two** *non-semi-simple elements. In particular, a linear group boundedly generated by semi-simple elements is virtually solvable.*

Question A. *Can* (BG) *possibly hold for an infinite S-arithmetic subgroup of an anisotropic simple algebraic group?*

In all known examples of S-arithmetic subgroups with (BG), the corresponding factorizations (BG) always involve non-semi- simple elements.

Question B. *Which linear groups are boundedly generated by semi-simple elements?*

Theorem (+ Demeio, 2023)

Let $\Gamma \subset \mathrm{GL}_n(K)$ *be a linear group,* $\operatorname{char} K = 0$, *which is* **not** *virtually solvable. Then any possible presentation* (BG) *for* Γ *involves at least* **two** *non-semi-simple elements. In particular, a linear group boundedly generated by semi-simple elements is virtually abelian.*

Corollary

An infinite S-arithmetic subgroup of a simple anisotropic algebraic group over a number field does not have (BG).

At the same time, there are numerous examples of S-arithmetic subgroups Γ of simple simply connected anisotopic groups over number fields that have CSP.

One shows that *congruence completion* $\overline{\Gamma}$ always has $(\mathrm{BG})_{\mathrm{pr}}$.

It follows that if Γ has CSP, then *profinite completion* $\widehat{\Gamma}$ has $(\mathrm{BG})_{\mathrm{pr}}$. But Γ fails to have (BG).

Thus, $(\mathrm{BG})_{\mathrm{pr}}$ for $\widehat{\Gamma} \not\Rightarrow$ (BG) for Γ.

While our non-(BG) theorem is a negative result, we hope to use techniques involved in its proof to address a *different problem* that people have been interested in for quite some time.

Problem

Find and explore various abstract characterizations of higher rank S-arithmetic subgroups.

More concretely, about 40 years ago, Platonov (generalizing Bass) conjectured that a representation rigid linear group should (basically) be S-arithmetic.

Bass and Lubotzky (2000) disproved this conjecture.

However, we believe that following should be true.

Conjecture

Let G be an absolutely almost simple $\mathbb{Q}$-group. If $\Gamma \subset G(\mathbb{Z})$ is a Zariski-dense subgroup having (BG) *then* $[G(\mathbb{Z}) : \Gamma] < \infty$.

More generally, if $\Gamma \subset G(\mathbb{Q})$ is a Zariski-dense subgroup with (BG) *then Γ is commensurable with $G(\mathbb{Z}_S)$ for some finite set of primes S.*

- This immediately generalizes to absolutely almost simple groups over any number field, but then one needs to consider *field of definition* of Γ.
- For G semi-simple, Γ may have S-arithmetic components coming from different fields and different sets S.

Proof of general form of this conjecture would demonstrate that **all** linear groups with (BG) can be obtained from S-arithmetic groups *by standard procedures*.

"**Plan**":

• Our non-(BG) theorem shows that a linear group with absolutely almost simple Zariski-closure and having (BG) **must** contain a non-semisimple element.

We would like to upgrade this result and show that such a group **must** contain a non-trivial unipotent element (in fact, "many" unipotent elements).

• Use results of Venkataramana, Hee Oh, Benoist, ... stating that *a Zariski-dense subgroup containing "enough" unipotents is arithmetic.*

BENOIST: Let G be a semi-simple real Lie group of rank $\geqslant 2$ and U be a nontrivial horosperical subgroup of G. If Γ is a Zariski-dense discrete subgroup of G that contains a lattice $\Delta \subset U$ then Γ is arithmetic.

Case of positive characteristic

ALBÉRT, LUBOTZKY, PYBER (2003): *A linear group over a field of positive characteristic that has* (BG) *is virtually abelian.*

One can still ask about bounded generation of Chevalley (and similar) groups over coordinate rings of curves over finite fields by *elementary subgroups*.

Many results have been generalized to positive characteristic in this context by Nica, Trost, Kunyavskiĭ, Plotkin, Vavilov, ... for groups of rank > 1.

The following result of KPV gives a uniform bound on the length in terms of root elements in **all** characteristics.

Theorem (Kunyavskiĭ, Plotkin, Vavilov, 2023)

Let Φ be a reduced irreducible root system of rank $\geqslant 2$. There exists a constant $L = L(\Phi)$ depending only on Φ such that any ring of S-integers R of a global field, every element of simply connected Chevalley group $G_{\mathrm{sc}}(\Phi, R)$ is a product of $\leqslant L$ elementary root unipotents.

