

Algebra & Number Theory

Volume 13

2019

No. 6

**The congruence topology,
Grothendieck duality and thin groups**

Alexander Lubotzky and Tyakal Nanjundiah Venkataramana



The congruence topology, Grothendieck duality and thin groups

Alexander Lubotzky and Tyakal Nanjundiah Venkataramana

This paper answers a question raised by Grothendieck in 1970 on the “Grothendieck closure” of an integral linear group and proves a conjecture of the first author made in 1980. This is done by a detailed study of the congruence topology of arithmetic groups, obtaining along the way, an arithmetic analogue of a classical result of Chevalley for complex algebraic groups. As an application we also deduce a group theoretic characterization of thin subgroups of arithmetic groups.

Introduction

If $\varphi: G_1 \rightarrow G_2$ is a polynomial map between two complex varieties, then in general the image of a Zariski closed subset of G_1 is not necessarily closed in G_2 . But here is a classical result:

Theorem (Chevalley). *If φ is a polynomial homomorphism between two complex algebraic groups then $\varphi(H)$ is closed in G_2 for every closed subgroup H of G_1 .*

There is an arithmetic analogue of this issue: Let G be a \mathbb{Q} -algebraic group, let $\mathbb{A}_f = \prod_{p \text{ prime}}^* \mathbb{Q}_p$ be the ring of finite adeles over \mathbb{Q} . The topology of $G(\mathbb{A}_f)$ induces the congruence topology on $G(\mathbb{Q})$. If K is a compact open subgroup of $G(\mathbb{A}_f)$ then $\Gamma = K \cap G(\mathbb{Q})$ is called a congruence subgroup of $G(\mathbb{Q})$. This defines the congruence topology on $G(\mathbb{Q})$ and on all its subgroups. A subgroup of $G(\mathbb{Q})$ which is closed in this topology is called congruence closed. A subgroup Δ of G commensurable to Γ is called an arithmetic group.

Now, if $\varphi: G_1 \rightarrow G_2$ is a \mathbb{Q} -morphism between two \mathbb{Q} -groups, which is a surjective homomorphism (as \mathbb{C} -algebraic groups) then the image of an arithmetic subgroup Δ of G_1 is an arithmetic subgroup of G_2 [Platonov and Rapinchuk 1994, Theorem 4.1, page 74], but the image of a congruence subgroup is not necessarily a congruence subgroup. It is well known that $\mathrm{SL}_n(\mathbb{Z})$ has congruence subgroups whose images under the adjoint map $\mathrm{SL}_n(\mathbb{Z}) \rightarrow \mathrm{PSL}_n(\mathbb{Z}) \hookrightarrow \mathrm{Aut}(M_n(\mathbb{Z}))$ are not congruence subgroups (see [Serre 1968] and Proposition 2.1 below for an exposition and explanation). So, the direct analogue of Chevalley’s theorem does not hold. Still, in this case, if Γ is a congruence subgroup of $\mathrm{SL}_n(\mathbb{Z})$, then $\varphi(\Gamma)$ is a normal subgroup of $\overline{\varphi(\Gamma)}$, the (congruence) closure of $\varphi(\Gamma)$ in $\mathrm{PSL}_n(\mathbb{Z})$, and the quotient is a finite abelian group. Our first technical result says that the general case is similar. It is especially important

MSC2010: primary 11E57; secondary 20G30.

Keywords: congruence subgroup, thin groups.

for us that when G_2 is simply connected, the image of a congruence subgroup of G_1 is a congruence subgroup in G_2 (see Proposition 0.1(ii) below).

Before stating the result, we give the following definition and set some notations for the rest of the paper.

Let G be a linear algebraic group over \mathbb{C} , G^0 its connected component, and $R = R(G)$ its solvable radical, i.e., the largest connected normal solvable subgroup of G . We say that G is *essentially simply connected* if $G_{ss} := G^0/R$ is simply connected.

Given a subgroup Γ of GL_n , we will throughout the paper denote by Γ^0 the intersection of Γ with G^0 , where G^0 is the connected component of G , the Zariski closure of Γ . Therefore, Γ^0 is always a finite index normal subgroup of Γ .

The notion “essentially simply connected” will play an important role in this paper due to the following proposition, which can be considered as the arithmetic analogue of Chevalley’s result above.

Proposition 0.1. (i) *If $\varphi: G_1 \rightarrow G_2$ is a surjective \mathbb{Q} -morphism of algebraic \mathbb{Q} -groups, then for every congruence closed subgroup Γ of $G_1(\mathbb{Q})$, the image $\varphi(\Gamma^0)$ is normal in its congruence closure $\overline{\varphi(\Gamma^0)}$ and $\overline{\varphi(\Gamma^0)}/\varphi(\Gamma^0)$ is a finite abelian group.*

(ii) *If G_2 is essentially simply connected and Γ a congruence subgroup of G_1 then $\overline{\varphi(\Gamma)} = \varphi(\Gamma)$, i.e., the image of a congruence subgroup is congruence closed.*

This analogue of Chevalley’s theorem and a result of [Nori 1987; Weisfeiler 1984] enable us to prove:

Proposition 0.2. *If $\Gamma_1 \leq \mathrm{GL}_n(\mathbb{Z})$ is a congruence closed subgroup (i.e., closed in the congruence topology) with Zariski closure G , then there exists a congruence subgroup Γ of G , such that $[\Gamma, \Gamma] \leq \Gamma_1^0 \leq \Gamma$. If G is essentially simply connected then the image of Γ_1 in $G/R(G)$ is actually a congruence subgroup.*

We apply Proposition 0.1(ii) in two directions:

- (A) Grothendieck–Tannaka duality for discrete groups, and
- (B) a group theoretic characterization of thin subgroups of arithmetic groups.

Grothendieck closure. Grothendieck [1970] was interested in the following question:

Question 0.3. Assume $\varphi: \Gamma_1 \rightarrow \Gamma_2$ is a homomorphism between two finitely generated residually finite groups inducing an isomorphism $\hat{\varphi}: \hat{\Gamma}_1 \rightarrow \hat{\Gamma}_2$ between their profinite completions. Is φ already an isomorphism?

To tackle Question 0.3, he introduced the following notion. Given a finitely generated group Γ and a commutative ring A with identity, let $\mathrm{Cl}_A(\Gamma)$ be the group of all automorphisms of the forgetful functor from the category $\mathrm{Mod}_A(\Gamma)$ of all finitely generated A -modules with Γ action to $\mathrm{Mod}_A(\{1\})$, preserving tensor product. Recall that α is such an automorphism means that for every finitely generated A -module L with Γ action $\rho_L: \Gamma \rightarrow \mathrm{Aut}_A(L)$, we are given $\alpha_L \in \mathrm{Aut}_A(L)$ such that if $\varphi: L_1 \rightarrow L_2$ is an $A[\Gamma]$ -morphism between such modules then $\alpha_{L_2} \circ \varphi = \varphi \circ \alpha_{L_1}$. In particular, every $\tau \in \Gamma$ defines such α , by $\alpha_L = \rho_L(\tau)$. This gives a natural map from Γ to $\mathrm{Cl}_A(\Gamma)$.

Grothendieck's strategy was the following: he showed that, under the conditions of Question 0.3, φ induces an isomorphism from $\text{Mod}_A(\Gamma_2)$ to $\text{Mod}_A(\Gamma_1)$, and hence also between $\text{Cl}_A(\Gamma_1)$ and $\text{Cl}_A(\Gamma_2)$. He then asked:

Question 0.4. Is the natural map $\Gamma \hookrightarrow \text{Cl}_{\mathbb{Z}}(\Gamma)$ an isomorphism for a finitely generated residually finite group?

An affirmative answer to Question 0.4 would imply an affirmative answer to Question 0.3. Grothendieck then showed that arithmetic groups with the (strict) congruence subgroup property do indeed satisfy $\text{Cl}_{\mathbb{Z}}(\Gamma) \simeq \Gamma$. For a general survey on the congruence subgroup problem see [Raghunathan 1991].

Question 0.4 basically asks whether Γ can be recovered from its category of representations. The first author [Lubotzky 1980] phrased this question in the framework of Tannaka duality, which asks a similar question for compact Lie groups. He also gave a more concrete description of $\text{Cl}_{\mathbb{Z}}(\Gamma)$:

$$\text{Cl}_{\mathbb{Z}}(\Gamma) = \{g \in \hat{\Gamma} \mid \hat{\rho}(g)(V) = V, \forall (\rho, V) \in \text{Mod}_{\mathbb{Z}}(\Gamma)\}. \quad (0-1)$$

Here $\hat{\rho}$ is the continuous extension $\hat{\rho}: \hat{\Gamma} \rightarrow \text{Aut}(\hat{V})$ of the original representation $\rho: \Gamma \rightarrow \text{Aut}(V)$.

However, it is also shown in [Lubotzky 1980], that the answer to Question 0.4 is negative. The counterexamples provided there are the arithmetic groups for which the weak congruence subgroup property holds but not the strict one, i.e., the congruence kernel is finite but nontrivial. It was conjectured in [Lubotzky 1980, Conjecture A, page 184], that for an arithmetic group Γ , $\text{Cl}_{\mathbb{Z}}(\Gamma) = \Gamma$ if and only if Γ has the (strict) congruence subgroup property. The conjecture was left open even for $\Gamma = \text{SL}_2(\mathbb{Z})$.

In the almost 40 years since [Lubotzky 1980] was written various counterexamples were given to Question 0.3 [Platonov and Tavgen 1986; Bass and Lubotzky 2000; Bridson and Grunewald 2004; Pyber 2004] which also give counterexamples to Question 0.4, but it was not even settled whether $\text{Cl}_{\mathbb{Z}}(F) = F$ for finitely generated nonabelian free groups F .

We can now answer this and, in fact, prove the following surprising result, which gives an essentially complete answer to Question 0.4.

