CENTRALITY OF THE CONGRUENCE KERNEL FOR ELEMENTARY SUBGROUPS OF CHEVALLEY GROUPS OF RANK > 1 OVER NOETHERIAN RINGS

ANDREI S. RAPINCHUK AND IGOR A. RAPINCHUK

Abstract. Let G be a universal Chevalley-Demazure group scheme associated to a reduced irreducible root system of rank > 1. For a commutative ring R, we let $\Gamma = E(R)$ denote the elementary subgroup of the group of R-points $G(R)$. The congruence kernel $C(\Gamma)$ is then defined to be the kernel of the natural homomorphism $\widehat{\Gamma} \to \overline{\Gamma}$, where $\widehat{\Gamma}$ is the profinite completion of Γ and $\overline{\Gamma}$ is the congruence completion defined by ideals of finite index. The purpose of this note is to show that for an arbitrary noetherian ring R (with some minor restrictions if G is of type C_n or G_2), the congruence kernel $C(\Gamma)$ is central in $\widehat{\Gamma}$.

1. Introduction

Let G be a universal Chevalley-Demazure group scheme associated to a reduced irreducible root system Φ of rank > 1. Given a commutative ring R, we let $G(R)$ denote the group of R-points of G, and let $E(R) \subset G(R)$ be the corresponding elementary subgroup. (We recall that $E(R)$ is defined as the subgroup generated by the images $e_\alpha(R) =: U_\alpha(R)$ for all $\alpha \in \Phi$, where $e_\alpha \colon \mathbb{G}_a \to G$ is the canonical 1-parameter subgroup corresponding to a root $\alpha \in \Phi$ — see [3] for details.) The goal of this note is to make a contribution to the analysis of the congruence subgroup problem for $E(R)$ over a general commutative noetherian ring R (with some minor restrictions if Φ is of type C_n $(n \geq 2)$ or G_2).

While the congruence subgroup problem for S-arithmetic groups is a well-established subject (see [13] for a recent survey), its analysis over general rings, at least from the point of view we adopt in this note, has been rather limited, despite a large number of results dealing with arbitrary normal subgroups of Chevalley groups over commutative rings. For this reason, we begin with a careful description of our set-up. Let R be a commutative ring and $n \geq 1$. Then to every ideal $\mathfrak{a} \subset R$, one associates the congruence subgroup $GL_n(R, \mathfrak{a}) = \ker(GL_n(R) \to GL_n(R/\mathfrak{a}))$, where the map is the one induced by the canonical homomorphism $R \to R/\mathfrak{a}$. Clearly, if $\mathfrak{a}$ is of *finite index* (i.e. the quotient $R/\mathfrak{a}$ is a finite ring), then $GL_n(R, \mathfrak{a})$ is a normal subgroup of $GL_n(R)$ of *finite index*. Given a subgroup $\Gamma \subset GL_n(R)$, we set $\Gamma(\mathfrak{a}) = \Gamma \cap GL_n(R, \mathfrak{a})$. Then, by the congruence subgroup problem for Γ, we understand the following question:

(CSP) Does every normal subgroup $\Delta \subset \Gamma$ of *finite index* contain the congruence subgroup $\Gamma(\mathfrak{a})$ for some ideal $\mathfrak{a} \subset R$ of *finite index*?

The affirmative answer would give us information about the profinite completion $\widehat{\Gamma}$, which is precisely what is needed for the analysis of representations of Γ, as well as other issues (cf. [2], [9], [15]). However, even when Γ is S-arithmetic, the answer to (CSP) is often negative. So one is instead interested in the computation of the congruence kernel, which measures the deviation from a positive solution. For this, just as in the arithmetic case, we introduce two topologies on Γ: the profinite topology τ_p^Γ and the congruence topology τ_c^Γ. The fundamental system of neighborhoods of the identity for the former consists of all normal subgroups $N \subset \Gamma$ of finite index, and for the latter of the congruence subgroups $\Gamma(\mathfrak{a})$, where $\mathfrak{a}$ runs through all ideals of R of finite index. The

corresponding completions are then given by

$$\widehat{\Gamma} = \varprojlim \Gamma/N, \quad \text{where } N \lhd \Gamma \text{ and } [\Gamma : N] < \infty$$

and

$$\overline{\Gamma} = \varprojlim \Gamma/\Gamma(\mathfrak{a}), \quad \text{where } |R/\mathfrak{a}| < \infty.$$

As τ_p^Γ is stronger than τ_c^Γ, there exists a continuous surjective homomorphism $\pi^\Gamma \colon \widehat{\Gamma} \to \overline{\Gamma}$, whose kernel is called the *congruence kernel* and denoted $C(\Gamma)$. Clearly, $C(\Gamma)$ is trivial if and only if the answer to (CSP) is affirmative; in general, its size measures the extent of deviation from the affirmative answer. Unfortunately, as remarked above, in many situations, $C(\Gamma)$ is nontrivial, and the focus of this note is on a different property, viz. the *centrality* of $C(\Gamma)$ (which means that $C(\Gamma)$ is contained in the center of $\widehat{\Gamma}$). We note that in some cases, centrality is almost as good as triviality (cf. [9], [15]), and in arithmetic cases actually implies the finiteness of $C(\Gamma)$.

Returning to Chevalley groups, we observe that congruence subgroups $G(R, \mathfrak{a}) \subset G(R)$ can be defined either as pullbacks of the congruence subgroups $GL_n(R, \mathfrak{a})$ under a faithful representation of group schemes $G \hookrightarrow GL_n$ over $\mathbb{Z}$, or, intrinsically, as the kernel of the natural homomorphism $G(R) \to G(R/\mathfrak{a})$.

Our main result concerns the congruence kernel of the elementary group $\Gamma = E(R)$. We note that the congruence topology on Γ is induced by that on $G(R)$, i.e. is defined by the intersections $\Gamma \cap G(R, \mathfrak{a})$, where $\mathfrak{a}$ runs over all ideals $\mathfrak{a} \subset R$ of finite index. On the other hand, the profinite topology on Γ may *a priori* be different from the topology induced by the profinite topology of $G(R)$ (cf. the remarks at the end of §4).

Main Theorem. *Let G be a universal Chevalley-Demazure group scheme corresponding to a reduced irreducible root system Φ of rank > 1. Furthermore, let R be a noetherian commutative ring such that $2 \in R^\times$ if Φ is of type C_n ($n \geq 2$) or G_2, and let $\Gamma = E(R)$ be the corresponding elementary subgroup. Then the congruence kernel $C(\Gamma)$ is central.*

The centrality of the congruence kernel for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$) over rings of algebraic integers was proved by Bass, Milnor, and Serre [2]. Their result was generalized to arbitrary Chevalley groups of rank > 1 over rings of algebraic integers by Matsumoto [11]. The only known result for general rings is due to Kassabov and Nikolov [9], where centrality was established for $SL_n(\mathbb{Z}[x_1, \ldots, x_k])$, with $n \geq 3$, and hence for the elementary group $E_n(R)$ over any finitely generated ring R, using K-theoretic methods. Although our proof shares some elements with the argument in [9], it is purely group-theoretic and is inspired by the proof of centrality for SL_n ($n \geq 3$) over arithmetic rings given in [14]; in addition, we do not use any results of Matsumoto [11].

Conventions and notations. All of our rings will be assumed to be commutative and unital. Unless explicitly stated otherwise, G will always denote a universal Chevalley-Demazure group scheme corresponding to a reduced irreducible root system Φ of rank > 1. Furthermore, if R is a commutative ring, then for a subgroup $\Gamma \subset G(R)$, we let $\widehat{\Gamma}$ and $\overline{\Gamma}$ denote the profinite and congruence completions of Γ, respectively.

