Arithmetic aspects of algebraic groups

Alex Lubotzky (Weizmann Institute of Science)
Dave Morris (University of Lethbridge)
Mikhail Ershov (University of Virginia)
Gopal Prasad (University of Michigan)

06/12/2022–06/17/2022

1 Overview of the Field

Classical results and long-standing problems concerning algebraic groups over global fields are the foundation of the arithmetic theory of algebraic groups, but this workshop also considered more recent developments that extend local-global principles, finiteness results, and other aspects of the classical theory to algebraic groups over more general fields of arithmetic nature. This includes function fields of curves over local fields or global fields, and, in some cases, even arbitrary finitely generated fields. All aspects of the subject have close connections with number theory and arithmetic geometry, and many results have important applications in other areas, from group theory to geometry and combinatorics.

Algebraic groups over global fields

The origins of the arithmetic theory of algebraic groups can be traced back to the analysis of finite-index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ in connection with the classical theory of modular forms [Fricke, Klein, Poincaré] and the work of Gauss, Hermite, and later Minkowski and Hasse, on the theory of integral and rational quadratic forms. These results subsequently developed into the theory of arithmetic and S-arithmetic groups and the general local-global approach that has been successfully used in many situations. The theory was complemented by approximation results and results on the structure of the groups of rational points of algebraic groups over global fields. It has been an area of active research for over 50 years, with foundations laid by Borel, Harish-Chandra, and Serre in the 1960s, and with many new applications discovered in the last decade. Nevertheless, some critical question in the theory remain open, and one of the objectives of the workshop was to discuss the recent progress, and look for new approaches. Some specific topics that were discussed in the workshop include:

Congruence Subgroup Problem, its generalizations and applications. While it was known already to Fricke and Klein that $\mathrm{SL}_2(\mathbb{Z})$ has numerous finite-index subgroups that do not contain any congruence subgroups, it was not proved until the 1960s that if $n \geqslant 3$, then every infinite, normal subgroup of $\mathrm{SL}_n(\mathbb{Z})$ has finite index and contains a suitable congruence subgroup. This solution of the Congruence Subgroup Problem (CSP) for $\mathrm{SL}_n(\mathbb{Z})$ was followed by a period of very active research that generalized the result to S-arithmetic subgroups of many other simple algebraic groups over global fields. However, some important cases still remain open; in particular, the CSP has not been solved for arithmetic subgroups of the group $G = \mathrm{SL}_{1,D}$ of norm 1 elements in a central division K-algebra D — even when D is a quaternion algebra). In 2017, G. Prasad and A. Rapinchuk proposed a new approach that provides a simpler and shorter proof of many of the known cases, and one can expect this approach to lead to further progress on this long-standing problem. A few years earlier, in 2013, Y. Shalom and G. Willis proposed a generalization of the CSP, by formulating a precise conjecture on the homomorphisms of S-arithmetic groups into general locally compact groups. Very recently, the techniques developed to investigate the CSP were used by N. Avni, A. Lubotzky, and C. Meiri to establish a new form of rigidity, which can be called first-order rigidity: if G is a connected, isotropic, almost-simple algebraic group over $\mathbb{Q}$, such that $\operatorname{rank}_{\mathbb{R}} G \geq 2$, and Λ is any finitely generated group that satisfies precisely the same first-order axioms as some finite-index subgroup Γ of $G(\mathbb{Z})$, then Λ is isomorphic to Γ.

Bounded generation. An abstract group is said to be "boundedly generated" if it is a product of finitely many cyclic subgroups. This seemingly simple property has surprisingly strong and diverse consequences for abstract groups, and the implications are particularly striking for S-arithmetic groups. For example, an abstract boundedly generated group that satisfies one additional natural condition is known to have only finitely many inequivalent irreducible complex representations in each dimension. (This is a form of homomorphism rigidity.) For an S-arithmetic subgroup of an absolutely almost simple simply connected algebraic group, bounded generation implies the congruence subgroup property. And bounded generation has been used to estimate Kazhdan constants and to analyze the actions of arithmetic groups; it also played a significant role in the works of Shalom-Willis mentioned above. These applications illustrate that proving bounded generation of S-arithmetic groups is an important problem, with far-reaching consequences. In 1983, D. Carter and G. Keller proved that $\mathrm{SL}_n(\mathcal{O})$ has bounded generation for any $n \geqslant 3$ and any ring of algebraic integers $\mathcal{O}$. Since then, the list of S-arithmetic groups known to have bounded generation has been steadily increasing — with important results obtained in the last few years.

