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

ANDREI S. RAPINCHUK AND IGOR A. RAPINCHUK

(Communicated by Jonathan I. Hall)

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 $\hat{\Gamma} \to \Gamma$, where $\hat{\Gamma}$ is the profinite completion of $\Gamma$ and $\Gamma$ is the congruence completion defined by ideals of finite index. The purpose of this paper 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 $\hat{\Gamma}$.

1. Introduction

Let $G$ be a universal Chevalley-Demazure group scheme associated to a reduced irreducible root system $\Phi$ 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 $e_\alpha \colon G_\alpha \to G$ is the canonical 1-parameter subgroup corresponding to a root $\alpha \in \Phi$; see [3] for details.) The goal of this paper 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 $\Phi$ 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 paper, 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 $\Gamma$, we understand the following question:
(CSP) Does every normal subgroup $\Delta \subset \Gamma$ of finite index contain the congruence subgroup $\Gamma(a)$ for some ideal $a \subset R$ of finite index?

An affirmative answer would give us information about the profinite completion $\hat{\Gamma}$, which is precisely what is needed for the analysis of representations of $\Gamma$, as well as other issues (cf. [2], [9], [15]). However, even when $\Gamma$ 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. Unfortunately, the size measures the extent of deviation from the affirmative answer. Clearly, $\pi_0(\Gamma)$ 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 $\pi_0(\Gamma)$ is nontrivial, and the focus of this paper is on a different property, viz. the centrality of $\pi_0(\Gamma)$ (which means that $\pi_0(\Gamma)$ is contained in the center of $\hat{\Gamma}$). We note that in some cases centrality is almost as good as triviality (cf. [9], [15]), and in the arithmetic case it actually implies the finiteness of $\pi_0(\Gamma)$.

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

Our main result concerns the congruence kernel of the elementary group $\Gamma = E(R)$. We note that the congruence topology on $\Gamma$ is induced by that on $G(R)$, i.e. is defined by the intersections $\Gamma \cap G(R,a)$, where $a$ runs over all ideals $a \subset R$ of finite index. On the other hand, the profinite topology on $\Gamma$ 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 $\Phi$ of rank $> 1$. Furthermore, let $R$ be a noetherian commutative ring such that $2 \in R^\times$ if $\Phi$ 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.
using \(K\)-theoretic methods (note that \(SL_n(R) = E(R)\) for \(R = \mathbb{Z}[x_1, \ldots, x_k]\); see [19]). 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 notation. 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 \(\Phi\) of rank > 1. Furthermore, if \(R\) is a commutative ring, then for a subgroup \(\Gamma \subset G(R)\), we let \(\hat{\Gamma}\) denote the profinite and congruence completions of \(\Gamma\), respectively.

2. Structure of \(\widehat{G(R)}\)

Let \(\mathcal{I}\) be the set of all ideals \(a \subset R\) 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 2.3) that \(\widehat{G(R)}\) can be identified with the closure of the image of \(G(R)\) in \(G(\hat{R})\), where

\[
\hat{R} = \lim_{\leftarrow a \in \mathcal{I}} R/a
\]

is the profinite completion of \(R\). Note that we do not require that \(R\) satisfy

\[
\bigcap_{a \in \mathcal{I}} a = \{0\}.
\]

Thus the natural maps \(R \to \hat{R}\) and \(G(R) \to G(\hat{R})\) need not be injective. However, we observe that there are many rings, for example all finitely generated rings over \(\mathbb{Z}\), for which (11) does hold. The proof of the Main Theorem relies on the fact that \(G(\hat{R})\) has the bounded generation property with respect to the set \(\hat{S} = \{e_\alpha(t) | t \in \hat{R}, \alpha \in \Phi\}\) of elementaries, which we will establish at the end of this section (cf. Corollary 2.4). We begin, however, by describing the structure of \(\hat{R}\) itself. For each \(m \in \mathcal{M}\), we let

\[
R_m = \lim_{\leftarrow n} R/m^n
\]

denote the \(m\)-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

\[
\hat{R} = \prod_{m \in \mathcal{M}} R_m.
\]

(2) Each \(R_m\) is a complete local ring.