Theorem 0.5. *Let Γ be a finitely generated subgroup of $\text{GL}_n(\mathbb{Z})$. Then Γ satisfies Grothendieck–Tannaka duality, i.e., $\text{Cl}_{\mathbb{Z}}(\Gamma) = \Gamma$ if and only if Γ has the congruence subgroup property i.e., for some (and consequently for every) faithful representation $\Gamma \rightarrow \text{GL}_m(\mathbb{Z})$ such that the Zariski closure G of Γ is essentially simply connected, every finite index subgroup of Γ is closed in the congruence topology of $\text{GL}_n(\mathbb{Z})$. In such a case, the image of the group Γ in the semisimple (simply connected) quotient G/R is a congruence arithmetic group.*

The theorem is surprising as it shows that the cases proved by Grothendieck himself (which motivated him to suggest that the duality holds in general) are essentially the only cases where this duality holds.

Let us note that the assumption on G is not really restrictive. In Lemma 3.5, we show that for every $\Gamma \leq \text{GL}_n(\mathbb{Z})$ we can find an “over” representation of Γ into $\text{GL}_m(\mathbb{Z})$ (for some m) whose Zariski closure is essentially simply connected.

Theorem 0.5 implies Conjecture A of [Lubotzky 1980].

Corollary 0.6. *If G is a simply connected semisimple \mathbb{Q} -algebraic group, and Γ a congruence subgroup of $G(\mathbb{Q})$, then $\text{Cl}_{\mathbb{Z}}(\Gamma) = \Gamma$ if and only if Γ satisfies the (strict) congruence subgroup property.*

In particular:

Corollary 0.7. *$\text{Cl}_{\mathbb{Z}}(F) \neq F$ for every finitely generated free group on at least two generators; furthermore, $\text{Cl}_{\mathbb{Z}}(\text{SL}_2(\mathbb{Z})) \neq \text{SL}_2(\mathbb{Z})$.*

In fact, it will follow from our results that $\text{Cl}_{\mathbb{Z}}(F)$ is uncountable.

Before moving on to the last application, let us say a few words about how Proposition 0.1 helps to prove a result like Theorem 0.5. The description of $\text{Cl}_{\mathbb{Z}}(\Gamma)$ as in (0-1) implies that

$$\text{Cl}_{\mathbb{Z}}(\Gamma) = \varprojlim_{\rho} \overline{\rho(\Gamma)} \quad (0-2)$$

where the limit is over all (ρ, V) , where V is a finitely generated abelian group, ρ a representation $\rho: \Gamma \rightarrow \text{Aut}(V)$ and $\overline{\rho(\Gamma)} = \hat{\rho}(\hat{\Gamma}) \cap \text{Aut}(V) \subseteq \text{Aut}(\hat{V})$. This is an inverse limit of countable discrete groups, so one can not say much about it unless the connecting homomorphisms are surjective, which is, in general, not the case. Now, $\overline{\rho(\Gamma)}$ is the congruence closure of $\rho(\Gamma)$ in $\text{Aut}(V)$ and Proposition 0.1 shows that the corresponding maps are “almost” onto, and are even surjective if the modules V are what we call here “simply connected representations”, namely those cases where V is torsion free (and hence isomorphic to \mathbb{Z}^n for some n) and the Zariski closure of $\rho(\Gamma)$ in $\text{Aut}(\mathbb{C} \otimes_{\mathbb{Z}} V) = \text{GL}_n(\mathbb{C})$ is essentially simply connected. We show further that the category $\text{Mod}_{\mathbb{Z}}(\Gamma)$ is “saturated” with such modules (see Lemma 3.5) and we deduce that one can compute $\text{Cl}_{\mathbb{Z}}(\Gamma)$ as in (0-1) by considering only simply connected representations. We can then use Proposition 0.1(b), and get a fairly good understanding of $\text{Cl}_{\mathbb{Z}}(\Gamma)$. This enables us to prove Theorem 0.5. In addition, we also deduce:

Corollary 0.8. *If (ρ, V) is a simply connected representation, then the induced map $\text{Cl}_{\mathbb{Z}}(\Gamma) \rightarrow \text{Aut}(V)$ is onto $\text{Cl}_{\rho}(\Gamma) := \overline{\rho(\Gamma)}$ — the congruence closure of Γ .*

From Corollary 0.8 we can deduce our last application.

Thin groups. In recent years, following [Sarnak 2014] (see also [Kontorovich et al. 2019]), there has been a lot of interest in the distinction between thin subgroups and arithmetic subgroups of algebraic groups. Let us recall:

Definition 0.9. A subgroup $\Gamma \leq \text{GL}_n(\mathbb{Z})$ is called *thin* if it is of infinite index in $G \cap \text{GL}_n(\mathbb{Z})$, when G is its Zariski closure in GL_n . For a general group Γ , we will say that it is a *thin group* (or it *has a thin representation*) if for some n there exists a representation $\rho: \Gamma \rightarrow \text{GL}_n(\mathbb{Z})$ for which $\rho(\Gamma)$ is thin.

During the last five decades a lot of attention was given to the study of arithmetic groups, with many remarkable results, especially for those of higher rank (see [Margulis 1991; Platonov and Rapinchuk 1994]). Much less is known about thin groups. For example, it is not known if there exists a thin group with property (T) . Also, given a subgroup of an arithmetic group (say, given by a set of generators) it is difficult to decide whether it is thin or arithmetic (i.e., of finite or infinite index in its integral Zariski closure).

It is therefore of interest and perhaps even surprising that our results enable us to give a purely group theoretical characterization of thin groups $\Gamma \subset \text{GL}_n(\mathbb{Z})$. Before stating the precise result, we make the topology on $\text{Cl}_{\mathbb{Z}}(\Gamma)$ explicit. If we take the class of simply connected representations (ρ, V) for computing the group $\text{Cl}_{\mathbb{Z}}(\Gamma)$, one can then show that $\text{Cl}_{\mathbb{Z}}(\Gamma)/\Gamma$ is a *closed* subspace of the product $\prod_{\rho} (\text{Cl}_{\rho}(\Gamma)/\Gamma)$, where each $\text{Cl}_{\rho}(\Gamma)/\Gamma$ is given the discrete topology. This is the topology on the quotient space $\text{Cl}_{\mathbb{Z}}(\Gamma)/\Gamma$ in the following theorem. We can now state:

Theorem 0.10. *Let Γ be finitely generated \mathbb{Z} -linear group. Then Γ is a thin group if and only if it satisfies (at least) one of the following conditions:*

- (1) Γ is not FAb (namely, it does not have a finite index subgroup with an infinite abelianization).
- (2) $\text{Cl}_{\mathbb{Z}}(\Gamma)/\Gamma$ is not compact.

Warning. There are groups Γ which can be realized both as arithmetic groups as well as thin groups. For example, the free group is an arithmetic subgroup of $\text{SL}_2(\mathbb{Z})$, but at the same time a thin subgroup of every semisimple group, by a well-known result of Tits [1972]. In our terminology this is a thin group.

Remark 0.11. In the present paper, we have concentrated only on \mathbb{Z} modules which are Γ modules, and we have assumed that $\Gamma \subset \text{SL}_n(\mathbb{Z})$ for some n , so Γ is either a \mathbb{Q} -arithmetic group or a thin subgroup of such. Note that if \mathbb{Z} is replaced by \mathcal{O} — the ring of integers in a number field K — then by restriction of scalars every arithmetic subgroup of a K -algebraic group is commensurable to such one over \mathbb{Q} , so there is no loss of generality here. Moreover, the ring \mathbb{Z} can be replaced by the ring of S -integers \mathcal{O}_S , S is a finite set of places including all the archimedean ones and \mathcal{O}_S is the subring of K consisting of elements x in K such that for every (finite) place $v \notin S$ of K , x lies in the maximal compact subring \mathcal{O}_v of K_v (K_v is the completion of K at the place v). To be precise, one can consider finitely generated \mathcal{O}_S modules (in place of \mathbb{Z} modules) which are Γ modules, and one assumes that $\Gamma \subset \text{SL}_n(\mathcal{O}_S)$ i.e., Γ is a subgroup of an S -arithmetic group. One can then talk of the \mathcal{O}_S -closure $\text{Cl}_{\mathcal{O}_S}(\Gamma)$. The statements and proofs are almost identical, if notationally more tedious and hence we do not wish to pursue this further.

Note however, that one should not “mix between rings”, for example, if $\Gamma = \text{SL}_n(\mathbb{Z}[\frac{1}{p}])$, $n \geq 2$, p a prime, then $\text{Cl}_{\mathbb{Z}[1/p]}(\Gamma) = \Gamma$ as Γ satisfies the congruence subgroup property (CSP). But

$$\text{Cl}_{\mathbb{Z}}(\Gamma) = \hat{\Gamma} = \text{SL}_n(\widehat{\mathbb{Z}[\frac{1}{p}]}) = \prod_{q \neq p} \text{SL}_n(\mathbb{Z}_q),$$

since every representation of Γ on a finitely generated \mathbb{Z} -module factors through a finite quotient.

Notation 0.12. Throughout the paper, if W is a finitely generated \mathbb{Z} module, we denote by $W_{\mathbb{Q}}$ and $W_{\mathbb{C}}$ the \mathbb{Q} vector space $W \otimes_{\mathbb{Z}} \mathbb{Q}$ and the \mathbb{C} vector space $W \otimes_{\mathbb{Z}} \mathbb{C}$, respectively. If $\Gamma \subset \text{GL}(W)$, and G denotes the Zariski closure of Γ in $\text{GL}(W_{\mathbb{C}})$, then G acts on $W_{\mathbb{C}}$. The Zariski closure G is an algebraic group defined over \mathbb{Q} with respect to the \mathbb{Q} structure on $W_{\mathbb{C}} = W_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}$. It is well-known that $G(\mathbb{Q})$ is Zariski dense in G and $G(\mathbb{Q})$ acts on $W_{\mathbb{Q}}$. The action of G on $W_{\mathbb{C}}$ is completely determined by the action of $G(\mathbb{Q})$ on $W_{\mathbb{Q}}$. For these reasons, we do not distinguish between G acting on $W_{\mathbb{C}}$ and $G(\mathbb{Q})$ (by a mild abuse of notation, denoted G) acting on $W_{\mathbb{Q}}$.

