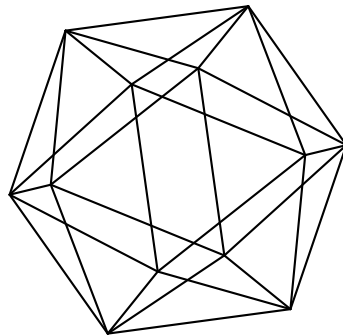


Max-Planck-Institut für Mathematik Bonn

Centrality

by

T. N. Venkataramana



Max-Planck-Institut für Mathematik
Preprint Series 2021 (16)

Date of submission: May 4, 2021

Centrality

by

T. N. Venkataramana

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400 005
India

CENTRALITY

T. N. VENKATARAMANA

ABSTRACT. We give a simple proof of the centrality of the congruence subgroup kernel in the higher rank isotropic case.

1. INTRODUCTION

In this paper, we give a simple proof of the well known centrality of the congruence subgroup kernel in the “higher rank” isotropic case ([R1], [R2]). That is, we prove the following (we refer to Section 1 for definitions of the terms involved).

Theorem 1. *The congruence subgroup kernel C associated to a connected \mathbb{Q} -simple simply connected linear algebraic group G defined over \mathbb{Q} with $\mathbb{Q} - \text{rank}(G) \geq 1$ and $\mathbb{R} - \text{rank}(G) \geq 2$, is **central** in the arithmetic completion \widehat{G} of $G(\mathbb{Q})$.*

The newest part of the proof is in the case when $\mathbb{Q} - \text{rank}(G) = 1$ and the group of integer points $L(\mathbb{Z})$ of the Levi of a minimal parabolic \mathbb{Q} -subgroup P is a virtually abelian group. To handle this case, we make use of the following result, which is quite general and may be of independent interest. The proof uses Dirichlet’s theorem on primes in arithmetic progressions.

Theorem 2. *Let $\Delta \subset GL_n(\mathbb{Z})$ be a subgroup. There exists an integer $g(n)$ dependent only on n such that for any two co-prime integers a, b and any fixed integer N the group $\Delta_{a,b}$ generated by the congruence subgroups $\{\Delta((a+bx)^N) := \Delta \cap GL_n((a+bx)^N\mathbb{Z}) : x \in \mathbb{Z}\}$, (is normal and) the exponent of the quotient group $\Delta/\Delta_{a,b}$ is bounded by $g(n)$ (i.e. depends only on n and not on the integers a, b , and N).*

Theorem 2 is proved in section 4. Using this, Theorem 1 is proved in section 5 in the case $\mathbb{Q} - \text{rank}(G) = 1$ and the group $L(\mathbb{Z})$ is infinite and virtually abelian. The case when $L(\mathbb{Z})$ is not virtually abelian is proved in section 6. The other sections establish some preliminaries.

2020 *Mathematics Subject Classification.* Primary 20H05 Secondary 22E40
T. N. Venkataramana, School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay - 400 005, INDIA. venky@math.tifr.res.in.

Remark. In the generality stated here, Theorem 1 is due to Raghunathan; his proof was quite different in the two cases (1) \mathbb{Q} -rank(G) ≥ 2 [R1], and (2) \mathbb{Q} -rank(G) = 1, \mathbb{R} -rank(G) ≥ 2 [R2]. For earlier work (especially in the case SL_n and Sp_{2n} [BMS]) we refer to the bibliography in [R1]. [At the time that [R1] and [R2] were written, the Kneser-Tits problem (we refer to [Gille] for the statement over number fields and for references to previous work) had not been completely resolved and consequently the formulation of Raghunathan was slightly different]. In the present paper we give a different proof especially in the case when \mathbb{Q} -rank(G) = 1 (and the group of integer points of the Levi subgroup of a minimal parabolic \mathbb{Q} -subgroup is virtually abelian).

Remark. To prove the centrality in the \mathbb{Q} -rank one case (with integral points of the Levi being virtually abelian), Raghunathan uses the centrality (proved by Serre [Ser]) when $G = R_{K/\mathbb{Q}}(SL_2)$ is the Weil restriction of scalars from K to \mathbb{Q} of SL_2 , where K a number field having infinitely many units. The proof of centrality in [Ser] makes crucial use of the Artin reciprocity law. In contrast, we use only Dirichlet's theorem on infinitude of primes in arithmetic progressions. Thus the proof is new even in the case considered by Serre (we note that Prasad and Rapinchuk [Pr-Ra2] also proved centrality; the present paper has considerable overlap with [Pr-Ra2] and [Pr-Ra2] contains much more than what is proved in the present paper. However, the method of proof in our paper is quite different and it seems worthwhile to record the proof here).

Remark. Raghunathan first proved centrality for the group $SU(2, 1)$: suppose L/K is a quadratic extension of number fields with $K \neq \mathbb{Q}$, h is an isotropic non-degenerate form in three variables defined on L^3 and hermitian with respect to L/K , G is the unit group of h i.e. $G = R_{K/\mathbb{Q}}(SU(2, 1))$ where $R_{K/\mathbb{Q}}$ is the Weil restriction of scalars. The proof of this also makes use of Artin Reciprocity. In the present paper, we completely avoid the use of $SU(2, 1)$. This is especially important since, in [R2], a deep theorem on the embedding of suitable SL_2 and $SU(2, 1)$ is used (which in turn is based on the classification of rank one groups over number fields) to obtain the centrality in the general case from these two cases. In contrast, we (by appealing to a theorem of Jacobson and Morozov) use only a suitably embedded SL_2 (and Dirichlet's theorem on primes in arithmetic progressions) to get the general case directly. In particular, we get another proof for $SU(2, 1)$ as well.