They also have results for Steinberg groups and Kac-Moody groups.

In a joint work with B. Kunyavskiĭ, we treated $G = \mathrm{SL}_2$ over global fields of positive characteristic.

Let

- C be a smooth projective geometrically integral curve over a finite field F,
- $S \subset C$ be a finite set of closed points,
- $\mathcal{O}_S$ be coordinate ring of $C \setminus S$ over F.

Theorem (Kunyavskiĭ, R., 2023)

If $|S| \geqslant 2$ then every matrix in $\mathrm{SL}_2(\mathcal{O}_S)$ is a product of $\leqslant 8$ elementary matrices. If $|S| = 1$ then $\mathrm{SL}_2(\mathcal{O}_S)$ is not boundedly generated by elementaries.

Case $|S| \geqslant 2$ relies on Lenstra's generalization of Artin's Primitive Root Conjecture (proved in positive characteristic by Bilharz (1937) conditionally on Riemann hypothesis which was established by A. Weil (1948); see S. Kim and R. Murty (2020) for a modern treatement).

Explicit estimates on elementary width of $\mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O}$ is ring of S-integers in a global field with infinite $\mathcal{O}^\times$, lead to explicit estimates of elementary width L in KPV theorem over such rings.

It turns out that one can take

$$L = 8 \cdot |\Phi^+|$$

where Φ^+ is set of positive roots.

BG of SL_n over other rings

Van der Kallen (1980) showed that there is no bound w such that every matrix in $\mathrm{SL}_3(\mathbb{C}[x])$ is a product of $\leqslant w$ elementaries.

Whether there is such w for $\mathrm{SL}_3(\mathbb{Q}[x])$ or $\mathrm{SL}_3(\mathbb{Z}[x])$ is unknown.

Stronger question: *Is there w and $\delta\colon \mathbb{N} \to \mathbb{N}$ such that every $A = (a_{ij}) \in \mathrm{SL}_3(\mathbb{Z}[x])$ of degree $d := \max \deg a_{ij}$ is a product of $\leqslant w$ elementaries $e_{k\ell}(\alpha_{k\ell})$ with $\deg \alpha_{k\ell} \leqslant \delta(d)$?*

The answer is no.

On the proof of Non-(BG) Theorem

Non-(BG) Theorem

Let $\Gamma \subset \mathrm{GL}_n(K)$ *be a linear group,* $\operatorname{char} K = 0$, *which is* **not** *virtually solvable. Then any possible presentation* (BG) *for* Γ *involves at least* **two** *non-semi-simple elements. In particular, a linear group boundedly generated by semi-simple elements is virtually solvable.*

First, we make two reductions:

1. By a specialization argument, we show that it is enough to prove Main Theorem when K is a number field, i.e. $\Gamma \subset \mathrm{GL}_n(\overline{\mathbb{Q}})$.

2. Assuming that Γ is not virtually solvable, one reduces to case where connected component G° of Zariski-closure G of Γ is *nontrivial* semi-simple group.

For $\gamma \in \mathrm{GL}_n(\overline{\mathbb{Q}})$, let $\Lambda(\gamma)$ denote subgroup of $\overline{\mathbb{Q}}^\times$ generated by eigenvalues of γ. Key statement is the following.

Theorem

Let $\gamma_1, \ldots, \gamma_r \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ be semi-simple with one possible exception, and let $\gamma \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ be another semi-simple matrix.

Assume that γ has an eigenvalue λ which is not a root of unity and which satisfies

$$\langle \lambda \rangle \bigcap [\Lambda(\gamma_1) \cdots \Lambda(\gamma_r)] = \{1\}.$$

Then $\langle \gamma \rangle \bigcap \langle \gamma_1 \rangle \cdots \langle \gamma_r \rangle$ is finite. In particular,

$$\langle \gamma \rangle \not\subset \langle \gamma_1 \rangle \cdots \langle \gamma_r \rangle.$$

To complete proof of Main Theorem we need to show that given $\gamma_1, \ldots, \gamma_r \in \Gamma$, there exists a semi-simple $\gamma \in \Gamma$ of infinite order such that

$$\Lambda(\gamma) \bigcap [\Lambda(\gamma_1) \cdots \Lambda(\gamma_r)] = \{1\}.$$

This follows from existence of *generic elements* in Zariski-dense subgroups of semi-simple groups (Prasad, R., 2003).

