ISSN 0081-5438, Proceedings of the Steklov Institute of Mathematics, 2016, Vol. 292, pp. 216–246. © Pleiades Publishing, Ltd., 2016.

On the Congruence Kernel for Simple Algebraic Groups

Gopal Prasad[a] **and Andrei S. Rapinchuk**[b]

Received January 11, 2015

To V.P. Platonov on his 75th birthday

Abstract—This paper contains several results about the structure of the congruence kernel $C^{(S)}(G)$ of an absolutely almost simple simply connected algebraic group G over a global field K with respect to a set of places S of K. In particular, we show that $C^{(S)}(G)$ is always trivial if S contains a generalized arithmetic progression. We also give a criterion for the centrality of $C^{(S)}(G)$ in the general situation in terms of the existence of commuting lifts of the groups $G(K_v)$ for $v \notin S$ in the S-arithmetic completion $\widehat{G}^{(S)}$. This result enables one to give simple proofs of the centrality in a number of cases. Finally, we show that if K is a number field and G is K-isotropic, then $C^{(S)}(G)$ as a normal subgroup of $\widehat{G}^{(S)}$ is almost generated by a single element.

DOI: 10.1134/S0081543816010144

1. INTRODUCTION

Let G be an absolutely almost simple simply connected algebraic group defined over a global field K, and let S be a nonempty subset of the set V^K of all places of K containing the set V_∞^K of archimedean places. We fix a K-embedding $G \hookrightarrow \mathrm{SL}_n$ and define

$$G(\mathcal{O}(S)) = G(K) \cap \mathrm{SL}_n(\mathcal{O}(S)),$$

where $\mathcal{O}(S)$ is the ring of S-integers in K. One then introduces two topologies, τ_{a} and τ_{c}, on the group of K-rational points $G(K)$, called the *S-arithmetic topology* and the *S-congruence topology*, respectively, by taking for a fundamental system of neighborhoods of the identity all normal subgroups of finite index $N \subset G(\mathcal{O}(S))$ for τ_{a}, and the congruence subgroups $G(\mathcal{O}(S), \mathfrak{a}) = G(K) \cap \mathrm{SL}_n(\mathcal{O}(S), \mathfrak{a})$ corresponding to nonzero ideals $\mathfrak{a}$ of $\mathcal{O}(S)$[1] for τ_{c}. One shows that these topologies in fact do not depend on the choice of a K-embedding of G into SL_n, and furthermore, the group $G(K)$ admits completions with respect to both τ_{a} and τ_{c}. These completions will be denoted $\widehat{G}^{(S)}$ and $\overline{G}^{(S)}$ and called respectively the S-arithmetic and the S-congruence completions. As the topology τ_{a} is finer than τ_{c}, there is a natural continuous homomorphism $\pi^{(S)}\colon \widehat{G}^{(S)} \to \overline{G}^{(S)}$, which turns out to be surjective. Its kernel $C^{(S)}(G)$ is called the *S-congruence kernel*. Clearly, $C^{(S)}(G)$ is trivial if and only if every normal subgroup $N \subset G(\mathcal{O}(S))$ contains a congruence subgroup $G(\mathcal{O}(S), \mathfrak{a})$ for some $\mathfrak{a}$, which means that we have an affirmative answer to the classical congruence subgroup problem for the group $G(\mathcal{O}(S))$. In general, $C^{(S)}(G)$ measures the deviation from the affirmative answer, so by the congruence subgroup problem in a broader sense one means the task of computing $C^{(S)}(G)$. (In the sequel, we will omit the superscript (S) if this cannot lead to confusion.)

[a] Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, USA.

[b] Department of Mathematics, University of Virginia, Charlottesville, VA 22904-4137, USA.

E-mail addresses: gprasad@umich.edu (G. Prasad), asr3x@virginia.edu (A.S. Rapinchuk).

[1] As usual, $\mathrm{SL}_n(\mathcal{O}(S), \mathfrak{a}) = \{A \in \mathrm{SL}_n(\mathcal{O}(S)) \mid A \equiv I_n \pmod{\mathfrak{a}}\}$.

The investigation of the congruence subgroup problem has two parts: the first is to prove that in certain cases $C^{(S)}(G)$ is finite and then determine it precisely, and the other is to understand the structure of $C^{(S)}(G)$ in the cases where it is infinite. We recall that the expected conditions for $C^{(S)}(G)$ to be finite/infinite are given in the following conjecture of Serre [58]:

> *$C^{(S)}(G)$ should be finite if $\operatorname{rk}_S G := \sum_{v\in S}\operatorname{rk}_{K_v} G$ is ≥ 2 and G is K_v-isotropic for all $v \in S \setminus V_\infty^K$, and $C^{(S)}(G)$ should be infinite if $\operatorname{rk}_S G = 1$.*

(In the sequel, we will always assume that $\operatorname{rk}_S G > 0$ as otherwise the group $G(\mathcal{O}(S))$ is finite and hence $C^{(S)}(G)$ is trivial.) The results of the current paper contribute to both aspects of the congruence subgroup problem. (We refer the reader to the surveys [39, 43] and references therein for information about the very impressive body of work in this area.)

To give the precise formulations, we need to recall the statement of the Margulis–Platonov conjecture (MP) for the group $G(K)$:

> *Let $\mathcal{A} = \{v \in V^K \setminus V_\infty^K \mid \operatorname{rk}_{K_v} G = 0\}$ be the set of nonarchimedean places of K where G is anisotropic, let $G_{\mathcal{A}} = \prod_{v\in\mathcal{A}} G(K_v)$, and let $\delta\colon G(K) \to G_{\mathcal{A}}$ be the diagonal map. Then for any noncentral normal subgroup N of $G(K)$, there is an open normal subgroup U of $G_{\mathcal{A}}$ such that $N = \delta^{-1}(U)$; in particular, if $\mathcal{A} = \varnothing$ (which is always the case if G is not of type A_n), then $G(K)$ does not contain any proper noncentral normal subgroups.*

We note that (MP) has been established in all cases where G is K-isotropic (see [15]) and also in many cases where G is K-anisotropic (see [31, Ch. 9] and [54, Appendix A]). Throughout this paper, we reserve the notation $\mathcal{A} = \mathcal{A}(G)$ for the set of anisotropic places, i.e. the nonarchimedean places of K where G is anisotropic, and *assume that* (MP) *holds for $G(K)$ and that $\mathcal{A} \cap S = \varnothing$*. (As shown in [40, § 6], the general case can be reduced to the case where $\mathcal{A} \cap S = \varnothing$, but if this condition fails then $C^{(S)}(G)$ is always infinite.) It is known that $C^{(S)}(G)$ is finite if and only if it is *central* (i.e., is contained in the center of $\widehat{G}^{(S)}$), in which case it is isomorphic to the Pontryagin dual of the *metaplectic kernel* $M(S, G)$ (cf. [39, § 3]). Since the metaplectic kernel has completely been determined in [36] in all cases relevant for the congruence subgroup problem (for example, we know that $M(S, G)$ is trivial if S is infinite), the first of the two aspects of the congruence subgroup problem we mentioned above reduces to proving that $C^{(S)}(G)$ is central in the expected cases. Our first basic result (Theorem 4.3) is the following. This result was proved in [36, § 9] in the case where K is a number field.

Theorem. *Let G be an absolutely almost simple simply connected algebraic group over a global field K, and assume that* (MP) *holds for $G(K)$. Then for any finite set V of nonarchimedean places of K that contains the set $\mathcal{A}$ of anisotropic places and for $S = V^K \setminus V$, the congruence kernel $C^{(S)}(G)$ is central and hence trivial.*

This result will be used to prove the following theorem which provides a new, and particularly effective, criterion for the centrality of $C^{(S)}(G)$. We observe that since $\operatorname{rk}_S G > 0$, it follows from the strong approximation property (cf. [26, 29, 33]; see also [52] for a recent survey) that the congruence completion $\overline{G}^{(S)}$ can be naturally identified with the group of S-adeles $G(\mathbb{A}(S))$, which enables us to view the group $G(K_v)$ for any $v \in V^K \setminus S$ as a subgroup of $\overline{G}^{(S)}$. As above, we let $\pi\colon \widehat{G} \to \overline{G}$ denote the natural continuous homomorphism (we suppress the superscript (S)).

Theorem A. *Let G be an absolutely almost simple simply connected algebraic group over a global field K, and let S be* any *subset of $V^K \setminus \mathcal{A}$ containing V_∞^K. Assume that for every $v \notin S$, there is a subgroup $\mathscr{G}_v$ of $\widehat{G}$ so that the following conditions are satisfied*:

(i) *$\pi(\mathscr{G}_v) = G(K_v)$ for all $v \notin S$;*

(ii) *$\mathscr{G}_{v_1}$ and $\mathscr{G}_{v_2}$ commute elementwise for all $v_1, v_2 \notin S$, $v_1 \neq v_2$;*

(iii) *the subgroup generated by the $\mathscr{G}_v$, for $v \notin S$, is dense in $\widehat{G}$.*

Then $C^{(S)}(G)$ is central in $\widehat{G}$.

(We note that this theorem was already stated in [50, Theorem 7] and that Proposition 4.5 contains a somewhat more general result which is sometimes useful.) We will show in Section 4 how Theorem A can be used to establish the centrality of the congruence kernel for $G = \mathrm{SL}_n$, $n \geq 3$, and $G = \mathrm{SL}_2$ when $\mathrm{rk}_S G \geq 2$ (i.e., when the group of units $\mathcal{O}(S)^\times$ is infinite)—see Examples 4.6 and 4.7.

To formulate our next result, we need to recall the definition of a *generalized arithmetic progression*. For a global field K, we let V_{f}^K denote the set of all nonarchimedean places of K (i.e., $V_{\mathrm{f}}^K = V^K \setminus V_\infty^K$). Now, let F/K be a Galois extension (not necessarily abelian) with Galois group $\mathcal{G} := \mathrm{Gal}(F/K)$. Given $v \in V_{\mathrm{f}}^K$ which is unramified in F, for every extension $w|v$ one defines the Frobenius automorphism $\mathrm{Fr}_{F/K}(w|v) \in \mathcal{G}$; recall that $\mathrm{Fr}_{F/K}(w|v)$ for *all* extensions $w|v$ fill a conjugacy class of $\mathcal{G}$ (cf. [2, Ch. VII]). Now, fix a conjugacy class $\mathscr{C}$ of $\mathcal{G}$.

Definition. A *generalized arithmetic progression* $\mathscr{P}(F/K, \mathscr{C})$ is the set of all $v \in V_{\mathrm{f}}^K$ such that v is unramified in F/K and for some (equivalently, any) extension $w|v$, the Frobenius automorphism $\mathrm{Fr}_{F/K}(w|v)$ is in the conjugacy class $\mathscr{C}$.

We can now formulate our next result.

Theorem B. *Let G be an absolutely almost simple simply connected algebraic group over a global field K, and let L be the minimal Galois extension of K over which G is an inner form of a split group. Let S be a subset of V^K which is disjoint from $\mathcal{A}$, contains V_∞^K, and also contains all but finitely many places belonging to a generalized arithmetic progression $\mathscr{P}(F/K, \mathscr{C})$ such that $\sigma|(F \cap L) = \mathrm{id}_{F\cap L}$ for some (equivalently, any) $\sigma \in \mathscr{C}$ (which is automatically true if G is an inner form of a split group over K). Then $C^{(S)}(G)$ is central, and hence in fact trivial.*

In Section 6 we will give a new proof of Lubotzky's conjecture on the congruence subgroup property for arithmetic groups with adelic profinite completion. A profinite group Δ is called *adelic* if for some $n \geq 1$, there exists a continuous embedding $\iota\colon \Delta \hookrightarrow \mathrm{GL}_n(\widehat{\mathbb{Z}})$, where $\widehat{\mathbb{Z}} = \prod_{q \text{ prime}} \mathbb{Z}_q$. It was conjectured by A. Lubotzky that if for $\Gamma = G(\mathcal{O}(S))$ the profinite completion $\widehat{\Gamma}$ is adelic then Γ has the *congruence subgroup property* (CSP), i.e. the congruence kernel $C^{(S)}(G)$ is finite. This was proved by Platonov and Sury in [32] using some rather technical constructions developed earlier in [30] to establish (CSP) for arithmetic groups with bounded generation. Subsequently, Liebeck and Pyber [19] showed that *any finitely generated* subgroup of $\mathrm{GL}_n(\widehat{\mathbb{Z}})$ has bounded generation, which allows one to prove Lubotzky's conjecture by directly quoting the results of [22, 30] on (CSP) for arithmetic groups with bounded generation. We note that it is essential in both [19] and [32] that Γ be finitely generated (i.e., S be finite). We give a rather short proof of Lubotzky's conjecture that does not rely on finite generation (hence is applicable even when S is infinite).

Theorem C. *Let G be an absolutely almost simple simply connected algebraic group defined over a number field K, $S \subset V^K \setminus \mathcal{A}$ be a subset containing V_∞^K, and $\Gamma = G(\mathcal{O}(S))$. If the profinite completion $\widehat{\Gamma}$ is adelic, then $C^{(S)}(G)$ is central, hence finite.*

Our last result addresses the second aspect of the congruence subgroup problem, viz. the structure of the congruence kernel $C = C^{(S)}(G)$ when it is infinite. It is known (cf. Proposition 2.9) that in this case the group C is not finitely generated; for its precise structure in certain cases see [21, 27, 28, 71, 72]. Lubotzky [24] showed however that the congruence kernel C is always finitely generated as a *normal* subgroup of $\widehat{\Gamma}$. We will prove that when K is a number field and G is K-isotropic, C as a normal subgroup of $\widehat{G}$ is almost generated by *one* element (this result was announced more than ten years ago and is mentioned in [24], but its proof given below appears in print for the first time).

Theorem D. *Let G be an absolutely almost simple simply connected algebraic group over a number field K with $\mathrm{rk}_K G = 1$. Then there exists c in $C := C^{(S)}(G)$ such that if D is the*

closed normal subgroup of $\widehat{G}$ generated by c, then the quotient C/D is a quotient of the metaplectic kernel $M(S,G)$; in particular, it is a finite cyclic group.

(We note that if G is K-isotropic and $\operatorname{rk}_S G \geq 2$, then $C^{(S)}(G)$ is known to be central (Raghunathan [40, 41]) and hence isomorphic to $M(S,G)$, so the theorem trivially holds with $c = 1$. Thus, the core case in the theorem is where $\operatorname{rk}_S G = 1$.)

2. PRELIMINARIES ON THE CONGRUENCE KERNEL

Let G ($\hookrightarrow \mathrm{SL}_n$) be an absolutely almost simple simply connected algebraic group over a global field K, $\mathcal{A}$ be the finite set of nonarchimedean places of K where G is anisotropic, and $S \subset V^K$ be a nonempty subset containing V_∞^K when K is a number field and such that $\mathcal{A} \cap S = \varnothing$ and $\operatorname{rk}_S G > 0$. Let $\Gamma = G(\mathcal{O}(S))$. The discussion in Section 1 leads to the following exact sequence of topological groups for the congruence kernel $C := C^{(S)}(G)$:

$$1 \to C \to \widehat{G} \xrightarrow{\pi} \overline{G} \to 1 \tag{C}$$

(we omit the superscript (S) whenever possible). It is an immediate consequence of the definitions that (C) splits over the subgroup $G(K)$ of K-rational points in the category of abstract groups (with the image of this splitting being dense in $\widehat{G}$). Furthermore, as we already pointed out in Section 1, it follows from the strong approximation property that the S-congruence completion $\overline{G}$ can be naturally identified with the group of S-adeles $G(\mathbb{A}(S))$. We now recall the following *universal property* of (C).

Proposition 2.1. *Let*

$$1 \to D \to E \xrightarrow{\rho} G(\mathbb{A}(S)) \to 1$$

be an exact sequence of locally compact topological groups with D a profinite group. Assume that there exists a splitting $\varphi\colon G(K) \to E$ for ρ over $G(K)$ whose image is dense in E. Then there exists a continuous surjective homomorphism $\sigma\colon C \to D$. In particular, if C is trivial then so is D.

Proof. Since the closure $\overline{\Gamma}$ of Γ in $\overline{G}$ is an open profinite subgroup and the group D is also profinite, we see that $\Omega := \rho^{-1}(\overline{\Gamma})$ is an open profinite subgroup of E. Then

$$\varphi(G(K)) \cap \Omega = \varphi(G(K) \cap \overline{\Gamma}) = \varphi(\Gamma)$$

is a dense subgroup of Ω. By the universal property of the profinite completion, there exists a continuous surjective homomorphism $\widehat{\varphi}\colon \widehat{\Gamma} \to \Omega$ which coincides with φ on Γ. As φ is a section for ρ over $G(K)$, the composition $\rho \circ \widehat{\varphi}\colon \widehat{\Gamma} \to \overline{\Gamma}$ restricts to the identity map on Γ and therefore coincides with π on $\widehat{\Gamma}$. Since $\widehat{\varphi}\colon \widehat{\Gamma} \to \Omega$ is surjective, we now conclude that

$$D = \widehat{\varphi}(\widehat{\varphi}^{-1}(D)) = \widehat{\varphi}(C),$$

so $\sigma := \widehat{\varphi}|C$ is as required. $\square$

The goal of this section is to develop some techniques that will be used later to establish the centrality of C in certain situations. For further use, it is convenient to deal not only with the extension (C) itself, but also with its quotients. So, let $D \subset \widehat{G}$ be a closed normal subgroup contained in C. Consider the quotient of (C) by D:

$$1 \to F = C/D \to H = \widehat{G}/D \xrightarrow{\theta} G(\mathbb{A}(S)) \to 1. \tag{F}$$

We note that just like (C), the sequence (F) splits over the group $G(K)$, and the map θ is open and closed. The following set of places plays an important role in examining when (F) is a central

extension:

$$\mathfrak{Z}(F) = \big\{v \in V^K \setminus (S \cup \mathcal{A}) \;\big|\; \theta(Z_H(F)) \supset G(K_v)\big\}$$

where $Z_H(F)$ denotes the centralizer of F in H, the set $\mathcal{A}$ consists of those nonarchimedean $v \in V^K$ where G is anisotropic, and $G(K_v)$ is naturally identified with a subgroup of $\overline{G} = G(\mathbb{A}(S))$. We will write $\mathfrak{Z}$ for $\mathfrak{Z}(C)$ if this will not lead to confusion. We note that Proposition 2.1 is independent of the Margulis–Platonov conjecture (MP), but in the rest of this section we do invoke our standing assumption that (MP) holds for $G(K)$ and $S \cap \mathcal{A} = \varnothing$.

We begin with a couple of results that give sufficient conditions for a place $v \in V^K \setminus (S \cup \mathcal{A})$ to belong to $\mathfrak{Z}(F)$.

Proposition 2.2. *Let $v \in V^K \setminus (S \cup \mathcal{A})$. Assume there exists a noncentral $a \in G(K_v)$ such that $a \in \theta(Z_H(x))$ for every $x \in F$. Then $v \in \mathfrak{Z}(F)$.*

Proof. Let $\mathcal{F}$ be the set of conjugacy classes in F. The conjugation action of H on F gives rise to a group homomorphism $\overline{G} \xrightarrow{\tau} \mathrm{Perm}(\mathcal{F})$ to the group of permutations of $\mathcal{F}$. Our assumption means that $\tau(a) = \mathrm{id}_{\mathcal{F}}$. Since $G(K_v)$ does not have proper noncentral normal subgroups (cf. [29] and also [15, 35, 66]), this implies that $\tau(G(K_v)) = \{\mathrm{id}_{\mathcal{F}}\}$. In particular, any open normal subgroup $W \subset F$ is normalized by $H_v := \theta^{-1}(G(K_v))$, so the latter acts on the finite group F/W. Let $\lambda_W \colon H_v \to \mathrm{Aut}(F/W)$ be the corresponding group homomorphism, and set $\mathcal{L}_W = \mathrm{Ker}\,\lambda_W$. We need the following lemma.