1. Preliminaries on algebraic groups over \mathbb{Q}

We recall the definition of an essentially simply connected group.

Definition 1.1. Let G be a linear algebraic group over \mathbb{C} with maximal connected normal solvable subgroup R (i.e., the radical of G) and identity component G^0 . We say that G is *essentially simply connected* if the semisimple part $G^0/R = H$ is a simply connected.

Note that G is essentially simply connected if and only if, the quotient G^0/U of the group G^0 by its unipotent radical U is a product $H_{ss} \times S$ with H_{ss} simply connected and semisimple, and S is a torus.

For example, a semisimple connected group is essentially simply connected if and only if it is simply connected. The group $\mathbb{G}_m \times \mathrm{SL}_n$ is essentially simply connected; however, the radical of the group GL_n is the group R of scalars and $\mathrm{GL}_n/R = \mathrm{SL}_n/\text{center}$, so GL_n is *not* essentially simply connected. We will show later (Lemma 1.3(iii)) that every group has a finite cover which is essentially simply connected.

Lemma 1.2. *Suppose $G \subset G_1 \times G_2$ is a subgroup of a product of two essentially simply connected linear algebraic groups G_1, G_2 over \mathbb{C} ; suppose that the projection π_i of G to G_i is surjective for $i = 1, 2$. Then G is also essentially simply connected.*

Proof. Assume, as we may, that G is connected. Let R be the radical of G . The projection of R to G_i is normal in G_i since $\pi_i: G \rightarrow G_i$ is surjective. Moreover, $G_i/\pi_i(R)$ is the image of the semisimple group G/R ; the latter has a Zariski dense compact subgroup, hence so does $G_i/\pi_i(R)$; therefore, $G_i/\pi_i(R)$ is reductive and is its own commutator. Hence $G_i/\pi_i(R)$ is semisimple and hence $\pi_i(R) = R_i$ where R_i is the radical of G_i . Let $R^* = G \cap (R_1 \times R_2)$. Since $R_1 \times R_2$ is the radical of $G_1 \times G_2$, it follows that R^* is a solvable normal subgroup of G and hence its connected component is contained in R . Since $R \subseteq R_1 \times R_2$, it follows that R is precisely the connected component of the identity of R^* . We then have the inclusion $G/R^* \subset G_1/R_1 \times G_2/R_2$ with projections again being surjective.

By assumption, each $G_i/R_i = H_i$ is semisimple, simply connected. Moreover $G/R^* = H$ where H is connected, semisimple. Thus we have the inclusion $H \subset H_1 \times H_2$. Now, $H \subset H_1 \times H_2$ is such that the projections of H to H_i are surjective, and each H_i is simply connected. Let K be the kernel of the map $H \rightarrow H_1$ and K^0 its identity component. Then $H/K^0 \rightarrow H_1$ is a surjective map of connected algebraic groups with finite kernel. The simple connectedness of H_1 then implies that $H/K^0 = H_1$ and hence that $K = K^0 \subset \{1\} \times H_2$ is normal in H_2 .

Write $H_2 = F_1 \times \cdots \times F_t$ where each F_i is *simple* and simply connected. Now, K being a closed normal subgroup of H_2 must be equal to $\prod_{i \in X} F_i$ for some subset X of $\{1, \dots, t\}$, and is simply connected. Therefore, $K = K^0$ is simply connected.

From the preceding two paragraphs, we have that both H/K and K are simply connected, and hence so is $H = G/R^*$. Since R is the connected component of R^* and G/R^* is simply connected, it follows that $G/R = G/R^*$ and hence G/R is simply connected. This completes the proof of the lemma. \square

Arithmetic groups and congruence subgroups. In the introduction, we defined the notion of arithmetic and congruence subgroup of $G(\mathbb{Q})$ using the adelic language. One can define the notion of arithmetic

and congruence groups in more concrete terms as follows. Given a linear algebraic group $G \subset \mathrm{SL}_n$ defined over \mathbb{Q} , we will say that a subgroup $\Gamma \subset G(\mathbb{Q})$ is an *arithmetic group* if it is commensurable to $G \cap \mathrm{SL}_n(\mathbb{Z}) = G(\mathbb{Z})$; that is, the intersection $\Gamma \cap G(\mathbb{Z})$ has finite index both in Γ and in $G(\mathbb{Z})$. It is well known that the notion of an arithmetic group does not depend on the specific linear embedding $G \subset \mathrm{SL}_n$. As in [Serre 1968], we may define the *arithmetic completion* \hat{G} of $G(\mathbb{Q})$ as the completion of the group $G(\mathbb{Q})$ with respect to the topology on $G(\mathbb{Q})$ as a topological group, obtained by designating arithmetic groups as a fundamental systems of neighborhoods of identity in $G(\mathbb{Q})$.

Given $G \subset \mathrm{SL}_n$ as in the preceding paragraph, we will say that an arithmetic group $\Gamma \subset G(\mathbb{Q})$ is a *congruence subgroup* if there exists an integer $m \geq 2$ such that Γ contains the “principal congruence subgroup” $G(m\mathbb{Z}) = \mathrm{SL}_n(m\mathbb{Z}) \cap G$ where $\mathrm{SL}_n(m\mathbb{Z})$ is the kernel to the residue class map $\mathrm{SL}_n(\mathbb{Z}) \rightarrow \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$. We then get the structure of a topological group on the group $G(\mathbb{Q})$ by designating congruence subgroups of $G(\mathbb{Q})$ as a fundamental system of neighborhoods of identity. The completion of $G(\mathbb{Q})$ with respect to this topology, is denoted \bar{G} . Again, the notion of a congruence subgroup does not depend on the specific linear \mathbb{Q} -embedding $G \rightarrow \mathrm{SL}_n$.

Since every congruence subgroup is an arithmetic group, there exists a map from $\pi : \hat{G} \rightarrow \bar{G}$ which is easily seen to be surjective, and the kernel $C(G)$ of π is a compact profinite subgroup of \hat{G} . This is called the *congruence subgroup kernel*. One says that $G(\mathbb{Q})$ has the *congruence subgroup property* if $C(G)$ is trivial. This is easily seen to be equivalent to the statement that every arithmetic subgroup of $G(\mathbb{Q})$ is a congruence subgroup.

It is known (see page 108, last but one paragraph of [Raghunathan 1976] or [Chahal 1980]) that solvable groups G have the congruence subgroup property.

Moreover, every solvable subgroup of $\mathrm{GL}_n(\mathbb{Z})$ is polycyclic. In such a group, every subgroup is intersection of finite index subgroups. So every solvable subgroup of an arithmetic group is congruence closed. We will use these facts frequently in the sequel.

Another (equivalent) way of viewing the congruence completion is (see [Serre 1968, page 276, Remarque]) as follows: let \mathbb{A}_f be the ring of finite adeles over \mathbb{Q} , equipped with the standard adelic topology and let $\mathbb{Z}_f \subset \mathbb{A}_f$ be the closure of \mathbb{Z} . Then the group $G(\mathbb{A}_f)$ is also a locally compact group and contains the group $G(\mathbb{Q})$. The congruence completion \bar{G} of $G(\mathbb{Q})$ may be viewed as the closure of $G(\mathbb{Q})$ in $G(\mathbb{A}_f)$.

Lemma 1.3. *Let H and H^* be linear algebraic groups defined over \mathbb{Q} .*

- (i) *Suppose $\pi : H^* \rightarrow H$ is a surjective \mathbb{Q} -morphism. Let $(\rho, W_{\mathbb{Q}})$ be a representation of H defined over \mathbb{Q} . Then there exists a faithful \mathbb{Q} -representation $(\tau, V_{\mathbb{Q}})$ of H^* such that $(\rho \circ \pi, W_{\mathbb{Q}})$ is a subrepresentation of $(\tau, V_{\mathbb{Q}})$.*
- (ii) *If $H^* \rightarrow H$ is a surjective map defined over \mathbb{Q} , then the image of an arithmetic subgroup of H^* under the map $H^* \rightarrow H$ is an arithmetic subgroup of H .*
- (iii) *If H is connected, then there exists a connected essentially simply connected algebraic group H^* with a surjective \mathbb{Q} -defined homomorphism $H^* \rightarrow H$ with finite kernel.*

(iv) *If $H^* \rightarrow H$ is a surjective homomorphism of algebraic \mathbb{Q} -groups which are essentially simply connected, then the image of a congruence subgroup of $H^*(\mathbb{Q})$ is a congruence subgroup of $H(\mathbb{Q})$.*

Proof. Let $\theta: H^* \rightarrow \text{GL}(E)$ be a faithful representation of the linear algebraic group H^* defined over \mathbb{Q} and $\tau = \rho \oplus \theta$ as H^* -representation. Clearly τ is faithful for H^* and contains ρ . This proves (i).

Part (ii) is the statement of Theorem (4.1) of [Platonov and Rapinchuk 1994].

We now prove (iii). Write $H = RG$ as a product of its radical R and a semisimple group G . Let $H_{\text{ss}}^* \rightarrow G$ be the simply connected cover of G . Hence H_{ss}^* acts on R through G , via this covering map. Define $H^* = R \rtimes H_{\text{ss}}^*$ as a semidirect product. Clearly, the map $H^* \rightarrow H$ has finite kernel and satisfies the properties of (iii).