2. Structure of $\overline{G(R)}$

Let $\mathcal{I}$ be the set of all ideals $\mathfrak{a} \subset R$ of finite index, and let $\mathcal{M} \subset \mathcal{I}$ be the subset of maximal ideals. It is not difficult to see (cf. the proof of Proposition 2.5) that $\overline{G(R)}$ can be identified with the closure of the image of $G(R)$ in $G(\widehat{R})$, where

$$\widehat{R} = \varprojlim_{\mathfrak{a} \in \mathcal{I}} R/\mathfrak{a}$$

is the profinite completion of R. The proof of the Main Theorem relies on the fact that $G(\widehat{R})$ has the bounded generation property with respect to the set $\widehat{S} = \{e_\alpha(t) \mid t \in \widehat{R},\ \alpha \in \Phi\}$ of elementaries, which we will establish at the end of this section (cf. Corollary 2.4). We begin, however, by describing the structure of $\widehat{R}$ itself. For each $\mathfrak{m} \in \mathcal{M}$, we let

$$R_{\mathfrak{m}} = \varprojlim R/\mathfrak{m}^n$$

denote the $\mathfrak{m}$-adic completion of R (cf. [1], Chapter 10).

Lemma 2.1. *Let R be a noetherian ring.*

(1) *There exists a natural isomorphism of topological rings*

$$\widehat{R} = \prod_{\mathfrak{m}\in\mathcal{M}} R_{\mathfrak{m}}.$$

(2) *Each $R_{\mathfrak{m}}$ is a complete local ring.*

Proof. (1) Since R is noetherian, for any $\mathfrak{a} \in \mathcal{I}$ and any $n \geq 2$, the quotient $\mathfrak{a}^{n-1}/\mathfrak{a}^n$ is a finitely generated $R/\mathfrak{a}$-module, hence finite. It follows that $R/\mathfrak{a}^n$ is finite for any $n \geq 1$. In particular, for any $\mathfrak{m} \in \mathcal{M}$ and $n \geq 1$, there exists a natural continuous surjective projection

$$\rho_{\mathfrak{m},n}\colon \widehat{R} \to R/\mathfrak{m}^n.$$

For a fixed $\mathfrak{m}$, the inverse limit of the $\rho_{\mathfrak{m},n}$ over all $n \geq 1$ yields a continuous ring homomorphism $\rho_{\mathfrak{m}}\colon \widehat{R} \to R_{\mathfrak{m}}$. Taking the direct product of the $\rho_{\mathfrak{m}}$ over all $\mathfrak{m} \in \mathcal{M}$, we obtain a continuous ring homomorphism

$$\rho\colon \widehat{R} \to \prod_{\mathfrak{m}\in\mathcal{M}} R_{\mathfrak{m}} =: \overline{R}.$$

We claim that ρ is the required isomorphism.

Note that ideals of the form

$$\overline{\mathfrak{a}} = \mathfrak{m}_1^{\alpha_1} R_{\mathfrak{m}_1} \times \cdots \times \mathfrak{m}_n^{\alpha_n} R_{\mathfrak{m}_n} \times \prod_{\mathfrak{m}\neq\mathfrak{m}_i} R_{\mathfrak{m}},$$

where $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\} \subset \mathcal{M}$ is a finite subset and $\alpha_i \geq 1$, form a base of neighborhoods of zero in $\overline{R}$, with

$$\overline{R}/\overline{\mathfrak{a}} = R/\mathfrak{m}_1^{\alpha_1} \times \cdots \times R/\mathfrak{m}_n^{\alpha_n}$$

(cf. [1], Proposition 10.15). Set $\mathfrak{a} = \mathfrak{m}_1^{\alpha_1} \cdots \mathfrak{m}_n^{\alpha_n}$. By the Chinese Remainder Theorem,

$$R/\mathfrak{a} \simeq R/\mathfrak{m}_1^{\alpha_1} \times \cdots \times R/\mathfrak{m}_n^{\alpha_n},$$

which implies that the composite map

$$\widehat{R} \to \overline{R} \to \overline{R}/\overline{\mathfrak{a}}$$

is surjective. Since this is true for all $\overline{\mathfrak{a}}$, we conclude that the image of ρ is dense. On the other hand, $\widehat{R}$ is compact, so the image is closed, and we obtain that ρ is in fact surjective.

To prove the injectivity of ρ, we observe that for any $\mathfrak{a} \in \mathcal{I}$, the quotient $R/\mathfrak{a}$, being a finite, hence artinian ring, is a product of finite local ring $R_1, \ldots, R_r$ ([1], Theorem 8.7). Furthermore, for each maximal ideal $\mathfrak{n}_i \subset R_i$, there exists $\beta_i \geq 1$ such that $\mathfrak{n}_i^{\beta_i} = 0$ (cf. [1], Proposition 8.4). Letting $\mathfrak{m}_i$ denote the pullback of $\mathfrak{n}_i$ in R, we obtain that $\mathfrak{a}$ contains $\mathfrak{b} := \mathfrak{m}_1^{\beta_1} \cdots \mathfrak{m}_r^{\beta_r} \in \mathcal{I}$. It follows that any nonzero $x \in \widehat{R}$ will have a nonzero projection to some $R/\mathfrak{b} = R/\mathfrak{m}_1^{\beta_1} \times \cdots \times R/\mathfrak{m}_r^{\beta_r}$, and hence to some $R_{\mathfrak{m}_i}$, as required.

(2) It is well-known that $R_{\mathfrak{m}}$ is both complete and local (cf. [1], Propositions 10.5 and 10.16). $\square$

As a first step towards establishing bounded generation of $G(\widehat{R})$ with respect to the set of elementaries, we prove

Proposition 2.2. *There exists an integer $N = N(\Phi)$, depending only on the root system Φ, such that for any commutative local ring $\mathcal{R}$, any element of $G(\mathcal{R})$ is a product of $\leq N$ elements of $S = \{e_\alpha(r) \mid r \in \mathcal{R},\ \alpha \in \Phi\}$.*

Proof. Fix a system of simple roots $\Pi \subset \Phi$, and let Φ^+ and Φ^- be the corresponding sets of positive and negative roots. Let $T \subset G$ be the canonical maximal torus, and U^+ and U^- be the canonical unipotent $\mathbb{Z}$-subschemes corresponding to Φ^+ and Φ^-. It is well-known (see, for example, [3], Lemma 4.5) that the product map $\mu\colon U^- \times T \times U^+ \to G$ is an isomorphism onto a principal open subscheme $\Omega \subset G$ defined by some $d \in \mathbb{Z}[G]$. We have decompositions

$$U^{\pm} = \prod_{\alpha \in \Phi^{\pm}} U_\alpha \quad \text{and} \quad T = \prod_{\alpha \in \Pi} T_\alpha,$$

where T_α is the maximal diagonal torus in $G_\alpha =< U_\alpha, U_{-\alpha} >= SL_2$. So, the identity

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1-a & 1 \end{pmatrix} \begin{pmatrix} 1 & a^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a(a-1) & 1 \end{pmatrix}$$

shows that there exists $N_1 = N_1(\Phi)$ such that any element of $\Omega(R)$ is a product of $\leq N_1$ elementaries, for *any* ring $\mathcal{R}$.