Lemma 2.3. *Let $\kappa \colon \mathcal{H} \to \mathcal{G}$ and $\lambda \colon \mathcal{H} \to \mathcal{M}$ be two continuous homomorphisms of locally compact topological groups with kernels $\mathcal{K}$ and $\mathcal{L}$, respectively. Assume that*

(1) *κ is closed and surjective, $\mathcal{K}$ is compact, and $\mathcal{G}$ does not have proper closed normal subgroups of finite index;*

(2) *$\mathcal{M}$ is profinite.*

Then $\mathcal{H} = \mathcal{K}\mathcal{L}$, or equivalently $\kappa(\mathcal{L}) = \mathcal{G}$.

Proof. Assume that $\mathcal{N} := \mathcal{K}\mathcal{L}$ is properly contained in $\mathcal{H}$. Then, since $\mathcal{K}$ is compact, the image $\lambda(\mathcal{N}) = \lambda(\mathcal{K})$ is a closed subgroup of $\mathcal{M}$ that is properly contained in $\lambda(\mathcal{H})$. Since $\mathcal{M}$ is profinite, there exists a proper open subgroup $\mathscr{U} \subset \mathcal{M}$ that contains $\lambda(\mathcal{N})$ but not $\lambda(\mathcal{H})$. Then $\mathcal{V} := \lambda^{-1}(\mathscr{U})$ is a proper open subgroup of $\mathcal{H}$ of finite index that contains $\mathcal{N}$. It follows that $\kappa(\mathcal{V})$ is a proper closed subgroup of $\mathcal{G}$ of finite index. Then the intersection of all conjugates of $\kappa(\mathcal{V})$ would be a proper *normal* closed subgroup of $\mathcal{G}$ of finite index, but by our assumption such a subgroup cannot exist. A contradiction. $\square$

Applying the lemma to the homomorphisms $H_v \xrightarrow{\theta} G(K_v)$ and $H_v \xrightarrow{\lambda_W} \mathrm{Aut}(F/W)$, we find that $\theta(\mathcal{L}_W) = G(K_v)$ for every open normal subgroup W of F. Thus, for any $g \in G(K_v)$, the fiber $\theta^{-1}(g)$ meets the closed subgroup $\mathcal{L}_W$. Using the fact that $\mathcal{L}_{W_1} \cap \ldots \cap \mathcal{L}_{W_d} = \mathcal{L}_{W_1 \cap \ldots \cap W_d}$ for any open normal subgroups $W_1, \ldots, W_d$ of F and the compactness of $\theta^{-1}(g)$, we conclude that

$$\theta^{-1}(g) \cap \left(\bigcap_W \mathcal{L}_W\right) \neq \varnothing,$$

where W runs through all open normal subgroups of F. But $\bigcap_W \mathcal{L}_W$ clearly coincides with $\theta^{-1}(G(K_v)) \cap Z_H(F)$. So, $g \in \theta(Z_H(F))$, implying that $G(K_v) \subset \theta(Z_H(F))$; hence $v \in \mathfrak{Z}(F)$. $\square$

Proposition 2.4. *Let V be a subset of $V^K \setminus S$, and let $T = V^K \setminus V$. Assume that the congruence kernel $C^{(T \setminus \mathcal{A})}(G)$ is trivial and there exist subgroups H_1 and H_2 of H such that*

(i) *$\theta(H_1)$ and $\theta(H_2)$ are dense subgroups of $G(\mathbb{A}(S \cup V))$ and $G(\mathbb{A}(T))$, respectively;*

(ii) *H_1 and H_2 commute elementwise and together generate a dense subgroup of H.*

Then H_2 centralizes F, and therefore $V \setminus \mathcal{A}$ is contained in $\mathfrak{Z}(F)$.

Proof. We note that $G(\mathbb{A}(S)) = G(\mathbb{A}(T)) \times G(\mathbb{A}(S \cup V))$. Replacing the subgroups H_1 and H_2 with their closures, we may assume that they are actually closed. Since θ is a closed map, we then see that

$$\theta(H_1) = G(\mathbb{A}(S \cup V)) \qquad \text{and} \qquad \theta(H_2) = G(\mathbb{A}(T)).$$

Now, we define the following closed normal subgroup of H_1:

$$H_1' = H_1 \cap \theta^{-1}(G(\mathbb{A}(S \cup V \cup \mathcal{A}))).$$

It follows from condition (ii) that the normalizer $N_H(H_1')$ contains H_1 and H_2 and hence coincides with H. Thus, we can take the quotient of the extension (F) by H_1', which yields the following exact sequence:

$$1 \to F/(F \cap H_1') \to H/H_1' \to G(\mathbb{A}(T \setminus \mathcal{A})) \to 1.$$

We now observe that this sequence inherits from (F) a splitting over $G(K)$ whose image is dense in H/H_1'. Since the congruence kernel $C^{(T\setminus\mathcal{A})}(G)$ is trivial by assumption, we conclude from Proposition 2.1 that $F \subset H_1'$, which implies that H_2 centralizes F. Then for any $v \in V$ we have

$$G(K_v) \subset \theta(H_2) \subset \theta(Z_H(F)),$$

proving that $v \in \mathfrak{Z}(F)$ and establishing the inclusion $V \setminus \mathcal{A} \subset \mathfrak{Z}(F)$. $\square$

Next, we will show how information about $\mathfrak{Z}(F)$ can be used to conclude that (F) is a central extension.

Proposition 2.5. *If there exists a subset V of $\mathfrak{Z}(F)$ such that the congruence kernel $C^{(S\cup V)}(G)$ is trivial, then the extension* (F) *is central. In particular,* (F) *is central whenever $\mathfrak{Z}(F) = V^K \setminus (S \cup \mathcal{A})$.*

We begin with the following elementary lemma.

Lemma 2.6. *Let*

$$1 \to \mathcal{F} \to \mathcal{H} \xrightarrow{\nu} \mathcal{G} \to 1 \tag{2.1}$$

be an exact sequence of groups. Given a subgroup $\mathcal{H}' \subset \mathcal{H}$ that centralizes $\mathcal{F}$ and an element $a \in \mathcal{H}$ such that $\nu(a)$ centralizes $\nu(\mathcal{H}')$, the map

$$\gamma_a\colon\ x \mapsto [a,x] = axa^{-1}x^{-1} \qquad \text{for} \quad x \in \mathcal{H}'$$

is a group homomorphism $\mathcal{H}' \to \mathcal{F}$.

Proof. For $x \in \mathcal{H}'$ we have $\nu([a,x]) = [\nu(a), \nu(x)] = 1$, implying that $\gamma_a(x) \in \mathcal{F}$. Furthermore, for $x, y \in \mathcal{H}'$ we have

$$\gamma_a(xy) = [a,xy] = [a,x](x[a,y]x^{-1}) = \gamma_a(x)\gamma_a(y),$$

as required. $\square$

Corollary 2.7. *Assume that* (2.1) *is a central extension. Then for any elementwise commuting subgroups $\mathcal{G}_1, \mathcal{G}_2 \subset \mathcal{G}$, the map*

$$c\colon\ \mathcal{G}_1 \times \mathcal{G}_2 \to \mathcal{F}, \qquad (x,y) \mapsto [\widetilde{x}, \widetilde{y}\,] \quad \text{for} \quad \widetilde{x} \in \nu^{-1}(x), \quad \widetilde{y} \in \nu^{-1}(y),$$

is a well-defined bimultiplicative pairing.

Indeed, since $\mathcal{F}$ is central in $\mathcal{H}$, the commutator $[\widetilde{x}, \widetilde{y}\,]$ does not depend on the choice of lifts $\widetilde{x}$ and $\widetilde{y}$, making the map c well-defined. It follows from the lemma that $c(\mathcal{G}_1, \mathcal{G}_2) \subset \mathcal{F}$ and that for any $x \in \mathcal{G}_1$ and $y_1, y_2 \in \mathcal{G}_2$ we have

$$c(x, y_1y_2) = \gamma_{\widetilde{x}}(\widetilde{y}_1\widetilde{y}_2) = \gamma_{\widetilde{x}}(\widetilde{y}_1)\gamma_{\widetilde{x}}(\widetilde{y}_2) = c(x,y_1)c(x,y_2),$$

proving that c is multiplicative in the second variable. The multiplicativity in the first variable is established by a similar computation.

Proof of Proposition 2.5. To prove the first claim, we need to construct subgroups H_1 and H_2 of H with the properties similar to those described in Proposition 2.4. Set $H_1 = \theta^{-1}(G(\mathbb{A}(S \cup V)))$. To define H_2, we first consider $H' = \theta^{-1}(G(\mathbb{A}(T))) \cap Z_H(F)$, where $T = V^K \setminus V$. Clearly, the groups $G(K_v)$ for $v \in V$ generate a dense subgroup of $G(\mathbb{A}(T))$. This fact has two implications relevant to our argument. First, since $V \subset \mathfrak{Z}(F)$ and θ is a closed map, the image $\theta(H')$ is a closed subgroup of $G(\mathbb{A}(T))$ containing $G(K_v)$ for all $v \in V$; hence $\theta(H') = G(\mathbb{A}(T))$. Second, for any $v \in V$, the group G is K_v-isotropic, and therefore $G(K_v)$ contains no proper normal subgroup of finite index (as we already mentioned above). It follows that $G(\mathbb{A}(T))$ contains no proper *closed* normal subgroup of finite index. Now, it follows from Lemma 2.6 that for any $a \in H_1$, the map $\gamma_a \colon x \mapsto [a, x]$ is a (continuous) group homomorphism $H' \to F$. We now consider the profinite group

$$\mathscr{M} = \prod_{a \in H_1} F_a, \qquad \text{where} \quad F_a = F \quad \text{for all} \quad a \in H_1,$$

define a continuous homomorphism $\lambda \colon H' \to \mathscr{M}$, $x \mapsto (\gamma_a(x))$, and let $H_2 = \operatorname{Ker} \lambda$. Applying Lemma 2.3, we see that $\theta(H_2) = G(\mathbb{A}(T))$. This easily implies that $H = H_1 H_2$, and on the other hand, by our construction the subgroups H_1 and H_2 commute elementwise. In particular, H_2 is normal in H, and hence (F) gives rise to the following exact sequence:

$$1 \to F/(F \cap H_2) \to H/H_2 \to G(\mathbb{A}(S))/G(\mathbb{A}(T)) = G(\mathbb{A}(S \cup V)) \to 1.$$

Since $C^{(S \cup V)}(G)$ is trivial by assumption, Proposition 2.1 implies that $F \subset H_2$. It follows that H_1 centralizes F, and therefore so does $H = H_1 H_2$ as $H_2 \subset Z_H(F)$ by our construction. (While this can be derived directly from Proposition 2.4, we gave an independent argument in order to avoid cumbersome notations.)

For the second assertion, we observe that for $V = V^K \setminus (S \cup \mathcal{A})$, the triviality of $C^{(S \cup V)}(G)$ is equivalent to our standing assumption that (MP) holds for $G(K)$ and $S \cap \mathcal{A} = \varnothing$. $\square$

Proposition 2.8. *Assume that $\mathcal{A} \cap S = \varnothing$ and there is a partition $V^K \setminus (S \cup \mathcal{A}) = \bigcup_{i \in I} V_i$ such that one can find subgroups $H_{\mathcal{A}}$ and H_i $(i \in I)$ of H satisfying the following conditions*:

(i) *for each $i \in I$ and $V_i' := \bigcup_{j \neq i} V_j$, the congruence kernel $C^{(S \cup V_i')}(G)$ is trivial*;

(ii) *$\theta(H_{\mathcal{A}})$ is a dense subgroup of $G_{\mathcal{A}} = \prod_{v \in \mathcal{A}} G(K_v)$, and $\theta(H_i)$ is a dense subgroup of $G(\mathbb{A}(V^K \setminus V_i))$ for all $i \in I$*;

(iii) *any two of the subgroups $H_{\mathcal{A}}$ and H_i for $i \in I$ commute elementwise*;

(iv) *the subgroups $H_{\mathcal{A}}$ and H_i for $i \in I$ generate a dense subgroup of H.*

Then (F) *is a central extension.*

Proof. Fix $i \in I$, and let $V = \mathcal{A} \cup V_i$; then the corresponding T in Proposition 2.4 is $S \cup V_i'$. Now to apply Proposition 2.4, we let H_1 denote the subgroup generated by the H_j, $j \neq i$, and let H_2 denote the subgroup generated by $H_{\mathcal{A}}$ and H_i. From Proposition 2.4, we conclude that $V_i \subset \mathfrak{Z}(F)$. Since this is true for all $i \in I$, we see that actually $\mathfrak{Z}(F) = V^K \setminus (S \cup \mathcal{A})$. Then (F) is central by Proposition 2.5. (We note that in the case $\mathcal{A} = \varnothing$, the proof in fact does not require Proposition 2.5.) $\square$

The following assertion goes back to [48] (see also [22; 25, Proposition 7.1.3; 30]).

Proposition 2.9. *If* (F) *is not central then F possesses closed subgroups $F_2 \subset F_1$, both of which are normal in H, such that the quotient F/F_1 is finite and the quotient F_1/F_2 is isomorphic to $\prod_{i \in I} \Phi_i$ where I is an* infinite *set and $\Phi_i = \Phi$, the same finite simple group, for all $i \in I$. Consequently, if F is finitely generated then it is central, hence finite.*

3. A CRITERION FOR CENTRALITY

We begin with one additional notation. Let $v \in V^K$, fix a maximal K_v-torus T of G, and let T^{reg} denote its Zariski-open subvariety of regular elements. It follows from the implicit function theorem that the map

$$\varphi_{v,T}\colon\ G(K_v) \times T^{\mathrm{reg}}(K_v) \to G(K_v), \qquad (g,t) \mapsto gtg^{-1}, \tag{3.1}$$

is open; in particular,

$$\mathscr{U}(v,T) := \varphi_{v,T}\big(G(K_v) \times T^{\mathrm{reg}}(K_v)\big)$$

is an open subset of $G(K_v)$. It follows from the definition that $\mathscr{U}(v,T)$ is *conjugation-invariant* and *solid*; i.e., it intersects every open subgroup of $G(K_v)$ (the latter property is primarily used when v is nonarchimedean). Let θ be as in the short exact sequence (F) of the preceding section.

Theorem 3.1. (i) *If the extension* (F) *is central, then there exists a positive integer n such that for any maximal K-torus T of G and any $t \in T(K)$, we have the inclusion*

$$\theta(Z_H(t)) \supset T(\mathbb{A}(S))^n \tag{3.2}$$

(*here we view the group of S-adeles $T(\mathbb{A}(S))$ as a subgroup of $G(\mathbb{A}(S)) = \overline{G}$, and use t to denote also the lift of $t \in T(K)$ in H provided by the splitting of* (F) *over $G(K)$*).

(ii) *Conversely, assume that there is an integer $n > 1$, a finite subset $V \subset V^K \setminus S$, and maximal K_v-tori $T(v)$ of G for $v \in V$ such that for any element $t \in G(K) \cap U$ with $U = \prod_{v\in V} \mathscr{U}(v,T(v))$ which is regular semi-simple,*[2] *the inclusion* (3.2) *holds with $T = Z_G(t)^\circ$. Then* (F) *is a central extension.*

Proof of (i). Assume (F) is central. Then the finiteness of the metaplectic kernel $M(S,G)$ [36, Theorem 2.7] implies that F is finite (cf. [39, Sects. 3.4–3.6]). Set $n = |F|$. Now, let T be a maximal K-torus of G, let $t \in T(K)$, and let $\mathscr{T} = \theta^{-1}(T(\mathbb{A}(S)))$. By Lemma 2.6, the map $\gamma_t\colon x \mapsto [t,x]$ yields a group homomorphism $\mathscr{T} \to F$. It follows that $\gamma_t(\mathscr{T}^n) = \{1\}$, i.e. $\mathscr{T}^n \subset Z_H(t)$. On the other hand, $\theta(\mathscr{T}^n) = T(\mathbb{A}(S))^n$, and our assertion follows. $\square$

For the proof of part (ii) we need the following proposition in which we use $\overline{X}$ and $\widehat{X}$ to denote the closure of a subset X of $G(K)$ in $\overline{G}$ and $\widehat{G}$, respectively.

Proposition 3.2 (cf. [42, Proposition 3.2])**.** *Assume that there exists a positive integer n, a finite set of places $V \subset V^K \setminus S$, and maximal K_v-tori $T(v)$ of G for $v \in V$ such that for every regular semi-simple element $t \in G(K) \cap U$, where $U = \prod_{v\in V} \mathscr{U}(v,T(v))$, the inclusion* (3.2) *holds for $T = Z_G(t)^\circ$. Then for any normal subgroup N of $\Gamma = G(\mathcal{O}(S))$ of finite index and any $x \in \overline{N} \cap \Gamma$, we have*

$$Z(N,x)(\overline{N} \cap \Gamma) \supset (\Gamma \cap U)^n, \tag{3.3}$$

where $Z(N,x) := \{\gamma \in \Gamma \mid [x,\gamma] \in N\}$.

(Note that $Z(N,x)$ is simply the pullback of the centralizer of xN in Γ/N under the canonical homomorphism $\Gamma \to \Gamma/N$.)

Proof. For proving (3.3), we may replace N with a smaller normal subgroup of Γ of finite index to assume that $\overline{N} = \prod_{v\notin S} N_v$, where $N_v \subset G(\mathcal{O}_v)$ is an open normal subgroup for all $v \notin S$ and $N_v = G(\mathcal{O}_v)$ for all $v \in V^K \setminus (S \cup V')$ for a suitable finite *nonempty* subset $V' \subset V^K \setminus S$.

We need to show that for any $z \in \Gamma \cap U$, we have

$$z^n \in Z(N,x)(\overline{N} \cap \Gamma). \tag{3.4}$$

[2] Of course, any $t \in G(K) \cap U$ is automatically regular semi-simple if $V \neq \varnothing$.

If $V \neq \varnothing$, then z is automatically regular semi-simple. If $V = \varnothing$, then $\Gamma \cap U = \Gamma$, and using the Zariski-density of N in G in conjunction with the fact that the set of regular semi-simple elements is Zariski-open in G, we see that the coset zN contains a regular semi-simple element $z' \in \Gamma \cap U$. Hence, in proving (3.4), we may assume z to be regular semi-simple. Let $T_0 = Z_G(z)^\circ$ be the maximal K-torus of G containing z. For $v \in V'' := V \cup V'$ consider the open set $W_v := \varphi_{v,T_0}(N_v \times T_0^{\mathrm{reg}}(K_v))$ of $G(K_v)$ (see (3.1)), and then set

$$\mathcal{W} = \prod_{v \in V''} W_v \qquad \text{and} \qquad \mathcal{N} = \prod_{v \in V''} N_v.$$

Since N_v is an open subgroup, it meets $T_0^{\mathrm{reg}}(K_v)$ for every $v \in V''$, which implies that $\mathcal{W} \cap \mathcal{N}$ is a *nonempty* open subset of $\mathcal{N}$, and hence $\mathcal{N} \subset \mathcal{W}N$. Since $x \in \overline{N} \cap \Gamma$, there exists $y \in N$ such that

$$xy = gbg^{-1} \tag{3.5}$$

for some $g = (g_v)$ and $b = (b_v)$, with $g_v \in N_v$ and $b_v \in T_0^{\mathrm{reg}}(K_v)$ for $v \in V''$. As $V'' \neq \varnothing$, the element $t := xy$ is automatically regular semi-simple. Let $T = Z_G(t)^\circ$ be the maximal K-torus of G containing t.