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

\[
\rho_{m,n}: \hat{R} \to R/m^n.
\]

For a fixed \(m\), the inverse limit of the \(\rho_{m,n}\) over all \(n \geq 1\) yields a continuous ring homomorphism \(\rho_m: \hat{R} \to R_m\). Taking the direct product of the \(\rho_m\) over all \(m \in \mathcal{M}\),
we obtain a continuous ring homomorphism
\[ \rho: \hat{R} \to \prod_{m \in \mathcal{M}} R_m =: \hat{R}. \]

We claim that \( \rho \) is the required isomorphism.

Note that ideals of the form \( a = m_1^{\alpha_1} R_{m_1} \times \cdots \times m_n^{\alpha_n} R_{m_n} \times \prod_{m \neq m_i} R_m \), where \( \{m_1, \ldots, m_n\} \subset \mathcal{M} \) is a finite subset and \( \alpha_i \geq 1 \), form a base of neighborhoods of zero in \( \hat{R} \), with
\[ \overline{R/a} = R/m_1^{\alpha_1} \times \cdots \times R/m_n^{\alpha_n} \]
(cf. [1], Proposition 10.15). Set \( a = m_1^{\alpha_1} \cdots m_n^{\alpha_n} \). By the Chinese Remainder Theorem,
\[ R/a \simeq R/m_1^{\alpha_1} \times \cdots \times R/m_n^{\alpha_n}, \]
which implies that the composite map
\[ \hat{R} \to R \to \overline{R/a} \]
is surjective. Since this is true for all \( \overline{a} \), we conclude that the image of \( \rho \) is dense.

On the other hand, \( \hat{R} \) is compact, so the image is closed, and we obtain that \( \rho \) is in fact surjective.

To prove the injectivity of \( \rho \), we observe that for any \( a \in \mathcal{I} \), the quotient \( R/a \), being a finite, hence artinian ring, is a product of the finite local ring \( R_1, \ldots, R_r \) ([1], Theorem 8.7). Furthermore, for each maximal ideal \( n_i \subset R_i \), there exists \( \beta_i \geq 1 \) such that \( n_i^{\beta_i} = 0 \) (cf. [1], Proposition 8.4). Letting \( m_i \) denote the pullback of \( n_i \) in \( R \), we obtain that \( a \) contains \( b := m_1^{\beta_1} \cdots m_r^{\beta_r} \in \mathcal{I} \). It follows that any nonzero \( x \in \hat{R} \) will have a nonzero projection to some \( R/b = R/m_1^{\beta_1} \times \cdots \times R/m_r^{\beta_r} \), and hence to some \( R_{m_i} \), as required.

(2) It is well-known that \( R_m \) is both complete and local (cf. [1], Propositions 10.5 and 10.16).

Remark (added in proof). M. Kassabov has pointed out to us that the profinite completion \( \hat{R} \) of any (not necessarily noetherian) commutative ring \( R \) has a structure similar to that described in Lemma 2.1. More precisely,
\[ \hat{R} = \prod_{m \in \mathcal{M}} R_m, \]
where
\[ R_m = \lim_{\leftarrow} R/a, \]
with the limit taken over all \( a \in \mathcal{I} \) that contain a suitable power \( m^n \) of \( m \) (this requires only minor modifications in the proof of Lemma 2.1). Ultimately, one can see that the noetherian assumption in the Main Theorem can actually be omitted. We thank Kassabov for this observation.

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

**Proposition 2.2.** There exists an integer \( N = N(\Phi) \), depending only on the root system \( \Phi \), such that for any commutative local ring \( R \), any element of \( G(R) \) is a product of the \( \leq N \) elements of \( S = \{ e_\alpha(r) \mid r \in R, \ \alpha \in \Phi \} \).
Proof. Fix a system of simple roots $\Pi \subseteq \Phi$, and let $\Phi^+$ and $\Phi^-$ be the corresponding sets of positive and negative roots. Let $T \subseteq G$ be the canonical maximal torus, and let $U^+$ and $U^-$ be the canonical unipotent $\mathbb{Z}$-subschemas corresponding to $\Phi^+$ and $\Phi^-$. It is well-known (see, for example, [3], Lemma 4.5) that the product map $\mu: U^- \times T \times U^+ \rightarrow G$ is an isomorphism onto a principal open subscheme $\Omega \subseteq G$ defined by some $d \in \mathbb{Z}[G]$. We have decompositions

$$U^\pm = \prod_{\alpha \in \Phi^\pm} U_\alpha$$

and $T = \prod_{\alpha \in \Pi} T_\alpha$,

where $T_\alpha$ is the maximal diagonal torus in $G_\alpha = \langle U_\alpha, U_{-\alpha} \rangle = SL_2$. 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 field $R$.