Remark. Most importantly, Raghunathan [R1] proved that once the congruence subgroup kernel C is central for any G (no assumptions on

\mathbb{Q} -rank), then C is *finite*; a much simpler proof of the finiteness was later given by Gopal Prasad in [P]. Moreover, once C is central, C can be computed: it is a precisely determined subgroup of the group of roots of unity in a number field K (K is such that $G = R_{K/\mathbb{Q}}(\mathcal{G})$ is the Weil restriction of scalars of an absolutely almost simple simply connected group \mathcal{G} defined over K). Important progress on the computation of (the central) C was made in [Pr-R1], [Pr-R2], and its complete determination was done by Prasad and Rapinchuk in [Pr-Ra].

Our paper does not deal with this question at all, and is concerned only with the centrality of the congruence subgroup kernel in the cases considered in the theorem.

Remark. The proof here works only for arithmetic groups in characteristic zero but the proof of centrality in [R1],[R2] works for all global fields and for S -arithmetic groups; it seems possible to adapt the present proof to the S -arithmetic case, but it appears to be rather long.

Acknowledgments: Most of the mathematics I have learnt at TIFR has been from Raghunathan, Prasad, Nori and my fellow student Sury. I am especially grateful to Gopal for suggesting many topics to work on, patiently answering my questions and going through my early papers (and righting so many wrongs in those papers). It is a pleasure to dedicate this paper to him on his 75th birthday.

This paper owes a great deal to the methods of [R1], [R2] and I am grateful to Raghunathan for explaining his proof in detail.

I am grateful to the organisers for their invitation to contribute to this volume honouring Gopal.

A sizeable part of the work was done during the author's visit to Max Planck Institut, Bonn, Germany during 2019-2020. I thank MPIM for hospitality and support. The support of JC Bose fellowship for the period 2020-2025 is gratefully acknowledged.

2. GENERALITIES

2.1. The Congruence Subgroup Kernel. The following definitions and observations are well known and we recall them without reference.

Let G be a linear algebraic group defined over \mathbb{Q} . Fix an embedding $G \subset SL_n$ defined over \mathbb{Q} and call a subgroup of finite index in $G(\mathbb{Z}) = G \cap SL_n(\mathbb{Z})$ an *arithmetic subgroup* of $G(\mathbb{Q})$. We assume that $G(\mathbb{Z})$ is Zariski dense in G . Denote by $SL_n(m\mathbb{Z})$ the kernel to the natural map $SL_n(\mathbb{Z}) \rightarrow SL_n(\mathbb{Z}/m\mathbb{Z})$; a subgroup of $G(\mathbb{Z})$ which contains $G(m\mathbb{Z}) := G \cap SL_n(m\mathbb{Z})$ for some non-zero integer m is called a *congruence subgroup* of $G(\mathbb{Q})$. The notion of arithmetic subgroups and congruence subgroups of $G(\mathbb{Q})$ does not depend on the specific \mathbb{Q} -embedding $G \rightarrow SL_n$.

There is a topological group structure on $G(\mathbb{Q})$ obtained by designating a fundamental system of neighbourhoods of identity in $G(\mathbb{Q})$ to be arithmetic groups (respectively congruence subgroups) in $G(\mathbb{Z})$; this is called the *arithmetic* (resp. *congruence*) topology on $G(\mathbb{Q})$; the group $G(\mathbb{Q})$ admits a completion with respect to this topology; this is the **arithmetic** (respectively **congruence**) completion of $G(\mathbb{Q})$, denoted \widehat{G} (resp \overline{G}). These completions are locally compact, totally disconnected and Hausdorff. Since the arithmetic topology on $G(\mathbb{Q})$ is finer than the congruence topology, we have a homomorphism $\widehat{G} \rightarrow \overline{G}$ of completions of $G(\mathbb{Q})$ with kernel C , say. We have an exact sequence of topological groups

$$1 \rightarrow C \rightarrow \widehat{G} \rightarrow \overline{G} \rightarrow 1,$$

and C is called the **congruence subgroup kernel**. The exact sequence splits over $G(\mathbb{Q})$.

The restriction of the arithmetic topology on $G(\mathbb{Q})$ to the subgroup $\Gamma = G(\mathbb{Z})$ is just the profinite topology on $G(\mathbb{Z})$; the closure of $G(\mathbb{Z})$ in \widehat{G} is simply the profinite completion $\widehat{\Gamma}$ of $G(\mathbb{Z})$; the closure of $G(\mathbb{Z})$ in \overline{G} is the congruence completion $\overline{\Gamma}$ of Γ ; it is not difficult to see that $C \subset \widehat{\Gamma}$ and that we have the exact sequence

$$1 \rightarrow C \rightarrow \widehat{\Gamma} \rightarrow \overline{\Gamma} \rightarrow 1,$$

which shows that C is a compact profinite group.

If G is a unipotent algebraic group, then every subgroup of finite index in $G(\mathbb{Z})$ is a congruence subgroup and C is trivial. In particular, if

$U \subset G$ is a unipotent algebraic \mathbb{Q} -subgroup and $\Gamma \subset G(\mathbb{Q})$ is an arithmetic group, then there exists an integer $m \neq 0$ such that $U(m\mathbb{Z}) \subset \Gamma$.