For $v \notin S$, define

$$a_v = \begin{cases} g_v z^n g_v^{-1} & \text{if } \ v \in V'', \\ 1 & \text{if } \ v \notin S \cup V''. \end{cases}$$

It follows from (3.5) that the S-adele $a = (a_v)$ belongs to $T(\mathbb{A}(S))^n$. So, by (3.2) there exists $s \in Z_H(t)$ such that $\theta(s) = a$. In fact, $a \in \overline{\Gamma}$, so $s \in \widehat{\Gamma}$, and therefore $\Gamma \cap s\widehat{N}$ is nonempty. Pick $c \in \Gamma \cap s\widehat{N}$. Then

$$[x, c] \in [t, c]\widehat{N} = [t, s]\widehat{N} = \widehat{N},$$

implying that $c \in Z(N, x)$ (note that, being of finite index in Γ, the normal subgroup N is open (and hence closed) in the profinite topology on the former, so $\Gamma \cap \widehat{N} = N$). On the other hand,

$$c \in \theta(s)\overline{N} = a\overline{N} = z^n\overline{N}$$

as $az^{-n} \in \overline{N}$ because $a_v z^{-n} = [g_v, z^n] \in N_v$ since $g_v \in N_v$ for $v \in V''$, and $a_v z^{-n} = z^{-n} \in G(\mathcal{O}_v) = N_v$ for $v \in V^K \setminus (S \cup V'')$. $\square$

Proof of Theorem 3.1(ii). First, we will derive from Proposition 3.2 that for any $x \in F$ we have the inclusion

$$\theta(Z_H(x)) \supset (\overline{\Gamma \cap U})^n. \tag{3.6}$$

Consider the profinite group $\Delta = \theta^{-1}(\overline{\Gamma})$, which is a quotient of $\widehat{\Gamma}$, and take any $\gamma \in \Gamma \cap U$. We identify Γ with a dense subgroup of Δ using the splitting of θ over $G(K)$. Let $\mathscr{R}$ be the family of all open normal subgroups of Δ. For $R \in \mathscr{R}$, set

$$N_R := \Gamma \cap R \qquad \text{and} \qquad \widetilde{R} := \theta^{-1}(\overline{N_R})$$

and pick $x_R \in \Gamma \cap (xR)$. Applying Proposition 3.2 to N_R and x_R, we find that

$$\gamma^n \widetilde{R} \cap \widetilde{Z}(R, x) \neq \varnothing \qquad \text{for any} \quad R \in \mathscr{R}, \tag{3.7}$$

where $\widetilde{Z}(R, x) := \{\delta \in \Delta \mid [x, \delta] \in R\} = \{\delta \in \Delta \mid [x_R, \delta] \in R\}$. Using the compactness of F, one easily derives from this that

$$\gamma^n F \cap Z_\Delta(x) \neq \varnothing. \tag{3.8}$$

Indeed, one observes that

$$\bigcap_{R\in\mathscr{R}} \widetilde{R} = F, \qquad \bigcap_{R\in\mathscr{R}} \widetilde{Z}(R,x) = Z_\Delta(x),$$

and for any $R_1,\dots,R_d\in\mathscr{R}$, we have

$$\widetilde{Z}(R_1,x)\cap\ldots\cap\widetilde{Z}(R_d,x) = \widetilde{Z}(R_1\cap\ldots\cap R_d,x).$$

So, if (3.8) does not hold, there exists $R'\in\mathscr{R}$ such $\gamma^n F\cap Z(R',x)=\varnothing$. Next, using the compactness of $Z(R',x)$, we see that there exists $R''\in\mathscr{R}$ such that $\gamma^n R''\cap Z(R',x)=\varnothing$. Then for $R=R'\cap R''$, (3.7) fails to hold, a contradiction.

We have proved that $(\Gamma\cap U)^n\subset\theta(Z_\Delta(x))$. Since $\theta(Z_\Delta(x))$ is closed, passing to the closure, we obtain (3.6). Furthermore, we have $\overline{\Gamma\cap U}=\prod_{v\notin S}\overline{\Omega_v}$, where $\Omega_v=G(\mathcal{O}_v)\cap\mathscr{U}(v,T(v))$ for $v\in V$ and $\Omega_v=G(\mathcal{O}_v)$ for $v\in V^K\setminus(S\cup V)$. For all v, Ω_v is a *nonempty* open subset of $G(K_v)$; hence it is Zariski-dense. It follows that $(\Omega_v)^n$ is always infinite. Now, we conclude from (3.6) and Proposition 2.2 that $\mathfrak{Z}(F)$ equals $V^K\setminus(S\cup\mathcal{A})$. Then the extension (F) is central by Proposition 2.5. □

4. FIRST APPLICATIONS AND PROOF OF THEOREM A

To verify the inclusion (3.2) in Theorem 3.1, we observe that for $t\in T(K)$, the centralizer $Z_H(t)$ contains $T(K)$ and hence the closure $\widehat{\overline{T(K)}}$, and therefore $\theta(Z_H(t))$ contains $\theta(\widehat{\overline{T(K)}})=\overline{T(K)}$. So, we could immediately derive the centrality of (F) using Theorem 3.1 if we knew that there exists an integer $n>0$ such that for any maximal K-torus T of G (or at least for any maximal K-torus with specified local behavior at finitely many places), the quotient $T(\mathbb{A}(S))/\overline{T(K)}$ has exponent dividing n ("almost strong approximation property" up to exponent n). Unfortunately, when S is finite, the latter quotient may have infinite exponent (cf. [37, Proposition 4]), which forces us to use some additional considerations (cf. Proposition 4.5 and Examples 4.6 and 4.7 below). In the next section, we will establish the almost strong approximation property in the case where S contains all but finitely many elements of a generalized arithmetic progression (see Theorem 5.3), which will lead to Theorem B of the Introduction. In this section we will consider separately a basic case where $V:=V^K\setminus S$ is finite (i.e., S is cofinite) as this case has some interesting consequences (like Theorem A of the Introduction). Since in this case the corresponding ring of S-integers $\mathcal{O}(S)$ is the intersection of finitely many discrete valuation subrings of K corresponding to the places in V, and hence is semi-local, we will refer to this case as *semi-local*.

We begin with the following proposition which was already implicitly established in [36, § 9].

Proposition 4.1 (almost weak approximation)**.** *For every $d\ge 1$, there exists an integer $n=n(d)\ge 1$ such that given a K-torus T of dimension $\le d$, for any finite set of places $V\subset V^K$, the quotient $T_V/\overline{T(K)}$, where $T_V=\prod_{v\in V}T(K_v)$ and $\overline{T(K)}$ denotes the closure of $T(K)$ in T_V, has exponent dividing n.*

Proof. Pick a positive integer $n=n(d)$ which is divisible by the order of any finite subgroup of the group $\mathrm{GL}_d(\mathbb{Z})$ (it follows from Minkowski's lemma that one can take n to be the index in $\mathrm{GL}_d(\mathbb{Z})$ of the principal congruence subgroup modulo 3). Let T be an arbitrary K-torus of dimension $\le d$. We let $E:=K_T$ denote the minimal splitting field of T over K, and set $\mathcal{G}=\mathrm{Gal}(E/K)$. The natural action of $\mathcal{G}$ on the character group $X(T)$ defines its faithful representation in $\mathrm{GL}_m(\mathbb{Z})$, so the order $|\mathcal{G}|$ divides $n(d)$. Then, for the dual module of co-characters $X_*(T)$, there is a surjective homomorphism $\phi\colon\mathbb{Z}[\mathcal{G}]^\ell\to X_*(T)$. Let $M=\operatorname{Ker}\phi$. Let T' and T'' be the K-tori that split over E and have $\mathbb{Z}[\mathcal{G}]^\ell$ and M as their co-character modules; clearly, $T'=\mathrm{R}_{E/K}(\mathrm{GL}_1)^\ell$; hence it is quasi-split. We have the following exact sequence of K-tori:

$$1\to T''\to T'\xrightarrow{\eta}T\to 1.$$

This sequence gives rise to the following commutative diagram with exact bottom row:

$$\begin{array}{ccccc} T'(K) & \xrightarrow{\eta_K} & T(K) & & \\ \downarrow & & \downarrow & & \\ T'_V & \xrightarrow{\eta_V} & T_V & \longrightarrow & \prod_{v\in V} H^1(K_v, T'') \end{array}$$

Being quasi-split, hence rational over K, the torus T' has the weak approximation property with respect to any finite set of places (cf. [31, Proposition 7.3]), i.e. $\overline{T'(K)} = T'_V$. It follows that $\overline{T(K)}$ contains $\eta_V(T'_V)$. On the other hand, the quotient $T_V/\eta_V(T'_V)$ embeds into $\prod_{v\in V} H^1(K_v, T'')$. But for $v \in V$, as a consequence of Hilbert's Theorem 90 for tori we have $H^1(K_v, T'') = H^1(\mathcal{G}_w, T''(E_w))$ where $\mathcal{G}_w$ is the decomposition group $\mathrm{Gal}(E_w/K_v)$ for some extension $w|v$. By our construction, the order $|\mathcal{G}_w|$ divides n. Therefore, the quotient $T_V/\eta_V(T'_V)$ has exponent dividing n, and our claim follows. (We note that the proof enables us to somewhat optimize our choice of n: all we need is that n be divisible by the order of any finite *solvable* subgroup of $\mathrm{GL}_d(\mathbb{Z})$.) $\square$

Corollary 4.2. *Let G be a reductive K-group. There exists $n \geq 1$ such that for any maximal K-torus T of G and any finite set of places $V \subset V^K$, the quotient $T_V/\overline{T(K)}$ has exponent dividing n.*

Now, let G be an absolutely almost simple simply connected algebraic group over a global field K, and let V be a finite set of nonarchimedean places of K containing the set $\mathcal{A}$ of anisotropic places. Set $S = V^K \setminus V$. Then for any maximal K-torus T of G the group $T(\mathbb{A}(S))$ can be identified with the group T_V in the above notation. Thus, Corollary 4.2 asserts the existence of $n \geq 1$ (independent of T) such that the closure $\overline{T(K)}$ of $T(K)$ in $T(\mathbb{A}(S))$ contains $T(\mathbb{A}(S))^n$ for *any* maximal K-torus T of G. Let us use this fact to analyze the congruence sequence (C) appearing in Section 2. As we observed at the beginning of this section, for a maximal K-torus T of G and any $t \in T(K)$, the image $\pi(Z_{\widehat{G}}(t))$ of the corresponding centralizer contains $\overline{T(K)}$ and hence $T(\mathbb{A}(S))^n$. This enables us to use Theorem 3.1 to conclude that the congruence kernel $C^{(S)}(G)$ is central. Furthermore, it follows from our computations of the metaplectic kernel [36] that in the situation at hand $M(S, G)$ is trivial, so being central, $C^{(S)}(G)$ is actually trivial (provided that (MP) holds for $G(K)$, which we assume). Thus, we obtain the following:

Theorem 4.3. *Let G be an absolutely almost simple simply connected algebraic group over a global field K, and assume that* (MP) *holds for $G(K)$. Then for any finite set V of nonarchimedean places of K that contains the set $\mathcal{A}$ of anisotropic places and for $S = V^K \setminus V$, the congruence kernel $C^{(S)}(G)$ is central and hence trivial.*

Remark 4.4. Sury [62] showed that for absolutely almost simple simply connected anisotropic groups of type A_1 as well as for simply connected groups of classical types associated with bilinear and certain hermitian/skew-hermitian forms, the methods used to prove (MP) (see [31, Ch. 9]) can be adapted to prove Theorem 4.3. This does not appear to be the case for the anisotropic inner forms of type A_n with $n > 1$, i.e. for the groups of the form $G = \mathrm{SL}_{1,D}$, where D is a central division algebra over K of degree $d > 2$. Indeed, in this case the proof of (MP) is derived from the following result which is valid over *any* field: *Let D be a finite-dimensional division algebra over a field K. Then $D^\times$ cannot have a nonabelian finite simple group as a quotient* (see [57] and also [54]). *In fact, every finite quotient of $D^\times$ is solvable* [55]. (See also [51] for another proof of (MP) along these lines.) All these results rely on the following fact: *For a finite index subgroup N of $D^\times$, we have $D = N - N$* [4, 69]. However, there is no analog of this fact for finite-index subgroups of $\mathcal{D}^\times$, where $\mathcal{D}$ is an order in D over a semi-local subring $\mathcal{O}$ of K that has finite homomorphic images (see [4] regarding the case where $\mathcal{D}$ has no such images).

Combining Theorem 4.3 with Proposition 2.8, we obtain the following.

Proposition 4.5. *Assume that $\mathcal{A} \cap S = \varnothing$ and there is a partition $V^K \setminus (S \cup \mathcal{A}) = \bigcup_{i\in I} V_i$, with all V_i's* finite, *such that one can find subgroups $H_{\mathcal{A}}$ and H_i $(i \in I)$ of H satisfying the following conditions*:

(i) *$\theta(H_{\mathcal{A}})$ is a dense subgroup of $G_{\mathcal{A}} = \prod_{v\in\mathcal{A}} G(K_v)$, and $\theta(H_i)$ is a dense subgroup of $G(\mathbb{A}(V^K \setminus V_i))$ for all $i \in I$*;

(ii) *any two of the subgroups $H_{\mathcal{A}}$ and H_i for $i \in I$ commute elementwise*;

(iii) *the subgroups $H_{\mathcal{A}}$ and H_i for $i \in I$ generate a dense subgroup of H.*

Then (F) *is a central extension.*

Proof of Theorem A. We apply Proposition 4.5 to $H = \widehat{G}^{(S)}$ and $F = C^{(S)}(G)$ by considering the partition of $V^K \setminus (S \cup \mathcal{A})$ into one-element subsets (singletons). We let $H_{\mathcal{A}}$ be the subgroup generated by $\mathscr{G}_v$ (notations as in the statement of Theorem A) for $v \in \mathcal{A}$, and set $H_v = \mathscr{G}_v$ for $v \in V^K \setminus (S \cup \mathcal{A})$. Then the assumptions of Theorem A immediately show that the conditions of Proposition 4.5 are satisfied and the centrality of $C^{(S)}(G)$ follows. □

We will now show how Theorem A can be used to establish the centrality of $C^{(S)}(G)$ in some known cases.

Example 4.6. Let $G = \mathrm{SL}_n$ with $n \geq 3$ and $S \subset V^K$ be an arbitrary subset containing V^K_∞. The first proof of centrality in this case was given by Bass, Milnor, and Serre in [3]. In order to apply Theorem A and give an alternative argument, for $1 \leq i, j \leq n$, $i \neq j$, we consider the corresponding 1-dimensional unipotent subgroup U_{ij} of G together with its canonical parametrization $e_{ij}\colon \mathbb{G}_a \to U_{ij}$. The following commutation relation for elementary matrices is well-known:

$$[e_{ij}(s), e_{lm}(t)] = \begin{cases} 1, & i \neq m,\ j \neq l, \\ e_{im}(st), & j = l,\ i \neq m, \\ e_{lj}(-st), & j \neq l,\ i = m. \end{cases} \tag{4.1}$$

It is easy to see that the topologies τ_{a} and τ_{c} of $G(K)$ induce the same topology on each $U_{ij}(K)$ (cf. [3, Theorem 7.5(e)]). So, if $\widehat{U}_{ij}$ and $\overline{U}_{ij}$ denote the closures of $U_{ij}(K)$ in $\widehat{G}$ and $\overline{G}$, respectively, then $\widehat{G} \xrightarrow{\pi} \overline{G}$ restricts to an isomorphism $\widehat{U}_{ij} \xrightarrow{\pi_{ij}} \overline{U}_{ij}$. By the strong approximation property for the additive group $\mathbb{G}_a$, the isomorphism $(e_{ij})_K\colon K^+ \to U_{ij}(K)$ extends to an isomorphism $\overline{e}_{ij}\colon \mathbb{A}(S) \to \overline{U}_{ij}$. Then $\widehat{e}_{ij} := \pi_{ij}^{-1} \circ \overline{e}_{ij}$ is an isomorphism $\mathbb{A}(S) \to \widehat{U}_{ij}$. We will let $\mathscr{G}_v$ for $v \notin S$ denote the subgroup of $\widehat{G}$ generated by $\widehat{e}_{ij}(t)$ for all $t \in K_v \subset \mathbb{A}_S$ and all $i \neq j$. Clearly, the $\mathscr{G}_v$'s satisfy condition (i) of Theorem A. Since K_v for $v \in V^K \setminus S$ additively generate a dense subgroup of $\mathbb{A}(S)$, the closed subgroup of $\widehat{G}$ generated by the $\mathscr{G}_v$, $v \notin S$, contains $\widehat{e}_{ij}(\mathbb{A}(S))$ for all $i \neq j$. In particular, it contains $\widehat{e}_{ij}(K)$ for all $i \neq j$, hence $G(K)$, and therefore coincides with $\widehat{G}$, verifying condition (iii). Finally, to check (ii), we observe that the density of K in $\mathbb{A}(S)$ implies that (4.1) entails a similar expression for $[\widehat{e}_{ij}(s), \widehat{e}_{lm}(t)]$ for any $s, t \in \mathbb{A}(S)$. Now, for $s \in K_{v_1}$ and $t \in K_{v_2}$, where $v_1 \neq v_2$, we have $st = 0$ in $\mathbb{A}(S)$, which implies that $\widehat{e}_{ij}(s)$ and $\widehat{e}_{lm}(t)$ commute except possibly when $l = j$ and $m = i$. In the latter case, as $n \geq 3$, we can pick $l \neq i, j$ and then write $\widehat{e}_{ji}(t) = [\widehat{e}_{jl}(t), \widehat{e}_{li}(1_{K_{v_2}})]$. Since $\widehat{e}_{ij}(s)$ is already known to commute with $\widehat{e}_{jl}(t)$ and $\widehat{e}_{li}(1_{K_{v_2}})$, it commutes with $\widehat{e}_{ji}(t)$ as well. This shows that $\mathscr{G}_{v_1}$ and $\mathscr{G}_{v_2}$ commute elementwise, which verifies condition (ii) of Theorem A. Then the latter yields the centrality of $C^{(S)}(G)$.

(We note that the idea of using commuting lifts of "local" groups is useful in the analysis of the congruence subgroup problem not only in the context of algebraic groups over the rings of S-integers in global fields; it was used in [53] together with the result of M. Stein [61] on the centrality of K_2 over semi-local rings to prove the centrality of the congruence kernel for elementary subgroups of Chevalley groups of rank > 1 over arbitrary Noetherian rings. It is worth noting that the argument in [53] which is based on almost weak approximation in maximal tori and the action of the group

of rational points on the congruence kernel enables one to bypass the rather technical computations of Stein, but the exact trade-off between these two approaches is not apparent.)

Example 4.7. Let $G = \mathrm{SL}_2$, and let $S \subset V^K$ be a subset that contains V_∞^K and is of size $|S| > 1$; by Dirichlet's unit theorem (see [2, Ch. II, Theorem 18.1]), the latter is equivalent to the existence of a unit $\varepsilon \in \mathcal{O}(S)^\times$ of infinite order. The centrality of $C^{(S)}(G)$ in this case was first established by Serre [58]. We will now show that this can also be derived from Theorem A. (We note that the argument below, unlike Serre's original proof, does not use Chebotarev's density theorem.) We let U^+, U^-, and T denote the subgroups of upper and lower unitriangular matrices and of diagonal matrices, respectively, and fix the following standard parametrizations of these groups:

$$u^+(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \qquad u^-(b) = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, \qquad h(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

($a, b \in \mathbb{G}_a$, $t \in \mathrm{GL}_1$). For $a, b \in K$ such that $ab \neq 1$, one easily verifies the following commutator identity:

$$[u^+(a), u^-(b)] = u^+\biggl(-\frac{a^2 b}{1-ab}\biggr)\, h\biggl(\frac{1}{1-ab}\biggr)\, u^-\biggl(\frac{ab^2}{1-ab}\biggr). \tag{4.2}$$

We let $\widehat{U}^\pm$ and $\overline{U}^\pm$ denote the closures of $U^\pm(K)$ in $\widehat{G}$ and $\overline{G}$, respectively. Again, it is easy to check that the topologies τ_{a} and τ_{c} of $G(K)$ induce the same topology on $U^+(K)$ and $U^-(K)$ (cf. [58, n° 1.4, Proposition 1]), so $\widehat{G} \xrightarrow{\pi} \overline{G}$ restricts to isomorphisms $\widehat{U}^\pm \xrightarrow{\pi^\pm} \overline{U}^\pm$. Furthermore, $(u^\pm)_K$ extend to isomorphisms $\overline{u}^\pm\colon \mathbb{A}(S) \to \overline{U}^\pm$. So, the maps $\widehat{u}^\pm := (\pi^\pm)^{-1} \circ \overline{u}^\pm$ give isomorphisms $\mathbb{A}(S) \to \widehat{U}^\pm$. For $v \in V^K \setminus S$, we let $\mathscr{G}_v$ denote the subgroup of $\widehat{G}$ generated by $\widehat{u}^+(K_v)$ and $\widehat{u}^-(K_v)$. As in Example 4.6, one checks that the subgroups $\mathscr{G}_v$ clearly satisfy conditions (i) and (iii) of Theorem A, so we only need to verify condition (ii). In other words, we need to show that for $v_1 \neq v_2$, the subgroups $\widehat{u}^+(K_{v_1})$ and $\widehat{u}^-(K_{v_2})$ commute elementwise.