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 $R$. Indeed, let $m \subseteq R$ be the maximal ideal, and let $k = R/m$ be the residue field. As $G(k)$ is generated by elementaries, the canonical homomorphism $\omega: G(R) \rightarrow G(k)$ is surjective. Given $g \in G(R)$, there exists $h \in G(R)$ 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 $d(t) \neq 0(mod m)$. Since $R$ is local, this means that $d(t) \in R^\times$, and therefore $t \in \Omega(R)$. Thus, $t$ is a product of $\leq N_1$ elementaries, and the required fact follows.

Next, we have the following lemma.

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

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

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 $t_\alpha \in \mathcal{R}$.\qed

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 $G(\hat{R})$ is a product of $\leq M$ elementaries from the set $\hat{S} = \{e_\alpha(t) \mid t \in R, \alpha \in \Phi\}$.

As we noted earlier, one can identify the congruence completion $\overline{G(R)}$ with the closure of the image of $G(R)$ in $G(\hat{R})$. The following proposition gives more precise information.
Proposition 2.5. Let $R$ be a noetherian ring. Then $E(R) = G(R)$ can be naturally identified with $G(R)$. Furthermore, there exists an integer $M > 0$ such that any element of $E(R) = G(R)$ is a product of $\leq M$ elements of the set $\mathcal{S} := \{e_\alpha(r) \mid \alpha \in \Phi, r \in R\}$ (closure in the congruence topology).

Proof. For any $a \in \mathcal{I}$, there exists a natural injective homomorphism

$$\omega_a : G(R)/G(R, a) \to G(R/a),$$

where as before, $G(R, a)$ is the principal congruence subgroup of level $a$. Taking the inverse limit over all $a \in \mathcal{I}$, we obtain a continuous injective homomorphism

$$\omega : G(R) \to \hat{G}.$$

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

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

where $\hat{r}$ is the image of $r$ in $\hat{R}$. It follows that $\omega$ maps $\hat{S}$ onto $\hat{S} = \{e_\alpha(t) \mid \alpha \in \Phi, t \in \hat{R}\}$. Since by Corollary 2.4, $\hat{S}$ generates $G(\hat{R})$, we obtain that $\omega(E(R)) = G(\hat{R})$, and consequently $\omega$ identifies $E(R) = G(R)$ with $G(\hat{R})$. Furthermore, if $M$ is the same integer as in Corollary 2.4 then since every element of $G(\hat{R})$ is a product of $\leq M$ elements of $\hat{S}$, 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 $X^{(n)} = X \cdots X$ (an $n$-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 $G(\hat{R})$ by $\hat{S}$, or that of $G(\hat{R})$ by $\hat{S}$, automatically yields bounded generation.