Suppose $\Gamma = G(\mathbb{Z})$ and $\{\Gamma_m \subset \Gamma\}$ a “cofinal” family of arithmetic groups which are normal in Γ (i.e. such that every arithmetic subgroup of Γ contains some Γ_m). Since the closure of Γ in the congruence completion \overline{G} is open, it follows that the closure $\overline{\Gamma_m}$ in \overline{G} is also open for every Γ_m ; hence the intersection $Cl(\Gamma_m) = \Gamma \cap \overline{\Gamma_m}$ is a congruence subgroup of Γ containing Γ_m : it is called the congruence closure of Γ_m . It follows from the definitions that C is the inverse limit of $Cl(\Gamma_m)/\Gamma_m$:

$$(1) \quad C = \varprojlim Cl(\Gamma_m)/\Gamma_m.$$

We will say that relative to a finite set S of primes, and a fixed integer e , an integer m is sufficiently deep if m is divisible by all the powers p^e for all the primes p in S . In the inverse limit for C , may may only choose m sufficiently deep relative to any finite subset S of primes. We will use this observation repeatedly in the sequel.

If $\theta : H \rightarrow G$ is a morphism of algebraic \mathbb{Q} -groups, then it induces maps $\hat{H} \rightarrow \hat{G}$ and $\overline{H} \rightarrow \overline{G}$ and also a homomorphism $\theta : C_H \rightarrow C_G$ of the corresponding congruence subgroup kernels.

If $G(\mathbb{Z})$ is Zariski dense in G as before, and G is simply connected, then *strong approximation* holds and the congruence completion \overline{G} of G is just the group $G(\mathbb{A}_f)$ of points of G with coefficients in the ring \mathbb{A}_f of finite adeles.

Notation 1. If $a, b \in \Gamma$ are elements in an abstract group Γ , we write ${}^a(b) = aba^{-1}$, $[a, b] = aba^{-1}b^{-1}$. If $m \in \Gamma$ and $A \subset \Gamma$ is a subset, we denote by ${}^m(A)$ the subset mAm^{-1} . If A, B are subgroups, then $[A, B]$ denotes the “commutator subgroup” generated by the commutators $[a, b] = aba^{-1}b^{-1}$ for $a \in A, b \in B$. Abusing notation slightly, we sometimes write, for subsets $X, Y \subset \Gamma$, $[X, Y]$ for the *set* of commutators $[x, y]$ with $x \in X, y \in Y$. If $M \subset \Gamma$ is a subset and $A \subset \Gamma$ is a subgroup, we denote by ${}^M(A)$ the *subgroup* generated by the conjugates ${}^m(A)$.

2.2. Maps in the Congruence topology. Suppose $\mathbb{A}^a, \mathbb{A}^b$ are affine spaces of dimensions a, b respectively. We fix the standard bases of $\mathbb{A}^a, \mathbb{A}^b$; then the coordinate functions X_i, Y_j with respect to these bases generate the respective coordinate rings of $\mathbb{A}^a, \mathbb{A}^b$. The polynomial rings $\mathbb{Z}[X_i]_{1 \leq i \leq a}$ and $\mathbb{Z}[Y_j]_{1 \leq j \leq b}$ with integer coefficients will be referred to as rings of integral polynomials. Suppose $\theta : \mathbb{A}^a \rightarrow \mathbb{A}^b$ is a morphism of varieties defined over \mathbb{Q} . Then it follows that there exist finitely many

vectors $w_\nu \in \mathbb{Q}^b$, indexed by a finite set of elements $\nu \in \mathbb{Z}_+^a$ (thus the ν have non-negative integral entries) such that

$$\theta(X) = \sum_{\nu} w_\nu X^\nu.$$

By taking a common denominator D of the finite set w_ν of vectors, it follows that

$$\theta(X) = \frac{1}{D} \sum_{\nu} w'_\nu X^\nu,$$

for some integral vectors w'_ν . We will say that $D(\theta(X))$ is an integral polynomial with values in \mathbb{Z}^b .

If the coordinate X is replaced by DX , then we get from the preceding that

$$(2) \quad \theta(DX) = \theta(0) + \sum_{\nu \neq 0} w''_\nu X^\nu = \theta(0) + \sum_{i=1}^a X_i P_i(X),$$

for some *integral* vectors w''_ν , and some \mathbb{Z}^b -valued integral polynomials P_i on the affine space \mathbb{A}^a .

If all the entries of X are rational and have denominator a say, then we can write, from (2), that

$$(3) \quad \theta\left(\frac{1}{a}X\right) = \theta(0) + \frac{1}{Da^N} \sum_{\nu \neq 0} v_\nu X^\nu$$

for some *integral* vectors $v_\nu \in \mathbb{Z}^b$, and for some integer N depending on the total degree of the polynomial θ .

Lemma 3. *Suppose $\theta : H \rightarrow G$ is a morphism of algebraic groups defined over \mathbb{Q} . Then there exists an integer $D \geq 1$ such that for all $m \geq 1$, $\theta(H(Dm\mathbb{Z})) \subset G(m\mathbb{Z})$.*

Proof. Fix an embedding $G \subset SL_B$ defined over \mathbb{Q} ; then G is a \mathbb{Q} -defined closed subvariety of M_B , the affine space of dimension B^2 viewed as the vector space of $B \times B$ -matrices (with the matrices E_{ij} -whose entries are all zero except the ij -th entry which is 1- forming a preferred basis). Similarly $H \subset SL_A \subset M_A$ as a \mathbb{Q} subvariety. The composite $\theta : H \rightarrow G \subset M_B$ is then a matrix valued polynomial function on H . By the definition of the topology on H , θ is then a polynomial function (also denoted $\theta : X \mapsto \theta(X)$) on M_A with values in M_B , and defined over \mathbb{Q} i.e. has coefficients in \mathbb{Q} with respect to the basis X_{ij} of matrix entries. Consequently $\theta(h) = \frac{1}{D}N(h)$ for all $h \in M_A$ where the ‘‘denominator’’ D is an integer so chosen that it is divisible by the denominators of all the coefficients of the polynomial θ , and the

“numerator” $N(h)$ is a polynomial on M_A with *integer* coefficients.