First, we construct *nonzero* $a_0 \in K_{v_1}$ and $b_0 \in K_{v_2}$ such that $\widehat{u}^+(a_0)$ and $\widehat{u}^-(b_0)$ commute in $\widehat{G}$. Let us enumerate the valuations in $V^K \setminus (S \cup \{v_1, v_2\})$ as $v_3, v_4, \ldots$. If d is the class number of $\mathcal{O}(S)$, then for each $i = 1, 2, 3, \ldots$, we can pick an element $p_i \in \mathcal{O}(S)$ such that $v_i(p_i) = d$ and $v_j(p_i) = 0$ for $j \neq i$. Fix a unit $\varepsilon \in \mathcal{O}(S)^\times$ of infinite order. Then for any $m \geq 2$ we can find an integer $n(m)$ divisible by $m!$ so that

$$\varepsilon^{n(m)} \equiv 1 \pmod{(p_1 \ldots p_m)^{2m}}.$$

We can then write $1 - \varepsilon^{n(m)} = a_m b_m$ with $a_m, b_m \in \mathcal{O}(S)$ satisfying

$$a_m \equiv 0 \pmod{(p_2 \ldots p_m)^m}, \qquad v_1(a_m) < d, \tag{a}$$

and

$$b_m \equiv 0 \pmod{(p_1 p_3 \ldots p_m)^m}, \qquad v_2(b_m) < d. \tag{b}$$

Since $a_m, b_m \in \mathcal{O}(S)$, there exists a subsequence $\{m_j\}$ such that $a_{m_j} \to a_0$ and $b_{m_j} \to b_0$ in $\mathbb{A}(S)$. In fact, it follows from (a) and (b) that $a_0 \in K_{v_1}^\times$ and $b_0 \in K_{v_2}^\times$. To show that $\widehat{u}^+(a_0)$ and $\widehat{u}^-(b_0)$ commute, we observe that

$$[\widehat{u}^+(a_0), \widehat{u}^-(b_0)] = \lim_{j\to\infty} [u^+(a_{m_j}), u^-(b_{m_j})] \qquad \text{in } \widehat{G}.$$

On the other hand, using (4.2), we obtain

$$[u^+(a_m), u^-(b_m)] = u^+\bigl(-a_m^2 b_m \varepsilon^{-n(m)}\bigr) h\bigl(\varepsilon^{-n(m)}\bigr) u^-\bigl(a_m b_m^2 \varepsilon^{-n(m)}\bigr) \to 1 \qquad \text{in } \widehat{G},$$

because $a_m^2 b_m, a_m b_m^2 \to 0$ in $\mathbb{A}(S)$ and $h(\varepsilon^{n(m)}) \to 1$ in $\widehat{G}$ as $n(m)$ is divisible by $m!$ and hence $h(\varepsilon^{n(m)})$ belongs to any given finite index normal subgroup N of $G(\mathcal{O}(S))$ for all sufficiently large m.

Thus, $[\widehat{u}^+(a_0), \widehat{u}^-(b_0)] = 1$. Now, for $t \in K^\times$, the automorphism σ_t of G given by conjugation by $\mathrm{diag}(t, 1)$ extends to an automorphism $\widehat{\sigma}_t$ of $\widehat{G}$. Then

$$1 = \sigma_t([\widehat{u}^+(a_0), \widehat{u}^-(b_0)]) = [\widehat{u}^+(ta_0), \widehat{u}^-(t^{-1}b_0)]$$

for any $t \in K^\times$. Since $K^\times$ is dense in $K_{v_1}^\times \times K_{v_2}^\times$ by weak approximation, we find that $[\widehat{u}^+(a), \widehat{u}^-(b)] = 1$ for *all* $a \in K_{v_1}$, $b \in K_{v_2}$, as required.

Remark 4.8. The argument given in Example 4.6 can be generalized to prove the centrality of $C^{(S)}(G)$ for any absolutely almost simple simply connected algebraic K-group G with $\mathrm{rk}_K G \geq 2$. The first proof of this fact was given by M.S. Raghunathan in [40]; a shorter argument was given in [43]. The case where $\mathrm{rk}_K G = 1$ and $\mathrm{rk}_S G \geq 2$ (which generalizes Example 4.7) is more complicated; it was treated by Raghunathan in [41] by a different method. One can give an alternative (shorter) argument (at least when $\mathrm{char}\, K \neq 2$) based on Proposition 4.5; details will be published elsewhere. Theorem A can also be used to simplify the proof of Serre's conjecture for some anisotropic exceptional groups [47].

5. STRONG APPROXIMATION PROPERTY IN TORI WITH RESPECT TO ARITHMETIC PROGRESSIONS AND THE PROOF OF THEOREM B

Strong approximation property in tori with respect to (generalized) arithmetic progressions was analyzed in [37], and we begin by reviewing some of the results obtained therein (we refer the reader to [12] and references therein for the analysis of strong approximation from a different perspective). Let $\mathscr{P}(F/K, \mathscr{C})$ be a generalized arithmetic progression, where F/K is a finite Galois extension with Galois group $\mathcal{G}$ and $\mathscr{C}$ is a conjugacy class in $\mathcal{G}$ (for definition see Section 1). For a finite extension E/K, we let $\mathbb{I}_E$ denote the group of ideles of E. Furthermore, given a subset S of V^K, we let $\overline{S}$ denote the set of all extensions of places from S to E, and then let $\mathbb{I}_E(\overline{S})$ denote the group of $\overline{S}$-ideles and let $\overline{E^\times}^{(\overline{S})}$ be the closure of (the diagonally embedded) $E^\times$ in $\mathbb{I}_E(\overline{S})$.

Proposition 5.1 (cf. [37, Proposition 3])**.** *Let $\mathscr{P}(F/K, \mathscr{C})$ be a generalized arithmetic progression, $\mathscr{P}_0 \subset \mathscr{P}(F/K, \mathscr{C})$ be a finite (possibly, empty) subset, and let*

$$S = (\mathscr{P}(F/K, \mathscr{C}) \setminus \mathscr{P}_0) \cup V_\infty^K.$$

Furthermore, let E/K be a finite separable extension. If $\mathscr{C}$ contains an automorphism that acts trivially on $E \cap F$ (in particular, if $\mathscr{C} = \{e\}$ or $E \cap F = K$), then the index

$$\left[\mathbb{I}_E(\overline{S}) : \overline{E^\times}^{(\overline{S})}\right] \quad \textit{is finite and divides} \quad [F : K].$$

Proof. By the reduction theory for ideles (cf. [2, Ch. II, § 16]), the quotient $\mathbb{I}_E^1/E^\times$, where $\mathbb{I}_E^1$ is the group of ideles with content 1, is compact. On the other hand, for any $w \in V^E$, the product $E_w^\times \mathbb{I}_E^1$ is a closed subgroup and the quotient $\mathbb{I}_E/E_w^\times \mathbb{I}_E^1$ is compact (in fact, this quotient is trivial if w is archimedean and is finite in the function field case). It follows that for any *nonempty* $T \subset V^E$, the quotient $\mathbb{I}_E(T)/\overline{E^\times}^{(T)}$ is compact. Since S contains V_∞^K, we conclude that, in our notation, the quotient $\mathbb{I}_E(\overline{S})/\overline{E^\times}^{(\overline{S})}$ is a profinite group; hence

$$\overline{E^\times}^{(\overline{S})} = \bigcap B,$$

where B runs through all open subgroups of $\mathbb{I}_E(\overline{S})$ that contain $E^\times$ (note that these automatically have finite index). Thus, it suffices to show that for any such B, the index $[\mathbb{I}_E(\overline{S}) : B]$ divides $[F : E \cap F] = [EF : E]$. Let M be the preimage of B under the natural projection $\mathbb{I}_E \to \mathbb{I}_E(\overline{S})$. By class field theory, for the norm subgroup $N = N_{EF/E}(\mathbb{I}_{EF})E^\times$, the index $[\mathbb{I}_E : N]$ equals the degree

of the maximal abelian subextension of EF/E and hence divides $[EF:E]$. So, it is enough to show that M contains N, or equivalently, the abelian extension P of E with the norm subgroup M is contained in EF. We note that by our construction for every $w \in \overline{S}$, the multiplicative group $E_w^\times$ is contained in M, and hence the extension P/E splits at w (cf. [2, Exercise 3]).

Let R be the minimal Galois extension of K that contains E, F, and P. Let $\sigma \in \mathscr{C}$ be an automorphism that acts trivially on $E \cap F$; then there exists $\widetilde{\sigma} \in \mathrm{Gal}(EF/E)$ whose restriction to F is σ. We will now show that actually $P \subset (EF)^{\widetilde{\sigma}}$. Assume the contrary. Then there exists $\tau \in \mathrm{Gal}(R/K)$ such that $\tau|EF = \widetilde{\sigma}$ and $\tau|P \neq \mathrm{id}_P$. (Indeed, let $\tau_0 \in \mathrm{Gal}(R/K)$ be some lift of $\widetilde{\sigma}$. If $P \subset EF$ then we can simply take $\tau = \tau_0$. So, suppose $P \not\subset EF$. If every lift $\tau \in \mathrm{Gal}(R/K)$ of $\widetilde{\sigma}$ acted trivially on P, we would have the inclusion $\tau_0\mathrm{Gal}(R/EF) \subset \mathrm{Gal}(R/P)$. Then $\mathrm{Gal}(R/EF) \subset \mathrm{Gal}(R/P)$; hence $P \subset EF$, a contradiction. This proves the existence of a required lift τ in all cases.) By Chebotarev's density theorem (cf. [2, Ch. VII, Sect. 2.4]), there exists a nonarchimedean $v \in V^K \setminus \mathscr{P}_0$ such that R is unramified at v and for a suitable extension u we have $\mathrm{Fr}_{R/K}(u|v) = \tau$. Clearly, $v \in \mathscr{P}(F/K, \mathscr{C}) \setminus \mathscr{P}_0$, so the restriction w of u to E lies in $\overline{S}$. On the other hand, since τ restricts to P nontrivially, we see that P does not split at w, a contradiction. $\square$

Remark 5.2. The above argument is a modification of the argument given in [37] in the case of arithmetic progressions defined by an abelian extension F/K. We note that our argument here shows the index $[\mathbb{I}_E(\overline{S}) : \overline{E^\times}^{(\overline{S})}]$ in fact divides the degree $[F^\sigma : K]$ for any $\sigma \in \mathscr{C}$ that acts trivially on $E \cap F$ (for this one needs to observe that $[(EF)^{\widetilde{\sigma}} : E]$ equals $[F^\sigma : E \cap F]$ and hence divides $[F^\sigma : K]$). We also point out that [37, Proposition 4] provides a converse in the case where F/K is abelian, viz. if $\mathscr{C} = \{\sigma\}$ and σ acts on $E \cap F$ nontrivially, then the quotient $\mathbb{I}_E(\overline{S})/\overline{E^\times}^{(\overline{S})}$ has infinite exponent.

Proposition 5.1 gives a form of the almost strong approximation property with respect to generalized arithmetic progressions. We now combine this with the method used in the proof of Proposition 4.1 to obtain the following.

Theorem 5.3 (almost strong approximation property, cf. [37, Theorem 3])**.** *For every $d, m \geq 1$ there exists an integer $n = n(d,m) \geq 1$ such that given a K-torus T of dimension $\leq d$, a generalized arithmetic progression $\mathscr{P}(F/K, \mathscr{C})$ with $[F:K] = m$, and a finite subset $\mathscr{P}_0 \subset \mathscr{P}(F/K, \mathscr{C})$, for the set $S = (\mathscr{P}(F/K, \mathscr{C}) \setminus \mathscr{P}_0) \cup V_\infty^K$, the closure $\overline{T(K)}^{(S)}$ of $T(K)$ in $T(\mathbb{A}(S))$ contains $T(\mathbb{A}(S))^n$, provided that some (equivalently, every) element of $\mathscr{C}$ acts trivially on $K_T \cap F$, where K_T is the splitting field of T.*

Proof. Let $n' = n'(d)$ be an integer divisible by the order of any finite subgroup of the group $\mathrm{GL}_d(\mathbb{Z})$ (see the proof of Proposition 4.1). We will show that $n(d,m) := n'(d) \cdot m$ is as required. Let T be a K-torus of dimension $\leq d$ such that for the splitting field $E := K_T$ some (equivalently, every) element of $\mathscr{C}$ acts trivially on $E \cap F$. As in the proof of Proposition 4.1, we can construct an exact sequence of K-tori

$$1 \to T'' \to T' \xrightarrow{\eta} T \to 1 \qquad (*)$$

with $T' = \mathrm{R}_{E/K}(\mathrm{GL}_1)^\ell$ for some $\ell \geq 1$. Since all the tori in $(*)$ split over E, we have the exact sequence of the groups of $\overline{S}$-adeles, where $\overline{S}$ consists of all extensions of places from S to E:

$$1 \to T''(\mathbb{A}_E(\overline{S})) \to T'(\mathbb{A}_E(\overline{S})) \xrightarrow{\eta_{\mathbb{A}_E(\overline{S})}} T(\mathbb{A}_E(\overline{S})) \to 1. \qquad (**)$$

This exact sequence induces the following commutative diagram with exact bottom row:

$$\begin{array}{ccccc} T'(K) & \xrightarrow{\eta_K} & T(K) & & \\ \downarrow & & \downarrow & & \\ T'(\mathbb{A}(S)) & \xrightarrow{\eta_{\mathbb{A}(S)}} & T(\mathbb{A}(S)) & \longrightarrow & H^1\big(\mathrm{Gal}(E/K), T''(\mathbb{A}_E(\overline{S}))\big) \end{array}$$

Clearly, $\overline{T(K)}^{(S)}$ contains $\eta_{A(S)}(\overline{T'(K)}^{(S)})$. But it follows from Proposition 5.1 that $\overline{T'(K)}^{(S)}$ contains $T'(\mathbb{A}(S))^m$. By the exactness of the bottom row, $T(\mathbb{A}(S))/\eta_{A(S)}(T'(\mathbb{A}(S)))$ has exponent dividing $[E:K]$ and hence $n'(d)$. So, our assertion follows. □

Remark 5.4. With some more work, one can prove the following full analog of Proposition 5.1 for arbitrary tori: *There exists $N = N(d,m)$ such that given a K-torus T of dimension $\le d$, a generalized arithmetic progression $\mathscr{P}(F/K,\mathscr{C})$ with $[F:K] = m$, and a finite $\mathscr{P}_0 \subset \mathscr{P}(F/K,\mathscr{C})$, for the set $S = (\mathscr{P}(F/K,\mathscr{C}) \setminus \mathscr{P}_0) \cup V_\infty^K$, the index $[T(\mathbb{A}(S)) : \overline{T(K)}^{(S)}]$ is finite and divides N, provided that some (equivalently, every) element of $\mathscr{C}$ acts trivially on $K_T \cap F$, where K_T/K is the splitting field of T.* Since this more precise statement is not needed in the proof of centrality of the congruence kernel, we will give the details elsewhere.

Proof of Theorem B. The assumption that S almost contains a generalized arithmetic progression $\mathscr{P}(F/K,\mathscr{C})$, of course, means that there exists a finite set $\mathscr{P}_0 \subset \mathscr{P}(F/K,\mathscr{C})$ such that S contains $S_0 := (\mathscr{P}(F/K,\mathscr{C}) \setminus \mathscr{P}_0) \cup V_\infty^K$. Besides, we are assuming that every element of $\mathscr{C}$ acts trivially on $F \cap L$, where L is the minimal Galois extension of K over which G is an inner form of a split group. Since S_0 contains a nonarchimedean place v such that G is K_v-isotropic, our computation of the metaplectic kernel shows that $M(S,G) = 1$ (see [36, Main Theorem]). This means that once we know that $C^{(S)}(G)$ is central, we can actually conclude that it is trivial. We will derive the centrality from Theorem 3.1, just as we did in the proof of Theorem 4.3; however, the difference is that while almost weak approximation property holds uniformly for all maximal K-tori T of G (see Corollary 4.2), Theorem 5.3 guarantees the almost strong approximation property only in the case where $\mathscr{C}$ is trivial on $K_T \cap F$. To show that this information is still sufficient for the proof of centrality, we need the following:

Lemma 5.5 (cf. [38, Theorem 2])**.** *Let G be a semi-simple algebraic group over a global field K, and let L be the minimal Galois extension of K over which G is an inner form of a split group. Furthermore, suppose we are given a finite subset $\mathcal{S} \subset V^K$ and a finite Galois extension F/K. Then there exists a finite subset $V \subset V^K \setminus \mathcal{S}$ and maximal K_v-tori $T(v)$ of G for $v \in V$ such that for any maximal K-torus T of G which is $G(K_v)$-conjugate to $T(v)$, the minimal splitting field K_T satisfies*

$$K_T \cap F = L \cap F. \tag{5.1}$$

Proof. Let $\tau_1, \dots, \tau_t$ be all the nontrivial elements of $\mathrm{Gal}(F/(F \cap L))$. We extend each τ_i to $\overline{\tau}_i \in \mathrm{Gal}(FL/K)$ by letting it act trivially on L. There exists a finite subset V_0 of V^K such that G is quasi-split over K_v for all $v \in V^K \setminus V_0$ (see [31, Theorem 6.7]). By Chebotarev's density theorem [2, Ch. VII, Sect. 2.4], we can find $v_1, \dots, v_t \in V_{\mathrm{f}}^K \setminus (S \cup V_0)$ such that FL is unramified at v_i and for an appropriate extension $w_i|v_i$, one has $\mathrm{Fr}_{FL/K}(w_i|v_i) = \overline{\tau}_i$, for each $i = 1, \dots, t$. Set $V = \{v_1, \dots, v_t\}$. Since $\overline{\tau}_i$ acts on L trivially, we conclude that $L \subset K_{v_i}$. Combining this with the fact that by our construction G is quasi-split over K_{v_i}, we find that G actually splits over K_{v_i}, and we let $T(v_i)$ denote its maximal K_{v_i}-split torus. We claim that these tori are as required. Indeed, let T be a maximal K-torus of G as in the statement of the lemma. Then its splitting field K_T satisfies $K_T \subset K_{v_i}$ for all $i = 1, \dots, t$. If we assume that $K_T \cap F \not\subset L \cap F$, then there exists an i such that τ_i acts nontrivially on $K_T \cap F$. Since $\tau_i = \mathrm{Fr}_{F/K}(v_i)$ lies in the local Galois group $\mathrm{Gal}(FK_{v_i}/K_{v_i})$, we see that $K_T \cap F \not\subset K_{v_i}$. A contradiction, proving the inclusion $\subset$ in (5.1). The opposite inclusion follows from the fact that L is contained in the splitting field of every maximal K-torus of G. □

To implement the above strategy (although with some variations) and prove Theorem B, we set $\mathcal{S} = \mathcal{A}(G) \cup V_\infty^K$ and use Lemma 5.5 to find a finite subset $V \subset V^K \setminus \mathcal{S}$ and maximal K_v-tori $T(v)$ of G for $v \in V$ with the properties described therein. Then set

$$S' = \big(\mathscr{P}(F/K,\mathscr{C}) \setminus (\mathscr{P}_0 \cup V)\big) \cup V_\infty^K.$$

Clearly, S' is contained in S and, in particular, is disjoint from $\mathcal{A}$ and V. Now, let t be any regular semi-simple element in $G(K) \cap U$ where $U = \prod_{v \in V} \mathscr{U}(v, T(v))$ in the notations introduced prior to the statement of Theorem 3.1, and let $T = Z_G(t)^\circ$ be the corresponding maximal K-torus of G. Then by construction T is $G(K_v)$-conjugate to $T(v)$ for all $v \in V$, so by Lemma 5.5 we have $K_T \cap F = F \cap L$. This means that the elements of $\mathscr{C}$ act trivially on $K_T \cap F$, and therefore Theorem 5.3 yields the inclusion $\overline{T(K)}^{(S')} \supset T(\mathbb{A}(S'))^n$ where $n = n(d, [F:K])$ is the number from this theorem and d is the absolute rank of G. On the other hand, we obviously have the inclusion $\pi^{(S')}(Z_{\widehat{G}^{(S')}}(t)) \supset \overline{T(K)}^{(S')}$. This verifies the assumptions of Theorem 3.1(ii) for the congruence sequence (C) associated with the set S' and, therefore, enables us to conclude that $C^{(S')}$ is central. As we explained at the beginning of the proof, since there exists a nonarchimedean $v \in S'$ such that G is K_v-isotropic, this implies that $C^{(S')}(G)$ is actually trivial. Finally, since $S' \subset S$ and $S \setminus S'$ does not contain any anisotropic places for G, there exists a natural *surjective* homomorphism $C^{(S')}(G) \to C^{(S)}(G)$ (cf. [40, Lemma 6.2]), so $C^{(S)}(G)$ is also trivial. $\square$

6. CONGRUENCE SUBGROUP PROPERTY FOR ARITHMETIC GROUPS WITH ADELIC PROFINITE COMPLETION: PROOF OF THEOREM C

Before we embark on the proof of Theorem C (of the Introduction), we would like to point out that for infinite arithmetic groups in positive characteristic the profinite completion is *never* adelic (see Remark 6.2 below), so we limited the statement of Theorem C to the case of number fields. The proof relies on the following properties of the group of adeles.