We would like to point out that the fact that $G(R) = E(R)$ is not used in the proof of the Main Theorem; all we need is that $E(R)$ is boundedly generated by $\mathcal{S}$. 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 $E(\hat{R})$ by $\hat{S} = \{e_\alpha(t) \mid \alpha \in \Phi, t \in \hat{R}\}$ (indeed, this will show that $E(\hat{R})$ is a continuous image of $\hat{R}^N$ for some $N > 0$, hence compact, implying that the map $\omega$ from the proof of Proposition 2.5 identifies $E(\hat{R})$ with $E(\hat{R})$, and also $\mathcal{S}$ with $\hat{S}$). In turn, by the same argument as above, we see that to prove bounded generation of $E(\hat{R})$, it suffices to show that there exists an integer $N > 0$ depending only on $\Phi$ such that
for any local ring $R$, any element of $E(R)$ is a product of $\leq N$ elementary. We will show that in fact
\[(2) \quad E(R) = (U^+(R)U^-(R))^4,\]
so one can take $N = 4 \cdot |\Phi|$. Let us now prove (2) by induction on the rank $\ell$ of $\Phi$. 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 (2) is valid for every reduced irreducible root system of rank $\leq \ell - 1$, with $\ell \geq 2$, and prove it for a root system $\Phi$ of rank $\ell$. 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 [10] in §4), to prove (2) 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 $\Phi$. Let $\Phi_0$ (resp., $\Phi_1$) be the set of roots in $\Phi$ that do not contain (resp., contain) $\alpha$, and let $\Phi_{1}^{\pm} = \Phi_0 \cap \Phi^\pm$. Then $\Phi_0$ is an irreducible root system having $\Delta_0 = \Delta \setminus \{\alpha\}$ as a system of simple roots; in particular, $\Phi_0$ 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 notation. Let $U_{0}^{\pm}(R)$ be the subgroup generated by $e_{\alpha}(r)$ for $\alpha \in \Phi_{1}^{\pm}$ (resp., $\alpha \in \Phi_{1}^{-}$) and $r \in R$. Then $U_{0}^{\pm}(R) = U_{1}^{\pm}(R)U_{1}^{\pm}(R)$, and according to [13], Lemma 17,
\[U_{0}^{+}(R)U_{1}^{+}(R) = U_{1}^{+}(R)U_{0}^{+}(R).\]
Therefore,
\[X = (U^+_0(R)U^+_1(R)U^-_0(R)U^-_1(R))^4 = (U^+_0(R)U^-_0(R))^4(U^+_1(R)U^-_1(R))^4 = E_0(R)(U^+_1(R)U^-_1(R))^4.\]
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 $\Phi$ be a reduced irreducible root system of rank $\geq 2$, $G$ 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 $\Phi$ is not of type $C_n$ ($n \geq 2$) or $G_2$, then there exists an ideal $a \subset R$ of finite index such that
\[(3) \quad e_{\alpha}(a) \subset N \cap U_{\alpha}(R)\]
for all $\alpha \in \Phi$, where $e_{\alpha}(a) = \{e_{\alpha}(t) \mid t \in a\}$. The same conclusion holds for $\Phi$ 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 $\alpha \in \Phi$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Proof. We begin with two preliminary remarks. First, for any root $\alpha \in \Phi$, 
$$a(\alpha) := \{ t \in R \mid e_\alpha(t) \in N \}$$
is obviously a finite index subgroup of the additive group of $R$. What one needs to show is that either $a(\alpha)$ 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 $\tilde{\omega}$ of the Weyl group $W(\Phi)$ such that $\alpha_2 = \tilde{\omega} \cdot \alpha_1$. 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 
$$a(\alpha_1) = a(\alpha_2).$$
Thus, it is enough to find a finite index ideal $a \subset R$ such that (3) holds for a single root of each length.

Let us now prove our claim for $\Phi$ of type $A_2$ using explicit computations with commutator relations. We will use the standard realization of $\Phi$, 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 $a(\alpha_1)$ is an ideal of $R$, and then it will follow from our previous remarks that $a := a(\alpha_1)$ is as required. Let $r \in a(\alpha_1)$ and $s \in R$. Since $N \triangleleft E(R)$, the (well-known) relation 
$$[e_{12}(r), e_{23}(s)] = e_{13}(rs),$$
where $[g, h] = ghg^{-1}h^{-1}$, shows that $rs \in a(\alpha_2)$ for $\alpha_2 = \varepsilon_1 - \varepsilon_2$. But then (4) yields $rs \in a(\alpha_1)$, completing the argument.

Now let $\Phi$ be any root system of rank $\geq 2$ in which all roots have the same length. Then clearly $\Phi$ contains a subsystem $\Phi_0$ of type $A_2$, so our previous considerations show that there exists a finite index ideal $a \subset R$ with the property that $a \subset a(\alpha)$ 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 $\Phi$ 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 $\Phi$ is of type $F_4$ as well. We will use the standard realization of $\Phi$ 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 $\Phi$ contains a subsystem $\Phi_0$ of type $A_{n-1}$, all of whose roots are long roots in $\Phi$. Arguing as above, we see that there exists an ideal $a \subset R$ of finite index such that (3) 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:

$$[e_{\varepsilon_1+\varepsilon_2}(r), e_{-\varepsilon_2}(s)] = e_{\varepsilon_1}(rs)e_{\varepsilon_1-\varepsilon_2}(-rs^2)$$
for any $r, s \in R$. Now, if $r \in a$, then $e_{\varepsilon_1+\varepsilon_2}(r), e_{\varepsilon_1-\varepsilon_2}(-r) \in N$. So, setting $s = 1$ in (5) and noting that $[e_{\varepsilon_1+\varepsilon_2}(r), e_{-\varepsilon_2}(1)] \in N$ as $N \triangleleft E(R)$, we obtain that $e_{\varepsilon_1}(r) \in N$. Thus, (3) holds for $\alpha = \varepsilon_1$, and therefore for all short roots.