To prove (iv), we may assume that H and H^* are connected. If U^* and U are the unipotent radicals of H^* and H , the assumptions of (iv) do not change for the quotient groups H^*/U^* and H/U . Moreover, since H^* is the semidirect product of U^* and H^*/U^* (and similarly for H and U) and the unipotent \mathbb{Q} -algebraic group U has the congruence subgroup property, it suffices to prove (iv) when both H^* and H are reductive. By assumption, H^* and H are essentially simply connected; i.e., $H^* = H_{\text{ss}}^* \times S^*$ and $H = H_{\text{ss}} \times S$ where S, S^* are tori and $H_{\text{ss}}^*, H_{\text{ss}}$ are simply connected semisimple groups. Thus we have connected reductive \mathbb{Q} -groups H^*, H with a surjective map such that their derived groups are simply connected (and semisimple), and the abelianization $(H^*)^{\text{ab}}$ is a torus (similarly for H).

Now, $[H^*, H^*] = H_{\text{ss}}^*$ is a simply connected semisimple group and hence it is a product $F_1 \times \cdots \times F_s$ of simply connected \mathbb{Q} -simple algebraic groups F_i . Being a factor of $[H^*, H^*] = H_{\text{ss}}^*$, the group $[H, H] = H_{\text{ss}}$ is a product of a (smaller) number of these F_i 's. After a renumbering of the indices, we may assume that H_{ss} is a product $F_1 \times \cdots \times F_r$ for some $r \leq s$ and the map π on H_{ss}^* is the projection to the first r factors. Hence the image of a congruence subgroup of H_{ss}^* is a congruence subgroup of H_{ss} .

The tori S^* and S have the congruence subgroup property by a result of Chevalley (as already stated at the beginning of this section, this is true for all solvable algebraic groups). Hence the image of a congruence subgroup of S^* is a congruence subgroup of S . We thus need only prove that every subgroup of the reductive group H of the form $\Gamma_1\Gamma_2$, where $\Gamma_1 \subset H_{\text{ss}}$ and $\Gamma_2 \subset S$ are congruence subgroups, is itself a congruence subgroup of H . We use the adelic form of the congruence topology. Suppose K is a compact open subgroup of the $H(\mathbb{A}_f)$ where \mathbb{A}_f is the ring of finite adeles. The image of $H(\mathbb{Q}) \cap K$ under the quotient map $H \rightarrow H^{\text{ab}} = S$ is a congruence subgroup in the torus S and hence $H(\mathbb{Q}) \cap K' \subset (H_{\text{ss}}(\mathbb{Q}) \cap K)(S(\mathbb{Q}) \cap K)$ for some possibly smaller open subgroup $K' \subset H(\mathbb{A}_f)$. This proves (iv). □

Note that part (iii) and (iv) prove Proposition 0.1(ii).

2. The arithmetic Chevalley theorem

In this section, we prove Proposition 0.1(i). Assume that $\varphi: G_1 \rightarrow G_2$ is a surjective morphism of \mathbb{Q} -algebraic groups. We are to prove that $\varphi(\Gamma^0)$ contains the commutator subgroup of a congruence subgroup of $G_2(\mathbb{Q})$ containing it.

Before starting on the proof, let us note that in general, the image of a congruence subgroup of $G_1(\mathbb{Z})$ under φ need not be a congruence subgroup of $G_2(\mathbb{Z})$. The following proposition gives a fairly general situation when this happens.

Proposition 2.1. *Let $\pi : G_1 \rightarrow G_2$ be a finite covering of semisimple algebraic groups defined over \mathbb{Q} with G_1 simply connected and G_2 not. Assume $G_1(\mathbb{Q})$ is dense in $G_1(\mathbb{A}_f)$. Write K for the kernel of π and K_f for the kernel of the map $G_1(\mathbb{A}_f) \rightarrow G_2(\mathbb{A}_f)$. Let Γ be a congruence subgroup of $G_1(\mathbb{Q})$ and H its closure in $G_1(\mathbb{A}_f)$. Then the image $\pi(\Gamma) \subset G_2(\mathbb{Q})$ is a congruence subgroup if and only if $KH \supset K_f$.*

Before proving the proposition, let us note that while K is finite, the group K_f is a product of infinitely many finite abelian groups and that K_f is central in \overline{G}_1 . This implies:

Corollary 2.2. (i) *There are infinitely many congruence subgroups Γ_i with $\pi(\Gamma_i)$ noncongruence subgroups of unbounded finite index in their congruence closures $\overline{\Gamma}_i$.*

(ii) *For each of these $\Gamma = \Gamma_i$, the image $\pi(\Gamma)$ contains the commutator subgroup $[\overline{\Gamma}, \overline{\Gamma}]$ and is normal in $\overline{\Gamma}$ (with abelian quotient).*

We now prove Proposition 2.1.

Proof. Let G_3 be the image of the rational points of $G_1(\mathbb{Q})$:

$$G_3 = \pi(G_1(\mathbb{Q})) \subset G_2(\mathbb{Q}).$$

Define a subgroup Δ of G_3 to be a *quasicongruence subgroup* if the inverse image $\pi^{-1}(\Delta)$ is a congruence subgroup of $G_1(\mathbb{Q})$. Note that the quasicongruence subgroups of G_3 are exactly the images of congruence subgroups of $G_1(\mathbb{Q})$ by π . It is routine to check that by declaring quasicongruence subgroups to be open, we get the structure of a topological group on G_3 . This topology is weaker or equal to the arithmetic topology on G_3 . However, it is strictly stronger than the congruence topology on G_3 . The last assertion follows from the fact that the completion of $G_3 = G_1(\mathbb{Q})/K(\mathbb{Q})$ is the quotient \overline{G}_1/K where \overline{G}_1 is the congruence completion of $G_1(\mathbb{Q})$, whereas the completion of G_3 with respect to the congruence topology is \overline{G}_1/K_f .

Now let $\Gamma \subset G_1(\mathbb{Q})$ be a congruence subgroup and $\Delta_1 = \pi(\Gamma)$; let Δ_2 be its congruence closure in G_3 . Then both Δ_1 and Δ_2 are open in the quasicongruence topology on G_3 . Denote by G_3^* the completion of G_3 with respect to the quasicongruence topology, so $G_3^* = \overline{G}_1/K$ and denote by Δ_1^*, Δ_2^* the closures of Δ_1, Δ_2 in G_3^* . We then have the equalities

$$\Delta_2/\Delta_1 = \Delta_2^*/\Delta_1^*, \quad \Delta_2^* = \Delta_1^*K_f/K.$$

Hence $\Delta_1^* = \Delta_2^*$ if and only if $K\Delta_1^* \supset K_f$. This proves Proposition 2.1.

The proof shows that Δ_1^* is normal in Δ_2^* (since K_f is central) with abelian quotient. The same is true for Δ_1 in Δ_2 and the corollary is also proved. □

To continue with the proof of Proposition 0.1, assume, as we may (by replacing G_1 with the Zariski closure of Γ), that G_1 has no characters defined over \mathbb{Q} . For, suppose that G_1 is the Zariski closure of

$\Gamma \subset G_1(\mathbb{Z})$. Let $\chi: G_1 \rightarrow \mathbb{G}_m$ be a nontrivial (and therefore surjective) homomorphism defined over \mathbb{Q} ; then the image of the arithmetic group $G_1(\mathbb{Z})$ in $\mathbb{G}_m(\mathbb{Q})$ is a Zariski dense arithmetic group. However, the only arithmetic groups in $\mathbb{G}_m(\mathbb{Q})$ are finite and cannot be Zariski dense in \mathbb{G}_m . Therefore, χ cannot be nontrivial. We can also assume that G_1 is connected.

We start by proving Proposition 0.1 for the case that Γ is a congruence subgroup.

If we write $G_1 = R_1 H_1$ where H_1 is semisimple and R_1 is the radical, we may assume that G_1 is essentially simply connected (Lemma 1.3(iii)), without affecting the hypotheses or the conclusion of Proposition 0.1.

Hence $G_1 = R_1 \rtimes H_1$ is a semidirect product. Then clearly, every congruence subgroup of G_1 contains a congruence subgroup of the form $\Delta \rtimes \Phi$ where $\Delta \subset R_1$ and $\Phi \subset H_1$ are congruence subgroups. Similarly, write $G_2 = R_2 H_2$. Since φ is easily seen to map R_1 onto R_2 and H_1 onto H_2 , it is enough to prove the proposition for R_1 and H_1 separately.

We first recall that if G is a solvable linear algebraic group defined over \mathbb{Q} then the congruence subgroup property holds for G , i.e., every arithmetic subgroup of G is a congruence subgroup (for a reference see page 108, last but one paragraph of [Raghunathan 1976] or [Chahal 1980]). Consequently, by Lemma 1.3(ii), the image of a congruence subgroup in R_1 is an arithmetic group in R_2 and hence a congruence subgroup. Thus we dispose of the solvable case.

In the case of semisimple groups, denote by H_2^* by the simply connected cover of H_2 . The map $\varphi: H_1 \rightarrow H_2$ lifts to a map from H_1 to H_2^* . For simply connected semisimple groups, a surjective map from H_1 to H_2^* sends a congruence subgroup to a congruence subgroup by Lemma 1.3(iv).

We are thus reduced to the situation $H_1 = H_2^*$ and $\varphi: H_1 \rightarrow H_2$ is the simply connected cover of H_2 .

By our assumptions, H_1 is now connected, simply connected and semisimple. We claim that for any nontrivial \mathbb{Q} -simple factor L of H_1 , $L(\mathbb{R})$ is not compact. Otherwise, the image of Γ , the arithmetic group, there is finite and as Γ is Zariski dense, so H_1 is not connected. The strong approximation theorem [Platonov and Rapinchuk 1994, Theorem 7.12] gives now that $H_1(\mathbb{Q})$ is dense in $H_1(\mathbb{A}_f)$. So Proposition 2.1 can be applied to finish the proof of Proposition 0.1 in the case Γ is a congruence subgroup.