Lemma 6.1. *Let* $\Omega = \mathrm{GL}_n(\widehat{\mathbb{Z}}) = \prod_{q \text{ prime}} \mathrm{GL}_n(\mathbb{Z}_q)$, *and fix a prime* p.

(1) *There exists* $d \geq 1$ (*depending only on* n) *such that for any pro-*p *subgroup* $\mathscr{P}$ *of* Ω, *one has*

$$\left[\mathscr{P}^{(d)}, \mathscr{P}^{(d)}\right] \subset \mathrm{GL}_n(\mathbb{Z}_p),$$

where $\mathscr{P}^{(d)}$ *denotes the* (*closed*) *subgroup generated by the* d*-th powers of elements of* $\mathscr{P}$.

(2) *If* $\mathscr{P} \subset \Omega$ *is an analytic pro-*p *subgroup satisfying the following condition*:

(O) *for any open subgroup* $\mathscr{P}' \subset \mathscr{P}$, *the commutator subgroup* $[\mathscr{P}', \mathscr{P}']$ *is also open in* $\mathscr{P}$,

then the kernel of the projection $\mathscr{P} \to \prod_{q \neq p} \mathrm{GL}_n(\mathbb{Z}_q)$ *is open in* $\mathscr{P}$.

Proof. (1) By Jordan's theorem (cf., for example, [13]), there exists $\ell = \ell(n)$ such that every finite subgroup $J \subset \mathrm{GL}_n(F)$, where F is a field of characteristic zero, contains an abelian normal subgroup of index $\leq \ell$. Set $d = \ell!$ and observe that the exponent of any group of order $\leq \ell$ divides d. For a prime q, we let $\mathrm{pr}_q \colon \Omega \to \mathrm{GL}_n(\mathbb{Z}_q)$ denote the corresponding projection. The first congruence subgroup $\mathrm{GL}_n(\mathbb{Z}_q, q)$ is a normal pro-q subgroup of $\mathrm{GL}_n(\mathbb{Z}_q)$ of finite index. This means that for any $q \neq p$, the image $\mathrm{pr}_q(\mathscr{P})$ has trivial intersection with $\mathrm{GL}_n(\mathbb{Z}_q, q)$ and hence is finite. Then our choice of d forces $\mathrm{pr}_q(\mathscr{P}^{(d)}) = \mathrm{pr}_q(\mathscr{P})^{(d)}$ to be abelian, implying that $\mathrm{pr}_q([\mathscr{P}^{(d)}, \mathscr{P}^{(d)}])$ is trivial. This being true for all $q \neq p$, we conclude that $[\mathscr{P}^{(d)}, \mathscr{P}^{(d)}]$ is contained in $\mathrm{GL}_n(\mathbb{Z}_p)$, as asserted.

(2) Let d be the integer from assertion (1). Since $\mathscr{P}$ is analytic, it follows from the implicit function theorem that the map $\mathscr{P} \to \mathscr{P}$, $x \mapsto x^d$, is open, and therefore $\mathscr{P}^{(d)}$ is an open subgroup of $\mathscr{P}$. (We note that as follows from the affirmative solution of the restricted Burnside problem by E.I. Zel'manov [73, 74], the subgroup $\mathscr{P}^{(d)}$ is open in $\mathscr{P}$ for *any finitely generated* profinite group $\mathscr{P}$ and any integer $d \geq 1$, so the assumption of analyticity here can be replaced by just requiring finite generation.) Then, due to assumption (O), the commutator subgroup $[\mathscr{P}^{(d)}, \mathscr{P}^{(d)}]$ is also open in $\mathscr{P}$. On the other hand, assertion (1) states that $[\mathscr{P}^{(d)}, \mathscr{P}^{(d)}]$ is contained in the kernel of the projection $\mathscr{P} \to \prod_{q \neq p} \mathrm{GL}_n(\mathbb{Z}_q)$, which therefore is open in $\mathscr{P}$. $\square$

Remark 6.2. Combining Lemma 6.1 with the results of [17] (we thank M. Ershov for this reference), one shows that for an S-arithmetic subgroup Γ of an absolutely almost simple simply

connected algebraic group G over a global field K of characteristic $p > 0$, the profinite completion $\widehat{\Gamma}$ is not adelic provided that $\mathrm{rk}_S G > 0$ (i.e., Γ is infinite) and $S \neq V^K$. Indeed, pick $v \in V^K \setminus S$ and let $P = G(\mathcal{O}_v, \mathfrak{p}_v)$ be the congruence subgroup modulo the valuation ideal $\mathfrak{p}_v$ of the valuation ring $\mathcal{O}_v \subset K_v$. We will view P as a pro-p subgroup of $\overline{\Gamma}$, and let $\mathscr{P}$ be a Sylow pro-p subgroup of $\pi^{-1}(P)$, so that $\pi(\mathscr{P}) = P$. Assume that there exists an embedding $\widehat{\Gamma} \hookrightarrow \mathrm{GL}_n(\widehat{\mathbb{Z}})$. According to Lemma 6.1, for some $d \geq 1$, the subgroup $\mathscr{P}_0 = [\mathscr{P}^{(d)}, \mathscr{P}^{(d)}]$ is contained in $\mathrm{GL}_n(\mathbb{Z}_p)$ and hence is a p-adic analytic group. Then $P_0 := \pi(\mathscr{P}_0)$ is also p-adic analytic. On the other hand, it follows from [17, Theorem 1.7] or from [56] that P_0 is an open subgroup of P and therefore cannot be analytic (see [17, Theorem 1.5] or [14, Theorem 13.23]). A contradiction.

To proceed with the proof of Theorem C, for a prime p we let $V(p)$ denote the finite set $\{v \in V^K \setminus S \mid v(p) \neq 0\}$, and let Π be the finite set of primes p for which $V(p) \cap \mathcal{A}(G) \neq \varnothing$. To prove Theorem C, it is enough to show that

$$V_0 := \bigcup_{p \notin \Pi} V(p)$$

is contained in $\mathfrak{Z} := \mathfrak{Z}(C^{(S)}(G))$. Indeed, since the complement $V^K \setminus (S \cup V_0)$ is finite, by Theorem 4.3 the congruence kernel $C^{(S \cup V_0)}(G)$ is trivial. So, the inclusion $V_0 \subset \mathfrak{Z}$ would enable us to derive the centrality of $C^{(S)}(G)$ from Proposition 2.5.

The rest of the argument focuses on proving the inclusion $V(p) \subset \mathfrak{Z}$ for a fixed $p \notin \Pi$. By our assumption there exists a continuous embedding $\iota \colon \widehat{\Gamma} \hookrightarrow \prod_q \mathrm{GL}_n(\mathbb{Z}_q)$. Then

$$\mathscr{P} := \iota^{-1}(\mathrm{GL}_n(\mathbb{Z}_p, p))$$

is an analytic pro-p normal subgroup of $\widehat{\Gamma}$.

Lemma 6.3. *$\pi(\mathscr{P})$ contains an open subgroup of $G_{V(p)} = \prod_{v \in V(p)} G(K_v)$.*

Proof. Let $\mathcal{S}_p$ be a Sylow pro-p subgroup of $\widehat{\Gamma}$ (cf., for example, [59, Ch. I, § 1.5]). Then $\pi(\mathcal{S}_p)$ is a Sylow pro-p subgroup of $\overline{\Gamma} = \prod_{v \notin S} G(\mathcal{O}_v)$ [59, Ch. I, § 1, Proposition 4]. Since for every $v \in V(p)$, the congruence subgroup $G(\mathcal{O}_v, \mathfrak{p}_v)$ modulo the maximal ideal $\mathfrak{p}_v$ of $\mathcal{O}_v$ is a normal pro-p subgroup of $G(\mathcal{O}_v)$, the conjugacy theorem for Sylow pro-p subgroups of profinite groups [59, Ch. I, § 1, Proposition 3] implies that

$$\prod_{v \in V(p)} G(\mathcal{O}_v, \mathfrak{p}_v) \subset \pi(\mathcal{S}_p),$$

and consequently

$$\prod_{v \in V(p)} \big[G(\mathcal{O}_v, \mathfrak{p}_v)^{(d)}, G(\mathcal{O}_v, \mathfrak{p}_v)^{(d)}\big] \subset \pi\big(\big[\mathcal{S}_p^{(d)}, \mathcal{S}_p^{(d)}\big]\big) \tag{6.1}$$

for any $d \geq 1$. We will use this for the integer d given by Lemma 6.1(1). Then $\iota\big(\big[\mathcal{S}_p^{(d)}, \mathcal{S}_p^{(d)}\big]\big)$ is contained in $\mathrm{GL}_n(\mathbb{Z}_p)$. So, the intersection $\mathscr{P} \cap \big[\mathcal{S}_p^{(d)}, \mathcal{S}_p^{(d)}\big]$ is of finite index in $\big[\mathcal{S}_p^{(d)}, \mathcal{S}_p^{(d)}\big]$, and therefore $\pi(\mathscr{P}) \cap \pi\big(\big[\mathcal{S}_p^{(d)}, \mathcal{S}_p^{(d)}\big]\big)$ is of finite index in $\pi\big(\big[\mathcal{S}_p^{(d)}, \mathcal{S}_p^{(d)}\big]\big)$. On the other hand, as in the proof of Lemma 6.1(1), the map $G(K_v) \to G(K_v)$, $x \mapsto x^d$, is open, making $G(\mathcal{O}_v, \mathfrak{p}_v)^{(d)}$ an open subgroup of $G(K_v)$. Furthermore, since G is an absolutely almost simple group, its Lie algebra (as an analytic group over $\mathbb{Q}_p$) is semi-simple, which by way of the implicit function theorem implies that the commutator subgroup of any open subgroup of $G(K_v)$ is again open (cf. [56]). Combining these two facts, we see that the left-hand side of (6.1) is open in $G_{V(p)}$. Then $\pi(\mathscr{P})$ is also open, as required. $\square$

Since $\mathscr{P}$ is an analytic pro-p group, it follows from Cartan's theorem (cf. [8, Ch. III, § 8, n° 2; 14]) and the preceding lemma that $\mathscr{U} := \mathscr{P} \cap \pi^{-1}(G_{V(p)})$ is also an analytic pro-p normal subgroup of $\widehat{\Gamma}$ having the property that $\pi(\mathscr{U}) \subset G_{V(p)}$ is open. The latter means that for the $\mathbb{Q}_p$-Lie algebras $\mathfrak{u}$ and $\mathfrak{g}$ of $\mathscr{U}$ and $G_{V(p)}$ respectively (as analytic pro-p groups) and for the differential of π we have

$$d\pi(\mathfrak{u}) = \mathfrak{g}. \tag{6.2}$$

The rest of the proof relies on the analysis of conjugates $g\mathscr{U}g^{-1}$ for $g \in \widehat{G}$. This analysis, however, is complicated by the fact that $\mathscr{U}$ may not satisfy condition (O) of Lemma 6.1(2). To bypass this difficulty, we first replace $\mathscr{U}$ with a smaller subgroup that satisfies this condition and retains other significant properties of $\mathscr{U}$. More precisely, let

$$\mathfrak{u}_0 = \mathfrak{u}, \qquad \mathfrak{u}_{i+1} = [\mathfrak{u}_i, \mathfrak{u}_i] \quad \text{for} \quad i \geq 0$$

be the derived series of $\mathfrak{u}$. Pick $\ell \geq 0$ so that $\mathfrak{u}_{\ell+1} = \mathfrak{u}_\ell$, set $\mathfrak{w} = \mathfrak{u}_\ell$, and let $\mathcal{W} \subset \mathscr{U}$ be a closed subgroup with the Lie algebra $\mathfrak{w}$. Since by construction $[\mathfrak{w}, \mathfrak{w}] = \mathfrak{w}$, the subgroup $\mathcal{W}$ satisfies (O). At the same time, it follows from (6.2) and our construction that $d\pi(\mathfrak{w}) = \mathfrak{g}$, and therefore $\pi(\mathcal{W})$ is open in $G_{V(p)}$.

Lemma 6.4. *For any $g \in \widehat{G}$, the subgroups $\mathcal{W}$ and $g\mathcal{W}g^{-1}$ are commensurable.*

Proof. First, note that both $\widehat{\Gamma}$ and $g\widehat{\Gamma}g^{-1}$ are open compact subgroups of $\widehat{G}$ and hence are commensurable. It follows that there exists an open subgroup $\mathcal{W}' \subset \mathcal{W}$ such that $\widetilde{\mathcal{W}} := g\mathcal{W}'g^{-1} \subset \widehat{\Gamma}$. Since $\mathcal{W}$, hence also $\mathcal{W}'$, satisfies condition (O), Lemma 6.1(2) tells us that after replacing $\mathcal{W}'$ with a smaller open subgroup we may assume that $\iota(\widetilde{\mathcal{W}})$ is contained in $\mathrm{GL}_n(\mathbb{Z}_p)$ and even in $\mathrm{GL}_n(\mathbb{Z}_p, p)$, i.e. $\widetilde{\mathcal{W}} \subset \mathscr{P}$. At the same time, since $G_{V(p)}$ is normal in $\overline{G}$, we see that $\pi(\widetilde{\mathcal{W}}) \subset G_{V(p)}$, and eventually $\widetilde{\mathcal{W}} \subset \mathscr{P} \cap \pi^{-1}(G_{V(p)}) = \mathscr{U}$. The Lie algebra $\widetilde{\mathfrak{w}}$ is isomorphic to $\mathfrak{w}$ and hence is its own commutator. It follows that $\widetilde{\mathfrak{w}}$ is contained in the ℓth term of the derived series $\mathfrak{u}_\ell = \mathfrak{w}$, and therefore $\widetilde{\mathfrak{w}} = \mathfrak{w}$. But since $\widetilde{\mathcal{W}}$ and $\mathcal{W}$ are both closed subgroups of the analytic pro-p group $\mathscr{U}$, the fact that they have the same Lie algebras means that they share an open subgroup and hence are commensurable, and our assertion follows. □

For an arbitrary $g \in \widehat{G}$, the corresponding inner automorphism $\operatorname{Int} g$ induces a continuous group homomorphism $g^{-1}\mathcal{W}g \to \mathcal{W}$ of analytic pro-p groups, which is then analytic. It follows from Lemma 6.4 that both groups have the same Lie algebra $\mathfrak{w}$, so we obtain an action of g on the latter. Furthermore, using the fact that for any $g_1, g_2 \in \widehat{G}$, all four subgroups $\mathcal{W}$, $g_1^{-1}\mathcal{W}g_1$, $g_2^{-1}\mathcal{W}g_2$, and $(g_1g_2)^{-1}\mathcal{W}(g_1g_2)$ are pairwise commensurable, it is easy to see that in fact we obtain a continuous representation $\rho\colon \widehat{G} \to \mathrm{GL}(\mathfrak{w})$.

Lemma 6.5. *For $C = C^{(S)}(G)$, the image $\rho(C)$ is finite.*

Proof. Since C is compact, the image $\rho(C)$ is a compact subgroup of $\mathrm{GL}(\mathfrak{w}) = \mathrm{GL}_m(\mathbb{Q}_p)$ where $m = \dim_{\mathbb{Q}_p} \mathfrak{w}$. Since $\mathrm{GL}_m(\mathbb{Q}_p)$ is a p-adic analytic group, we conclude that $\rho(C)$ is finitely generated (cf. [14]). Now, applying Proposition 2.9 to $F = C/(C \cap \operatorname{Ker}\rho)$, we see that $\rho(C)$ is finite. □

Let $C_0 := C \cap \operatorname{Ker}\rho$ be an open normal subgroup of C normalized by $\widehat{G}$. Then the conjugation action of C_0 on $\mathcal{W}$ induces the trivial action on the Lie algebra $\mathfrak{w}$. This means that we can replace $\mathcal{W}$ with an open subgroup to ensure that C_0 centralizes $\mathcal{W}$ (we note that after this replacement, the image $\overline{\mathcal{W}} := \pi(\mathcal{W})$ will still be open in $G_{V(p)}$).

Lemma 6.6. *There exists $g \in G_{V(p)}$ such that $\overline{\mathcal{W}}$ and $g\overline{\mathcal{W}}g^{-1}$ generate $G_{V(p)}$.*

Proof. It is enough to show that given $v \in V(P)$ and an open subgroup W of $G(K_v)$, there exists $g \in G(K_v)$ such that

$$G(K_v) = \langle W, gWg^{-1} \rangle. \tag{6.3}$$

Note that $G(K_v)$ has only finitely many open compact subgroups $W_1, \dots, W_r$ that contain W (cf. [31, Proposition 3.16]). Pick a regular semi-simple element $t \in W$. It is well-known that the conjugacy class of t in $G(K_v)$ is closed and noncompact. So, one can find $g \in G(K_v)$ such that

$$gtg^{-1} \notin \bigcup_{i=1}^{r} W_i.$$

Then this g is as required. Indeed, in this case the right-hand side of (6.3) is an open noncompact subgroup and therefore, by a theorem due to Tits (see [34]), contains $G(K_v)^+$, the subgroup generated by the K_v-points of the K_v-defined parabolics of G. But since G is simply connected and $v \notin \mathcal{A}(G)$, we have $G(K_v)^+ = G(K_v)$ (see the discussion at the beginning of Section 7), and (6.3) follows. $\square$

Now, let $g \in G(K_v)$ be as in Lemma 6.6, pick a lift $\widehat{g} \in \pi^{-1}(g)$, and set $C_1 = C_0 \cap \widehat{g} C_0 \widehat{g}^{-1}$. Clearly, C_1 is an open normal subgroup of C that is centralized by $\mathcal{W}$ and $\widehat{g}\,\mathcal{W}\widehat{g}^{-1}$. So, if we let $\mathcal{G} = \pi^{-1}(G_{V(p)})$ and $\mathcal{Z} = Z_{\mathcal{G}}(C_1)$, then it follows from our construction that $\pi(\mathcal{Z}) = G_{V(p)}$. Let $\mathcal{Z}_1$ denote the kernel of the natural action of $\mathcal{Z}$ on the finite group C/C_1. Since $G_{V(p)}$ does not have proper normal subgroups of finite index, we will still have $\pi(\mathcal{Z}_1) = G_{V(p)}$. Then as in Lemma 2.6, for any $c \in C$, the map $x \mapsto [c, x]$ defines a continuous group homomorphism $\chi_c \colon \mathcal{Z}_1 \to C_1$, and we can consider

$$\chi \colon \mathcal{Z}_1 \to \mathcal{C} := \prod_{c \in C} X_c, \qquad \text{where} \quad X_c = C_1 \quad \text{for all} \quad c \in C,$$

given by $\chi(x) = (\chi_c(x))$. It follows from Lemma 2.3 that for $\mathcal{H} := \operatorname{Ker} \chi$, we have $\pi(\mathcal{H}) = G_{V(p)}$. At the same time, by our construction, $\mathcal{H} \subset Z_{\widehat{G}}(C)$, which implies that $V(p) \subset \mathfrak{Z}$, as required. This completes the proof of Theorem C.