A very important development in this area occurred in the year prior to the workshop. In a remarkable paper by Corvaja, A. Rapinchuk, Ren and Zannier, it was shown that if a linear group over a field of characteristic zero is boundedly generated by semi-simple elements, it must be virtually solvable. This implies that infinite S-arithmetic subgroups of absolutely almost simple anisotropic algebraic groups over number fields are never boundedly generated. A whole series of other "boundedness" conditions are also being investigated (and applied). For example, Chevalley groups over the rings of integers in function fields are not boundedly generated, but in the past year it was shown that such groups in the higher rank case possess *bounded elementary generation*, that is, can be written as products of finitely many root subgroups. Another related condition is "bounded generation by the conjugacy class." (This means that the normal subgroup generated by an arbitrary element is a product of finitely many copies of the conjugacy class of that element and its inverse.) While this property is known, for example, for $\mathrm{SL}_n(\mathcal{O})$ (where $n \geqslant 3$ and $\mathcal{O}$ is a ring of algebraic integers), its general consequences have not been explored yet. For example, it is not known whether this property for an S-arithmetic subgroup of an absolutely almost simple simply connected algebraic group implies the congruence subgroup property.

New local-global principles. Local-global principles are at the heart of the arithmetic theory of algebraic groups: they provide a uniform perspective on the analysis of many phenomena, and serve as an important technical tool in the investigation of others. They are often expressed in terms of the injectivity of certain global-to-local maps for Galois cohomology, but others are of a different nature. In the last decade, a number of new local-global principles have been established. In particular, while the norm principle for finite extensions of global fields has been investigated for a long time, an understanding of the local-global principle for the products of norms from several extensions was achieved only (relatively) recently. This is known as the multinorm principle, and, surprisingly, it often holds when the usual norm principle fails for each of the individual extensions. This principle was used in the investigation of the Margulis-Platonov conjecture for anisotropic inner forms of type A_n, and also in the analysis of another local-global principle that governs the existence of an embedding of an etale algebra with an involutive automorphism into a simple algebra with involution. This embedding principle is important for understanding the maximal tori of simple groups of classical types over global fields. The *genus* of a given simple algebraic group G is the collection of isomorphism classes of simple groups with the same maximal tori as G, and it is reasonable to hope that these results will make it possible to determine the cardinality of the genus of any simple group of classical type. (This would have applications to the analysis of isospectral and length-commensurable locally symmetric spaces in differential geometry.) In addition, the multinorm principle can be stated as the vanishing of the Tate-Shafarevich group of an associated "multinorm torus," and this torus can be realized as a maximal torus of an isotropic inner form of type A_n, so a natural generalization would provide useful conditions that ensure the triviality of the Tate-Shafarevich group of maximal tori in other simple isotropic algebraic groups of classical types.

Algebraic groups over more general fields

Results obtained in the last decade have lead to the realization that many classical results over global fields should be considered in the broader context of finitely generated fields. For example, the genus is expected to be finite over arbitrary finitely generated fields, and this has already been established for inner forms of type A_n (and also for the related notion of genus of a finite-dimensional division algebra). Very recently, the finiteness of the genus was established for the spinor groups of quadratic forms and some other groups of classical types over 2-dimensional arithmetic fields. The general case, which remains wide open, is the subject of active investigation.

It was discovered that the study of the genus of a simple algebraic group G over a finitely generated field K is closely related to the problem of analyzing the K-forms of G that have good reduction at a divisorial set of places V of K. This is a totally new area of research at the meeting ground of the theory of algebraic groups and arithmetic geometry. Previously, simple algebraic groups over $\mathbb{Q}$ with good reduction at all primes were considered by B.H. Gross, but more general situations have never been analyzed. In addition to the finiteness of the genus, another important consequence of the finiteness of the number of forms with good reduction is the properness of the map $H^1(K, \overline{G}) \to \prod_{v \in V} H^1(K_v, \overline{G})$ for the Galois cohomology of the adjoint group $\overline{G}$. (Over global fields, the properness is known for all groups.)