In particular, if $X, Y \in M_A(\mathbb{Z})$ are matrices with integer entries, then (cf. equation (2)) we get $\theta(X + DmY) = \frac{1}{D}N(X + DmY)$ and $N(X + DmY) - N(X) = DmP(X, Y)$ where $P(X, Y)$ is a M_B valued polynomial function on $M_A \times M_A$ with *integer* coefficients. Hence

$$\theta(X + DmY) - \theta(X) = mP(X, Y) \equiv 0 \pmod{m}.$$

In particular, taking $X = Id_A \in M_A(\mathbb{Z})$ we get $\theta(H(Dm\mathbb{Z})) \subset Id_B + mM_B(\mathbb{Z})$ is an integral matrix congruent to identity modulo m and this proves the lemma.

(The same construction (see equation (3)) shows that if N is the total degree of the polynomial $\theta(h)$ as above, then

$$(4) \quad \theta\left(\frac{1}{a}M_A(\mathbb{Z})\right) \subset \frac{1}{Da^N}M_B(\mathbb{Z}).$$

□

Notation 2. Let $i : M \rightarrow G$ be an embedding of linear algebraic groups defined over \mathbb{Q} ; the groups M, G are Zariski closed \mathbb{Q} -defined subvarieties of M_B say, where M_B is the affine space of dimension B^2 viewed as the set of $B \times B$ matrices. A polynomial on M_B is said to have integral coefficients if it is a polynomial in the matrix entries of M_B with integral coefficients.

Consider the commutator map $M \times G \rightarrow G$ given by $(t, x) \mapsto txt^{-1}x^{-1}$. We denote this commutator $[t, x]$. This is defined over \mathbb{Q} , and extends to a morphism $\phi : M_B \times M_B \rightarrow M_B$ defined over \mathbb{Q} . In particular, there exists an M_B valued polynomial P with integral coefficients on $M_B \times M_B$, and an integer $D \geq 1$ such that $\phi(X, Y) = \frac{1}{D}P(X, Y)$ with $X, Y \in M_A$.

If $r \in \mathbb{Q}$ is a nonzero rational number, denote by $rM_B(\mathbb{Z})$ the set of matrices whose entries are rX_{ij} with $X = (X_{ij}) \in M_B(\mathbb{Z})$.

Lemma 4. *With the preceding notation, we have the inclusion of the commutator*

$$[M(Da\mathbb{Z}), G \cap (1_B + \frac{m}{a}M_B(\mathbb{Z}))] \subset G(m\mathbb{Z}),$$

for some integer D depending only on the embedding $M \subset G$.

Proof. The commutator map $M \times G \rightarrow G$ given by $(t, x) \mapsto txt^{-1}t^{-1}$ extends to a morphism $\phi : M_B \times B_B \rightarrow M_B$ defined over \mathbb{Q} . Hence there exists an M_B -valued *integral* polynomial $P(t, x)$ such that $\phi(t, x) =$

$$\frac{1}{D}P(t, x).$$

If $f(z) \in \mathbb{Z}[z]$ then $f(z) = f(0) + zg(z)$ where $g \in \mathbb{Z}[z]$; using this it follows by induction on n (see equation (2)) that if $f \in \mathbb{Z}[t_1, \dots, t_n]$ then $f(t_1, \dots, t_n) = f(0) + t_1g_1(t) + \dots + t_ng_n(t)$ for some integral polynomials $g_i \in \mathbb{Z}[t_1, t_2, \dots, t_n]$. This implies that

$$P(1_B + Da^nT, x) = P(1_B, x) + Da^nQ(T, x),$$

for some integral polynomial Q on $M_B \times M_B$ (with values in M_B). If $x \in G$, then (since the commutator of identity with x is trivial), we see that $\phi(1_B + Da^nT, x) = \phi(1_B, x) + a^nQ(T, x) = 1_B + a^nQ(T, x)$. Further, if $x = 1_B + \frac{m}{a^N}X$ with X integral, we get (since the commutator of any element $1 + Da^NT$ with 1_B is 1_B),

$$\phi(1_B + Da^NT, 1_B + \frac{m}{a^N}X) = 1_B + ma^N \frac{1}{a^N}R(T, X) = 1_B + mR(T, X),$$

for some M_B valued integral polynomial $R(T, X)$ on $M_B \times M_B$. The latter is an integral matrix in $G(\mathbb{Z})$ congruent to identity modulo m . This proves the lemma. \square

3. ISOTROPIC GROUPS

Notation 3. G is a \mathbb{Q} simple connected simply connected, semi-simple algebraic group defined over \mathbb{Q} with Lie algebra \mathfrak{g} . Assume that G is *isotropic* i.e. $\mathbb{Q} - \text{rank}(G) \geq 1$ and that P_0 is a minimal parabolic subgroup of G defined over \mathbb{Q} , with $U_0 = U_0^+$ the unipotent radical of P_0 . Fix a Levi decomposition (over \mathbb{Q}) $P_0 = L_0U_0$ of P_0 . Write $\mathfrak{p}_0, \mathfrak{u}_0, \mathfrak{l}_0$ for the Lie algebras of P_0, U_0, L_0 respectively. The *opposite* group U_0^- may be defined (as the unipotent subgroup whose Lie algebra \mathfrak{u}_0^- is the subspace of \mathfrak{g} , as a module over the Levi subgroup L_0 , the dual of \mathfrak{u}_0). It is known [Tits] that the group $G(\mathbb{Q})^+$ generated by $U_0^\pm(\mathbb{Q})$ is simple modulo the centre of $G(\mathbb{Q})^+$. The resolution of the Kneser-Tits conjecture (see [Gille] for the most general case) says that $G(\mathbb{Q}) = G(\mathbb{Q})^+$ hence $G(\mathbb{Q})$ is also a simple group modulo its centre.