On the other hand, it follows from the existence of the Bruhat decomposition in Chevalley groups over fields that there exists $N_2 = N_2(\Phi)$ such that any element of $G(k)$ is a product of $\leq N_2$ elementaries, for any field k. We will now show that $N := N_1 + N_2$ has the required property for any local ring $\mathcal{R}$. Indeed, let $\mathfrak{m} \subset \mathcal{R}$ be the maximal ideal, and $k = \mathcal{R}/\mathfrak{m}$ be the residue field. As $G(k)$ is generated by elementaries, the canonical homomorphism $\omega\colon G(\mathcal{R}) \to G(k)$ is surjective. Given $g \in G(\mathcal{R})$, there exists $h \in G(\mathcal{R})$ that is a product of $\leq N_2$ elementaries and for which we have $\omega(g) = \omega(h)$. Then, for $t = gh^{-1}$, we have $\omega(t) = 1$ (in particular, $\omega(t) \in \Omega(k)$), and therefore $d(t) \not\equiv 0 (\mathrm{mod}\ \mathfrak{m})$. Since $\mathcal{R}$ is local, this means that $d(t) \in \mathcal{R}^\times$, and therefore $t \in \Omega(\mathcal{R})$. Thus, t is a product of $\leq N_1$ elementaries, and the required fact follows. □

Next, we have the following

Lemma 2.3. *Let $\mathcal{R}_i$ $(i \in I)$ be a family of commutative rings such that there exists an integer N with the property that for any $i \in I$, any $x_i \in G(\mathcal{R}_i)$ is a product of $\leq N$ elementaries. Set $\mathcal{R} = \prod_{i \in I} \mathcal{R}_i$. Then any $x \in G(\mathcal{R})$ is a product of $\leq N \cdot |\Phi|$ elementaries.*

Proof. It is enough to observe that any element of the form

$$(e_{\alpha_i}(r_i)) \in G(\mathcal{R}) = \prod_{i \in I} G(\mathcal{R}_i),$$

with $\alpha_i \in \Phi$, $r_i \in \mathcal{R}_i$, can be written as

$$\prod_{\alpha \in \Phi} e_\alpha(t_\alpha)$$

for some $t_\alpha \in \mathcal{R}$. □

Using this result, together with Lemma 2.1 and Proposition 2.2, we obtain

Corollary 2.4. *Let R be a noetherian ring. Then there exists an integer $M > 0$ such that any element of $G(\widehat{R})$ is a product of $\leq M$ elementaries from the set $\widehat{S} = \{e_\alpha(t) \mid t \in \widehat{R}, \alpha \in \Phi\}$.*

As we noted earlier, one can identify the congruence completion $\overline{G(R)}$ with the closure of the image of $G(R)$ in $G(\widehat{R})$. The following proposition gives more precise information.

Proposition 2.5. *Let R be a noetherian ring. Then $\overline{E(R)} = \overline{G(R)}$ can be naturally identified with $G(\widehat{R})$. Furthermore, there exists an integer $M > 0$ such that any element of $\overline{E(R)} = \overline{G(R)}$ is a product of $\leq M$ elements of the set $\overline{S} := \overline{\{e_\alpha(r) \mid \alpha \in \Phi, r \in R\}}$ (closure in the congruence topology).*

Proof. For any $\mathfrak{a} \in \mathcal{I}$, there exists a natural injective homomorphism $\omega_\mathfrak{a}\colon G(R)/G(R,\mathfrak{a}) \to G(R/\mathfrak{a})$, where as before, $G(R,\mathfrak{a})$ is the principal congruence subgroup of level $\mathfrak{a}$. Taking the inverse limit over all $\mathfrak{a} \in \mathcal{I}$, we obtain a continuous injective homomorphism

$$\omega\colon \overline{G(R)} \to G(\widehat{R}).$$

Clearly, the image of ω coincides with the closure of the image of the natural homomorphism $G(R) \to G(\widehat{R})$. From the definitions, one easily sees that if $\overline{e_\alpha(r)}$ is the image of $e_\alpha(r)$ ($\alpha \in \Phi, r \in R$) in $\overline{G(R)}$, then

$$\omega(\overline{e_\alpha(r)}) = e_\alpha(\hat{r}),$$

where $\hat{r}$ is the image of r in $\widehat{R}$. It follows that ω maps $\overline{S}$ onto $\widehat{S} = \{e_\alpha(t) \mid \alpha \in \Phi,\ t \in \widehat{R}\}$. Since by Corollary 2.4, $\widehat{S}$ generates $G(\widehat{R})$, we obtain that $\omega(\overline{E(R)}) = G(\widehat{R})$, and consequently ω identifies $\overline{E(R)} = \overline{G(R)}$ with $G(\widehat{R})$. Furthermore, if M is the same integer as in Corollary 2.4, then since every element of $G(\widehat{R})$ is a product of $\leq M$ elements of $\widehat{S}$, our second claim follows. □

Remark. Recall that a group $\mathcal{G}$ is said to have *bounded generation* with respect to a generating set $X \subset \mathcal{G}$ if there exists an integer $N > 0$ such that every $g \in \mathcal{G}$ can be written as $g = x_1^{\varepsilon_1} \cdots x_d^{\varepsilon_d}$ with $x_i \in X$, $d \leq N$, and $\varepsilon_i = \pm 1$. It follows from the Baire category theorem (cf. [12], Theorem 48.2) that if a compact topological group $\mathcal{G}$ is (algebraically) generated by a compact subset X, then in fact, $\mathcal{G}$ is automatically *boundedly* generated by X. Indeed, replacing X by $X \cup X^{-1} \cup \{1\}$, we may assume that $X = X^{-1}$ and $1 \in X$. Set $X^{(n)} = X \cdots X$ (n-fold product). Then the fact that $\mathcal{G} =< X >$ means that

$$\mathcal{G} = \bigcup_{n \geq 1} X^{(n)}.$$

Since each $X^{(n)}$ is compact, hence closed, we conclude from Baire's theorem that for some $n \geq 1$, $X^{(n)}$ contains an open set. Then $\mathcal{G}$ can be covered by finitely many translates of $X^{(n)}$, and therefore there exists $M > 0$ such that $X^{(M)} = \mathcal{G}$, as required. This remark shows, in particular, that (algebraic) generation of $\overline{G(R)}$ by $\overline{S}$, or that of $G(\widehat{R})$ by $\widehat{S}$, automatically yields bounded generation.

We would like to point out that the fact that $\overline{G(R)} = \overline{E(R)}$ is not used in the proof of the Main Theorem; all we need is that $\overline{E(R)}$ is boundedly generated by $\overline{S}$. So, we will indicate another way to prove this based on some ideas of Tavgen (cf. [20], Lemma 1), which also gives an explicit bound on the constant M in Proposition 2.5. First we observe that it is enough to establish the bounded generation of $E(\widehat{R})$ by $\widehat{S} = \{e_\alpha(t) \mid \alpha \in \Phi,\ t \in \widehat{R}\}$ (indeed, this will show that $E(\widehat{R})$ is a continuous image of $\widehat{R}^N$ for some $N > 0$, hence compact, implying that the map ω from the proof of Proposition 2.5 identifies $\overline{E(R)}$ with $E(\widehat{R})$, and also $\overline{S}$ with $\widehat{S}$). In turn, by the same argument as above, we see that to prove bounded generation of $E(\widehat{R})$, it suffices to show that there exists an integer $N > 0$ depending only on Φ such that for any local ring R, any element of $E(R)$ is a product of $\leq N$ elementaries. We will show that in fact

$$E(R) = (U^+(R)U^-(R))^4, \tag{1}$$

so one can take $N = 4 \cdot |\Phi|$. Let us now prove (1) by induction on the rank ℓ of Φ. If $\ell = 1$, then $G = SL_2$, and one easily checks that