Next, we proceed to the case of $\Phi$ of type $B_2 = C_2$, where we assume that $2 \in R^\times$. We will use the same realization of $\Phi$ as in the previous paragraph (for
n = 2). Set $a = a(ε_1)$. Then for $r \in a$, $s \in R$, one can check by direct computation that

$$[e_{ε_1}(r), e_{ε_2}(s/4)] = e_{ε_1+ε_2}(rs/2) \in N.$$  

Next, using (5), in conjunction with the fact that $e_{ε_1}(u)$ and $e_{ε_1-ε_2}(v)$ commute for all $u, v \in R$, we obtain

$$[e_{ε_1+ε_2}(rs/2), e_{−ε_2}(1)] [e_{ε_1+ε_2}(rs/2), e_{−ε_2}(−1)] = e_{ε_1}(rs) \in N,$$

i.e. $rs \in a$, which shows that $a$ is an ideal. Furthermore, from (6), we see that for any $r \in a$, we have

$$[e_{ε_1}(r), e_{ε_2}(1/2)] = e_{ε_1+ε_2}(r) \in N.$$  

Thus, $e_{ε_1+ε_2}(a) \subset N$, and therefore (3) holds for all $α \in Φ$. As above, the truth of our claim for $Φ$ of type $C_2$ implies its truth for $Φ$ of type $C_n$ for any $n ≥ 2$.

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 short roots of $Φ$ are

$$±k, ±(3c + k), ±(3c + 2k)$$

and the short roots are

$$±c, ±(c + k), ±(2c + k).$$

Set $a = a(k)$. Since the long roots of $Φ$ form a subsystem of type $A_2$, it follows from the above analysis that $a$ is a finite index ideal in $R$ and that (3) holds for all long roots. To show that (3) 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 [1 Theorem 1.1]:

$$[e_k(s), e_c(t)] = e_{c+k}(ε_1st)e_{2c+k}(ε_2st^2)e_{3c+k}(ε_3st^3)e_{3c+2k}(ε_4s^2t^3),$$

$$[e_{c+k}(s), e_{2c+k}(t)] = e_{3c+2k}(3ε_5st),$$

where $ε_i = ±1$. Using (7), we obtain

$$[e_k(s), e_c(1)] [e_k(s), e_c(−1)] = e_{c+k}(ε_1s)e_{2c+k}(ε_2s)e_{3c+k}(ε_3s)e_{3c+2k}(ε_4s^2)
\times e_{c+k}(−ε_1s)e_{2c+k}(ε_2s)e_{3c+k}(−ε_3s)e_{3c+2k}(−ε_4s^2).$$

Since the terms $e_{3c+k}(−ε_3s)$ and $e_{3c+2k}(−ε_4s^2)$ commute with all other terms, the last expression reduces to

$$e_{c+k}(ε_1s)e_{2c+k}(ε_2s)e_{c+k}(−ε_1s)e_{2c+k}(ε_2s),$$

which, using (8), can be written in the form

$$e_{3c+2k}(3ε_5ε_1ε_2s^2)e_{2c+k}(2ε_2s).$$

Hence if $s \in a$, we obtain that

$$[e_k(s/2), e_c(1)] [e_k(s/2), e_c(−1)] = e_{3c+2k}(3ε_5ε_1ε_2s^2/4)e_{2c+k}(ε_2s) \in N.$$  

But $e_{3c+2k}(3ε_5ε_1ε_2s^2/4) \in N$, from which it follows that $e_{2c+k}(a) \subset N$. 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 additional assumptions.