The inclusion of U_0^\pm in G is defined over \mathbb{Q} and induces a map of arithmetic completions $\widehat{U_0^\pm} \rightarrow \widehat{G}$ of the groups $U_0^\pm(\mathbb{Q})$ and $G(\mathbb{Q})$ respectively; since (as was noted at the beginning of this section) the unipotent groups $U_0^\pm(\mathbb{Q})$ satisfy the congruence subgroup property, it follows that $\widehat{U_0^\pm} = U_0^\pm(\mathbb{A}_f)$: thus the exact sequence

$$1 \rightarrow C \rightarrow \widehat{G} \rightarrow \overline{G} \rightarrow 1,$$

splits over the subgroups $U_0^\pm(\mathbb{A}_f)$.

Notation 4. (Definition of M)

Let P be a proper *maximal* parabolic subgroup of G containing P_0 , with unipotent radical U with $U \subset U_0$, and fix a Levi decomposition $P = LU$ of P with $L \supset L_0$. We write, as we may, $L = S_1 S_2 M_s M'$ as an almost direct product of: $S = S_1$ a maximal \mathbb{Q} -split torus, S_2 a maximal torus which is \mathbb{Q} -anisotropic and M_s (if not the trivial group) is the product of all semisimple and \mathbb{Q} simple *isotropic groups* (i.e. those which have a \mathbb{Q} -split torus contained in it) factors of L , and M' the product of semi-simple \mathbb{Q} simple anisotropic factors of L . Since P is a maximal proper parabolic subgroup, we have: $S = S_1 \simeq \mathbb{G}_m$ has \mathbb{Q} -rank one.

The \mathbb{Q} -rank of L is then 1 (the dimension of S_1) plus the \mathbb{Q} rank of M_s ; the rest of the factors have \mathbb{Q} -rank zero.

[1] If $\mathbb{Q}\text{-rank}(G) \geq 2$, the preceding paragraph implies that M_s has positive dimension. In particular, the connected component of identity of the Zariski closure of (the group of integer points) $L(\mathbb{Z})$ contains M_s ; in this case we write $M = M_s$.

We note that if \mathbb{Q} -rank of G is one, then $P = P_0$, S_1 has dimension one, and M_s is trivial. Consequently, $L_0(\mathbb{Z})$ is contained in $S_2 M'$ (up to finite index). We write M for the connected component of identity of $L_0(\mathbb{Z})$. We will distinguish the cases

[2] $\mathbb{Q}\text{-rank}(G) = 1$ and M is abelian and

[3] $\mathbb{Q}\text{-rank}(G) = 1$ and M is not abelian.

In general, since G is simply connected, it follows that M_s is also simply connected. The simplicity - modulo centre - of $G^+(\mathbb{Q})$ implies (as is easily seen) that $U^\pm(\mathbb{Q})$ also generates $G^+(\mathbb{Q})$.

Since the unipotent groups U^\pm have the congruence subgroup property, every arithmetic subgroup in $G(\mathbb{Z})$ contains $U^\pm(m\mathbb{Z})$ for some integer m . Thus the inclusion $U^\pm \rightarrow G$ induces embeddings $U^\pm(\mathbb{A}_f) \rightarrow \widehat{G}$ of arithmetic completions. Denote by $E(m)$ the *normal* subgroup of $G(\mathbb{Z})$ generated by $U^\pm(m\mathbb{Z})$. It may or may not have finite index, but it is easily seen that the closure of $E(m)$ in $G(\mathbb{A}_f)$ is open. Thus, there is a smallest congruence subgroup containing $E(m)$; we call it the congruence closure of $E(m)$ and denote it $Cl(E(m))$. Moreover, C is the inverse limit as m varies, of the profinite completions of the quotient

$Cl(E(m))/E(m)$:

$$(5) \quad C = \varprojlim \left(\frac{Cl(\widehat{E(m)})}{E(m)} \right),$$

where the roof denotes the profinite completion of the group involved, and m varies over all integers as in equation (1).

Denote by C' the image of the congruence kernel C_L in C induced by the inclusion $L \rightarrow G$.

Lemma 5. *The group C' is central in the arithmetic completion \widehat{G} of $G(\mathbb{Q})$.*

Proof. The group \widehat{L} acts on the completions $\widehat{U}^\pm \simeq U^\pm(\mathbb{A}_f)$. However, the action being linear, descends to an action of the congruence completion \overline{L} of $L(\mathbb{Q})$. Consequently, the kernel C_L acts trivially on $U^\pm(\mathbb{A}_f)$. Since $U^\pm(\mathbb{Q})$ is a subgroup of $U^\pm(\mathbb{A}_f)$ it follows that C' commutes with $U^\pm(\mathbb{Q})$ and hence with the group generated by them. It was already seen that this subgroup is $G(\mathbb{Q})$ (using the resolution of the Kneser-Tits problem [Gille]) and hence is dense in \widehat{G} . Therefore, C' is central in \widehat{G} . \square

The group C/C' is the kernel to the map \widehat{G}/C' . For any integer k denote by $F(k)$ the normal subgroup in $G(\mathbb{Z})$ generated by $P(k\mathbb{Z}), U^-(k\mathbb{Z})$. Then $F(k) \subset \Gamma(k)$ and $F(m') \subset \Gamma(m')$. Let $Cl(F(m))$ denote the smallest congruence subgroup of $G(\mathbb{Z})$ containing $F(m)$.