$$G(R) = E(R) = (U^+(R)U^-(R))^4.$$

Now, we assume that (1) is valid for every reduced irreducible root system of rank $\leq \ell - 1$, with $\ell \geq 2$, and prove it for a root system Φ of rank ℓ. Set $X = (U^+(R)U^-(R))^4$, and let $\Delta \subset \Phi$ be a system of simple roots. Since the group $E(R)$ is generated by $e_{\pm\beta}(t)$ for $\beta \in \Delta$ and $t \in R$ (cf. the proof of (9) in §4), to prove (1), it suffices to show that

$$e_{\pm\beta}(t)X \subset X.$$

Pick $\alpha \in \Delta$, $\alpha \neq \beta$, that corresponds to an extremal node in the Dynkin diagram of Φ. Let Φ_0 (resp., Φ_1) be the set of roots in Φ that do not contain (resp., contain) α, and let $\Phi_i^{\pm} = \Phi_i \cap \Phi^{\pm}$. Then Φ_0 is an irreducible root system having $\Delta_0 = \Delta \setminus \{\alpha\}$ as a system of simple roots; in particular, Φ_0 has rank $\ell - 1$. If we let G_0 denote the corresponding universal Chevalley-Demazure group scheme, then by the induction hypothesis

$$E_0(R) = (U_0^+(R)U_0^-(R))^4,$$

with the obvious notations. Let $U_1^{\pm}(R)$ be the subgroup generated by $e_\alpha(r)$ for $\alpha \in \Phi_1^+$ (resp., $\alpha \in \Phi_1^-$) and $r \in R$. Then $U^{\pm}(R) = U_0^{\pm}(R)U_1^{\pm}(R)$, and according to ([18], Lemma 17),

$$U_0^{\pm}(R)U_1^{\mp}(R) = U_1^{\mp}(R)U_0^{\pm}(R).$$

So,

$$X = (U_0^+(R)U_1^+(R)U_0^-(R)U_1^-(R))^4 = (U_0^+(R)U_0^-(R))^4(U_1^+(R)U_1^-(R))^4 = E_0(R)(U_1^+(R)U_1^-(R))^4.$$

Since $e_{\pm\beta}(t) \in E_0(R)$, we obtain that

$$e_{\pm\beta}(t)X = e_{\pm\beta}(t)E_0(R)(U_1^+(R)U_1^-(R))^4 = X,$$

as required.

3. Profinite and congruence topologies coincide on 1-parameter root subgroups

Proposition 3.1. *Let Φ be a reduced irreducible root system of rank ≥ 2, G be the corresponding universal Chevalley-Demazure group scheme, and $E(R)$ be the elementary subgroup of the group $G(R)$ over a commutative ring R. Furthermore, suppose $N \subset E(R)$ is a normal subgroup of finite index. If Φ is not of type C_n ($n \geq 2$) or G_2, then there exists an ideal $\mathfrak{a} \subset R$ of finite index such that*

$$e_\alpha(\mathfrak{a}) \subset N \cap U_\alpha(R) \tag{2}$$

for all $\alpha \in \Phi$, where $e_\alpha(\mathfrak{a}) = \{e_\alpha(t) \mid t \in \mathfrak{a}\}$. The same conclusion holds for Φ of type C_n ($n \geq 2$) and G_2 if $2 \in R^\times$. Thus, in these cases, the profinite and the congruence topologies of $E(R)$ induce the same topology on $U_\alpha(R)$, for all $\alpha \in \Phi$.

Proof. We begin with two preliminary remarks. First, for any root $\alpha \in \Phi$,

$$\mathfrak{a}(\alpha) := \{t \in R \mid e_\alpha(t) \in N\}$$

is obviously a finite index subgroup of the additive group of R. What one needs to show is that either $\mathfrak{a}(\alpha)$ itself is an ideal of R, or that it at least contains an ideal of finite index. Second, if $\alpha_1, \alpha_2 \in \Phi$ are roots of the same length, then by ([7], 10.4, Lemma C), there exists an element $\tilde{w}$ of the Weyl group $W(\Phi)$ such that $\alpha_2 = \tilde{w} \cdot \alpha_1$. Consequently, it follows from ([16], 3.8, relation (R4)) that we can find $w \in E(R)$ such that

$$we_{\alpha_1}(t)w^{-1} = e_{\alpha_2}(\varepsilon(w)t)$$

for all $t \in R$, where $\varepsilon(w) \in \{\pm 1\}$ is independent of t. Since N is a normal subgroup of $E(R)$, we conclude that

$$\mathfrak{a}(\alpha_1) = \mathfrak{a}(\alpha_2). \tag{3}$$

Thus, it is enough to find a finite index ideal $\mathfrak{a} \subset R$ such that (2) holds for a *single* root of each length.

Let us now prove our claim for Φ of type A_2 using explicit computations with commutator relations. We will use the standard realization of Φ, described in [5], where the roots are of the form $\varepsilon_i - \varepsilon_j$, with $i, j \in \{1, 2, 3\}, i \neq j$. To simplify notation, we will write $e_{ij}(t)$ to denote $e_\alpha(t)$ for $\alpha = \varepsilon_i - \varepsilon_j$. Set $\alpha_1 = \varepsilon_1 - \varepsilon_2$. We will now show that $\mathfrak{a}(\alpha_1)$ is an ideal of R, and then it will follow from our previous remarks that $\mathfrak{a} := \mathfrak{a}(\alpha_1)$ is as required. Let $r \in \mathfrak{a}(\alpha_1)$ and $s \in R$. Since $N \lhd E(R)$, the (well-known) relation

$$[e_{12}(r), e_{23}(s)] = e_{13}(rs),$$

where $[g, h] = ghg^{-1}h^{-1}$, shows that $rs \in \mathfrak{a}(\alpha_2)$ for $\alpha_2 = \varepsilon_1 - \varepsilon_2$. But then (3) yields $rs \in \mathfrak{a}(\alpha_1)$, completing the argument.

Now let Φ be any root system of rank ≥ 2 in which all roots have the same length. Then clearly Φ contains a subsystem Φ_0 of type A_2, so our previous considerations show that there exists a finite index ideal $\mathfrak{a} \subset R$ with the property that $\mathfrak{a} \subset \mathfrak{a}(\alpha)$ for all $\alpha \in \Phi_0$. But then, by (3), the same inclusion holds for all $\alpha \in \Phi$.

Next, we consider the case of Φ of type B_n with $n \geq 3$. Note that since the system of type F_4 contains a subsystem of type B_3, this will automatically take care of the case when Φ is of type F_4 as well. We will use the standard realization of Φ of type B_n, where the roots are of the form $\pm\varepsilon_i$, $\pm\varepsilon_i \pm \varepsilon_j$ with $i, j \in \{1, \ldots, n\}, i \neq j$. The system Φ contains a subsystem Φ_0 of type A_{n-1}, all of whose roots are long roots in Φ. Arguing as above, we see that there exists an ideal $\mathfrak{a} \subset R$ of finite index such that (2) holds for all $\alpha \in \Phi_0$, and hence for all long roots $\alpha \in \Phi$. To show that the same ideal also works for short roots, we will use the following relation, which is verified by direct computation:

$$[e_{\varepsilon_1+\varepsilon_2}(r), e_{-\varepsilon_2}(s)] = e_{\varepsilon_1}(rs)e_{-\varepsilon_1-\varepsilon_2}(-rs^2). \tag{4}$$

for any $r, s \in R$. Now, if $r \in \mathfrak{a}$, then $e_{\varepsilon_1+\varepsilon_2}(r), e_{-\varepsilon_1-\varepsilon_2}(-r) \in N$. So, setting $s = 1$ in (4) and noting that $[e_{\varepsilon_1+\varepsilon_2}(r), e_{-\varepsilon_2}(1)] \in N$ as $N \lhd E(R)$, we obtain that $e_{\varepsilon_1}(r) \in N$. Thus, (2) holds for $\alpha = \varepsilon_1$, and therefore for all short roots.