Proof of key statement critically depends on

Laurent's Theorem

Let Ω be a finitely generated subgroup of $(\overline{\mathbb{Q}}^{\times})^N$, and let $\Sigma \subset \Omega$. Then Zariski-closure of Σ in $T = (\mathbb{G}_m)^N$ is a finite union of translates of algebraic subgroups of T.

We consider case where all γ_i are semi-simple.

We can find $g, g_1, \ldots, g_r \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ so that

$$g^{-1}\gamma g = \mathrm{diag}(\lambda_1, \ldots, \lambda_n), \quad \lambda_1 = \lambda,$$
$$g_i^{-1}\gamma_i g_i = \mathrm{diag}(\lambda_{i1}, \ldots, \lambda_{in}), \quad i = 1, \ldots, r.$$

Let $p(x_{11}, \ldots, x_{rn}) \in \overline{\mathbb{Q}}[x_{11}, \ldots, x_{rn}]$ be (11)-entry of

$$g^{-1} \cdot \left[\prod_{i=1}^{r} (g_i \cdot \mathrm{diag}(x_{i1}, \ldots, x_{in}) \cdot g_i^{-1}) \right] \cdot g.$$

Let $J = \{ m \in \mathbb{Z} \mid \gamma^m \in \langle \gamma_1 \rangle \cdots \langle \gamma_r \rangle \}$.

Then for each $m \in J$ there exist $a_1(m), \ldots, a_r(m) \in \mathbb{Z}$ so that

$$\gamma^m = \gamma_1^{a_1(m)} \cdots \gamma_r^{a_r(m)}.$$

By our choice of p we have

$$\lambda^m = p\left(\lambda_{11}^{a_1(m)}, \ldots, \lambda_{rn}^{a_r(m)}\right).$$

This polynomial identity holds on

$$\Sigma = \{ (\lambda^m, \lambda_{11}^{a_1(m)}, \ldots, \lambda_{rm}^{a_r(m)}) \mid m \in J \} \subset$$

$$\subset \Omega = \langle \lambda \rangle \times \langle \lambda_{11} \rangle \times \cdots \times \langle \lambda_{rn} \rangle \subset \overline{\mathbb{Q}}^{\times (1+rn)}.$$

Assuming that J is infinite and using description of Zariski-closure $\overline{\Sigma}$ provided by Laurent's Theorem, we obtain

$$\lambda^{\ell} \in \Lambda(\gamma_1) \cdots \Lambda(\gamma_r) \quad \text{for some} \quad \ell \neq 0.$$

A contradiction.

Genus of a division algebra

AMITSUR (1955): *Let* D_1 *and* D_2 *be finite-dimensional central division* K*-algebras. If* D_1 *and* D_2 *have same splitting fields then*

$$\deg D_1 = \deg D_2 \text{ and } \langle [D_1] \rangle = \langle [D_2] \rangle \text{ in } \mathrm{Br}(K).$$

($P \supset K$ is a *splitting field* for D if $D \otimes_K P \simeq M_n(P)$.)

Amitsur's Theorem is no longer true if one considers only splitting fields of finite degree over K or maximal subfields of D.

Definition 1. *Let* D *be a finite-dimensional central division algebra over* K*. The genus* $\mathbf{gen}(D)$ *= set of* $[D'] \in \mathrm{Br}(K)$ *where* D' *has same maximal subfields as* D*.*

Genus of an algebraic group

Reductive K-groups G_1 and G_2 have same isomorphism classes of maximal K-tori if every maximal K-torus $T_1 \subset G_1$ is K-isomorphic to a maximal K-torus $T_2 \subset G_2$, and vice versa.

Definition 2. *Let G be an absolutely almost simple algebraic K-group. The genus $\mathbf{gen}_K(G)$ = set of K-isomorphism classes of inner twists G' of G having same isomorphism classes of maximal K-tori as G.*

Finiteness of $\mathbf{gen}_K(G)$ over a finitely generated K is part of package of finiteness properties that includes finiteness of forms with good reduction and finiteness of Tate-Shafarevich set for divisorial sets of places of K. Remain conjectural in general case.