The congruence kernel C is the inverse limit of $\overline{\Gamma(m)/E(m)}$ as m varies; the action of $M(\mathbb{Z})$ on all these groups induces an action on C and they are compatible with this action. By Lemma 5, the group C' is central and C/C' is the kernel to the map $\widehat{G}/C' \rightarrow G(\mathbb{A}_f)$. Moreover, the topology on $P(\mathbb{Q})$ induced by its inclusion in $G(\mathbb{Q}) \subset \widehat{G}/C'$ is the congruence topology since we have gone modulo the congruence kernel of $L =$ the congruence kernel of P . We then have, analogously to equation (5),

$$(6) \quad C/C' = \varprojlim \left(\frac{Cl(\widehat{F(m)})}{F(m)} \right)$$

expressing C/C' as an inverse limit of the profinite completions of the quotient groups $Cl(F(m))/F(m)$.

3.1. The open set $\mathcal{U} = U^-P \subset G$. The map $U^- \times P \rightarrow G$ given by multiplication $(u^-, p) \mapsto u^-p$ is a map of affine \mathbb{Q} -varieties which is an isomorphism onto its image which is a Zariski open set \mathcal{U} in G . If $g \in \mathcal{U}(\mathbb{Q}) = u^-p$, then the uniqueness of this decomposition says that $u^- \in U^-(\mathbb{Q}), p \in P(\mathbb{Q})$.

Given a prime p , the subset $U^-(\mathbb{Z}_p)P(\mathbb{Z}_p) = \mathcal{U}(\mathbb{Q}_p)$ is open in the \mathbb{Q}_p topology and contains 1. Hence there is a compact open subgroup K_p of $G(\mathbb{Z}_p)$ contained in $U^-(\mathbb{Z}_p)P(\mathbb{Z}_p)$.

The conjugation action of M on G stabilises all the groups U^\pm, M, P^+ and hence M stabilises the open set \mathcal{U} . Fix an integer m ; if S is the set of primes dividing m , denote by R the ring $\prod_{p \in S} \mathbb{Z}_p$; this is a compact open subring in $G_S = \prod_{l \in S} \mathbb{Q}_p$ and the principal ideal mR generated by m is a compact open ideal in R . Thus $\mathcal{U}(mR) = U^-(mR)P(mR)$ is an open set (containing identity) in the product group G_S . By the topology on G_S there exists a compact open subgroup $K_S = G(m'R) \subset \mathcal{U}(mR)$ of G_S for some integer m' . We may choose m' to be divisible only by primes in S since the other primes are units in R . Hence K_S is open normal of finite index in $G(R)$. Consequently $\Gamma(m')_S = G(\mathbb{Z}) \cap K_S$ is a congruence normal subgroup in $G(\mathbb{Z})$ with m' divisible by m and only by primes that divide m .

We now compute the action of $M(\mathbb{Z})$ on the latter group $\Gamma(m')$.

Given $x \in \Gamma(m')$, write, as we may, $x = u^-p$ with $u^- \in U^-(\mathbb{Q})$ and $p \in P(\mathbb{Q})$. On the other hand, viewed as an element of $G(R)$ we have $x = u^-_R p_R$ with $u^- \in U^-(mR), p_R \in P(mR)$. The uniqueness of expressing an element of $G(\mathbb{Q})$ as a product u^-p then shows that $u^- = u^-_R, p = p_R$ and are therefore integral in \mathbb{Z}_p for all primes p dividing m and hence have denominators coprime to m and all off diagonal entries have numerators divisible by m .

We have fixed a linear \mathbb{Q} -embedding $G \subset SL_B \subset M_B$; Thus u^-, p and p^{-1} viewed as matrices in $M_B(\mathbb{Q})$ of the form identity plus a matrix having a common denominator a^N (we write a^N instead of a keeping in mind a future application) with a is coprime to m and numerators which are all divisible by m :

$$u^- \in U^- \cap \left(1 + \frac{m}{a^N} M_B(\mathbb{Z})\right), \quad p, p^{-1} \in P \cap \left(1 + \frac{m}{a} M_B(\mathbb{Z})\right).$$

By Lemma 4, there exists an integer $D \geq 1$ (D independent of the a chosen, and depend only on the embedding $G \subset SL_B$) so that we have the inclusion of the commutator subgroups:

$$[M(Da^N), U^- \cap (1 + \frac{m}{a^N} M_B(\mathbb{Z}))] \subset U^-(m\mathbb{Z}) \subset F(m'),$$

and

$$[M(Da^N), P \cap (1 + \frac{m}{a^N} M_B(\mathbb{Z}))] \subset P(m\mathbb{Z}) \subset F(m').$$

Fix $x \in G(m')$; this determines the integer $a = a(x)$ is in the preceding paragraph. Fix $t \in M(Da^N\mathbb{Z})$. We compute the conjugate ${}^t(x)$ for $x \in G(m')$: write $x = u^-p$; we have seen that u^-, p have denominators a coprime to m and numerators divisible by m . Then

$$\begin{aligned} {}^t(x) &= {}^t(u^-) {}^t(p) = tu^-t^{-1}(u^-)^{-1}u^-pp^{-1}tpt^{-1} = \\ &= [t, u^-]u^-p[p^{-1}, t] = [t, u^-]x[p^{-1}, t] \end{aligned}$$

and the foregoing inclusion of commutator subgroups shows that

$$(7) \quad {}^t(x) \in F(m)xF(m) = xF(m),$$

(the last equality holds since $F(m)$ is normal). Therefore, the congruence group $M(Da^N\mathbb{Z})$ fixes the coset $xF(m) \in G(m')F(m)/F(m)$ through the element x ; the integer $a = a(x)$ depends on x and is coprime to the integer m .