Next, we proceed to the case of Φ of type $B_2 = C_2$, where we assume that $2 \in R^\times$. We will use the same realization of Φ as in the previous paragraph (for $n = 2$). Set $\mathfrak{a} = \mathfrak{a}(\varepsilon_1)$. Then for $r \in \mathfrak{a}$, $s \in R$, one can check by direct computation that

$$[e_{\varepsilon_1}(r), e_{\varepsilon_2}(s/4)] = e_{\varepsilon_1+\varepsilon_2}(rs/2) \in N. \tag{5}$$

Next, using (4), in conjunction with the fact that $e_{\varepsilon_1}(u)$ and $e_{\varepsilon_1-\varepsilon_2}(v)$ commute for all $u, v \in R$, we obtain

$$[e_{\varepsilon_1+\varepsilon_2}(rs/2), e_{-\varepsilon_2}(1)][e_{\varepsilon_1+\varepsilon_2}(rs/2), e_{-\varepsilon_2}(-1)]^{-1} = e_{\varepsilon_1}(rs) \in N,$$

i.e. $rs \in \mathfrak{a}$, which shows that $\mathfrak{a}$ is an ideal. Furthermore, from (5), we see that for any $r \in \mathfrak{a}$, we have

$$[e_{\varepsilon_1}(r), e_{\varepsilon_2}(1/2)] = e_{\varepsilon_1+\varepsilon_2}(r) \in N.$$

Thus, $e_{\varepsilon_1+\varepsilon_2}(\mathfrak{a}) \subset N$, and therefore (2) holds for all $\alpha \in \Phi$.

Finally, suppose that Φ is of type G_2 and assume again that $2 \in R^\times$. We will use the realization of Φ described in [4]: one picks a system of simple roots $\{k, c\}$ in Φ, where k is long and c is short, and then the long roots of Φ are

$$\pm k, \pm(3c + k), \pm(3c + 2k),$$

and the short roots are

$$\pm c, \pm(c + k), \pm(2c + k).$$

Set $\mathfrak{a} = \mathfrak{a}(k)$. Since the long roots of Φ form a subsystem of type A_2, for which our claim has already been established, we conclude that $\mathfrak{a}$ is a finite index ideal in R and that (2) holds for all

long roots. To show that (2) is true for the short roots as well, we need to recall the following explicit forms of the Steinberg commutator relations that were established in ([4], Theorem 1.1):

$$[e_k(s), e_c(t)] = e_{c+k}(\varepsilon_1 st)e_{2c+k}(\varepsilon_2 st^2)e_{3c+k}(\varepsilon_3 st^3)e_{3c+2k}(\varepsilon_4 s^2t^3), \tag{6}$$

$$[e_{c+k}(s), e_{2c+k}(t)] = e_{3c+2k}(3\varepsilon_5 st), \tag{7}$$

where $\varepsilon_i = \pm 1$. Using (6), we obtain

$$[e_k(s), e_c(1)][e_k(s), e_c(-1)] =$$

$$= e_{c+k}(\varepsilon_1 s)e_{2c+k}(\varepsilon_2 s)e_{3c+k}(\varepsilon_3 s)e_{3c+2k}(\varepsilon_4 s^2)e_{c+k}(-\varepsilon_1 s)e_{2c+k}(\varepsilon_2 s)e_{3c+k}(-\varepsilon_3 s)e_{3c+2k}(-\varepsilon_4 s^2).$$

Since the terms $e_{3c+k}(-\varepsilon_3 s)$ and $e_{3c+2k}(-\varepsilon_4 s^2)$ commute with all other terms, the last expression reduces to

$$e_{c+k}(\varepsilon_1 s)e_{2c+k}(\varepsilon_2 s)e_{c+k}(-\varepsilon_1 s)e_{2c+k}(\varepsilon_2 s),$$

which, using (7), can be written in the form

$$e_{3c+2k}(3\varepsilon_5\varepsilon_1\varepsilon_2 s^2)e_{2c+k}(2\varepsilon_2 s).$$

Hence if $s \in \mathfrak{a}$, we obtain that

$$[e_k(s/2), e_c(1)][e_k(s/2), e_c(-1)] = e_{3c+2k}(3\varepsilon_5\varepsilon_1\varepsilon_2 s^2/4)e_{2c+k}(\varepsilon_2 s) \in N.$$

But $e_{3c+2k}(3\varepsilon_5\varepsilon_1\varepsilon_2 s^2/4) \in N$, from which it follows that $e_{2c+k}(\mathfrak{a}) \subset N$. This completes the proof. □

Remark. If R is the ring of algebraic S-integers, then any subgroup of finite index of the additive group of R contains an ideal of finite index, so the conclusion of Proposition 3.1 holds for root systems of rank > 1 of all types without any additional restrictions on R. On the other hand, if R is the ring of S-integers in a global field of positive characteristic > 2, then $2 \in R^\times$, and Proposition 3.1 again applies to all root systems without any extra assumptions.

4. Proof of the main theorem

We return to the notations introduced in §1. In particular, we set $\Gamma = E(R)$, where R is a commutative noetherian ring such that $2 \in R^\times$ if our root system Φ is of type C_n ($n \geq 2$) or G_2, and let $\widehat{\Gamma}$ and $\overline{\Gamma}$ denote the profinite and congruence completions of Γ, respectively. Furthermore, we let $\pi\colon \widehat{\Gamma} \to \overline{\Gamma}$ denote the canonical continuous homomorphism, so that $C(\Gamma) := \ker \pi$ is the congruence kernel. For each root $\alpha \in \Phi$, we let $\widehat{U}_\alpha$ and $\overline{U}_\alpha$ denote the closures of the images of the natural homomorphisms $U_\alpha(R) \to \widehat{\Gamma}$ and $U_\alpha(R) \to \overline{\Gamma}$. By Proposition 3.1, the profinite and congruence topologies of Γ induce the same topology on each $U_\alpha(R)$, which implies that $\pi|_{\widehat{U}_\alpha}\colon \widehat{U}_\alpha \to \overline{U}_\alpha$ is a group isomorphism. From the definitions, it is clear that $\overline{U}_\alpha$ coincides with $\overline{e}_\alpha(\widehat{R})$, where $\overline{e}_\alpha\colon \widehat{R} \to G(\widehat{R}) = \overline{G(R)}$ is the 1-parameter subgroup associated with α over the ring $\widehat{R}$. Set

$$\widehat{e}_\alpha = (\pi|_{\widehat{U}_\alpha})^{-1} \circ \overline{e}_\alpha.$$

Then $\widehat{e}_\alpha\colon \widehat{R} \to \widehat{U}_\alpha$ is an isomorphism of topological groups, and in particular, we have

$$\widehat{e}_\alpha(r+s) = \widehat{e}_\alpha(r)\widehat{e}_\alpha(s)$$

for all $r, s \in \widehat{R}$ and any $\alpha \in \Phi$.