4. Proof of the Main Theorem

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

\[
\hat{e}_\alpha = (\pi|_{U_\alpha})^{-1} \circ \pi_\alpha.
\]

Then \( \hat{e}_\alpha: \hat{R} \to U_\alpha \) is an isomorphism of topological groups, and in particular, we have

\[
\hat{e}_\alpha(r + s) = \hat{e}_\alpha(r)\hat{e}_\alpha(s)
\]

for all \( r, s \in \hat{R} \) and any \( \alpha \in \Phi \).

Before establishing some further properties of the \( \hat{e}_\alpha \), 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

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

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 \( N_{i,j}^{s,t} \) are integers depending only on \( \alpha, \beta \in \Phi \) and the order of the factors in \( \text{[9]} \), but not on \( s, t \in S \). Furthermore, recall that the abstract group \( \hat{G}(S) \) with generators \( \hat{x}_\alpha(s) \) for all \( s \in S \) and \( \alpha \in \Phi \) subject to the relations

\[
\begin{align*}
\text{(R1)} \quad &\hat{x}_\alpha(s)\hat{x}_\alpha(t) = \hat{x}_\alpha(s + t); \\
\text{(R2)} \quad &[\hat{x}_\alpha(s), \hat{x}_\beta(t)] = \prod \hat{x}_{i\alpha + j\beta}(N_{i,j}^{s,t} s^it^j), \text{ where } N_{i,j}^{s,t} \text{ are the same integers, and} \\
&\text{the roots are listed in the same order, as in } \text{[9]},
\end{align*}
\]

is called the Steinberg group. It follows from \( \text{[9]} \) that there exists a canonical homomorphism \( \hat{G}(S) \to G(S) \), defined by \( \hat{x}_\alpha(s) \mapsto e_\alpha(s) \), whose kernel is denoted by \( K_2(\Phi, S) \).

Lemma 4.1. (1) For any \( \alpha, \beta \in \Phi, \beta \neq -\alpha \), and \( s, t \in \hat{R} \), we have \([\hat{e}_\alpha(s), \hat{e}_\beta(t)] = \prod \hat{e}_{i\alpha + j\beta}(N_{i,j}^{s,t} s^it^j)\). Let \( \hat{R} = \prod_{\mathfrak{m} \in \mathcal{M}} R_{\mathfrak{m}} \) be the decomposition from Lemma \( 2.1 \) and for \( \mathfrak{m} \in \mathcal{M} \), let \( \hat{\Gamma}_\mathfrak{m} \) (resp., \( \hat{\Gamma}_m \)) be the subgroup of \( \hat{\Gamma} \) (algebraically) generated by \( \hat{e}_\alpha(r) \) for all \( r \in R_{\mathfrak{m}} \) (resp., \( r \in R_m^\prime := \prod_{\mathfrak{n} \neq \mathfrak{m}} R_{\mathfrak{n}} \)) and all \( \alpha \in \Phi \). Then
Lemma 4.2. The kernel \( R \) which is not orthogonal to \( \Pi \), \( \delta \) with respect to the same length as \( m \). Following this, fix a system of simple roots \( \Pi \) of \( \Phi \) of simple roots (this follows, for example, from the fact that the Weyl group \( W \) of \( \Phi \) 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). So, to prove (11), it is enough to show that for any \( \alpha \in \Phi \), one can find a system of simple roots \( \Pi \subset \Phi \) such that \( \alpha \notin \Pi \cup (-\Pi) \). For this, fix a system of simple roots \( \Pi_0 \subset \Phi \), and let \( \gamma \in \Pi_0 \) be a root having the same length as \( \alpha \). Since \( \Phi \) is irreducible of rank \( \geq 2 \), we can pick \( \delta \in \Pi_0 \setminus \{ \gamma \} \) which is not orthogonal to \( \gamma \). Then \( \alpha_0 := w_\delta(\gamma) \), where \( w_\delta \) is the reflection with respect to \( \delta \), is a positive nonsimple root with respect to the ordering defined by \( \Pi_0 \), having the same length as \( \alpha \). There exists \( w \in W \) such that \( \alpha = w(\alpha_0) \), and then the system \( \Pi = w(\Pi_0) \) is as required.