Yet another important finiteness property in the classical theory is the finiteness of the class number of a global field; its generalization to algebraic groups states that for any algebraic group over a global field, the number of double cosets of the adele group modulo its subgroups of integral and principal adeles is finite (and the analog for regular schemes of finite type over $\mathbb{Z}$ or its localizations). One can introduce adele groups for algebraic groups over any field with respect to any set of discrete valuations subject to some mild assumptions, and then formulate a condition that naturally generalizes both finiteness results. The question is when does this condition hold? At this point, the affirmative answer is known only for reductive split groups over the function fields of curves over finitely generated fields with respect to the set of geometric places. The argument uses a variant of strong approximation for split groups. While strong approximation has been fully investigated for the groups over global fields, its analysis for anisotropic groups over the function fields of curves over general fields is only beginning.

Theorems on homomorphism rigidity and the congruence subgroup problem have been proved for split simple groups over rings other than the rings of S-integers of global fields. (For example, there is now a fairly explicit description of all finite-dimensional complex representations of the group $SL_n(\mathbb{Z}[X])$.) These results need to be extended to more general isotropic groups; in particular, this work is expected to give a proof of the Borel-Tits conjecture on abstract homomorphisms of the groups of rational points of simple isotropic groups. And there is the following very general conjecture of Prasad-Rapinchuk: if G is an absolutely almost simple algebraic group over an arbitrary field K, then any finite quotient of $G(K)$ is solvable.

2 Presentation Highlights

Abid Ali (Rutgers University)
Integrality of unipotent subgroups of Kac-Moody groups

Let G be a Kac-Moody group over $\mathbb{Q}$. There are several approaches to defining its "$\mathbb{Z}$-form" $G(\mathbb{Z})$, including the functorial definition proposed by Tits, and in most cases it is unknown whether different definitions yield isomorphic groups. In this talk the speaker discussed some recent progress on finding a relationship between different $\mathbb{Z}$-forms of G. The talk was based on a joint work with Lisa Carbone (Rutgers), Dongwen Liu (Zhejiang) and Scott S Murray (Toronto) which generalizes Chevalley's fundamental theorem on the integrality for finite dimensional semisimple Lie groups.

Nir Avni (Northwestern University)
Distributions of words in unitary groups

Let G be a compact group, and let w be a nontrivial word in the free group F_r, so w defines a function from G^r to G. Let μ_w be the image of Haar measure under this map. (Thus, μ_w is the distribution of a random value of w when the variables are i.i.d.) The talk presented recent work (and provided historical background) on the Fourier coefficients of this measure in the case where G is a unitary group U_d.

For each character χ of U_d, the corresponding Fourier coefficient of the measure μ_w is the expectation $\mathbb{E}\,\chi\big(w(x_1,\ldots,x_r)\big)$. The maximum value of $\chi\big(w(x_1,\ldots,x_r)\big)$ is $\chi(1)$, and it is conjectured that the expected value is substantially smaller than this: $\forall w \neq 1, \exists\epsilon > 0, \forall d, \forall\chi, \mathbb{E}\,\chi\big(w(x_1,\ldots,x_r)\big) < \chi(1)^{1-\epsilon}$.

This talk was based on a joint work with Itay Glazer, which proved that the conjecture is true for the fundamental representations of U_d. In more elementary terms, this means that the expected value of the kth coefficient of the characteristic polynomial of $w(x_1,\ldots,x_r)$ is bounded by $\binom{d}{k}^{1-\epsilon}$.

Rony Bitan (Afeka Academic College)
$\tau(G) = \tau(G_1)$: An equality of Tamagawa numbers

Given a smooth, geometrically connected and projective curve C defined over a finite field k, let $K = k(C)$ be the function field of rational functions on C. The Tamagawa number $\tau(G)$ of a semisimple K-group G is defined as the covolume of the discrete group $G(K)$ (embedded diagonally) in the adelic group $G(A)$ with respect to the Tamagawa measure. The Weil conjecture, recently proved by Gaitsgory and Lurie, states that if G is simply connected then $\tau(G) = 1$.

This talk was based on a work in progress (joint with Gunter Harder, Ralf Kohl and Claudia Schoemann) whose aim is to prove, without relying on the Weil conjecture, the following fact: Let G be a quasi-split inner form of a split semisimple and simply-connected K-group G_1. Then $\tau(G) = \tau(G_1)$. This theorem can serve as a part of an alternative proof to the Weil conjecture.