Before establishing some further properties of the $\widehat{e}_\alpha$, let us recall that for any commutative ring S and any $\alpha, \beta \in \Phi$, $\beta \neq -\alpha$, there is a relation in $G(S)$ of the form

$$[e_\alpha(s), e_\beta(t)] = \prod e_{i\alpha+j\beta}(N_{\alpha,\beta}^{i,j} s^i t^j) \tag{8}$$

for all $s,t \in S$, where the product is taken over all roots of the form $i\alpha + j\beta$ with $i,j \in \mathbb{Z}^+$, listed in an arbitrary (but *fixed*) order, and the $N_{\alpha,\beta}^{i,j}$ are integers depending only on $\alpha,\beta \in \Phi$ and the order of the factors in (8), but not on $s,t \in S$. Furthermore, recall that the abstract group $\tilde{G}(S)$ with generators $x_\alpha(s)$ for all $s \in S$ and $\alpha \in \Phi$ subject to the relations

(R1) $\tilde{x}_\alpha(s)\tilde{x}_\alpha(t) = \tilde{x}_\alpha(s+t)$,

(R2) $[\tilde{x}_\alpha(s), \tilde{x}_\beta(t)] = \prod \tilde{x}_{i\alpha+j\beta}(N_{\alpha,\beta}^{i,j} s^i t^j)$, where $N_{\alpha,\beta}^{i,j}$ are the same integers, and the roots are listed in the same order, as in (8),

is called the *Steinberg group*. It follows from (8) that there exists a canonical homomorphism $\tilde{G}(S) \to G(S)$, defined by $x_\alpha(s) \mapsto e_\alpha(s)$, whose kernel is denoted by $K_2(\Phi, S)$.

Lemma 4.1. (1) *For any $\alpha,\beta \in \Phi$, $\beta \neq -\alpha$, and $s,t \in \widehat{R}$, we have $[\widehat{e}_\alpha(s), \widehat{e}_\beta(t)] = \prod \widehat{e}_{i\alpha+j\beta}(N_{\alpha,\beta}^{i,j} s^i t^j)$.*

Let $\widehat{R} = \prod_{\mathfrak{m}\in\mathcal{M}} R_\mathfrak{m}$ be the decomposition from Lemma 2.1(1), and for $\mathfrak{m} \in \mathcal{M}$, let $\widehat{\Gamma}_\mathfrak{m}$ (resp. $\widehat{\Gamma}'_\mathfrak{m}$) be the subgroup of $\widehat{\Gamma}$ (algebraically) generated by $\widehat{e}_\alpha(r)$ for all $r \in R_\mathfrak{m}$ (resp., $r \in R'_\mathfrak{m} := \prod_{\mathfrak{n}\neq\mathfrak{m}} R_\mathfrak{n}$) and all $\alpha \in \Phi$. Then

(2) *There exists a surjective group homomorphism $\theta_\mathfrak{m}\colon \tilde{G}(R_\mathfrak{m}) \to \widehat{\Gamma}_\mathfrak{m}$ such that $x_\alpha(r) \mapsto \widehat{e}_\alpha(r)$ for all $r \in R_\mathfrak{m}$ and $\alpha \in \Phi$.*

(3) *$\widehat{\Gamma}_\mathfrak{m}$ and $\widehat{\Gamma}'_\mathfrak{m}$ commute elementwise inside $\widehat{\Gamma}$.*

Proof. (1) Define two continuous maps

$$\varphi\colon \widehat{R}\times\widehat{R} \to \widehat{\Gamma}, \quad (s,t) \mapsto [\widehat{e}_\alpha(s), \widehat{e}_\beta(t)]$$

and

$$\psi\colon \widehat{R}\times\widehat{R} \to \widehat{\Gamma}, \quad (s,t) \mapsto \prod \widehat{e}_{i\alpha+j\beta}(N_{\alpha,\beta}^{i,j} s^i t^j).$$

It follows from (8) that these maps coincide on $R \times R$. Since $R \times R$ is dense in $\widehat{R}\times\widehat{R}$, we have $\varphi \equiv \psi$, yielding our claim.

(2) Since we have shown that the $\widehat{e}_\alpha(r)$, $r \in R_\mathfrak{m}$, $\alpha \in \Phi$, satisfy the relations (R1) and (R2), the existence of the homomorphism $\theta_\mathfrak{m}$ follows.

(3) It suffices to show that for any $\alpha,\beta \in \Phi$ and any $r \in R_\mathfrak{m},\ s \in R'_\mathfrak{m}$, the elements $\widehat{e}_\alpha(r), \widehat{e}_\beta(s) \in \widehat{\Gamma}$ commute. Since $rs = 0$ in $\widehat{R}$, this fact immediately follows from (1) if $\beta \neq -\alpha$. To handle the remaining case $\beta = -\alpha$, we observe that for any ring S and the corresponding Steinberg group $\tilde{G}(S)$, we have

$$\tilde{G}(S) = < x_\gamma(r) \mid \gamma \in \Phi \setminus \{\alpha\}, r \in S > . \tag{9}$$

Indeed, it is well-known that $\tilde{G}(S)$ is generated by the elements $x_\gamma(r)$ for all $r \in R$ and all γ in an arbitrarily chosen system $\Pi \subset \Phi$ of simple roots (this follows, for example, from the fact that the Weyl group of Φ is generated by the reflections corresponding to simple roots, and moreover, every root lies in the orbit of a simple root under the action of the Weyl group). On the other hand, since Φ is of rank ≥ 2, for any $\alpha \in \Phi$, one can find a system of simple roots $\Pi \subset \Phi$ that does not contain α, and (9) follows. Using the homomorphism $\theta_\mathfrak{m}$ constructed in part (2), we conclude from (9) that $\widehat{\Gamma}_\mathfrak{m} = \theta_\mathfrak{m}(\tilde{G}(R_\mathfrak{m}))$ is generated by $\widehat{e}_\gamma(r)$ for $r \in R_\mathfrak{m}$, $\gamma \in \Phi \setminus \{\alpha\}$. So, since we already know that $\widehat{e}_{-\alpha}(s)$, with $s \in R'_\mathfrak{m}$, commutes with all of these elements, it also commutes with $\widehat{e}_\alpha(r)$, yielding our claim.

□

The following lemma, which uses results of Stein [17] on the computation of K_2 over semi-local rings, is a key ingredient in the proof of the Main Theorem.

Lemma 4.2. *The kernel $\ker(\pi|_{\widehat{\Gamma}_\mathfrak{m}})$ of the restriction $\pi|_{\widehat{\Gamma}_\mathfrak{m}}$ lies in the center of $\widehat{\Gamma}_\mathfrak{m}$, for any $\mathfrak{m} \in \mathcal{M}$.*

Proof. Stein has shown that if Φ has rank ≥ 2 and S is a semi-local ring which is generated by its units, then $K_2(\Phi, S)$ lies in the center of $\tilde{G}(S)$ (cf. [17], Theorem 2.13). Since $S = R_{\mathfrak{m}}$ is local, it is automatically generated by its units, hence $K_2(\Phi, R_{\mathfrak{m}}) = \ker(\tilde{G}(R_{\mathfrak{m}}) \xrightarrow{\mu} E(R_{\mathfrak{m}}))$ is central. On the other hand, μ admits the following factorization:

$$\tilde{G}(R_{\mathfrak{m}}) \xrightarrow{\theta_{\mathfrak{m}}} \widehat{\Gamma}_{\mathfrak{m}} \xrightarrow{\pi|_{\widehat{\Gamma}_{\mathfrak{m}}}} E(R_{\mathfrak{m}}).$$