We need to show that it is true also for the more general case when Γ is only congruence closed. To this end let us formulate the following proposition which is of independent interest.

Proposition 2.3. *Let $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Z})$, G its Zariski closure and $\mathrm{Der} = [G^0, G^0]$. Then Γ is congruence closed if and only if $\Gamma \cap \mathrm{Der}$ is a congruence subgroup of Der .*

Proof. If G^0 has no toral factors, this is proved in [Venkataramana 1999], in fact, in this case a congruence closed Zariski dense subgroup is a congruence subgroup. (Note that this is stated there for general G , but the assumption that there is no toral factor was mistakenly omitted as the proof there shows.)

Now, if there is a toral factor, we can assume G is connected, so $G^{\mathrm{ab}} = V \times S$ where V is unipotent and S a torus. Now $\Gamma \cap [G, G]$ is Zariski dense and congruence closed, so it is a congruence subgroup by [Venkataramana 1999] as before. For the other direction, note that the image of Γ is $U \times S$, being solvable, is always congruence closed, so the proposition follows. \square

Now, we can end the proof of Proposition 0.1 for congruence closed subgroups by looking at φ on $G_3 = \bar{\Gamma}$ the Zariski closure of Γ and apply the proof above to $\text{Der}(G_3^0)$. It also proves Proposition 0.2.

Of course, Proposition 2.3 is the general form of the following result from [Venkataramana 1999] (based on [Nori 1987; Weisfeiler 1984]), which is, in fact, the core of Proposition 2.3.

Proposition 2.4. *Suppose $\Gamma \subset G(\mathbb{Z})$ is Zariski dense, G simply connected and Γ a subgroup of $G(\mathbb{Z})$ which is closed in the congruence topology. Then Γ is itself a congruence subgroup.*

3. The Grothendieck closure

The Grothendieck closure of a group Γ .

Definition 3.1. Let $\rho: \Gamma \rightarrow \text{GL}(V)$ be a representation of Γ on a lattice V in a \mathbb{Q} -vector space $V \otimes \mathbb{Q}$. Then we get a continuous homomorphism $\hat{\rho}: \hat{\Gamma} \rightarrow \text{GL}(\hat{V})$ (where, for a group Δ , $\hat{\Delta}$ denotes its profinite completion) which extends ρ .

Denote by $\text{Cl}_\rho(\Gamma)$ the subgroup of the profinite completion of Γ , which preserves the lattice V : $\text{Cl}_\rho(\Gamma) = \{g \in \hat{\Gamma} : \hat{\rho}(g)(V) \subset V\}$. In fact, since $\det(\hat{\rho}(g)) = \pm 1$ for every $g \in \Gamma$ and hence also for every $g \in \hat{\Gamma}$, for $g \in \text{Cl}_\rho(\Gamma)$, $\hat{\rho}(g)(V) = V$, and hence $\text{Cl}_\rho(\Gamma)$ is a subgroup of $\hat{\Gamma}$. We denote by $\text{Cl}(\Gamma)$ the subgroup

$$\text{Cl}(\Gamma) = \{g \in \hat{\Gamma} : \hat{\rho}(g)(V) \subset V \forall \text{ lattices } V\}. \tag{3-1}$$

Therefore, $\text{Cl}(\Gamma) = \bigcap_\rho \text{Cl}_\rho(\Gamma)$ where ρ runs through all integral representations of the group Γ .

Suppose now that V is any finitely generated abelian group (not necessarily a lattice i.e., not necessarily torsion-free) which is also a Γ -module. Then the torsion in V is a (finite) subgroup with finite exponent n say. Then nV is torsion free. Since Γ acts on the finite group V/nV by a finite group via, say, ρ , it follows that $\hat{\Gamma}$ also acts on the finite group V/nV via $\hat{\rho}$. Thus, for $g \in \hat{\Gamma}$ we have $\hat{\rho}(g)(V/nV) = V/nV$. Suppose now that $g \in \text{Cl}(\Gamma)$. Then $g(nV) = nV$ by the definition of $\text{Cl}(\Gamma)$. Hence $g(V)/nV = V/nV$ for $g \in \text{Cl}(\Gamma)$. This is an equality in the quotient group \hat{V}/nV . This shows that $g(V) \subset V + nV = V$ which shows that $\text{Cl}(\Gamma)$ preserves *all* finitely generated abelian groups V which are Γ -modules.

By $\text{Cl}_{\mathbb{Z}}(\Gamma)$ we mean the *Grothendieck closure* of the (finitely generated) group Γ . It is essentially a result of [Lubotzky 1980] that the Grothendieck closure $\text{Cl}_{\mathbb{Z}}(\Gamma)$ is the same as the group $\text{Cl}(\Gamma)$ defined above (in [loc. cit.], the group considered was the closure with respect to *all* finitely generated \mathbb{Z} modules which are also Γ modules, whereas we consider only those finitely generated \mathbb{Z} modules which are Γ modules and which are torsion-free; the argument of the preceding paragraph shows that these closures are the same). From now on, we identify the Grothendieck closure $\text{Cl}_{\mathbb{Z}}(\Gamma)$ with the foregoing group $\text{Cl}(\Gamma)$.

Notation. Let Γ be a group, V a finitely generated torsion-free abelian group which is a Γ -module and $\rho: \Gamma \rightarrow \text{GL}(V)$ the corresponding Γ -action. Denote by G_ρ the Zariski closure of the image $\rho(\Gamma)$ in $\text{GL}(V \otimes \mathbb{Q})$, and G_ρ^0 its connected component of identity. Then both G_ρ, G_ρ^0 are linear algebraic groups defined over \mathbb{Q} , and so is $\text{Der}_\rho = [G_\rho^0, G_\rho^0]$.

Let $B = B_\rho(\Gamma)$ denote the subgroup $\hat{\rho}(\hat{\Gamma}) \cap \text{GL}(V)$. Since the profinite topology of $\text{GL}(\hat{V})$ induces the congruence topology on $\text{GL}(V)$, $B_\rho(\Gamma)$ is the congruence closure of $\rho(\Gamma)$ in $\text{GL}(V)$.

We denote by $D = D_\rho(\Gamma)$ the intersection of B with the derived subgroup $\text{Der}_\rho = [G^0, G^0]$. We thus have an exact sequence

$$1 \rightarrow D \rightarrow B \rightarrow A \rightarrow 1,$$

where $A = A_\rho(\Gamma)$ is an extension of a finite group G/G^0 by an abelian group (the image of $B \cap G^0$ in the abelianization $(G^0)^{\text{ab}}$ of the connected component G^0).

Simply connected representations.

Definition 3.2. We will say that ρ is *simply connected* if the group $G = G_\rho$ is *essentially simply connected*. That is, if U is the unipotent radical of G , the quotient G^0/U is a product $H \times S$ where H is semisimple and simply connected and S is a torus.

An easy consequence of Lemma 1.2 is that simply connected representations are closed under direct sums.

Lemma 3.3. *Let ρ_1, ρ_2 be two simply connected representations of an abstract group Γ . Then the direct sum $\rho_1 \oplus \rho_2$ is also simply connected.*

We also have:

Lemma 3.4. *Let $\rho: \Gamma \rightarrow \text{GL}(W)$ be a subrepresentation of a representation $\tau: \Gamma \rightarrow \text{GL}(V)$ such that both ρ, τ are simply connected. Then the map $r: B_\tau(\Gamma) \rightarrow B_\rho(\Gamma)$ is surjective.*

Proof. The image of $B_\tau(\Gamma)$ in $B_\rho(\Gamma)$ contains the image of D_τ . By Proposition 2.3, D_τ is a congruence subgroup of the algebraic group Der_τ . The map $\text{Der}_\tau \rightarrow \text{Der}_\rho$ is a surjective map between simply connected groups. Therefore, by part (iv) of Lemma 1.3, the image of D_τ is a congruence subgroup F of D_ρ . Now, by Proposition 2.3, $D_\rho \cdot \rho(\Gamma)$ is congruence closed, hence equal to B_ρ which is the congruence closure of $\rho(\Gamma)$ and $B_\tau \rightarrow B_\rho$ is surjective. □

Simply connected to general.

Lemma 3.5. *Every (integral) representation $\rho: \Gamma \rightarrow \text{GL}(W)$ is a subrepresentation of a representation $\tau: \Gamma \rightarrow \text{GL}(V)$ where τ is simply connected.*

Proof. Let $\rho: \Gamma \rightarrow \text{GL}(W)$ be a representation. Let Der be the derived subgroup of the identity component of the Zariski closure $H = G_\rho$ of $\rho(\Gamma)$. Then, by Lemma 1.3(iii), there exists a map $H^* \rightarrow H^0$ with finite kernel such that H^* is connected and $H^*/U^* = (H^*)_{\text{ss}} \times S^*$ where H^*_{ss} is a simply connected semisimple group. Denote by $W_{\mathbb{Q}}$ the \mathbb{Q} -vector space $W \otimes \mathbb{Q}$. By Lemma 1.3(i), $\rho: H^0 \rightarrow \text{GL}(W_{\mathbb{Q}})$ may be considered as a subrepresentation of a faithful representation $(\theta, E_{\mathbb{Q}})$ of the covering group H^* .

By (ii) of Lemma 1.3, the image of an arithmetic subgroup of H^* is an arithmetic group of H . Moreover, as $H(\mathbb{Z})$ is virtually torsion free, one may choose a normal, torsion-free arithmetic subgroup $\Delta \subset H(\mathbb{Z})$

such that the map $H^* \rightarrow H^0$ splits over Δ . In particular, the map $H^* \rightarrow H^0$ splits over a normal subgroup N of Γ of finite index. Thus, θ may be considered as a representation of the group N .