7. GENERATORS FOR THE CONGRUENCE KERNEL: PROOF OF THEOREM D

In this section we will assume that $\operatorname{char} K = 0$, and let G be an absolutely almost simple simply connected K-*isotropic* algebraic group. If a subset $S \subset V^K$ containing V_∞^K is such that $\operatorname{rk}_S G \geq 2$, then according to the results of Raghunathan [40, 41] that prove Serre's conjecture for isotropic groups, the congruence kernel $C^{(S)}(G)$ is central and hence is isomorphic to the metaplectic kernel $M(S, G)$, which in all cases is a finite cyclic group (often trivial). In the remaining case where $\operatorname{rk}_S G = 1$ (and therefore necessarily $\operatorname{rk}_K G = 1$ and $|S| = 1$; hence K is either $\mathbb{Q}$ or an imaginary quadratic field), according to Serre's conjecture $C^{(S)}(G)$ is expected to be infinite. This has been established in a number of cases, although we do not yet have a general result. The goal of this section is to provide several convenient systems of generators (or rather almost generators) for $C^{(S)}(G)$ *as a normal subgroup* of $\widehat{G}^{(S)}$ and eventually reduce one of them to a *single* element, proving thereby Theorem D (we recall that according to Proposition 2.9, if $C^{(S)}(G)$ is infinite, it cannot be finitely generated as a group). So, henceforth we will assume that $\operatorname{rk}_K G = 1$.

First, we fix some notations that will be kept throughout this section. Let T be a maximal K-split torus of G (so, $\dim T = 1$) and $M = Z_G(T)$. The root system $\Phi = \Phi(G, T)$ is either $\{\pm\alpha\}$ or $\{\pm\alpha, \pm 2\alpha\}$. For $\beta \in \Phi$, we let U_β denote the corresponding unipotent K-subgroup of G (cf. [5, 21.9; 6, § 5; 60, Sect. 15.4]); recall that $U_{\pm 2\alpha} \subset U_{\pm\alpha}$ if $2\alpha \in \Phi$; if $2\alpha \notin \Phi$, then $U_{\pm 2\alpha}$ will denote the trivial subgroup of U_α. The subgroups $P_{\pm\alpha} = M \cdot U_{\pm\alpha}$ (semi-direct product) are opposite minimal parabolic K-subgroups with the unipotent radicals U_α and $U_{-\alpha}$, respectively, and the common Levi subgroup $M = P_\alpha \cap P_{-\alpha}$. Following Tits [64], for a field extension F/K we let $G(F)^+$ denote the subgroup of $G(F)$ generated by the F-rational points of the unipotent radicals of parabolic F-subgroups (since $\operatorname{char} K = 0$, it is simply the subgroup generated by all unipotent elements of $G(F)$). It is known [7, 6.2(v)] that $G(F)^+$ is generated by $U_\alpha(F)$ and $U_{-\alpha}(F)$. On the

other hand, from the affirmative solution of the Kneser–Tits problem over local (see [29; 35; 31, § 7.2]) and global (see [15]) fields, one knows that $G(K)^+ = G(K)$ and $G(K_v)^+ = G(K_v)$ for any $v \in V^K$. Thus, $U_\alpha(K)$ and $U_{-\alpha}(K)$ generate $G(K)$, and $U_\alpha(K_v)$ and $U_{-\alpha}(K_v)$ generate $G(K_v)$ for any v.

We will now produce the first generating system for $C = C^{(S)}(G)$ as a normal subgroup of $\widehat{G}^{(S)}$ by generalizing the construction used in Examples 4.6 and 4.7. Since $\operatorname{char} K = 0$, the topologies τ_{a} and τ_{c} of $G(K)$ induce the same topology on $U_{\pm\alpha}(K)$ (cf. [43, Proposition 2.1]). It follows that $\pi^{(S)}$ induces isomorphisms

$$\widehat{U_{\pm\alpha}(K)} \to \overline{U_{\pm\alpha}(K)} = U_{\pm\alpha}(\mathbb{A}(S)),$$

and we let $\sigma_{\pm\alpha}\colon \overline{U_{\pm\alpha}(K)} \to \widehat{U_{\pm\alpha}(K)}$ denote the inverse isomorphisms. Consider the set

$$X = \bigcup X(v_1, v_2), \qquad \text{with} \quad X(v_1, v_2) := \big[\sigma_\alpha(U_\alpha(K_{v_1})), \sigma_{-\alpha}(U_{-\alpha}(K_{v_2}))\big],$$

where the union is taken over all $v_1, v_2 \in V^K \setminus S$, $v_1 \neq v_2$, and $[A, B]$ denotes the set of all commutators $[a, b]$ with $a \in A$ and $b \in B$. The fact that the groups $G(K_{v_1})$ and $G(K_{v_2})$ for such v_1 and v_2 commute elementwise inside $\overline{G}^{(S)} = G(\mathbb{A}(S))$ immediately implies that $X(v_1, v_2) \subset C$; hence $X \subset C$. Now, let D be the closed normal subgroup of $\widehat{G}^{(S)}$ generated by X and consider the corresponding extension (F) of Section 2. For $v \in V^K \setminus S$, we let H_v denote the image in $H = \widehat{G}^{(S)}/D$ of the subgroup $\mathscr{G}_v \subset \widehat{G}^{(S)}$ generated by $\sigma_\alpha(U_\alpha(K_v))$ and $\sigma_{-\alpha}(U_{-\alpha}(K_v))$. As we mentioned above, $G(K_v) = \langle U_\alpha(K_v), U_{-\alpha}(K_v)\rangle$, which implies that $\theta(H_v) = G(K_v)$. Furthermore, by our construction the subgroups H_{v_1} and H_{v_2} commute elementwise in H. Finally, the closed subgroup of $\widehat{G}^{(S)}$ generated by the $\mathscr{G}_v$'s for $v \in V^K \setminus S$ contains $\widehat{U_\alpha(K)}$ and $\widehat{U_{-\alpha}(K)}$; hence $G(K) = \langle U_\alpha(K), U_{-\alpha}(K)\rangle$, so it coincides with $\widehat{G}^{(S)}$. Now, applying Proposition 4.5 to the partition of $V^K \setminus S$ into singletons and the subgroups H_v constructed above, we conclude that (F) is a central extension. Thus, $F = C/D$ is a quotient of the metaplectic kernel $M(S, G)$; hence it is a finite cyclic group of order dividing the order $|\mu_K|$ of the group μ_K of roots of unity in K (cf. [36]).

Next, we will use a result of Raghunathan [41] to substantially reduce the above system of generators.

Proposition 7.1. *Fix $v_0 \in V^K \setminus S$, and set*

$$Y(v_0) = \bigcup_{v \in V^K \setminus (S \cup \{v_0\})} X(v_0, v).$$

Then $Y(v_0) \subset C$, and if D is the closed normal subgroup of $\widehat{G}^{(S)}$ generated by $Y(v_0)$, then C/D is a quotient of $M(S, G)$; hence it is a finite cyclic group of order dividing $|\mu_K|$.

Proof. The discussion above yields the inclusion $Y(v_0) \subset C$ and also shows that it is enough to prove that the corresponding sequence (F) is a central extension. Since there exists $\omega \in G(K)$ such that $\omega U_{\pm\alpha}\omega^{-1} = U_{\mp\alpha}$ (cf. [5, 21.2; 6, 5.3]), the group D contains $[\sigma_{-\alpha}(U(K_{v_0})), \sigma_\alpha(U(K_v))]$ for any $v \in V^K \setminus (S \cup \{v_0\})$. We will now use Proposition 2.8 to establish the centrality. Write $V^K \setminus S = V_1 \cup V_2$ where $V_1 = \{v_0\}$ and $V_2 = V^K \setminus (S \cup \{v_0\})$ (obviously, $\mathcal{A} = \varnothing$ in our situation); then $V_i' = V_{3-i}$. The congruence kernel $C^{(S \cup V_1')}(G) = C^{(V^K \setminus \{v_0\})}(G)$ is trivial by Theorem 4.3, and the congruence kernel $C^{(S \cup V_2')}(G) = C^{(S \cup \{v_0\})}(G)$ is central by [41] and hence is isomorphic to $M(S \cup \{v_0\}, G)$, but the latter is trivial [36], so $C^{(S \cup \{v_0\})}(G)$ is trivial as well. Let H_1 be the closed subgroup of H generated by the images of $\sigma_\alpha(U_\alpha(K_{v_0}))$ and $\sigma_{-\alpha}(U_{-\alpha}(K_{v_0}))$, and let H_2 be the closed subgroup generated by the images of $\sigma_\alpha(U_\alpha(K_v))$ and $\sigma_{-\alpha}(U_{-\alpha}(K_v))$ for $v \in V^K \setminus (S \cup \{v_0\})$ (or, equivalently, by the images of $\sigma_\alpha(U_\alpha(\mathbb{A}(S \cup \{v_0\})))$ and $\sigma_{-\alpha}(U_{-\alpha}(\mathbb{A}(S \cup \{v_0\})))$). Then $\theta(H_i) = G(\mathbb{A}(S \cup V_i'))$ for $i = 1, 2$, and moreover, H_1 and H_2 commute elementwise and together generate a

dense subgroup of H. In other words, H_1 and H_2 satisfy the assumptions of Proposition 2.8, and then the required centrality of (F) immediately follows from this proposition. $\square$

We will first establish Theorem D for $G = \mathrm{SL}_2$, where the (almost) generating element c can be written down explicitly. The argument here is inspired by the proof of Proposition 7.1, but relies only on the result of Example 4.7 (which is originally due to Serre [58]) rather than on the more general result of Raghunathan [41]. We will keep the notations introduced in Example 4.7. Fix $v_0 \in V^K \setminus S$, write $\mathbb{A}(S) = K_{v_0} \times \mathbb{A}(S \cup \{v_0\})$, and consider the elements

$$1_{v_0} \in K_{v_0} \qquad \text{and} \qquad 1'_{v_0} = (1, \dots, 1, \dots) \in \mathbb{A}(S \cup \{v_0\}).$$

Proposition 7.2. *Set $c(v_0) = [\widehat{u}^+(1_{v_0}), \widehat{u}^-(1'_{v_0})] \in C$, and let D be the closed normal subgroup of $\widehat{G}$ generated by $c(v_0)$. Then the quotient C/D is central in $\widehat{G}/D$; hence it is a finite cyclic group of order dividing $|\mu_K|$.*

Proof. First, we observe that the set

$$\Delta = \bigl\{(t^{-1}, t) \in K_{v_0} \times \mathbb{A}(S \cup \{v_0\}) \bigm| t \in K^\times\bigr\}$$

is dense in $\mathbb{A}(S)$. Indeed, any open set in $\mathbb{A}(S)$ contains an open set of the form $U_{v_0}^{-1} \times U'_{v_0}$ for some open sets $U_{v_0} \subset K_{v_0}^\times$ and $U'_{v_0} \subset \mathbb{A}(S \cup \{v_0\})$, and then our claim immediately follows from the density of K in $\mathbb{A}(S)$ (strong approximation with respect to S). Since

$$h(t)^{-1} c(v_0) h(t) = [\widehat{u}^+(t^{-2}), \widehat{u}^-(t^2)],$$

we find that D contains the set

$$\bigl\{[\widehat{u}^+(a), \widehat{u}^-(b)] \bigm| a \in K_{v_0}^2,\ b \in \mathbb{A}(S \cup \{v_0\})^2\bigr\}.$$

In particular, for any $v \in V^K \setminus (S \cup \{v_0\})$, all commutators

$$[\widehat{u}^+(a), \widehat{u}^-(b)] \qquad \text{with} \quad a \in K_{v_0}^2, \quad b \in K_v^2$$

lie in D. Since for any $w \in V_{\mathrm{f}}^K$, every element of K_w can be written as a sum of (at most four) squares, the identities

$$[xy, z] = (x[y, z]x^{-1})[x, z] \qquad \text{and} \qquad [x, yz] = [x, y](y[x, z]y^{-1})$$

imply that D in fact contains the set $X(v_0, v)$. Then D contains $Y(v_0)$, and our claim follows from Proposition 7.1. $\square$

Remark 7.3. As we already observed, if the group G is K-isotropic then $\mathrm{rk}_S G = 1$ is possible only if $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{-d})$, d square-free > 0, with S consisting of the unique archimedean place in both cases. If $K = \mathbb{Q}$ then $M(S, G)$ for any G is of order ≤ 2, and in fact $M(S, G)$ is trivial for $G = \mathrm{SL}_2$. The latter means that the congruence kernel for $\mathrm{SL}_2(\mathbb{Z})$ is generated as a normal subgroup of $\widehat{G}$ by the element $c(p)$ constructed above for any prime p. On the other hand, for $K = \mathbb{Q}(\sqrt{-d})$, the order of $M(S, G)$, hence also that of C/D, divides 2 (respectively, 4 and 6) if $d \ne 1, 3$ (respectively, $d = 1$ and $d = 3$).

It is worth mentioning that the construction of generators described in Proposition 7.2 has some other applications. Let $G_0 = \mathrm{SL}_2$ over $\mathbb{Q}$, and let $S_0 = V_\infty^{\mathbb{Q}}$ so that $\Gamma_0 = G(\mathcal{O}_{\mathbb{Q}}(S_0))$ is $\mathrm{SL}_2(\mathbb{Z})$. Furthermore, fix a square-free integer $d > 0$, and let $G_d = \mathrm{SL}_2$ over $K_d := \mathbb{Q}(\sqrt{-d})$ and $S_d = V_\infty^{K_d}$ so that $\Gamma_d = G(\mathcal{O}_{K_d}(S_d))$ is the Bianchi group $\mathrm{SL}_2(\mathcal{O}_d)$ where $\mathcal{O}_d$ is the ring of integers in K_d. Let $C_0 = C^{(S_0)}(G_0)$ and $C_d = C^{(S_d)}(G_d)$ be the corresponding congruence kernels. Then the natural embedding $\Gamma_0 \to \Gamma_d$ induces a continuous homomorphism $\iota_d \colon C_0 \to C_d$. It follows from the results

of [1] that ι_d is injective for all d. (Indeed, by [1, Theorem 8.1], the homomorphism of the profinite completions $\widehat{\mathrm{PSL}_2(\mathbb{Z})} \to \widehat{\mathrm{PSL}_2(\mathcal{O}_d)}$ is injective, which implies that the homomorphism $\widehat{\Gamma_0} \to \widehat{\Gamma_d}$ is injective, and the injectivity of ι_d follows.) On the other hand, the results of Serre [58] imply that for $d \neq 1, 3$, the homomorphism ι_d is *not* surjective. Moreover, we have the following.

Lemma 7.4. *Let E_d be the closed normal subgroup of $\widehat{\Gamma_d}$ generated by $\iota_d(C_0)$. Then for $d \neq 1, 3$, the quotient C_d/E_d is infinite.*

Proof. Since the image of E_d in $\overline{C_d} := C_d/(C_d \cap \widehat{[\Gamma_d, \Gamma_d]})$ is the same as that of C_0, it is enough to show that the image of C_0 in $\overline{C_d}$ is a subgroup of infinite index. It is well-known that the abelianization $\Gamma_0^{\mathrm{ab}} = \Gamma_0/[\Gamma_0, \Gamma_0]$ is finite (of order 12), so $C_0 \cap \widehat{[\Gamma_0, \Gamma_0]}$ has finite index in C_0, making the image of C_0 in $\overline{C_d}$ finite. On the other hand, according to the results in [58, n° 3.6], for $d \neq 1, 3$, the abelianization Γ_d^{ab} is infinite.[3] Then from the exact sequence

$$\overline{C_d} \to \widehat{\Gamma_d}/\widehat{[\Gamma_d, \Gamma_d]} \to \overline{\Gamma_d}/\overline{[\Gamma_d, \Gamma_d]}$$

and the finiteness of the last term in it (see [40]), we conclude that $\overline{C_d}$ is infinite, and our assertion follows. □

Nevertheless, we have the following in all cases.

Proposition 7.5. *Let L_d be the closed normal subgroup of $\widehat{G_d}$ generated by $\iota_d(C_0)$. Then C_d/L_d is a finite cyclic group of order dividing $|\mu_{K_d}|$ (so, its order is ≤ 2 if $d \neq 1, 3$, divides 4 if $d = 1$, and divides 6 if $d = 3$).*

Proof. Pick a prime p_0 that does not split in K_d, and let v_0 be the unique valuation of K_d extending the p_0-adic valuation of $\mathbb{Q}$. Consider the elements from Proposition 7.2 written for these valuations:

$$c(p_0) = [\widehat{u}^+(1_{p_0}), \widehat{u}^-(1'_{p_0})] \in C_0 \qquad \text{and} \qquad c(v_0) = [\widehat{u}^+(1_{v_0}), \widehat{u}^-(1'_{v_0})] \in C_d.$$

It is easy to see that these elements are related by $\iota_d(c(p_0)) = c(v_0)$. So, L_d contains the subgroup D from the statement of Proposition 7.2, and our claim follows from that proposition (cf. also Remark 7.3). □

The proof of Theorem D in the general case will be reduced to the SL_2-case by constructing a suitable K-homomorphism $\mathrm{SL}_2 \to G$ with the help of the Jacobson–Morozov lemma and then applying Proposition 7.2 in conjunction with the following statement.

Proposition 7.6. *Let G be an absolutely simple simply connected algebraic K-group of K-rank 1, let $\varphi\colon H \to G$ be a K-homomorphism of an absolutely simple simply connected K-group H to G, and let $\widehat{\varphi}\colon \widehat{H}^{(S)} \to \widehat{G}^{(S)}$ be the corresponding continuous homomorphism of S-arithmetic completions. Assume that $\varphi(H) \cap (U_\beta \setminus U_{2\beta}) \neq \varnothing$ for $\beta = \alpha$ and $-\alpha$. Let C_0 be a subgroup of $C^{(S)}(H)$ normalized by $\widehat{H}^{(S)}$ such that $\widehat{H}^{(S)}$ acts trivially on $C^{(S)}(G)/C_0$. Then for the closed normal subgroup D of $\widehat{G}^{(S)}$ generated by $\widehat{\varphi}(C_0)$, the group $\widehat{G}^{(S)}$ acts trivially on $C^{(S)}(G)/D$. Consequently, $C^{(S)}(G)/D$ is a quotient of the metaplectic kernel $M(S, G)$; hence it is a finite cyclic group of order dividing $|\mu_K|$.*

The proof requires one technical fact (Proposition 7.7 below) which we will prove in the Appendix. To state it, we observe that the centralizer $M = Z_G(T_{\mathrm{s}})$ of a maximal K-split torus T_{s} of G acts on each root subgroup U_β for $\beta \in \Phi(G, T_{\mathrm{s}})$ via the conjugation action, and consequently acts on the quotient $W_{\pm\alpha} := U_{\pm\alpha}/U_{\pm 2\alpha}$. Furthermore, it is known that $W_{\pm\alpha}$ is a vector group over K, and the above action gives rise to a K-linear representation $\rho_{\pm\alpha}\colon M \to \mathrm{GL}(W_{\pm\alpha})$ (cf. [5, § 21]).

[3] We note that for $d = 1, 3$, the abelianization Γ_d^{ab} is finite, as one can see from the explicit presentations found in [11, 63].

We also recall that since G has K-rank 1, its Tits index can have only one or two circled vertices (cf. [65]).