Since $\theta_{\mathfrak{m}}$ is surjective, we conclude that

$$\ker(\pi|_{\widehat{\Gamma}_{\mathfrak{m}}}) = \theta_{\mathfrak{m}}(K_2(\Phi, R_{\mathfrak{m}}))$$

is central in $\widehat{\Gamma}_{\mathfrak{m}}$. □

Now fix $\mathfrak{m} \in \mathcal{M}$ and let $\Delta_{\mathfrak{m}} = \widehat{\Gamma}_{\mathfrak{m}}\widehat{\Gamma}'_{\mathfrak{m}}$ be the subgroup of $\widehat{\Gamma}$ (algebraically) generated by $\widehat{\Gamma}_{\mathfrak{m}}$ and $\widehat{\Gamma}'_{\mathfrak{m}}$. Let $c \in C(\Gamma) \cap \Delta_{\mathfrak{m}}$, and write $c = c_1c_2$, with $c_1 \in \widehat{\Gamma}_{\mathfrak{m}}, c_2 \in \widehat{\Gamma}'_{\mathfrak{m}}$. We have $\overline{\Gamma} = \overline{\Gamma}_{\mathfrak{m}} \times \overline{\Gamma}'_{\mathfrak{m}}$, where $\overline{\Gamma}_{\mathfrak{m}} = E(R_{\mathfrak{m}})$ and $\overline{\Gamma}'_{\mathfrak{m}} = E(R'_{\mathfrak{m}})$. Since $\pi(c_1) \in \overline{\Gamma}_{\mathfrak{m}}$, $\pi(c_2) \in \overline{\Gamma}'_{\mathfrak{m}}$, we conclude from

$$\pi(c) = e = \pi(c_1)\pi(c_2)$$

that $\pi(c_1) = e$, i.e. $c_1 \in \ker(\pi|_{\widehat{\Gamma}_{\mathfrak{m}}})$. Then by Lemma 4.2, $\widehat{\Gamma}_{\mathfrak{m}}$ centralizes c_1. On the other hand, $\widehat{\Gamma}_{\mathfrak{m}}$ centralizes $c_2 \in \widehat{\Gamma}'_{\mathfrak{m}}$ by Lemma 4.1(3). So, $\widehat{\Gamma}_{\mathfrak{m}}$ centralizes c. Thus, we have shown that $C \cap \Delta_{\mathfrak{m}}$ is centralized by $\widehat{\Gamma}_{\mathfrak{m}}$. To prove that $\widehat{\Gamma}_{\mathfrak{m}}$ actually centralizes all of C, we need the following

Lemma 4.3. *Let $\varphi\colon \mathcal{G}_1 \to \mathcal{G}_2$ be a continuous homomorphism of topological groups, and let $\mathcal{F} = \ker\varphi$. Suppose $\Theta \subset \mathcal{G}_1$ is a dense subgroup such that there exists a compact set $\Omega \subset \Theta$ whose image $\varphi(\Omega)$ is a neighborhood of the identity in $\mathcal{G}_2$. Then $\mathcal{F} \cap \Theta$ is dense in $\mathcal{F}$.*

Proof. Since $\varphi(\Omega)$ is a neighborhood of the identity in $\mathcal{G}_2$, we can find an open set $U \subset \mathcal{G}_1$ such that

$$\mathcal{F} \subset U \subset \varphi^{-1}(\varphi(\Omega)) = \Omega\mathcal{F}.$$

Now since Θ is dense in $\mathcal{G}_1$, we have $U \subset \overline{\Theta \cap U}$, where the bar denotes the closure in $\mathcal{G}_1$. Thus,

$$\mathcal{F} \subset \overline{\Theta \cap U} \subset \overline{\Theta \cap \Omega\mathcal{F}}.$$

But $\Theta \cap \Omega\mathcal{F} = \Omega(\Theta \cap \mathcal{F})$, and since Ω is compact, the product $\Omega\overline{(\Theta \cap \mathcal{F})}$ is closed. So

$$\mathcal{F} \subset \overline{\Theta \cap \Omega\mathcal{F}} \subset \Omega\overline{(\Theta \cap \mathcal{F})}.$$

Since $\mathcal{F}$ is closed, we have $\overline{\Theta \cap \mathcal{F}} \subset \mathcal{F}$, so

$$\mathcal{F} = (\Omega \cap \mathcal{F})\overline{(\Theta \cap \mathcal{F})} \subset (\Theta \cap \mathcal{F})\overline{(\Theta \cap \mathcal{F})} = \overline{\Theta \cap \mathcal{F}},$$

as required. □

In order to apply Lemma 4.3 in our situation, we noted the following simple fact

Lemma 4.4. *The subgroup $\Delta \subset \widehat{\Gamma}$ (algebraically) generated by the $\widehat{\Gamma}_{\mathfrak{m}}$ for all $\mathfrak{m} \in \mathcal{M}$ is dense. Consequently, for any $\mathfrak{m} \in \mathcal{M}$, the subgroup $\Delta_{\mathfrak{m}} = \widehat{\Gamma}_{\mathfrak{m}}\widehat{\Gamma}'_{\mathfrak{m}} \subset \widehat{\Gamma}$ is dense.*

Proof. Let

$$R_0 := \sum_{\mathfrak{m} \in \mathcal{M}} R_{\mathfrak{m}} \subset \widehat{R} = \prod_{\mathfrak{m} \in \mathcal{M}} R_{\mathfrak{m}}.$$

Clearly R_0 is a dense subring of $\widehat{R}$. On the other hand, Δ obviously contains $\widehat{e}_\alpha(R_0)$ for any $\alpha \in \Phi$. So, the closure $\overline{\Delta}$ contains $\widehat{e}_\alpha(R)$ for all $\alpha \in \Phi$, and therefore coincides with $\widehat{\Gamma}$, yielding our first assertion. Furthermore, for any $\mathfrak{m} \in \mathcal{M}$, the subgroup $\Delta_{\mathfrak{m}}$ contains $\Gamma_{\mathfrak{n}}$ for all $\mathfrak{n} \in \mathcal{M}$, so our second assertion follows. □

Conclusion of the proof of the Main Theorem: Fix $\mathfrak{m} \in \mathcal{M}$. We have already seen that $\widehat{\Gamma}_{\mathfrak{m}}$ centralizes $C \cap \Delta_{\mathfrak{m}}$. We claim that $C \cap \Delta_{\mathfrak{m}}$ is dense in C, and hence $\widehat{\Gamma}_{\mathfrak{m}}$ centralizes C. Indeed, by Lemma 4.4, $\Delta_{\mathfrak{m}}$ is dense in $\widehat{\Gamma}$. On the other hand, it follows from Corollary 2.4 that there exists a string of roots $(\alpha_1, \ldots, \alpha_L)$ such that the map

$$\widehat{R}^L \to \overline{\Gamma}, \qquad (r_1, \ldots, r_L) \mapsto \prod_{i=1}^{L} \overline{e}_{\alpha_i}(r_i)$$

is surjective. Then

$$\Omega := \widehat{e}_{\alpha_1}(\widehat{R}) \cdots \widehat{e}_{\alpha_L}(\widehat{R}) = \left(\widehat{e}_{\alpha_1}(R_{\mathfrak{m}}) \cdots \widehat{e}_{\alpha_L}(R_{\mathfrak{m}})\right) \left(\widehat{e}_{\alpha_1}(R'_{\mathfrak{m}}) \cdots \widehat{e}_{\alpha_L}(R'_{\mathfrak{m}})\right)$$

is a compact subset of $\widehat{\Gamma}$ that is contained in $\Delta_{\mathfrak{m}}$ and has the property that $\pi(\Omega) = \overline{\Gamma}$. Invoking Lemma 4.3, we obtain that $C \cap \Delta_{\mathfrak{m}}$ is dense in C, as required.