Mikhail Borovoi (Tel Aviv University)
Galois cohomology of a real reductive group

The goal of this talk was to describe the first Galois cohomology set $H^1(R, G)$ of a connected reductive group G over the field of real numbers $\mathbb{R}$ by the method of Borel and Serre and by the method of Kac. The talk was based on the recent preprints [6] and [7].

Vladimir Chernousov (University of Alberta)
New evidence that cohomological invariants might determine Albert algebras/groups of type F_4 uniquely up to isomorphism

In this talk, based on a joint work with A. Lourdeaux and A. Pianzola, the speaker provided a sketch of a proof that Albert algebras arising from the first Tits construction are determined uniquely up to an isomorphism by the Rost cohomological invariant g_3.

Uriya First (University of Haifa)
Sheaves on simplicial complexes and 2-query locally testable codes

This talk was based on joint work with Tali Kaufman [12], which shows that if arithmetic groups with certain properties exist, then one can construct good 2-query locally testable codes. The device that enables this is a novel notion of sheaves on simplicial complexes. The latter are typically taken to be quotients of an affine building by an arithmetic group, e.g., Ramanujan complexes.

Julia Hartmann (University of Pennsylvania)
Bounding cohomology classes over semi global fields

This talk was based on a joint work with David Harbater and Daniel Krashen [14]. It provides a uniform bound for the index of cohomology classes in $H^i(F, \mu_\ell^{\otimes i-1})$ when F is a semiglobal field (i.e., a one variable function field over a complete discretely valued field K). The bound is given in terms of the analogous data for the residue field of K and its finitely generated extensions of transcendence degree at most one. An explicit bound is obtained in example cases when the information on the residue field is known.

Chen Meiri (Technion)
Conjugacy width in higher rank orthogonal groups

It is known that conjugacy classes of elements in orthogonal groups over number fields have finite width. (This means that every element of the group is a product of a bounded number of elements of the conjugacy class.) This talk was based on joint work with Nir Avni which presents evidence that the same is true for conjugacy classes of elements in higher rank arithmetic groups of orthogonal type. It is shown that the question whether a conjugacy class of such a group has a finite width can be viewed as a congruence subgroup problem on a non-standard saturated model of the group.

Alexander Merkurjev (UCLA)
Classification of special reductive groups

An algebraic group G over a field F is called special if for every field extension K/F all G-torsors (principle homogeneous G-spaces) over K are trivial. Examples of special groups are special linear groups, general linear groups, and symplectic groups. A. Grothendieck classified special groups over an algebraically closed field. In 2016, M. Huruguen classified special reductive groups over arbitrary fields. This talk was based on the recent preprint [18] where it is shown how to improve the classification given by Huruguen.

Raman Parimala (Emory University)
Pencils of quadrics and hyperellliptic curves

This talk discussed a weak Hasse principle for a smooth intersection of two quadrics in $\mathbb{P}^5$ and connections to period index questions for the associated hyperelliptic curves.

Eugene Plotkin (Bar Ilan University)
Bounded generation and commutator width of Chevalley groups and Kac-Moody groups: function case

This talk was based on a recent joint work with B. Kunyavskii and N. Vavilov [17] which provides new results on bounded elementary generation and bounded commutator width for Chevalley groups over Dedekind rings of arithmetic type in positive characteristic. In particular, Chevalley groups of rank greater than 1 over polynomial rings and Chevalley groups of arbitrary rank over Laurent polynomial rings (in both cases the coefficients are taken from a finite field) are boundedly elementarily generated. The speaker presented rather plausible explicit bounds and discussed applications to Kac-Moody groups and various model theoretic consequences and certain conjectures which look quite tempting.

Igor Rapinchuk (Michigan State University)
Algebraic groups with good reduction and applications

Techniques involving reduction are very common in number theory and arithmetic geometry. In particular, elliptic curves and general abelian varieties having good reduction have been the subject of very intensive investigations over the years. The purpose of this talk, based on joint papers with V. Chernousov and A. Rapinchuk, was to report on recent work that focuses on good reduction in the context of reductive linear algebraic groups over higher-dimensional fields.