Consider the induced representation $\text{Ind}_N^\Gamma(W_{\mathbb{Q}})$. Since $W_{\mathbb{Q}}$ is a representation of Γ , it follows that $\text{Ind}_N^\Gamma(W_{\mathbb{Q}}) = W_{\mathbb{Q}} \otimes \text{Ind}_N^\Gamma(\text{triv}_N) \supset W_{\mathbb{Q}}$. Since, by the first paragraph of this proof, $W_{\mathbb{Q}} \subset E_{\mathbb{Q}}$ as H^* modules, it follows that $W_{\mathbb{Q}}|_N \subset E_{\mathbb{Q}}$ and hence $W_{\mathbb{Q}} \subset \text{Ind}_N^\Gamma(E_{\mathbb{Q}}) =: V_{\mathbb{Q}}$. Write $\tau = \text{Ind}_N^\Gamma(E_{\mathbb{Q}})$ for the representation of Γ on $V_{\mathbb{Q}}$. The normality of N in Γ implies that the restriction representation $\tau|_N$ is contained in a direct sum of the N -representations $n \rightarrow \theta(\gamma n \gamma^{-1})$ as γ varies over the finite set Γ/N .

Write $G_{\theta|_N}$ for the Zariski closure of the image $\theta(N)$. Since $G_{\theta|_N}$ has H^* as its Zariski closure and the group H_{ss}^* is simply connected, each θ composed with conjugation by γ is a simply connected representation of N . It follows from Lemma 3.3 that $\tau|_N$ is simply connected. Since simple connectedness of a representation is the same for subgroups of finite index, it follows that τ , as a representation of Γ , is simply connected.

We have now proved that there exists Γ -equivariant embedding of the module $(\rho, W_{\mathbb{Q}})$ into $(\tau, V_{\mathbb{Q}})$ where W, V are lattices in the \mathbb{Q} -vector spaces $W_{\mathbb{Q}}, V_{\mathbb{Q}}$. A basis of the lattice W is then a \mathbb{Q} -linear combination of a basis of V ; the finite generation of W then implies that there exists an integer m such that $mW \subset V$, and this inclusion is an embedding of Γ -modules. Clearly, the module (ρ, W) is isomorphic to (ρ, mW) the isomorphism given by multiplication by m . Hence the lemma follows. \square

The following is the main technical result of this section, from which the main results of this paper are derived:

Proposition 3.6. *The group $\text{Cl}(\Gamma)$ is the inverse limit of the groups $B_\rho(\Gamma)$ where ρ runs through simply connected representations and $B_\rho(\Gamma)$ is the congruence closure of $\rho(\Gamma)$. Moreover, if $\rho: \Gamma \rightarrow \text{GL}(W)$ is simply connected, then the map $\text{Cl}(\Gamma) \rightarrow B_\rho(\Gamma)$ is surjective.*

Proof. Denote temporarily by $\text{Cl}(\Gamma)_{\text{sc}}$ the subgroup of elements of $\hat{\Gamma}$ which stabilize the lattice V for all simply connected representations (τ, V) . Let W be an arbitrary finitely generated torsion-free lattice which is also a Γ -module; denote by ρ the action of Γ on W .

By Lemma 3.5, there exists a simply connected representation (τ, V) which contains (ρ, W) . If $g \in \text{Cl}(\Gamma)_{\text{sc}}$, then $\hat{\tau}(g)(V) \subset V$; since Γ is dense in $\hat{\Gamma}$ and stabilizes W , it follows that for all $x \in \hat{\Gamma}$, $\hat{\tau}(x)(\hat{W}) \subset \hat{W}$; in particular, for $g \in \text{Cl}(\Gamma)_{\text{sc}}$, $\hat{\rho}(g)(W) = \hat{\tau}(g)(W) \subset \hat{W} \cap V = W$. Thus, $\text{Cl}(\Gamma)_{\text{sc}} \subset \text{Cl}(\Gamma)$.

The group $\text{Cl}(\Gamma)$ is, by definition, the set of all elements g of the profinite completion $\hat{\Gamma}$ which stabilize all Γ stable torsion free lattices. It follows in particular, that these elements g stabilize all Γ -stable lattices V associated to simply connected representations (τ, V) ; hence $\text{Cl}(\Gamma) \subset \text{Cl}(\Gamma)_{\text{sc}}$. The preceding paragraph now implies that $\text{Cl}(\Gamma) = \text{Cl}(\Gamma)_{\text{sc}}$. This proves the first part of the proposition (see (0-2)).

We can enumerate all the simply connected integral representations ρ , since Γ is finitely generated. Write $\rho_1, \rho_2, \dots, \rho_n \dots$, for the sequence of simply connected representations of Γ . Write τ_n for the direct sum $\rho_1 \oplus \rho_2 \oplus \dots \oplus \rho_n$. Then $\tau_n \subset \tau_{n+1}$ and by Lemma 3.3 each τ is simply connected; moreover, the simply connected representation ρ_n is contained in τ_n .

By Lemma 3.4, it follows that $\text{Cl}(\Gamma)$ is the inverse limit of the *totally ordered family* $B_{\tau_n}(\Gamma)$; moreover, $B_{\tau_{n+1}}(\Gamma)$ maps *onto* $B_{\tau_n}(\Gamma)$. By taking inverse limits, it follows that $\text{Cl}(\Gamma)$ maps *onto* the group $B_{\tau_n}(\Gamma)$ for every n . It follows, again from Lemma 3.4, that every $B_{\rho_n}(\Gamma)$ is a homomorphic image of $B_{\tau_n}(\Gamma)$ and hence of $\text{Cl}(\Gamma)$. This proves the second part of the proposition. \square

Definition 3.7. Let Γ be a finitely generated group. We say that Γ is FAb if the abelianization Δ^{ab} is finite for every finite index subgroup $\Delta \subset \Gamma$.

Corollary 3.8. *If Γ is FAb then for every simply connected representation ρ , the congruence closure $B_\rho(\Gamma)$ of $\rho(\Gamma)$ is a congruence subgroup and $\text{Cl}(\Gamma)$ is an inverse limit over a totally ordered set τ_n of simply connected representations of Γ , of congruence groups B_n in groups $G_n = G_{\tau_n}$ with G_n^0 simply connected. Moreover, the maps $B_{n+1} \rightarrow B_n$ are surjective. Hence the maps $\text{Cl}(\Gamma) \rightarrow B_n$ are all surjective.*

Proof. If $\rho: \Gamma \rightarrow \text{GL}(V)$ is a simply connected representation, then for a finite index subgroup Γ^0 the image $\rho(\Gamma^0)$ has connected Zariski closure, and by assumption, $G^0/U = H \times S$ where S is a torus and H is simply connected semisimple. Since the group Γ is FAb it follows that $S = 1$ and hence $G^0 = \text{Der}(G^0)$. Now Proposition 2.4 implies that $B_\rho(\Gamma)$ is a congruence subgroup of $G_\rho(V)$. The Corollary is now immediate from the Proposition 3.6. We take $B_n = B_{\tau_n}$ in the proof of the proposition. \square

We can now prove Theorem 0.5. Let us first prove the direction claiming that the congruence subgroup property implies $\text{Cl}(\Gamma) = \Gamma$. This was proved for arithmetic groups Γ by Grothendieck, and we follow here the proof in [Lubotzky 1980] which works for general Γ . Indeed, if $\rho: \Gamma \rightarrow \text{GL}_n(\mathbb{Z})$ is a faithful simply connected representation such that $\rho(\Gamma)$ satisfies the congruence subgroup property, then it means that the map $\hat{\rho}: \hat{\Gamma} \rightarrow \text{GL}_n(\hat{\mathbb{Z}})$ is injective. Now $\rho(\text{Cl}(\Gamma)) \subseteq \text{GL}_n(\mathbb{Z}) \cap \hat{\rho}(\hat{\Gamma})$, but the last is exactly the congruence closure of $\rho(\Gamma)$. By our assumption, $\rho(\Gamma)$ is congruence closed, so it is equal to $\rho(\Gamma)$. So in summary $\hat{\rho}(\Gamma) \subset \hat{\rho}(\text{Cl}(\Gamma)) \subseteq \rho(\Gamma) = \hat{\rho}(\Gamma)$. As $\hat{\rho}$ is injective, $\Gamma = \text{Cl}(\Gamma)$.

In the opposite direction, assume $\text{Cl}(\Gamma) = \Gamma$. By the description of $\text{Cl}(\Gamma)$ in (0.1) or in (3.1), it follows that for every finite index subgroup Γ' of Γ , $\text{Cl}(\Gamma') = \Gamma'$ (see [Lubotzky 1980, Proposition 4.4]). Now, if ρ is a faithful simply connected representation of Γ , it is also such for Γ' and by Proposition 3.6, $\rho(\text{Cl}(\Gamma'))$ is congruence closed. In our case it means that for every finite index subgroup Γ' , $\rho(\Gamma')$ is congruence closed, i.e., $\rho(\Gamma)$ has the congruence subgroup property.

4. Thin groups

Let Γ be a finitely generated \mathbb{Z} -linear group, i.e., $\Gamma \subset \text{GL}_n(\mathbb{Z})$, for some n . Let G be its Zariski closure in $\text{GL}_n(\mathbb{C})$ and $\Delta = G \cap \text{GL}_n(\mathbb{Z})$. We say that Γ is a *thin* subgroup of G if $[\Delta: \Gamma] = \infty$, otherwise Γ is an arithmetic subgroup of G . In general, given Γ , (say, given by a set of generators) it is a difficult question to determine if Γ is thin or arithmetic. Our next result gives, still, a group theoretic characterization for the *abstract* group Γ to be thin. But first a warning: an abstract group can sometimes appear as an arithmetic subgroup and sometimes as a thin subgroup. For example, the free group on two generators $F = F_2$ is a finite index subgroup of $\text{SL}_2(\mathbb{Z})$, and so, arithmetic. But at the same time, by a well-known

result of Tits [1972] asserting that $SL_n(\mathbb{Z})$ contains a copy of F which is Zariski dense in SL_n ; it is also thin. To be precise, let us define:

Definition 4.1. A finitely generated \mathbb{Z} -linear group Γ is called a *thin group* if it has a faithful representation $\rho: \Gamma \rightarrow GL_n(\mathbb{Z})$ for some $n \in \mathbb{Z}$, such that $\rho(\Gamma)$ is of infinite index in $\overline{\rho(\Gamma)}^Z \cap GL_n(\mathbb{Z})$ where $\overline{\rho(\Gamma)}^Z$ is the Zariski closure of Γ in GL_n . Such a ρ will be called a thin representation of Γ .