Using good reduction in conjunction with Raghunathan-Ramanathan Theorem, one proves:

Theorem 3

Let G be an absolutely almost simple algebraic group over a finitely generated field k of $\operatorname{char} \neq 2$, *and let $K = k(x)$. Then every $H \in \mathbf{gen}_K(G \times_k K)$ is of the form $H = H_0 \times_k K$ for some $H_0 \in \mathbf{gen}_k(G)$.*

Using results on Galois cohomology, one can completely describe genus over number fields. This yields:

Corollary

Let G be an absolutely almost simple algebraic group over a number field k, and let $K = k(x_1, \ldots, x_m)$ be the field of rational functions in $m \geqslant 1$ variables. Then $\mathbf{gen}_K(G \times_k K)$ is finite and reduces to a single element if type of G is different from A_ℓ, $D_{2\ell+1}$ $(\ell > 1)$ or E_6.

- Corollary yields examples of finite genus for all types over fields having arbitrary transcendence degree over $\mathbb{Q}$.
- Theorem and corollary suggests that (at least in certain situations) maximal tori carry information about minimal field of definition of a simple group.

One can construct examples where G is defined over k, **but** for a finite extension K/k genus $\mathbf{gen}_K(G \times_k K)$ contains groups **not** defined over k. However, we don't have such examples when K is function field of a *geometrically integral* k-variety.

Question. *Describe field extensions K/k such for a simple k-group G, every group in $\mathbf{gen}_K(G \times_k K)$ is defined over k.*

Killing the genus

Theorem 3 is **not** a "stability theorem."
More precisely, we are **not** claiming that

$$H_0 \in \mathbf{gen}_k(G) \quad \Rightarrow \quad H_0 \times_k K \in \mathbf{gen}_K(G \times_k K).$$

We have opposite phenomenon termed *killing genus by a purely transcendental extension.*

Theorem 4

Let A be a central simple algebra of degree n over a finitely generated field k, let $G = \mathrm{SL}_{1,A}$. Let $K = k(x_1, \ldots, x_{n-1})$, and assume $\operatorname{char} k$ *is prime to n. Then $\mathbf{gen}_K(G \times_k K)$ consists of groups of the form $H \times_k K$, where $H = \mathrm{SL}_{1,B}$, B is a central simple k-algebra of degree n such that $[B] \in \mathrm{Br}(k)$ generates same subgroup as $[A]$.*

Proof uses Amitsur's Theorem and Saltman's results on function fields of Severi-Brauer varieties.

Killing the genus

Theorem 5

Let G be a simple group of type G_2 over a finitely generated field k of characteristic $\neq 2,3$, and $K = k(x_1, \dots, x_6)$. Then $\mathbf{gen}_K(G \times_k K)$ reduces to a single element.

Proof uses properties of Pfister forms.

Conjecture. *Let G be a simple group over a finitely generated field k. Assume $\operatorname{char} k$ is prime to $|W(G)|$. Then there exists a purely transcendental extension $K = k(x_1, \dots, x_m)$ with m depending only on type of G such that every $H \in \mathbf{gen}_K(G \times_k K)$ is of form $H_0 \times_k K$ where $H_0 \in \mathbf{gen}_k(G)$ has property that*

$$H_0 \times_k F \in \mathbf{gen}_F(G \times_k F)$$

for all field extensions F/k.

Motivic genus

MERKURJEV: Define $\mathbf{gen}_m(G)$ = set of k-isomorphism classes of (inner) k-twists G' of G such that

$$G' \times_k F \in \mathbf{gen}_F(G \times_k F) \quad \text{for all field extensions } F/k.$$

Theorem 4: motivic genus of $G = \mathrm{SL}_{1,A}$ is *finite* of size $\leqslant (n-1)$ and reduces to a single element if A has exponent 2.

Theorem 5: motivic genus of G of type G_2 reduces to a single element.

One can expect $\mathbf{gen}_m(G)$ to be *finite* in all situations.

OUR CONJECTURE: genus can always be reduced to motivic genus by a purely transecendental base change of transcendence degree depending only on type.

Motivic genus

Let q_1 and q_2 be n-dim quadratic forms over k, $\operatorname{char} k \neq 2$. Then condition

($*$) q_1 and q_2 have same Witt index over every field extension F/k

is equivalent to their motives being isomorphic (Vishik, Karpenko).

So, if $\mathrm{Spin}_n(q_1)$ and $\mathrm{Spin}_n(q_2)$ are in same motivic genus then q_1 and q_2 have isomorphic motives.

If n is *odd* then $(*) \Rightarrow q_1$ and q_2 are scalar multiples (Izhboldin).

So, motivic genus of $\mathrm{Spin}_n(q)$ with n odd is trivial.

One can expect motivic genus to be trivial also for types C_n, E_7, E_8 and F_4.