Zinovy Reichstein (University of British Columbia)
Hilbert's 13th Problem for algebraic groups

The algebraic form of Hilbert's 13th Problem asks for the resolvent degree $rd(n)$ of the general polynomial $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ of degree n, where $a_1, \ldots, a_n$ are independent variables. Here $rd(n)$ is the minimal integer d such that every root of $f(x)$ can be obtained in a finite number of steps, starting with $\mathbb{C}(a_1, \ldots, a_n)$ and adjoining an algebraic function in $\leq d$ variables at each step. It is known that $rd(n) = 1$ for every $n \leq 5$. It is not known whether or not $rd(n)$ is bounded as n tends to infinity; it is not even known whether or not $rd(n) > 1$ for any n. Recently Farb and Wolfson defined the resolvent degree $rd_k(G)$, where G is a finite group and k is a field of characteristic 0. In this setting $rd(n) = rd_C(S_n)$, where S_n is the symmetric group on n letters and $\mathbb{C}$ is the field of complex numbers. This talk was based on a recent preprint [21] which defines $rd_k(G)$ for any field k and any algebraic group G over k. Surprisingly, Hilbert's 13th Problem simplifies when G is connected. In particular, the speaker explained why $rd_k(G) \leq 5$ for an arbitrary connected algebraic group G defined over an arbitrary field k.

Jinbo Ren (Institute for Advanced Study)
Applications of Diophantine Approximation in Group Theory

An abstract group Γ has the property of "bounded generation" if it is equal to a product of finitely many fixed cyclic groups. Being a purely combinatorial property of groups, bounded generation has a number of interesting consequences and applications in different areas including Kazhdan's constants computation, semi-simple rigidity, the Margulis-Zimmer conjecture and the Serre's congruence subgroup problem.

This talk was based on a recent joint work Corvaja, A. Rapinchuk and Zannier [11] where the following result is proved: if a linear group $\Gamma \subset \mathrm{GL}_n(K)$ over a field K of characteristic zero is boundedly generated by semi-simple (diagonalizable) elements then it is virtually solvable. As a consequence, one obtains that infinite S-arithmetic subgroups of absolutely almost simple anisotropic algebraic groups over number fields are *never* boundedly generated. The proof relies on the subspace theorem (a far-reaching generalization of Roth's Fields medal work) from Diophantine approximation and properties of generic elements.

David J Saltman (Center for Communications Research - Princeton)
Cyclic Matters

This work was motivated by the problem of describing cyclic Galois extensions and differential crossed product algebras in mixed characteristic, with the the goal of lifting from arbitrary characteristic p rings to suitable characteristic 0 rings. The first step was the construction of Artin-Schreier like polynomials and extensions in mixed characteristic, where the group acts by $\sigma(x) = \rho x + 1$ ($\rho^p = 1$). This leads to Azumaya algebras A defined by $xy - \rho\, yx = 1$. Of course, a generalization to degrees higher than p is desirable. This leads to an Albert like criterion for extending cyclic Galois extensions of rings and to the definition and study of almost-cyclic Azumaya algebras, generalizing A above.

George Tomanov (Université Claude Bernard Lyon 1)
Actions of maximal tori on homogeneous spaces and applications to number theory

During the last decades long-standing conjectures in number theory have been reformulated and, subsequently, some of them successfully solved using the homogeneous dynamics approach. The approach is based on the description of the closures of orbits for the natural action of subgroups H of an algebraic group G on the homogeneous space G/Γ where Γ is an arithmetic subgroup of G. The closures of such orbits are well-understood when H is unipotent and considerably less when H is a torus. This talk described some recent results on the action of maximal (split or non-split) tori on G/Γ and related applications.

Charlotte Ure (University of Virginia)
Symbol Length in Brauer Groups of Elliptic Curves

Elements in the Brauer group of an elliptic curve E may be described as tensor products of symbol algebras over the function field of E by the Merkurjev-Suslin Theorem. The symbol length is the smallest number n so that every element in the Brauer group can be expressed as a tensor product of at most n symbols. This talk was based on a recent joint work with Mateo Attanasio, Caroline Choi, and Andrei Mandelshtam [1] which describes bounds on the symbol length of E. In particular, it is shown that the symbol length in the prime torsion for a prime q of a CM elliptic curve over a number field is bounded above by $q + 1$.