Using the homomorphism \( \theta_m \) constructed in part (2), we conclude from (10) that \( \hat{G}(\hat{R}_m) \) is generated by \( \hat{e}_\gamma(r) \) for \( r \in \hat{R}_m \), \( \gamma \in \Phi \setminus \{ \alpha \} \). So, since we already know that \( \hat{e}_{-\alpha}(s) \), with \( s \in \hat{R}_m' \), commutes with all of these elements, it also commutes with \( \hat{e}_\alpha(r) \), yielding our claim. \( \square \)

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 \( \ker(\pi|_{\hat{G}_m}) \) of the restriction \( \pi|_{\hat{G}_m} \) lies in the center of \( \hat{G}_m \), for any \( m \in \mathcal{M} \).

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

\[
\hat{G}(\hat{R}_m) \xrightarrow{\delta_m} \hat{G}_m \xrightarrow{\pi|_{\hat{G}_m}} E(\hat{R}_m).
\]
Since \( \theta_m \) is surjective, we conclude that
\[
\ker(\pi|_{\hat{\Gamma}_m}) = \theta_m(K_2(\Phi, R_m))
\]
is central in \( \hat{\Gamma}_m \).

Now fix \( m \in \mathcal{M} \) and let \( \Delta_m = \hat{\Gamma}_m \hat{\Gamma}'_m \) be the subgroup of \( \hat{\Gamma} \) (algebraically) generated by \( \hat{\Gamma}_m \) and \( \hat{\Gamma}'_m \). Let \( c \in C(\Gamma) \cap \Delta_m \), and write \( c = c_1c_2 \), with \( c_1 \in \hat{\Gamma}_m \), \( c_2 \in \hat{\Gamma}'_m \). We have \( \hat{\Gamma} = \Gamma_m \times \hat{\Gamma}'_m \), where \( \Gamma_m = E(R_m) \) and \( \hat{\Gamma}'_m = E(R'_m) \). Since \( \pi(c_1) \in \Gamma_m \), \( \pi(c_2) \in \Gamma'_m \), we conclude from
\[
\pi(c) = e = \pi(c_1)\pi(c_2)
\]
that \( \pi(c_1) = e \), i.e. \( c_1 \in \ker(\pi|_{\Gamma_m}) \). Then by Lemma 4.2, \( \hat{\Gamma}_m \) centralizes \( c_1 \). On the other hand, \( \hat{\Gamma}_m \) centralizes \( c_2 \in \hat{\Gamma}'_m \) by Lemma 4.1(3). So, \( \hat{\Gamma}_m \) centralizes \( c \). Thus, we have shown that \( C \cap \Delta_m \) is centralized by \( \hat{\Gamma}_m \). To prove that \( \hat{\Gamma}_m \) actually centralizes all of \( C \), we need the following.

**Lemma 4.3.** Let \( \varphi: \mathcal{G}_1 \rightarrow \mathcal{G}_2 \) 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 \( \Theta \) 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,
\[
\mathcal{F} \subset \overline{\Theta \cap U} \subset \Theta \cap \Omega \mathcal{F}.
\]
But \( \Theta \cap \Omega \mathcal{F} = \Omega(\Theta \cap \mathcal{F}) \), and since \( \Omega \) is compact, the product \( \Omega(\Theta \cap \mathcal{F}) \) is closed. So
\[
\mathcal{F} \subset \overline{\Theta \cap \Omega \mathcal{F}} \subset \Omega(\Theta \cap \mathcal{F}).
\]
Since \( \mathcal{F} \) is closed, we have \( \overline{\Theta \cap \mathcal{F}} \subset \mathcal{F} \), so
\[
\mathcal{F} = (\Omega \cap \mathcal{F})(\Theta \cap \mathcal{F}) \subset (\Theta \cap \mathcal{F})(\Theta \cap \mathcal{F}) = \Theta \cap \mathcal{F},
\]
as required. \( \square \)

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

**Lemma 4.4.** The subgroup \( \Delta \subset \hat{\Gamma} \) (algebraically) generated by the \( \hat{\Gamma}_m \) for all \( m \in \mathcal{M} \) is dense. Consequently, for any \( m \in \mathcal{M} \), the subgroup \( \Delta_m = \hat{\Gamma}_m \hat{\Gamma}'_m \subset \hat{\Gamma} \) is dense.