Proposition 7.7. *Let (W,ρ) denote either (W_α,ρ_α) or $(W_{-\alpha},\rho_{-\alpha})$, and assume* $\operatorname{char} K \neq 2$. *Then ρ is K-irreducible. More precisely, one of the following two possibilities holds*:

(i) *if the Tits index of G has only one circled vertex, then ρ is absolutely irreducible*;

(ii) *if the Tits index of G has two circled vertices, then $W = W_1 \oplus W_2$ where W_1 and W_2 are absolutely irreducible M-invariant subspaces defined over a quadratic extension L/K and $W_2 = W_1^\sigma$ for the nontrivial automorphism σ of L/K.*

Proof of Proposition 7.6. We only need to prove that the extension

$$1 \to F := C^{(S)}(G)/D \to \breve{G} := \widehat{G}^{(S)}/D \xrightarrow{\theta} \overline{G}^{(S)} \to 1 \tag{7.1}$$

is central, for which we will use our standard strategy. More precisely, we let $\breve{U}_\alpha$ and $\breve{U}_{-\alpha}$ denote the closures in $\breve{G}$ of $U_\alpha(K)$ and $U_{-\alpha}(K)$, respectively. Since the S-arithmetic and S-congruence topologies on $U_{\pm\alpha}(K)$ coincide, θ induces isomorphisms

$$\breve{U}_\alpha \to \overline{U_\alpha(K)} \simeq U_\alpha(\mathbb{A}(S)) \qquad \text{and} \qquad \breve{U}_{-\alpha} \to \overline{U_{-\alpha}(K)} \simeq U_{-\alpha}(\mathbb{A}(S)),$$

and we let $\sigma_{\pm\alpha}\colon U_{\pm\alpha}(\mathbb{A}(S)) \to \breve{U}_{\pm\alpha}$ denote the inverse (continuous) isomorphisms. For $v \in V^K \setminus S$, we let $\mathscr{G}_v$ denote the subgroup of $\breve{G}$ generated by $\sigma_\alpha(U_\alpha(K_v))$ and $\sigma_{-\alpha}(U_{-\alpha}(K_v))$. Repeating almost verbatim the argument used at the beginning of this section, we see that the subgroups $\mathscr{G}_v$ satisfy all the assumptions of Theorem A, which then yields the centrality of (7.1) provided we show that $\sigma_\alpha(U_\alpha(K_{v_1}))$ and $\sigma_{-\alpha}(U_{-\alpha}(K_{v_2}))$ commute elementwise for any $v_1, v_2 \in V^K \setminus S$, $v_1 \neq v_2$. So, the central part of the present argument is concerned with proving this fact. We will establish it in the following equivalent form. Define

$$c_{v_1,v_2}\colon\ U_\alpha(K_{v_1}) \times U_{-\alpha}(K_{v_2}) \to F, \qquad (u_1,u_2) \mapsto [\sigma_\alpha(u_1),\sigma_{-\alpha}(u_2)].$$

Clearly, c_{v_1,v_2} is continuous, and what we need to prove is

($\star$) $c_{v_1,v_2} \equiv 1$.

By our assumption, the extension

$$1 \to F_0 := C^{(S)}(H)/C_0 \to \breve{H} := \widehat{H}^{(S)}/C_0 \xrightarrow{\theta_0} \overline{H}^{(S)} \to 1$$

is central. Since H is clearly K-isotropic, the congruence completion $\overline{H}^{(S)}$ can, as usual, be identified with $H(\mathbb{A}(S))$. Then for any $v_1, v_2 \in V^K \setminus S$, $v_1 \neq v_2$, by Corollary 2.7, we can define a bimultiplicative pairing

$$c^0_{v_1,v_2}\colon\ H(K_{v_1}) \times H(K_{v_2}) \to F_0, \qquad (x_1,x_2) \mapsto [\widetilde{x}_1,\widetilde{x}_2] \quad \text{for } \widetilde{x}_i \in \theta_0^{-1}(x_i).$$

As we already mentioned, the group $H(K_{v_i})$ does not contain any proper noncentral normal subgroups; hence $H(K_{v_i}) = [H(K_{v_i}),H(K_{v_i})]$. Since F_0 is commutative, it follows that the pairing $c^0_{v_1,v_2}$ is trivial, and therefore the preimages $\theta_0^{-1}(H(K_{v_1}))$ and $\theta_0^{-1}(H(K_{v_2}))$ commute elementwise.

There exist unipotent K-subgroups $\mathscr{U}_+$ and $\mathscr{U}_-$ of H such that $\varphi(\mathscr{U}_\pm)$ is contained in $U_{\pm\alpha}$ but not in $U_{\pm 2\alpha}$. Then for any $u_1 \in \mathscr{U}_+(K_{v_1})$ and $u_2 \in \mathscr{U}_-(K_{v_2})$ we have

$$c_{v_1,v_2}(\varphi(u_1),\varphi(u_2)) = \breve{\varphi}(c^0_{v_1,v_2}(u_1,u_2)) = 1,$$

where $\breve{\varphi}\colon \breve{H} \to \breve{G}$ is induced by $\widehat{\varphi}$. Furthermore, the group $M(K)$ acts naturally on F by conjugation, and for any $m \in M(K)$ and any u_1, u_2 as above we have

$$c_{v_1,v_2}\bigl(m\varphi(u_1)m^{-1}, m\varphi(u_2)m^{-1}\bigr) = mc_{v_1,v_2}(\varphi(u_1),\varphi(u_2))m^{-1} = 1. \tag{7.2}$$

We now note the following.

Lemma 7.8 (weak approximation for M)**.** *For any finite subset V of V^K, the diagonal embedding $M(K) \hookrightarrow M_V := \prod_{v\in V} M(K_v)$ has dense image.*

Proof. By the Bruhat decomposition, the product map $\mu\colon U_{-\alpha} \times M \times U_\alpha \to G$ yields a K-isomorphism onto a Zariski-open set $\Omega \subset G$. Being simply connected, G has weak approximation with respect to any finite set of places; i.e., the diagonal embedding $G(K) \hookrightarrow G_V$ is dense (cf. [31, Theorem 7.8]). Since Ω is K-open, the diagonal embedding $\Omega(K) \hookrightarrow \Omega_V$ is also dense, and our assertion follows. □

Using this in conjunction with (7.2) and the continuity of c_{v_1,v_2}, we obtain

$$c_{v_1,v_2}(X_1(u_1), X_2(u_2)) = \{1\} \qquad \text{where} \qquad X_i(u_i) = \bigl\{m_i\varphi(u_i)m_i^{-1} \bigm| m_i \in M(K_{v_i})\bigr\}.$$

Then also

$$c_{v_1,v_2}(\langle X_1(u_1)\rangle, \langle X_2(u_2)\rangle) = \{1\}, \tag{7.3}$$

where $\langle X_i(u_i)\rangle$ is the subgroup generated by $X_i(u_i)$. Now, it follows from our assumptions and the Zariski-density of $\mathscr{U}_\pm(K)$ in $\mathscr{U}_\pm$ that one can pick $u_1 \in \mathscr{U}_+(K)$ and $u_2 \in \mathscr{U}_-(K)$ so that $\varphi(u_1) \notin U_{2\alpha}(K)$ and $\varphi(u_2) \notin U_{-2\alpha}(K)$. So, if we let $\nu_{\pm\alpha}\colon U_{\pm\alpha} \to U_{\pm\alpha}/U_{\pm 2\alpha} = W_{\pm\alpha}$ denote the quotient map, then $w_1 = \nu_\alpha(\varphi(u_1))$ and $w_2 = \nu_{-\alpha}(\varphi(u_2))$ are *nontrivial* elements in $W_\alpha(K)$ and $W_{-\alpha}(K)$. Taking into account the Zariski-density of $M(K)$ in M (cf. [5, 18.3]) and applying Proposition 7.7, we see that for any field extension P/K, the P-vector space $W_\alpha(P)$ (respectively, $W_{-\alpha}(P)$) is spanned by $\rho_\alpha(M(P)) \cdot w_1$ (respectively, $\rho_{-\alpha}(M(P)) \cdot w_2$). On the other hand, since $\alpha(T_{\mathrm{s}}(P))$ contains $P^{\times d}$ for some $d \geq 1$ and P is generated by $P^{\times d}$ as an additive group, the additive subgroup of $W_\alpha(P)$ (respectively, $W_{-\alpha}(P)$) generated by $\rho_\alpha(M(P)) \cdot w_1$ (respectively, $\rho_{-\alpha}(M(P)) \cdot w_2$) is automatically a P-vector subspace. Altogether, this means that

$$\nu_\alpha(\langle X_1(u_1)\rangle) = W_\alpha(K_{v_1}) \qquad \text{and} \qquad \nu_{-\alpha}(\langle X_2(u_2)\rangle) = W_{-\alpha}(K_{v_2}). \tag{7.4}$$

Clearly, $U_{\pm 2\alpha}$ is contained in the center of $U_{\pm\alpha}$, and since $U_{\pm 2\alpha}(P)$ coincides with the commutator subgroup of $U_{\pm\alpha}(P)$ for any field extension P/K (cf. [9, 5.3]; note that this fact is true over any infinite field of characteristic $\neq 2$), we conclude from (7.4) by passing to commutator subgroups that $\langle X_1(u_1)\rangle$ (respectively, $\langle X_2(u_2)\rangle$) contains $U_{2\alpha}(K_{v_1})$ (respectively, $U_{-2\alpha}(K_{v_2})$). Then (7.4) yields

$$\langle X_1(u_1)\rangle = U_\alpha(K_{v_1}) \qquad \text{and} \qquad \langle X_2(u_2)\rangle = U_{-\alpha}(K_{v_2}).$$

Combining this with (7.3), we obtain ($\star$), as required. □

Remark 7.9. 1. Proposition 7.6 for $C = C_0$ is essentially due to Rajan and Venkataramana [45] and in fact goes back to Raghunathan's argument in [41, § 3]. We note, however, that the discussion of the irreducibility of the action of M on $W_{\pm\alpha}$ (which is our Proposition 7.7) is limited in [45] to the groups $\mathrm{SO}(n,1)$ and $\mathrm{SU}(n,1)$, which are the main focus of that paper (see the penultimate paragraph in [45, p. 548]). It should also be pointed out that the assertion in the proof of [45, Theorem 7] that part (ii) of that theorem is a restatement of [41, Proposition 2.14] is not totally accurate as Proposition 2.14 of [41] involves one extra condition (see (iii) in its statement). Nevertheless, according to our Theorem A, the result described in [45, Theorem 7(ii)] is indeed valid, and not only for isotropic groups. In view of these technicalities, we chose—for the reader's convenience—to give a complete proof of Proposition 7.6.

2. It was pointed out in [44, 45] that the assertion of Proposition 7.6 has the following implication:

Given a congruence subgroup Γ of $G(\mathcal{O}(S))$ and a nontrivial group homomorphism $\phi\colon \Gamma \to \mathbb{Z}$, there exists a congruence subgroup Δ of $H(\mathcal{O}(S))$ and an element $g \in G(K)$ such that $\Delta' = g\Delta g^{-1}$ is contained in Γ and the restriction $\phi|\Delta'$ is nontrivial.

This is subsumed, however, in the "sandwich lemma" of Lubotzky [23, Lemma 2.4], which states that the above result is valid without any assumptions on the congruence kernels *if* $H(\mathcal{O}(S))$ satisfies the so-called *Selberg property*. We refer to [23] for precise definitions, and only mention that the Selberg property is in fact property (τ) for congruence subgroups. More importantly, the Selberg property is now known to hold in all situations (see [10], which concluded the efforts by various people), making the result of Lubotzky unconditional.

At the same time, proving Selberg's property even for SL_2 requires the heavy machinery of the theory of automorphic forms, so the approach developed in [44, 45] provides an algebraic alternative in some cases. (From this perspective, our Proposition 7.5 yields an algebraic proof of the following fact: *Given a congruence subgroup* Γ *of the Bianchi group* $\mathrm{SL}_2(\mathcal{O}_d)$, *where* $\mathcal{O}_d$ *is the ring of integers in* $K_d = \mathbb{Q}(\sqrt{-d})$ *with* d *a square-free integer* >0, *and a nontrivial homomorphism* $\phi\colon \Gamma \to \mathbb{Z}$, *there exists a congruence subgroup* Δ *of* $\mathrm{SL}_2(\mathbb{Z})$ *and* $g \in \mathrm{SL}_2(K_d)$ *such that* $\Delta' = g\Delta g^{-1}$ *is contained in* Γ *and the restriction* $\phi|\Delta'$ *is nontrivial* (this should be compared to the results in [58, n° 3.6]).)

3. One can ask whether it is possible to strengthen Proposition 7.6 and prove that for an absolutely almost simple simply connected K-group G and a proper K-subgroup H, the map of the congruence kernels $\iota^{(S)}_{G,H}\colon C^{(S)}(H) \to C^{(S)}(G)$ is actually surjective. This property can be helpful for proving the centrality of $C^{(S)}(G)$ in view of the following simple observation (cf. [39, Sect. 5.2, Proposition 2]): *Assume that* $G(K)$ *does not contain any proper noncentral normal subgroups. If there exists a* K*-subgroup* H *of* G *which is fixed elementwise by a nontrivial* K*-automorphism* σ *of* G *such that* $\iota^{(S)}_{G,H}$ *is surjective, then* $C^{(S)}(G)$ *is central and hence finite.* This observation (which can be traced back to [3]; see [39, Sect. 5.3] on how it can be used to establish the centrality of the congruence kernel for SL_n, $n \geq 3$) was employed by Kneser [20] to prove that if $G = \mathrm{Spin}_n(q)$ is the spinor group of a nondegenerate quadratic form q over K in $n \geq 5$ variables and $\mathrm{rk}_S G \geq 2$, then $C^{(S)}(G)$ is central. To this end, he proved that for any anisotropic $x \in K^n$ with the stabilizer $G(x)$ satisfying $\mathrm{rk}_S G(x) \geq 1$, the map $C^{(S)}(G(x)) \to C^{(S)}(G)$ is surjective (see [39, Sect. 5.2, Proposition 3] for an indication of the idea). Subsequently, analogs of these statements were established for groups of the classical types and type G_2 in [46, 47, 49, 67, 68]. To give an example where $\iota^{(S)}_{G,H}$ is not surjective, we consider an imaginary quadratic extension $L/\mathbb{Q}$ and let h be the corresponding 2-dimensional hyperbolic hermitian form. Set $f = h \perp g$, where g is a 1-dimensional hermitian form, and consider the natural embedding of (absolutely almost simple simply connected) $\mathbb{Q}$-groups

$$H := \mathrm{SU}(h) \to \mathrm{SU}(f) =: G.$$

We claim that for $S = \{\infty\}$, the map $\iota^{(S)}_{G,H}$ is *not* surjective. Indeed, it follows from the results of Kazhdan [18] and Wallach [70] that there exists a congruence subgroup Γ of $G(\mathbb{Z})$ with infinite abelianization Γ^{ab}, which immediately implies that the congruence kernel $C^{(S)}(G)$ is infinite (cf. [58, § 3]). Since H is fixed by the nontrivial automorphism $\sigma = \operatorname{Int} x$ of G, where $x = \mathrm{diag}(1, 1, -1) \in \mathrm{U}_3(f)$, this fact together with the above observation prevents $\iota^{(S)}_{G,H}$ from being surjective.

While $\iota^{(S)}_{G,H}$ may or may not be surjective, the available results (including those obtained in [44] for the embeddings $\mathrm{SO}(2m-1,1) \to \mathrm{SU}(2m-1,1)$ and $\mathrm{SO}(2m-1,1) \to \mathrm{SO}(2m+1,1)$ in the anisotropic case and for $C = C_0$) suggest that the assertion of Proposition 7.6 should always be true whenever G and H are absolutely almost simple simply connected K-groups and $\mathrm{rk}_S H > 0$. If proven, this would simplify the verification of centrality in a number of cases.

Proof of Theorem D. Recall that here $\operatorname{char} K = 0$. Propositions 7.2 and 7.6 imply that it is enough to construct a K-homomorphism $\varphi\colon H = \mathrm{SL}_2 \to G$ such that $\varphi(H) \cap (U_\beta \setminus U_{2\beta}) \neq \varnothing$ for $\beta = \alpha$ and $-\alpha$. For this we consider the Lie algebra $\mathfrak{g} = L(G)$ of G and pick a nonzero eigenvector $X \in \mathfrak{g}(K)$ for the adjoint action of the maximal K-split torus T_{s} with character α. Applying the

Jacobson–Morozov lemma (cf. [16, Ch. III, Theorem 17]), we can find a K-subalgebra $\mathfrak{r} \subset \mathfrak{g}$ that contains X and is isomorphic to $\mathfrak{sl}_2$. There exists an algebraic K-subgroup R of G with the Lie algebra $\mathfrak{r}$ (cf. [5, Corollary 7.9]), which is K-isogenous to SL_2. Let $\mathscr{U}$ be a 1-dimensional unipotent K-subgroup of R whose Lie algebra $L(\mathscr{U})$ is spanned by X, and let $\mathscr{T} \subset R$ be a 1-dimensional K-split torus that normalizes $\mathscr{U}$. Then $\mathscr{T}$ and T_{s} are conjugate by an element of $N_G(\mathscr{U})^\circ(K)$ (cf. [6]), and after performing this conjugation we can assume that $\mathscr{T} = T_{\mathrm{s}}$. Since $\mathfrak{r}$ also contains an eigenvector for $\operatorname{Ad}\mathscr{T}$ with character $-\alpha$, we obtain $R \cap (U_\beta \setminus U_{2\beta}) \neq \varnothing$ for $\beta = \pm\alpha$, so a K-isogeny $\varphi\colon H = \mathrm{SL}_2 \to R$ is a required homomorphism. $\square$

To conclude, we will briefly indicate how Theorem D can be partially extended to positive characteristic $p > 2$. The main distinction is that if $p > 0$ and $\operatorname{rk}_S G = 1$, then the arithmetic and congruence topologies of G may not coincide on $U_{\pm\alpha}(K)$. So, to use our approach we need to pass to the *reduced* congruence kernel $\overline{C}^{(S)}(G) = C^{(S)}(G)/N$ where N is the closed normal subgroup of $\widehat{G}^{(S)}$ generated by the kernels of the restrictions $\pi^{(S)}|\widehat{U_{\pm\alpha}(K)}$. Then Propositions 7.2 and 7.6 remain valid if one replaces the full congruence kernel with the reduced one in their statements. Furthermore, by going through the list of absolutely almost simple groups defined over a global field K of characteristic $p > 2$ and having K-rank 1, one verifies that there is a K-homomorphism $\varphi\colon H = \mathrm{SL}_2 \to G$ such that $\varphi(H) \cap (U_\beta \setminus U_{2\beta}) \neq \varnothing$ for $\beta = \pm\alpha$ (this assertion is false in characteristic 2). This puts all the ingredients of the proof of Theorem D in place, and taking into account the triviality of $M(S, G)$ in positive characteristic (cf. [36]), we arrive at the following conclusion: $\overline{C}^{(S)}(G)$ *is generated as a closed normal subgroup of* $\widehat{G}^{(S)}/N$ *by a single element.*

Appendix. PROOF OF PROPOSITION 7.7

We will give the argument for (W_α, ρ_α). Let T be a maximal K-torus of G containing T_{s}, and let $\Phi = \Phi(G, T)$ be the corresponding (absolute) root system. We fix compatible orderings on $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ and $X(T_{\mathrm{s}}) \otimes_{\mathbb{Z}} \mathbb{R}$ so that α is positive. Let Φ^+ (respectively, Δ) be the corresponding system of positive (respectively, simple) roots in Φ. Furthermore, we let Δ_0 denote the subset of Δ consisting of roots with trivial restriction to T_{s} (and then $\Delta \setminus \Delta_0$ is the set of distinguished roots). Since $\operatorname{rk}_K G = 1$, it follows from the tables in [65] that $|\Delta \setminus \Delta_0| \leq 2$; note that any $\delta \in \Delta \setminus \Delta_0$ is taken to α by the restriction map $X(T) \to X(T_{\mathrm{s}})$.