Kirill Zaynullin (University of Ottawa)
The canonical dimension of a semisimple group and the unimodular degree of a root system

This talk was based on a recent preprint [27], which provides a short and elementary algorithm to compute an upper bound for the canonical dimension of a split semisimple linear algebraic group. The key tools are the classical Demazure formula for the characteristic map and the elementary properties of divided-difference operators. Using this algorithm, one can confirm all previously known bounds by Karpenko and Devyatov as well as produce new bounds (e.g., for adjoint simple groups of type F_4 or E_6, and for some semisimple groups).

3 Open Problems

The workshop featured a problem session on Tuesday evening, during which 7 open problems were discussed. We are very grateful to Asher Auel for taking detailed notes from the problem session.

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

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, see [8]. 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 [11]. 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 [19], 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 $\widehat{\Gamma} = \overline{\langle\gamma_1\rangle} \cdots \overline{\langle\gamma_d\rangle}$.

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 [10], 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 [22] 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 $R = A[t_1, \ldots, t_m; t_1^{-1}, \ldots, t_\ell^{-1}]$ 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 [9]. 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 $R = A[t_1, \ldots, t_m; t_1^{-1}, \ldots, t_\ell^{-1}]$ is not a GE_2 ring.*

Theorem 3. *If $R = S[t, t^{-1}]$ 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 $R = A[t_1, \ldots, t_m; t_1^{-1}, \ldots, t_m^{-1}$ 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 $R = S[t, t^{-1}]$ 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 $\mathbb{Z}[t, t^{-1}]$ a GE_2 ring, i.e., is $\mathrm{SL}_2\big(\mathbb{Z}[t, t^{-1}]\big) = \mathrm{E}_2\big(\mathbb{Z}[t, t^{-1}]\big)$?

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

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

Question 2. Is it true for some/all/no fields F that $R = F[t_1, t_2, t_1^{-1}, t_2^{-1}]$ 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 [16].

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., [5], 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 [20] study of stably free modules, this technique has been developed in the past decade by Antieau and Williams [2, 3, 4] with dramatic results on the purity problem for torsors. The results in [5] and [23] 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 [15] 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 [13]. 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 [26]:

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 $y_1, \dots, y_n$ 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 $y_1, \dots, y_n$ 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 [6, 7].

This notion of L/K-admissible groups was introduced by Boris Weisfeiler (or Vesfeler) [24], [25], 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.

4 Outcome of the Meeting

We feel that the hybrid format worked very well for this meeting. For many participants this was the first in-person meeting in more than 2 years, and they enjoyed the opportunity to fully interact with their colleagues. At the same time, a number of mathematicians we invited could not travel for various reasons, so it was very helpful to have the virtual option as well. Several participants, including both in-person and online participants, indicated that thanks to this workshop, they were able to either start a new project or make progress on an existing project. We are very grateful to BIRS for allowing us to run the workshop at increased in-person capacity and for accommodating last minute changes.

References

[1] Mateo Attanasio, Caroline Choi, Andrei Mandelshtam, and Charlotte Ure *Symbol length in Brauer groups of elliptic curves*, preprint, https://arxiv.org/abs/2107.10886

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

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

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

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

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

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

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

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

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

[11] 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.

[12] Uriya A. First and Tali Kaufman, *On good* 2*-query locally testable codes from sheaves on high dimensional expanders*, preprint, https://arxiv.org/abs/2208.01778

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

[14] David Harbater, Julia Hartmann, and Daniel Krashen, *Bounding cohomology classes over semiglobal fields*, preprint, https://arxiv.org/abs/2203.06770

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

[16] 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

[17] Boris Kunyavskii, Eugene Plotkin and Nikolai Vavilov, *Bounded generation and commutator width of Chevalley groups: function case*, preprint, https://arxiv.org/abs/2204.10951

[18] Alexander Merkurjev, *Classification of special reductive groups*, https://www.math.ucla.edu/~merkurev/papers/special-1.pdf

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

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

[21] Zinovy Reichstein, *Hilbert's 13th Problem for Algebraic Groups*, https://arxiv.org/abs/2204.13202

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

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

[24] 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

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

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

[27] Kirill Zainoulline, *The canonical dimension of a semisimple group and the unimodular degree of a root system*, https://arxiv.org/abs/2108.07835.