We have assumed that $i: \Gamma \subset GL_n(\mathbb{Z})$. Assume also, as we may (see Lemma 3.5) that the representation i is simply connected. By Proposition 3.6, the group $Cl(\Gamma)$ is the subgroup of $\hat{\Gamma}$ which preserves the lattices V_n for a totally ordered set (with respect to the relation of being a subrepresentation) of faithful simply connected integral representations (ρ_n, V_n) of Γ with the maps $Cl(\Gamma) \rightarrow B_n$ being surjective, where B_n is the congruence closure of $\rho_n(\Gamma)$ in $GL(V_n)$. Hence, $Cl(\Gamma)$ is the inverse limit (as n varies) of the congruence closed subgroups B_n and Γ is the inverse limit of the images $\rho_n(\Gamma)$. Equip $B_n/\rho_n(\Gamma)$ with the discrete topology. Consequently, $Cl(\Gamma)/\Gamma$ is a closed subspace of the Tychonov product $\prod_n (B_n/\rho_n(\Gamma))$. This is the topology on $Cl(\Gamma)/\Gamma$ considered in the following theorem.

Theorem 4.2. *Let Γ be a finitely generated \mathbb{Z} -linear group, i.e., $\Gamma \subset GL_m(\mathbb{Z})$ for some n . Then Γ is not a thin group if and only if Γ satisfies both of the following two properties:*

- (a) Γ is a FAb group (i.e., for every finite index subgroup Λ of Γ , $\Lambda/[\Lambda, \Lambda]$ is finite).
- (b) The group $Cl(\Gamma)/\Gamma$ is compact.

Proof. Assume first that Γ is a thin group. If Γ is not FAb we are done. So, assume Γ is FAb. We must now prove that $Cl(\Gamma)/\Gamma$ is not compact. We know that Γ has a faithful thin representation $\rho: \Gamma \rightarrow GL_n(\mathbb{Z})$ which in addition, is simply connected. This induces a surjective map (see Proposition 3.6) $Cl(\Gamma) \rightarrow B_\rho(\Gamma)$ where $B_\rho(\Gamma)$ is the congruence closure of $\rho(\Gamma)$ in $GL_n(\mathbb{Z})$. As Γ is FAb, $B_\rho(\Gamma)$ is a congruence subgroup, by Corollary 3.8. But as ρ is thin, $\rho(\Gamma)$ has infinite index in $B_\rho(\Gamma)$. Thus, $Cl(\Gamma)/\Gamma$ is mapped onto the discrete infinite quotient space $B_\rho(\Gamma)/\rho(\Gamma)$. Hence $Cl(\Gamma)/\Gamma$ is not compact.

Assume now Γ is not a thin group. This implies that for every faithful integral representation $\rho(\Gamma)$ is of finite index in its integral Zariski closure. We claim that $\Gamma/[\Gamma, \Gamma]$ is finite. Otherwise, as Γ is finitely generated, Γ is mapped on \mathbb{Z} . The group \mathbb{Z} has a Zariski dense integral representation τ into $\mathbb{G}_a \times S$ where S is a torus; take any integral matrix $g \in SL_n(\mathbb{Z})$ which is neither semisimple nor unipotent, whose semisimple part has infinite order. Then both the unipotent and semisimple part of the Zariski closure H of $\tau(\mathbb{Z})$ are nontrivial and $H(\mathbb{Z})$ cannot contain $\tau(\mathbb{Z})$ as a subgroup of finite index since $H(\mathbb{Z})$ is commensurable to $\mathbb{G}_a(\mathbb{Z}) \times S(\mathbb{Z})$ and both factors are nontrivial and infinite. The representation $\rho \times \tau$ (where ρ is any faithful integral representation of Γ) will give a thin representation of Γ . This proves that $\Gamma/[\Gamma, \Gamma]$ is finite. A similar argument (using an induced representation) works for every finite index subgroup, hence Γ satisfies FAb.

We now prove that $Cl(\Gamma)/\Gamma$ is compact. We already know that Γ is FAb, so by Corollary 3.8, $Cl(\Gamma) = \varprojlim B_{\rho_n}(\Gamma)$ when $B_n = B_{\rho_n}(\Gamma)$ are congruence groups with surjective homomorphisms $B_{n+1} \rightarrow B_n$. Note that as Γ has a faithful integral representation, we can assume that all the representations ρ_n in the

sequence are faithful and

$$\Gamma = \varprojlim_n \rho_n(\Gamma). \tag{4-1}$$

This implies that $\text{Cl}(\Gamma)/\Gamma = \varprojlim_n B_n/\rho_n(\Gamma)$. Now, by our assumption, each $\rho_n(\Gamma)$ is of finite index in $B_n = B_{\rho_n}(\Gamma)$. So $\text{Cl}(\Gamma)/\Gamma$ is an inverse limit of finite sets and hence compact. \square

5. Grothendieck closure and super-rigidity

Let Γ be a finitely generated group. We say that Γ is *integral super-rigid* if there exists an algebraic group $G \subseteq \text{GL}_m(\mathbb{C})$ and an embedding $i : \Gamma_0 \mapsto G$ of a finite index subgroup Γ_0 of Γ , such that for every integral representation $\rho : \Gamma \rightarrow \text{GL}_n(\mathbb{Z})$, there exists an algebraic representation $\tilde{\rho} : G \rightarrow \text{GL}_n(\mathbb{C})$ such that ρ and $\tilde{\rho}$ agree on some finite index subgroup of Γ_0 . Note: Γ is integral super-rigid if and only if a finite index subgroup of Γ is integral super-rigid.

Examples of such super-rigid groups are, first of all, the irreducible (arithmetic) lattices in high rank semisimple Lie groups, but also the (arithmetic) lattices in the rank one simple Lie groups $\text{Sp}(n, 1)$ and \mathbb{F}_4^{-20} (see [Margulis 1991; Corlette 1992; Gromov and Schoen 1992]). But [Bass and Lubotzky 2000] shows that there are such groups which are thin groups.

Now, let Γ be a subgroup of $\text{GL}_m(\mathbb{Z})$, whose Zariski closure is essentially simply connected. We say that Γ satisfies the *congruence subgroup property* (CSP) if the natural extension of $i : \Gamma \rightarrow \text{GL}_m(\mathbb{Z})$ to $\hat{\Gamma}$, i.e., $\tilde{i} : \hat{\Gamma} \rightarrow \text{GL}_m(\hat{\mathbb{Z}})$ has finite kernel.

Theorem 5.1. *Let $\Gamma \subseteq \text{GL}_m(\mathbb{Z})$ be a finitely generated subgroup satisfying (FAb). Then:*

- (a) $\text{Cl}(\Gamma)/\Gamma$ is compact if and only if Γ is an arithmetic group which is integral super-rigid.
- (b) $\text{Cl}(\Gamma)/\Gamma$ is finite if and only if Γ is an arithmetic group satisfying the congruence subgroup property.

Remarks. (a) The finiteness of $\text{Cl}(\Gamma)/\Gamma$ implies, in particular, its compactness, so Theorem 5.1 recovers the well-known fact (see [Bass et al. 1967; Raghunathan 1976]) that the congruence subgroup property implies super-rigidity.

- (b) As explained in Section 2 (based on [Serre 1968]) the simple connectedness is a necessary condition for the CSP to hold. But by Lemma 3.5, if Γ has any embedding into $\text{GL}_n(\mathbb{Z})$ for some n , it also has a simply connected one.

We now prove Theorem 5.1.

Proof. Assume first $\text{Cl}(\Gamma)/\Gamma$ is compact in which case, by Theorem 4.2, Γ must be an arithmetic subgroup of some algebraic group G . Without loss of generality (using Lemma 3.5) we can assume that G is connected and simply connected, call this representation $\rho : \Gamma \rightarrow G$. Let θ be any other representation of Γ .

Let $\tau = \rho \oplus \theta$ be the direct sum. The group G_τ is a subgroup of $G_\rho \times G_\theta$ with surjective projections. Since both τ and ρ are embeddings of the group Γ , and Γ does not have thin representations, it follows (from Corollary 3.8) that the projection $\pi : G_\tau \rightarrow G_\rho$ yields an isomorphism of the arithmetic groups $\tau(\Gamma) \subset G_\tau(\mathbb{Z})$ and $\rho(\Gamma) \subset G_\rho(\mathbb{Z})$.

Assume, as we may, that Γ is torsion-free and Γ is an arithmetic group. Every arithmetic group in $G_\tau(\mathbb{Z})$ is virtually a product of the form $U_\tau(\mathbb{Z}) \rtimes H_\tau(\mathbb{Z})$ where U_τ and H_τ are the unipotent and semisimple parts of G_τ respectively (note that G_τ^0 cannot have torus as quotient since Γ is FAb). Hence $\Gamma \cap U_\tau(\mathbb{Z})$ may also be described as the virtually maximal normal nilpotent subgroup of Γ . Similarly for $\Gamma \cap U_\rho(\mathbb{Z})$. This proves that the groups U_τ and U_ρ have isomorphic arithmetic groups which proves that $\pi : U_\tau \rightarrow U_\rho$ is an isomorphism. Otherwise $\text{Ker}(\pi)$, which is a \mathbb{Q} -defined normal subgroup of U_τ , would have an infinite intersection with the arithmetic group $\Gamma \cap U_\tau$.