For $\beta \in \Phi$, we let $\mathscr{U}_\beta$ (respectively, $\mathfrak{g}_\beta$) denote the 1-dimensional connected unipotent subgroup of G (respectively, the 1-dimensional root subspace of the Lie algebra $\mathfrak{g} = L(G)$) corresponding to β (thus, $\mathfrak{g}_\beta = L(\mathscr{U}_\beta)$). Furthermore, we let $n_\delta(\beta)$ ($\delta \in \Delta$) denote the integers that arise in the decomposition $\beta = \sum_{\delta\in\Delta} n_\delta(\beta)\delta$. Let

$$\Theta = \left\{ \beta \in \Phi^+ \;\middle|\; \sum_{\delta\in\Delta-\Delta_0} n_\delta(\beta) = 1 \right\}.$$

Clearly, Θ is precisely the set of roots $\beta \in \Phi$ that restrict to α. It follows that $\mathfrak{u} = \sum_{\beta\in\Theta} \mathfrak{g}_\beta$ is the root space for T_{s} for the root α and hence is invariant under $\operatorname{Ad} M$, where $M = Z_G(T_{\mathrm{s}})$. It is well-known that the vector spaces $W_\alpha = U_\alpha/U_{2\alpha}$ and $\mathfrak{u}$ are isomorphic as M-modules. We also recall that for $\beta, \gamma \in \Phi$, we have

$$(\operatorname{Ad} g)(\mathfrak{g}_\beta) \subset \sum_{n\geq 1} \mathfrak{g}_{\beta+n\gamma} \qquad \text{for any} \quad g \in \mathscr{U}_\gamma, \tag{A.1}$$

where as usual we set $\mathfrak{g}_\delta = 0$ if $\delta \in X(T)$ is not a root. Furthermore, since we exclude characteristic 2 and also type G_2 (which does not have K-forms with K-rank 1), we have

$$[\mathfrak{g}_{\beta_1}, \mathfrak{g}_{\beta_2}] = \mathfrak{g}_{\beta_1+\beta_2} \qquad \text{for any} \quad \beta_1, \beta_2 \in \Phi. \tag{A.2}$$

Lemma A.1. *Fix $\delta_0 \in \Delta \setminus \Delta_0$ and set $\Theta(\delta_0) = \{\beta \in \Theta \mid n_{\delta_0}(\beta) = 1\}$. Then*

$$\mathfrak{u}(\delta_0) := \sum_{\beta \in \Theta(\delta_0)} \mathfrak{g}_\beta$$

is an irreducible M-module.

Proof. The group M is generated by T and $\mathscr{U}_\gamma$ for those $\gamma \in \Phi$ that restrict trivially to T_{s}. Since any such γ is a linear combination of elements of Δ_0, the inclusion (A.1) shows that $\mathfrak{u}(\delta_0)$ is $\operatorname{Ad} M$-invariant. Let $\mathfrak{v} \subset \mathfrak{u}(\delta_0)$ be a nonzero M-invariant subspace. As M contains T, we have $\mathfrak{v} = \bigoplus_{\beta \in \Theta'} \mathfrak{g}_\beta$ for some nonempty subset $\Theta' \subset \Theta(\delta_0)$ and $[\mathfrak{m}, \mathfrak{v}] \subset \mathfrak{v}$, where $\mathfrak{m} = L(M)$. For $\beta_1, \beta_2 \in \Phi$, we will write $\beta_1 \succ \beta_2$ if $\beta_1 - \beta_2$ is a sum of positive roots. We claim that if $\beta_1, \beta_2 \in \Theta(\delta_0)$ and $\beta_1 \succ \beta_2$, then

$$\mathfrak{g}_{\beta_1} \subset \mathfrak{v} \qquad \Leftrightarrow \qquad \mathfrak{g}_{\beta_2} \subset \mathfrak{v}. \tag{A.3}$$

Indeed, there exists a sequence of positive roots $\gamma_1, \ldots, \gamma_r \in \Phi^+$ such that $\beta_1 = \beta_2 + \gamma_1 + \ldots + \gamma_r$ and $\beta_2 + \gamma_1 + \ldots + \gamma_i$ is a root for $i = 1, \ldots, r$ (see the proof of [8, Ch. VI, § 1, n° 6, Proposition 19]). Since $n_\delta(\beta_1) = n_\delta(\beta_2)$ for any $\delta \in \Delta \setminus \Delta_0$, we have $n_\delta(\gamma_i) = 0$ and hence $\mathfrak{g}_{\pm\gamma_i} \subset \mathfrak{m}$ for all i. So, if $\mathfrak{g}_{\beta_1} \subset \mathfrak{v}$, then using repeatedly $[\mathfrak{m}, \mathfrak{v}] \subset \mathfrak{v}$ together with (A.2), we obtain

$$\mathfrak{g}_{\beta_2} = [\mathfrak{g}_{-\gamma_1}, [\mathfrak{g}_{-\gamma_2}, [\ldots [\mathfrak{g}_{-\gamma_r}, \mathfrak{g}_{\beta_1}] \ldots]]] \subset \mathfrak{v},$$

and vice versa, proving (A.3). Note that for any $\beta \in \Theta(\delta_0)$ we have $\beta \succ \delta_0$, so using (A.3), we see that if $\mathfrak{g}_{\beta_0} \subset \mathfrak{v}$ for *some* $\beta_0 \in \Theta(\delta_0)$, then $\mathfrak{g}_{\delta_0} \subset \mathfrak{v}$, and consequently $\mathfrak{g}_\beta \subset \mathfrak{v}$ for *every* $\beta \in \Theta(\delta_0)$. Thus, $\mathfrak{v} = \mathfrak{u}$, as claimed. □

If $\Delta \setminus \Delta_0 = \{\delta_0\}$ then the above lemma, together with the remarks made prior to its statement, immediately yields the irreducibility of W_α. Now, suppose that $\Delta \setminus \Delta_0 = \{\delta_1, \delta_2\}$. For $i = 1, 2$, set

$$\mathfrak{u}_i = \sum_{\beta \in \Theta(\delta_i)} \mathfrak{g}_\beta,$$

where $\Theta(\delta_i)$ is the subset of Θ defined in Lemma A.1 for $\delta_0 = \delta_i$, and let W_i be the subspace of W corresponding to $\mathfrak{u}_i$. Then clearly $W = W_1 \oplus W_2$, and according to Lemma A.1, each W_i is an (absolutely) irreducible M-module. Let $T_0 = Z(M)^\circ$ be the central torus of the (reductive) group M. Then the restrictions $\gamma_i = \delta_i | T_0$ for $i = 1, 2$ form a basis of $X(T_0) \otimes_{\mathbb{Z}} \mathbb{Q}$, and W_i is the eigenspace of T_0 with the character γ_i. It follows that the M-submodule of W containing $w = (w_1, w_2)$ with $w_i \in W_i$ contains w_1 and w_2 and hence coincides with W if both w_1 and w_2 are nonzero.

Since T_0 is 2-dimensional and contains the 1-dimensional (maximal) split torus T_{s}, it splits over a quadratic extension L/K, and then both subspaces W_1 and W_2 are defined over L. The nontrivial $\sigma \in \operatorname{Gal}(L/K)$ can either switch the weights γ_1 and γ_2 of T_0 or keep each of them fixed. However, in the second option T_0 would be K-split, which is not the case. Thus, $\sigma(\gamma_1) = \gamma_2$, and therefore $\sigma(W_1) = W_2$. It follows that if a nonzero $w \in W(K)$ is written in the form $w = (w_1, w_2)$ as above, then both w_1 and w_2 are *automatically* nonzero, so w generates W as M-module, implying that W is K-irreducible.

ACKNOWLEDGMENTS

Both authors were supported by the NSF (grants DMS-1401380 and DMS-1301800). We thank the referee for her/his comments.

REFERENCES

1. I. Agol, D. D. Long, and A. W. Reid, "The Bianchi groups are separable on geometrically finite subgroups," Ann. Math., Ser. 2, **153**, 599–621 (2001).
2. *Algebraic Number Theory: Proc. Instr. Conf., Univ. Sussex, Brighton, UK, 1965*, Ed. by J. W. S. Cassels and A. Fröhlich, 2nd ed. (London Math. Soc., London, 2010).
3. H. Bass, J. Milnor, and J.-P. Serre, "Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)," Publ. Math. Inst. Hautes Étud. Sci. **33**, 59–137 (1967).
4. V. Bergelson and D. B. Shapiro, "Multiplicative subgroups of finite index in a ring," Proc. Am. Math. Sos. **116**, 885–896 (1992).
5. A. Borel, *Linear Algebraic Groups* (Springer, New York, 1991), Grad. Texts Math. **126**.
6. A. Borel and J. Tits, "Groupes réductifs," Publ. Math. Inst. Hautes Étud. Sci. **27**, 55–150 (1965).
7. A. Borel and J. Tits, "Homomorphismes "abstraits" de groupes algébriques simples," Ann. Math., Ser. 2, **97**, 499–571 (1973).
8. N. Bourbaki, *Groupes et algèbres de Lie. Chapitres II, III* (Hermann, Paris, 1972); *Chapitres IV–VI* (Hermann, Paris, 1968), Éléments de mathématique.
9. C. J. Bushnell and G. Henniart, "On the derived subgroups of certain unipotent subgroups of reductive groups over infinite fields," Transform. Groups **7** (3), 211–230 (2002).
10. L. Clozel, "Démonstration de la conjecture τ," Invent. Math. **151**, 297–328 (2003).
11. P. M. Cohn, "A presentation of SL_2 for Euclidean imaginary quadratic number fields," Mathematika **15**, 156–163 (1968).
12. C. Demarche, "Le défaut d'approximation forte dans les groupes linéaires connexes," Proc. London Math. Soc., Ser. 3, **102**, 563–597 (2011).
13. J. D. Dixon, *The Structure of Linear Groups* (Van Nostrand Reinhold, London, 1971).
14. J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic Pro-p Groups*, 2nd ed. (Cambridge Univ. Press, Cambridge, 1999).
15. P. Gille, "Le problème de Kneser–Tits," in *Séminaire Bourbaki 2007/2008* (Soc. Math. France, Paris, 2009), Exp. 983, Astérisque **326**, pp. 39–81.
16. N. Jacobson, *Lie Algebras* (Dover Publ., New York, 1979).
17. A. Jaikin-Zapirain and B. Klopsch, "Analytic groups over general pro-p domains," J. London Math. Soc., Ser. 2, **76**, 365–383 (2007).
18. D. Kazhdan, "Some applications of the Weil representation," J. Anal. Math. **32**, 235–248 (1977).
19. M. W. Liebeck and L. Pyber, "Finite linear groups and bounded generation," Duke Math. J. **107** (1), 159–171 (2001).
20. M. Kneser, "Normalteiler ganzzahliger Spingruppen," J. Reine Angew. Math. **311–312**, 191–214 (1979).
21. A. Lubotzky, "Free quotients and the congruence kernel of SL_2," J. Algebra **77**, 411–418 (1982).
22. A. Lubotzky, "Subgroup growth and congruence subgroups," Invent. Math. **119**, 267–295 (1995).
23. A. Lubotzky, "Eigenvalues of the Laplacian, the first Betti number and the congruence subgroup problem," Ann. Math., Ser. 2, **144**, 441–452 (1996).
24. A. Lubotzky, "Finite presentations of adelic groups, the congruence kernel and cohomology of finite simple groups," Pure Appl. Math. Q. **1** (2), 241–256 (2005).
25. A. Lubotzky and D. Segal, *Subgroup Growth* (Birkhäuser, Basel, 2003).
26. G. A. Margulis, "Cobounded subgroups in algebraic groups over local fields," Funkts. Anal. Prilozh. **11** (2), 45–57 (1977) [Funct. Anal. Appl. **11**, 119–128 (1977)].
27. A. W. Mason, A. Premet, B. Sury, and P. A. Zalesskii, "The congruence kernel of an arithmetic lattice in a rank one algebraic group over a local field," J. Reine Angew. Math. **623**, 43–72 (2008).
28. O. V. Mel'nikov, "The congruence kernel of the group $\mathrm{SL}_2(\mathbb{Z})$," Dokl. Akad. Nauk SSSR **228** (5), 1034–1036 (1976) [Sov. Math., Dokl. **17**, 867–870 (1976)].
29. V. P. Platonov, "The problem of strong approximation and the Kneser–Tits conjecture for algebraic groups," Izv. Akad. Nauk SSSR, Ser. Mat. **33** (6), 1211–1219 (1969) [Math. USSR, Izv. **3**, 1139–1147 (1969)].
30. V. P. Platonov and A. S. Rapinchuk, "Abstract properties of S-arithmetic groups and the congruence subgroup problem," Izv. Ross. Akad. Nauk, Ser. Mat. **56** (3), 483–508 (1992) [Russ. Acad. Sci., Izv. Math. **40**, 455–476 (1993)].
31. V. P. Platonov and A. S. Rapinchuk, *Algebraic Groups and Number Theory* (Academic, Boston, 1994).
32. V. P. Platonov and B. Sury, "Adelic profinite groups," J. Algebra **193**, 757–763 (1997).
33. G. Prasad, "Strong approximation for semi-simple groups over function fields," Ann. Math., Ser. 2, **105**, 553–572 (1977).

34. G. Prasad, "Elementary proof of a theorem of Bruhat–Tits–Rousseau and of a theorem of Tits," Bull. Soc. Math. France **110**, 197–202 (1982).
35. G. Prasad and M. S. Raghunathan, "On the Kneser–Tits problem," Comment. Math. Helv. **60**, 107–121 (1885).
36. G. Prasad and A. S. Rapinchuk, "Computation of the metaplectic kernel," Publ. Math. Inst. Hautes Étud. Sci. **84**, 91–187 (1996).
37. G. Prasad and A. S. Rapinchuk, "Irreducible tori in semisimple groups," Int. Math. Res. Not. **2001** (23), 1229–1242 (2001).
38. G. Prasad and A. S. Rapinchuk, "Irreducible tori in semisimple groups (Erratum)," Int. Math. Res. Not. **2002** (17), 919–921 (2002).
39. G. Prasad and A. S. Rapinchuk, "Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre," in *Collected Papers of John Milnor*, Vol. V: *Algebra* (Am. Math. Soc., Providence, RI, 2010), pp. 307–325.
40. M. S. Raghunathan, "On the congruence subgroup problem," Publ. Math. Inst. Hautes Étud. Sci. **46**, 107–161 (1976).
41. M. S. Raghunathan, "On the congruence subgroup problem. II," Invent. Math. **85**, 73–117 (1986).
42. M. S. Raghunathan, "On the group of norm 1 elements in a division algebra," Math. Ann. **279**, 457–484 (1988).
43. M. S. Raghunathan, "The congruence subgroup problem," in *Proc. Conf. on Algebraic Groups, Hyderabad, India, 1989* (Manoj Prakashan, Madras, 1991), pp. 465–494.
44. M. S. Raghunathan and T. N. Venkataramana, "The first Betti number of arithmetic groups and the congruence subgroup problem," in *Linear Algebraic Groups and Their Representations* (Am. Math. Soc., Providence, RI, 1993), Contemp. Math. **153**, pp. 95–107.
45. C. S. Rajan and T. N. Venkataramana, "On the first cohomology of arithmetic groups," Manuscr. Math. **105**, 537–552 (2001).
46. A. S. Rapinchuk, "The congruence subgroup problem for algebraic groups and strong approximation for affine varieties," Dokl. Akad. Nauk BSSR **32** (7), 581–584 (1988).
47. A. S. Rapinchuk, "On the congruence problem for algebraic groups," Dokl. Akad. Nauk SSSR **306** (6), 1304–1307 (1989) [Sov. Math., Dokl. **39** (3), 618–621 (1989)].
48. A. S. Rapinchuk, "Combinatorial theory of arithmetic groups," Preprint 20(420) (Inst. Math., Acad. Sci. BSSR, Minsk, 1990).
49. A. S. Rapinchuk, "The congruence problem for algebraic groups," Doctoral (Phys.–Math.) Dissertation (Inst. Math., Acad. Sci. BSSR, Minsk, 1990).
50. A. S. Rapinchuk, "The congruence subgroup problem," in *Algebra, K-Theory, Groups, and Education: On the Occasion of Hyman Bass's 65th Birthday*, Ed. by T. Y. Lam and A. R. Magid (Am. Math. Soc., Providence, RI, 1999), Contemp. Math. **243**, pp. 175–188.
51. A. S. Rapinchuk, "The Margulis–Platonov conjecture for $\mathrm{SL}_{1,D}$ and 2-generation of finite simple groups," Math. Z. **252**, 295–313 (2006).
52. A. S. Rapinchuk, "Strong approximation for algebraic groups," in *Thin Groups and Superstrong Approximation* (Cambridge Univ. Press, Cambridge, 2014), Math. Sci. Res. Inst. Publ. **61**, pp. 269–298.
53. A. S. Rapinchuk and I. A. Rapinchuk, "Centrality of the congruence kernel for elementary subgroups of Chevalley groups of rank > 1 over Noetherian rings," Proc. Am. Math. Soc. **139**, 3099–3113 (2011).
54. A. S. Rapinchuk and Y. Segev, "Valuation-like maps and the congruence subgroup property," Invent. Math. **144**, 571–607 (2001).
55. A. S. Rapinchuk, Y. Segev, and G. M. Seitz, "Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable," J. Am. Math. Soc. **15**, 929–978 (2002).
56. C. Riehm, "The congruence subgroup problem over local fields," Am. J. Math. **92**, 771–778 (1970).
57. Y. Segev, "On finite homomorphic images of the multiplicative group of a division algebra," Ann. Math., Ser. 2, **149**, 219–251 (1999).
58. J.-P. Serre, "Le problème des groupes de congruence pour SL_2," Ann. Math., Ser. 2, **92**, 489–527 (1970).
59. J.-P. Serre, *Galois Cohomology* (Springer, Berlin, 1997).
60. T. A. Springer, *Linear Algebraic Groups*, 2nd ed. (Birkhäuser, Boston, 1998).
61. M. R. Stein, "Surjective stability in dimension 0 for K_2 and related functors," Trans. Am. Math. Soc. **178**, 165–191 (1973).
62. B. Sury, "Congruence subgroup problem for anisotropic groups over semilocal rings," Proc. Indian Acad. Sci., Math. Sci. **101**, 87–110 (1991).
63. R. G. Swan, "Generators and relations for certain special linear groups," Adv. Math. **6**, 1–77 (1971).
64. J. Tits, "Algebraic and abstract simple groups," Ann. Math., Ser. 2, **80**, 313–329 (1964).

65. J. Tits, "Classification of algebraic semisimple groups," in *Algebraic Groups and Discontinuous Groups* (Am. Math. Soc., Providence, RI, 1966), Proc. Symp. Pure Math. **9**, pp. 33–62.
66. J. Tits, "Groupes de Whitehead de groupes algébriques simples sur un corps (d'après V.P. Platonov et al.)," in *Séminaire Bourbaki 1976/1977* (Springer, Berlin, 1978), Exp. 505, Lect. Notes Math. **677**, pp. 218–236.
67. G. Tomanov, "On the congruence-subgroup problem for some anisotropic algebraic groups over number fields," J. Reine Angew. Math. **402**, 138–152 (1989).
68. G. M. Tomanov, "Congruence subgroup problem for groups of type G_2," C. R. Acad. Bulg. Sci. **42** (6), 9–11 (1989).
69. G. Turnwald, "Multiplicative subgroups of finite index in a division ring," Proc. Am. Math. Soc. **120**, 377–381 (1994).
70. N. R. Wallach, "Square integrable automorphic forms and cohomology of arithmetic quotients of $SU(p,q)$," Math. Ann. **266**, 261–278 (1984).
71. P. A. Zalesskii, "Normal subgroups of free constructions of profinite groups and the congruence kernel in the case of positive characteristic," Izv. Ross. Akad. Nauk, Ser. Mat. **59** (3), 59–76 (1995) [Izv. Math. **59**, 499–516 (1995)].
72. P. A. Zalesskii, "Profinite surface groups and the congruence kernel of arithmetic lattices in $\mathrm{SL}_2(\mathbb{R})$," Isr. J. Math. **146**, 111–123 (2005).
73. E. I. Zel'manov, "Solution of the restricted Burnside problem for groups of odd exponent," Izv. Akad. Nauk SSSR, Ser. Mat. **54** (1), 42–59 (1990) [Math. USSR, Izv. **36** (1), 41–60 (1991)].
74. E. I. Zel'manov, "A solution of the restricted Burnside problem for 2-groups," Mat. Sb. **182** (4), 568–592 (1991) [Math. USSR, Sb. **72** (2), 543–565 (1992)].

This article was submitted by the authors in English