We now see that $\widehat{\Gamma}_{\mathfrak{m}}$ centralizes C for all $\mathfrak{m} \in \mathcal{M}$. Since the subgroup $\Delta \subset \widehat{\Gamma}$ generated by the $\widehat{\Gamma}_{\mathfrak{m}}$ is dense in $\widehat{\Gamma}$ by Lemma 4.4, we obtain that $\widehat{\Gamma}$ centralizes C, completing the proof. □

To put our proof of the Main Theorem into perspective, we recall the following criterion for the centrality of the congruence kernel in the context of the congruence subgroup problem for algebraic groups over global fields (see [13], Theorem 4). Let G be an absolutely almost simple simply connected algebraic group over a global field K, and S be a set of places of K, which we assume to contain all archimedean places if K is a number field, such that the corresponding S-arithmetic group $G(\mathcal{O}_S)$ is infinite (where $\mathcal{O}_S$ is the ring of S-integers in K). Then by the Strong Approximation Theorem, the S-congruence completion $\overline{G(K)}$ of the group $G(K)$ of K-rational points can be identified with the group of S-adeles $G(\mathbb{A}_S)$, and in particular the group $G(K_v)$, for $v \notin S$, can be viewed as a subgroup of $\overline{G(K)}$. Assume furthermore that S contains no nonarchimedean anisotropic places for G and that G/K satisfies the Margulis-Platonov conjecture. If for each $v \in S$, there exists a subgroup H_v of the S-arithmetic completion $\widehat{G(K)}$ such that

(1) $\pi(H_v) = G(K_v)$ for all $v \notin S$, where $\pi\colon \widehat{G(K)} \to \overline{G(K)}$ is the canonical projection;

(2) H_{v_1} and H_{v_2} commute elementwise for $v_1 \neq v_2$;

(3) the H_v, for $v \notin S$, (algebraically) generate a dense subgroup of $\widehat{G(K)}$,

then the congruence kernel $C^S(G) := \ker \pi$ is central. So, this criterion basically states that in the arithmetic situation, the mere existence of elementwise commuting lifts of "local groups" implies the centrality of the congruence kernel. In our situation, the existence of elementwise commuting lifts (which we denoted $\widehat{\Gamma}_{\mathfrak{m}}$ above) also plays a part in the proof of centrality (cf. Lemma 4.2(3)), but some additional considerations (such as the result of Stein and the bounded generation property for $E(\widehat{R}) = G(\widehat{R})$) are needed; the facilitating factor in the arithmetic situation is the action of the group $G(K)$ on the congruence kernel, which is not available over more general rings.

Finally, we will relate our result on the centrality of the congruence kernel $C(\Gamma)$ for $\Gamma = E(R)$ to the congruence subgroup problem for $G(R)$. We have the following commutative diagram induced by the natural embedding $\Gamma \hookrightarrow G(R)$:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C(\Gamma) & \longrightarrow & \widehat{\Gamma} & \xrightarrow{\pi^{\Gamma}} & \overline{\Gamma} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
1 & \longrightarrow & C(G(R)) & \longrightarrow & \widehat{G(R)} & \xrightarrow{\pi^{G(R)}} & \overline{G(R)} & \longrightarrow & 1
\end{array}$$

We note that by Proposition 2.5, γ is an isomorphism. So, $\alpha(C(\Gamma)) = C(G(R)) \cap \beta(\widehat{\Gamma})$, and $\beta(\widehat{\Gamma})$ coincides with the closure $\check{\Gamma}$ of Γ in $\widehat{G(R)}$. Thus, our Main Theorem yields the following

Corollary 4.5. *$C(G(R)) \cap \check{\Gamma}$ is centralized by $\check{\Gamma}$.*

The exact relationship between $C(G(R))$ and $C(G(R)) \cap \check{\Gamma}$ (or $C(\Gamma)$) remains unclear except in a few cases. Matsumoto [11] showed that $G(R) = E(R)$ for any ring R of algebraic S-integers, which combined with our Main Theorem and the remark at the end of §3, yields the centrality of $C(E(R)) = C(G(R))$, established by Matsumoto himself. Furthermore, for $G = SL_n$ $(n \geq 3)$ and $R = \mathbb{Z}[x_1, \ldots, x_k]$, by a result of Suslin [19], we again have $G(R) = E(R)$, so $C(G(R)) = C(E(R))$ is central in $\widehat{E(R)} = \widehat{G(R)}$, which was established in [9]. On the other hand, there exist principal ideal domains R for which $SL_n(R) \neq E(R)$ (cf. [6], [8]), and then the analysis of $C(G(R))$ requires more effort. We only note that if $\Gamma = E(R)$ has finite index in $G(R)$, then the profinite topology on Γ is induced by the profinite topology of $G(R)$, which implies that β is injective, and therefore $C(\Gamma)$ is identified with a finite index subgroup of $C(G(R))$.

Acknowledgements. The first-named author was partially supported by NSF grant DMS-0965758 and the Humboldt Foundation. The paper was finalized when both authors were visiting SFB 701 (Bielefeld), whose hospitality is gratefully acknowledged.

References

1. M.F. Atiyah, I.G. MacDonald, *Introduction to Commutative Algebra*, Westview Press, 1969
2. H. Bass, J. Milnor, J.P. Serre, *Solution of the congruence subgroup problem for $SL_n (n \geq 3)$ and $Sp_{2n} (n \geq 2)$*, Publ. Math. IHES **33** (1967), 59-137
3. A. Borel, *Properties and linear representations of Chevalley groups*, Seminar on Algebraic Groups and Related Finite Groups, Lect. Notes Math. **131**, Springer, 1970
4. D. Costa, G. Keller, *On the normal subgroups of $G_2(A)$*, Trans. AMS **351** (1999), no. 12, 5051-5088
5. N. Bourbaki, *Lie Groups and Lie Algebras, Chapter 7-9*, Elements of Mathematics, Springer, 2005
6. D. Grayson, *SK_1 of an interesting principal ideal domain*, J. Pure Appl. Algebra **20** (1981), 157-163
7. J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, GTM 9, Springer, 1972
8. F. Ischebeck, *Hauptidealringe mit nichtrivialer SK_1-Gruppe*, Arch. Math. (Basel) **35** (1980), 138-139
9. M. Kassabov, N. Nikolov, *Universal lattices and property tau*, Invent. math. **165**, 209-224 (2006)
10. H. Matsumoto, *Subgroups of finite index in certain arithmetic groups*, Proc. Sym. Pure Math., AMS **9** (1966), 99-103
11. H. Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*, Ann. Sci. de l'É.N.S. (4) **2** (1969), 1-62
12. J.R. Munkres, *Topology*, Prentice Hall, 1975
13. G. Prasad, A.S. Rapinchuk, *Developments on the congruence subgroup problem after the work of Bass, Milnor, and Serre*, to appear in volume V of Milnor's collected work (AMS, 2010); available at arXiv: 0809.1622
14. A.S. Rapinchuk, *Combinatorial theory of arithmetic groups*, Preprint No. 20(420), Academy of Sciences of the Byelorussian SSR, Institute of Mathematics (April 1990)
15. D. Shenfeld, *On semisimple representations of $SL_n(\mathbb{Z}[x_1, \ldots, x_k])$*, Hebrew University Master's Thesis
16. M.R. Stein *Relations and coverings of Chevalley groups over commutative rings*, Amer. J. Math. **93** (1971), no. 4, 965-1004
17. M.R. Stein *Surjective Stability in dimension 0 for K_2 and related functors*, Trans. AMS **178** (1973), 165-191
18. R. Steinberg, *Lectures on Chevalley groups*, mimeographed lectures notes, Yale University Math. Dept., New Haven, CT, 1968
19. A.A. Suslin, *The structure of the special linear group over rings of polynomials*, Izv. Akad. Nauk SSSR Ser. Mat. **41** (1977), no. 2, 235-252, 477.
20. O.I. Tavgen, *Finite width of arithmetic subgroups of Chevalley groups of rank ≥ 2*, Soviet Math. Dokl. **41** (1990), no. 1

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
E-mail address: asr3x@virginia.edu

Department of Mathematics, Yale University, New Haven, CT 06502
E-mail address: igor.rapinchuk@yale.edu