Therefore, the arithmetic groups in H_τ and H_ρ are isomorphic and the isomorphism is induced by the projection $H_\tau \rightarrow H_\rho$. Since H_ρ is simply connected by assumption, and is a factor of H_τ , it follows that H_τ is a product $H_\rho H$ where H is a semisimple group defined over \mathbb{Q} with $H(\mathbb{Z})$ Zariski dense in H . But the isomorphism of the arithmetic groups in H_τ and H_ρ then shows that the group $H(\mathbb{Z})$ is finite which means that H is finite. Therefore, $\pi : H_\tau^0 \rightarrow H_\rho$ is an isomorphism and so the map $G_\tau^0 \rightarrow G_\rho$ is also an isomorphism since it is a surjective morphism between groups of the same dimension, and since G_ρ is simply connected.

This proves that Γ is a super-rigid group.

In [Lubotzky 1980], it was proved that if Γ satisfies super-rigidity in some simply connected group G , then (up to finite index) $\text{Cl}(\Gamma)/\Gamma$ is in one-to-one correspondence with

$$C(\Gamma) = \text{Ker}(\hat{\Gamma} \rightarrow G(\hat{\mathbb{Z}})).$$

This finishes the proof of both parts (a) and (b). □

Remark. In the situation of Theorem 5.1, Γ is an arithmetic group satisfying super-rigidity. The difference between parts (a) and (b), is whether Γ also satisfies CSP. As of now, there is no known arithmetic group (in a simply connected group) which satisfies super-rigidity without satisfying CSP. The conjecture of Serre about the congruence subgroup problem predicts that arithmetic lattices in rank one Lie groups fail to have CSP. These include Lie groups like $\text{Sp}(n, 1)$ and $\mathbb{F}_4^{(-20)}$ for which super-rigidity was shown (after Serre had made his conjecture). Potentially, the arithmetic subgroups of these groups can have $\text{Cl}(\Gamma)/\Gamma$ compact and not finite. But (some) experts seem to believe now that these groups do satisfy CSP. Anyway as of now, we do not know any subgroup Γ of $\text{GL}_n(\mathbb{Z})$ with $\text{Cl}(\Gamma)/\Gamma$ compact and not finite.

Acknowledgments

T.N. Venkataramana thanks the Math Department of the Hebrew University for great hospitality while a major part of this work was done. He would also like to thank the JC Bose fellowship (SR/S2/JCB-22/2017) for support during the period 2013–2018.

The authors thank the Math Department of the University of Marseilles, and the conference at Oberwolfach, where the work was completed. We would especially like to thank Bertrand Remy for many interesting discussions and for his warm hospitality.

A. Lubotzky is indebted for support from the NSF, the ISF and the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 692854).

References

- [Bass and Lubotzky 2000] H. Bass and A. Lubotzky, “Nonarithmetic superrigid groups: counterexamples to Platonov’s conjecture”, *Ann. of Math. (2)* **151**:3 (2000), 1151–1173. MR Zbl
- [Bass et al. 1967] H. Bass, J. Milnor, and J.-P. Serre, “Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)”, *Inst. Hautes Études Sci. Publ. Math.* **33** (1967), 59–137. MR Zbl
- [Bridson and Grunewald 2004] M. R. Bridson and F. J. Grunewald, “Grothendieck’s problems concerning profinite completions and representations of groups”, *Ann. of Math. (2)* **160**:1 (2004), 359–373. MR Zbl
- [Chahal 1980] J. S. Chahal, “Solution of the congruence subgroup problem for solvable algebraic groups”, *Nagoya Math. J.* **79** (1980), 141–144. MR Zbl
- [Corlette 1992] K. Corlette, “Archimedean superrigidity and hyperbolic geometry”, *Ann. of Math. (2)* **135**:1 (1992), 165–182. MR Zbl
- [Gromov and Schoen 1992] M. Gromov and R. Schoen, “Harmonic maps into singular spaces and p -adic superrigidity for lattices in groups of rank one”, *Inst. Hautes Études Sci. Publ. Math.* **76** (1992), 165–246. MR Zbl
- [Grothendieck 1970] A. Grothendieck, “Représentations linéaires et compactification profinie des groupes discrets”, *Manuscripta Math.* **2** (1970), 375–396. MR Zbl
- [Kontorovich et al. 2019] A. Kontorovich, D. D. Long, A. Lubotzky, and A. W. Reid, “What is . . . a thin group?”, *Notices Amer. Math. Soc.* **66**:6 (2019), 905–910.
- [Lubotzky 1980] A. Lubotzky, “Tannaka duality for discrete groups”, *Amer. J. Math.* **102**:4 (1980), 663–689. MR Zbl
- [Margulis 1991] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, *Ergebnisse der Mathematik (3)* **17**, Springer, 1991. MR Zbl
- [Nori 1987] M. V. Nori, “On subgroups of $GL_n(\mathbb{F}_p)$ ”, *Invent. Math.* **88**:2 (1987), 257–275. MR Zbl
- [Platonov and Rapinchuk 1994] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, *Pure and Appl. Math.* **139**, Academic Press, Boston, 1994. MR Zbl
- [Platonov and Tavgen 1986] V. P. Platonov and O. I. Tavgen, “On the Grothendieck problem of profinite completions of groups”, *Dokl. Akad. Nauk SSSR* **288**:5 (1986), 1054–1058. In Russian; translated in *Soviet Math. Dokl.* **33**:3 (1986), 822–825. MR Zbl
- [Pyber 2004] L. Pyber, “Groups of intermediate subgroup growth and a problem of Grothendieck”, *Duke Math. J.* **121**:1 (2004), 169–188. MR Zbl
- [Raghunathan 1976] M. S. Raghunathan, “On the congruence subgroup problem”, *Inst. Hautes Études Sci. Publ. Math.* **46** (1976), 107–161. MR Zbl
- [Raghunathan 1991] M. S. Raghunathan, “The congruence subgroup problem”, pp. 465–494 in *Proceedings of the Hyderabad Conference on Algebraic Groups* (Hyderabad, 1989), edited by S. Ramanan et al., Manoj Prakashan, Madras, 1991. MR Zbl
- [Sarnak 2014] P. Sarnak, “Notes on thin matrix groups”, pp. 343–362 in *Thin groups and superstrong approximation* (Berkeley, 2012), edited by E. Breuillard and H. Oh, *Math. Sci. Res. Inst. Publ.* **61**, Cambridge Univ. Press, 2014. MR Zbl
- [Serre 1968] J.-P. Serre, “Groupes de congruence (d’après H. Bass, H. Matsumoto, J. Mennicke, J. Milnor, C. Moore)”, exposé 330 in *Séminaire Bourbaki*, 1966/1967, W. A. Benjamin, Amsterdam, 1968. Reprinted as pp. 275–291 in *Séminaire Bourbaki* **10**, Soc. Math. France, Paris, 1995. MR Zbl
- [Tits 1972] J. Tits, “Free subgroups in linear groups”, *J. Algebra* **20** (1972), 250–270. MR Zbl
- [Venkataramana 1999] T. N. Venkataramana, “A remark on extended congruence subgroups”, *Int. Math. Res. Not.* **1999**:15 (1999), 835–838. MR Zbl
- [Weisfeiler 1984] B. Weisfeiler, “Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups”, *Ann. of Math. (2)* **120**:2 (1984), 271–315. MR Zbl

Communicated by Peter Sarnak

Received 2018-05-08 Revised 2019-01-20 Accepted 2019-03-08

alex.lubotzky@mail.huji.ac.il

Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Israel

venky@math.tifr.res.in

School of Mathematics, Tata Institute of Fundamental Research, Mumbai, India

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Richard E. Borcherds	University of California, Berkeley, USA	Martin Olsson	University of California, Berkeley, USA
Antoine Chambert-Loir	Université Paris-Diderot, France	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	University of California, Santa Cruz, USA	Michael Rapoport	Universität Bonn, Germany
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Christopher Skinner	Princeton University, USA
Wee Teck Gan	National University of Singapore	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Andrew Granville	Université de Montréal, Canada	J. Toby Stafford	University of Michigan, USA
Ben J. Green	University of Oxford, UK	Pham Huu Tiep	University of Arizona, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Roger Heath-Brown	Oxford University, UK	Michel van den Bergh	Hasselt University, Belgium
Craig Huneke	University of Virginia, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Philippe Michel	École Polytechnique Fédérale de Lausanne	Melanie Matchett Wood	University of Wisconsin, Madison, USA
Susan Montgomery	University of Southern California, USA	Shou-Wu Zhang	Princeton University, USA
Shigefumi Mori	RIMS, Kyoto University, Japan		

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US \$385/year for the electronic version, and \$590/year (+\$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2019 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 13 No. 6 2019

Positivity functions for curves on algebraic varieties BRIAN LEHMANN and JIAN XIAO	1243
The congruence topology, Grothendieck duality and thin groups ALEXANDER LUBOTZKY and TYAKAL NANJUNDIAH VENKATARAMANA	1281
On the ramified class field theory of relative curves QUENTIN GUIGNARD	1299
Blow-ups and class field theory for curves DAICHI TAKEUCHI	1327
Algebraic monodromy groups of l -adic representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ SHIANG TANG	1353
Weyl bound for p -power twist of $\text{GL}(2)$ L -functions RITABRATA MUNSHI and SAURABH KUMAR SINGH	1395
Examples of hypergeometric twistor \mathcal{D} -modules ALBERTO CASTAÑO DOMÍNGUEZ, THOMAS REICHELT and CHRISTIAN SEVENHECK	1415
Ulrich bundles on K3 surfaces DANIELE FAENZI	1443
Unlikely intersections in semiabelian surfaces DANIEL BERTRAND and HARRY SCHMIDT	1455
Congruences of parahoric group schemes RADHIKA GANAPATHY	1475
An improved bound for the lengths of matrix algebras YAROSLAV SHITOV	1501



1937-0652(2019)13:6;1-7