**Proof.** Let
\[
R_0 := \sum_{m \in \mathcal{M}} R_m \subset \hat{R} = \prod_{m \in \mathcal{M}} R_m.
\]
Clearly \( R_0 \) is a dense subring of \( \hat{R} \). On the other hand, \( \Delta \) obviously contains \( \hat{e}_\alpha(R_0) \) for any \( \alpha \in \Phi \). So, the closure \( \overline{\Delta} \) contains \( \hat{e}_\alpha(R) \) for all \( \alpha \in \Phi \), and therefore coincides with \( \hat{\Gamma} \), yielding our first assertion. Furthermore, for any \( m \in \mathcal{M} \), the subgroup \( \Delta_m \) contains \( \Gamma_n \) for all \( n \in \mathcal{M} \), so our second assertion follows. \( \square \)
Conclusion of the proof of the Main Theorem. Fix $m \in M$. We have already seen that $\hat{\Gamma}_m$ centralizes $C \cap \Delta_m$. We claim that $C \cap \Delta_m$ is dense in $C$, and hence $\hat{\Gamma}_m$ centralizes $C$. Indeed, by Lemma 4.3 $\Delta_m$ is dense in $\hat{\Gamma}$. 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

$$\hat{R}^L \to \Gamma, \quad (r_1, \ldots, r_L) \mapsto \prod_{i=1}^L \xi_{\alpha_i}(r_i)$$

is surjective. Then

$$\Omega := \hat{\xi}_{\alpha_1}(\hat{R}) \cdots \hat{\xi}_{\alpha_L}(\hat{R}) = (\hat{\xi}_{\alpha_1}(R_m) \cdots \hat{\xi}_{\alpha_L}(R_m)) (\hat{\xi}_{\alpha_1}(R'_m) \cdots \hat{\xi}_{\alpha_L}(R'_m))$$

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

We now see that $\hat{\Gamma}_m$ centralizes $C$ for all $m \in M$. Since the subgroup $\Delta \subset \hat{\Gamma}$ generated by the $\hat{\Gamma}_m$ is dense in $\hat{\Gamma}$ by Lemma 4.3 we obtain that $\hat{\Gamma}$ 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 let $S$ 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 $\hat{G}(K)$ of the group $G(K)$ of $K$-rational points can be identified with the group of $S$-adeles $G(A_S)$, and in particular the group $G(K_v)$, for $v \notin S$, can be viewed as a subgroup of $\hat{G}(K)$. 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 $\hat{G}(K)$ such that

1. $\pi(H_v) = G(K_v)$ for all $v \notin S$, where $\pi: \hat{G}(K) \to \hat{G}(K)$ is the canonical projection;
2. $H_v$ 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 $\hat{G}(K)$,

then the congruence kernel $CS^S(G) := \ker \pi$ 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 $\hat{\Gamma}_m$ 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 $E(\hat{R}) = G(\hat{R})$) 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 $\Gamma \hookrightarrow G(R)$:

$$
\begin{array}{c}
1 \\ \downarrow \alpha \downarrow \downarrow \downarrow \gamma \\
C(\Gamma) \longrightarrow \hat{\Gamma} \longrightarrow \hat{G}(R) \longrightarrow \hat{G}(R) \longrightarrow 1 \\
1 \\ \downarrow \beta \\
C(G(R)) \longrightarrow \hat{G}(R) \longrightarrow \hat{G}(R) \longrightarrow 1
\end{array}
$$

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

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

The exact relationship between $C(G(R))$ and $C(G(R)) \cap \hat{\Gamma}$ (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 $E(R) = G(R)$, 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 $\Gamma$ is induced by the profinite topology of $G(R)$, which implies that $\beta$ 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. The authors would like to thank Gopal Prasad for carefully reading an earlier version of this paper and for making useful suggestions. Thanks are also due to the referee for useful comments.

**References**

15. D. Shenfeld, On semisimple representations of $SL_n(Z[x_1,\ldots,x_k])$, Hebrew University Master’s Thesis.
18. R. Steinberg, Lectures on Chevalley groups, mimeographed lectures notes, Yale University Math. Dept., New Haven, CT, 1968. MR0405357 (53:6215)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE, VIRGINIA 22904
E-mail address: asr3x@virginia.edu

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, NEW HAVEN, CONNECTICUT 06502
E-mail address: igor.rapinchuk@yale.edu