3.2. Centrality in the semi-local case. If \mathbb{Z} is replaced by the semilocal subring \mathbb{Z}_S (i.e. S is the complement of a *finite set* of primes of \mathbb{Q}), then for the group $G(\mathbb{Z}_S)$ the congruence subgroup kernel is central: consider the completion \widehat{G}_A of the group $G(\mathbb{Q})$, with respect to the profinite topology on the group $G(A)$. We have the analogous exact sequence ($A = \mathbb{Z}_S$ in the following paragraph)

$$1 \rightarrow D \rightarrow \widehat{G}_A \rightarrow G(\widehat{A}) \rightarrow 1.$$

The group D is the inverse limit of $G(\widehat{mA})/\widehat{E}(mA)$ where the roof denotes the profinite completion (actually, the group is finite in the semi-local case, but we do not need to use it). Every element of a finite index subgroup $G(m'A)E(mA)/E(mA)$ (m' as before) may be replaced by an element of the form $u^-p = u^-zu$, where $u^- \in U^-$, $z \in L$, $u \in U$. But the elements u^- and u already lie in $U^\pm \cap G(mA_S) \subset E(m)$ since the denominators of these elements are coprime to m . It follows that D is the image C'_L (the congruence subgroup kernel of L) and is hence centralised by the central torus $S(\mathbb{Q})$ in $L(\mathbb{Q})$. However, all of $G(\mathbb{Q})$ still operates on D but $S(\mathbb{Q})$ acts trivially; therefore, by the simplicity

of $G(\mathbb{Q})$ modulo the centre, all of $G(\mathbb{Q})$ acts trivially; That is, the exact sequence

$$1 \rightarrow D \rightarrow \widehat{G}(A) \rightarrow G(\widehat{A}) \rightarrow 1$$

has central kernel D .

Remark. The group D is actually trivial; the congruence subgroup property for general G in the semilocal case has almost been proved ([Sury], [Pr-R2]) but we only need the centrality here.

3.3. Commuting subgroups. The following proposition was observed in [R1] and is in fact used in several proofs of centrality (see [Pr-R2]).

Proposition 6. *Denote, for each prime p of \mathbb{Q} , by G_p the closed subgroup of \widehat{G} generated by $U^\pm(\mathbb{Q}_p)$. Then C is central in \widehat{G} if and only if for each pair $p \neq q$, the groups G_p and G_q commute.*

Proof. Suppose G_p, G_q commute for different primes p, q . We have the exact sequence

$$1 \rightarrow C_p = C \cap G_p \rightarrow G_p \rightarrow G(K_p) \rightarrow 1.$$

This yields the exact sequence

$$1 \rightarrow C^p \rightarrow G^p \rightarrow G(\mathbb{A}_{K_f \setminus \{p\}}) \rightarrow 1.$$

Here, $\mathbb{A}_{f \setminus \{p\}}$ denotes the ring of finite adeles of \mathbb{Q} which is a restricted direct product of \mathbb{Q}_l for primes different from the prime p . G^p is the closed subgroup generated by G^q with $q \neq p$. C^p is the intersection of C with the closed subgroup G^p .

The group G_p is normal in \widehat{G} since it is normalised (even centralised) by $U^\pm(\mathbb{Q}_q)$ for each $q \neq p$ and normalised by (indeed, contains) $U^\pm(\mathbb{Q}_p)$ by assumption. Therefore, G_p is normalised by $U^\pm(\mathbb{Q})$. The group generated by $U^\pm(\mathbb{Q})$ is, by the solution to the Kneser-Tits problem, all of $G(\mathbb{Q})$, and since $G(\mathbb{Q})$ is dense in \widehat{G} , it follows that G_p is normalised by \widehat{G} . Hence G_p is a closed normal subgroup of \widehat{G} . Therefore, so is G^p . Thus we may form the quotient \widehat{G}/G^p which is a quotient of G_p . We have the short exact sequence

$$1 \rightarrow C/C^p \rightarrow \widehat{G}/G^p \rightarrow G(\mathbb{Q}_p) = G(\mathbb{A}_f)/G(\mathbb{A}_{f \setminus \{p\}}) \rightarrow 1$$

where in the quotient \widehat{G}/G^p the closure of the group $G(A_p)$ is a profinite group and maps to the congruence completion $G(\mathbb{Z}_p)$; A_p here is the semi-local ring consisting of rational numbers of the form $\frac{a}{b}$ with b coprime to the prime p . Moreover, we have the exact sequence

$$1 \rightarrow C/C^p \rightarrow \widehat{G(A_p)} \rightarrow G(\mathbb{Z}_p) \rightarrow 1.$$

By the preceding subsection, the group $G(A_p)$ has the congruence subgroup property (in the sense that the associated congruence subgroup kernel is central). Hence the extension C/C^p is central in \widehat{G}/C^p and hence the commutator subgroup $C' = [C, \widehat{G}]$ is contained in C^p for every prime p . In particular, C' is centralised by G_p for every prime p and hence C' is centralised by \widehat{G} .

Hence for $g \in \widehat{G}$ and $c \in C$, the map $\psi : g \mapsto gcg^{-1}c^{-1}$ is a homomorphism into the central subgroup C' . In view of the simplicity of $G(K)$ this means that the map ψ is trivial and hence that C is central in \widehat{G} . This proves the “if” part.

To prove the only if part, we argue as follows. Suppose C is central. Consider an element c in the commutator set: $c = [u, u^-] \in [U^+(\mathbb{Q}_p), U^-(\mathbb{Q}_q)]$. On this the group $S(\mathbb{Q})$ (of \mathbb{Q} rational points of the split torus S) acts by conjugation. The action of $S(\mathbb{Q})$ on c is trivial by assumption; hence $[u, u^-] = {}^s(u), {}^s(u^-)$ for all $s \in S(\mathbb{Q})$. By weak approximation, $S(\mathbb{Q})$ is dense in the product $S(\mathbb{Q}_p) \times S(\mathbb{Q}_q)$. It follows by the density that

$$[u, u^-] = [{}^s(u), u^-]$$

for all $s \in S(\mathbb{Q}_p)$. Since we can choose a sequence $s_k \in S(\mathbb{Q}_p)$ such that ${}^{s_k}(u)$ contracts to identity we get $[u, u^-] = 1$. Since u is arbitrary, it follows that $U^+(\mathbb{Q}_p)$ commutes with u^- . In other words, G_p commutes with G_q . \square

4. AN APPLICATION OF DIRICHLET'S THEOREM

4.1. Dirichlet theorem on primes. Let $M \subset GL_n$ be a linear algebraic group defined over \mathbb{Q} . Fix a prime l , and an integer $m \geq 2$. The unit group $(\mathbb{Z}/l^m\mathbb{Z})^*$ is cyclic of order $l^{m-1}(l-1)$ if l is odd and if $l = 2$, then it has an element of order 2^{m-2} . and consider the set S of primes p such that the order of p modulo l is either $l^{m-1}(l-1)$ if l is odd and 2^{m-2} if $l = 2$. By Dirichlet's theorem on infinitude of primes in arithmetic progressions, the set S is infinite.

Fix l and $p \in S$ as above. Write $e = e_l(p)$ for the largest integer such that the finite group $M(\mathbb{F}_p)$ has an element of exponent l^e .

Lemma 7. *The exponent $e_l(p)$ satisfies the estimate*

$$e_l(p) \leq \left\lfloor \frac{n}{l-1} \right\rfloor + \left\lfloor \frac{n}{l(l-1)} \right\rfloor + \cdots + \left\lfloor \frac{n}{l^{m-1}(l-1)} \right\rfloor,$$

where $\lfloor x \rfloor$ denotes the integral part.

Proof. We have $M \subset GL_n$. We need only prove the lemma for GL_n since the exponent of the subgroup $M(\mathbb{F}_p)$ divides the exponent of the larger group $GL_n(\mathbb{F}_p)$. The order of $GL_n(\mathbb{F}_p)$ is

$$(p^n - 1)(p^n - p^2) \cdots (p^n - p^{n-1}).$$

Now p is coprime to l , and generates the cyclic group $(\mathbb{Z}/l^m\mathbb{Z})^*$ (if l is odd). For $j \leq m$, let $X(l^j)$ denote the set of $i \leq n$ with $p^i \equiv 1 \pmod{l^j}$ and let $x(l^j)$ be the cardinality of the set $X(l^j)$. The assumption on p implies that if $i \in X(l^j)$, then i must be divisible by $l^{j-1}(l-1)$. Hence the number of $i \leq n$ such that l^j divides $p^i - 1$ is the integral part $[\frac{n}{l^{j-1}(l-1)}] = x(l^j)$.

The two preceding paragraphs imply that for each $j \leq m$, then number of factors in the product $\prod_{i=1}^n (p^i - 1)$ divisible by l^j is $x(l^j)$ ($=$ the integral part $[\frac{n}{l^{j-1}(l-1)}]$). Now, $X(l) \supset X(l^2) \supset \cdots \supset X(l^m)$; if $i \in X(l^j) \setminus X(l^{j+1})$, then the highest power of l dividing the factor $p^i - 1$ is j . Therefore, the largest power of l which divides the order of $GL_n(\mathbb{F}_p)$ is $1(x(l) - x(l^2)) + 2(x(l^2) - x(l^3)) + \cdots + mx(l^m) = x(l) + x(l^2) + x(l^3) + \cdots + x(l^m)$.

The last two paragraphs imply the lemma for GL_n and hence for arbitrary $M \subset GL_n$. \square

Corollary 1. *If $l \geq n + 2$, then $e_l(p) = 0$. Moreover, in all cases, $e_l(p) \leq 2n$. Let $R_l = l^{e_l(p)}$. Then $R_l \leq (n + 1)^{2n}$.*

Proof. The formula for $e_l(p)$ as a sum in the lemma is such that all the terms are bounded by the first term and the first term is $[\frac{n}{l-1}] = 0$ if $l \geq n + 2$. The formula also shows that

$$e_l(p) \leq \frac{n}{l-1} + \frac{n}{(l-1)l} + \cdots \leq 2n.$$

Hence for $l \geq n + 2$, $R_l = 1$ and otherwise, $R_l = l^{e_l(p)} \leq (n + 1)^{2n}$. \square

As before, we let $M \subset GL_n$ an algebraic subgroup defined over \mathbb{Q} and l a prime. Let $a \geq 1, b \geq 2$ be coprime integers. Consider the arithmetic progression $a + bx : x = 0, 1, 2, \dots$. For $m \in \mathbb{Z}$, denote by $M(m)$ the principal congruence subgroup of level m in $M(\mathbb{Z})$, and $R_l(m)$ be the l -exponent (the largest power of l which divides the exponent) of $M(\mathbb{Z}/m\mathbb{Z})$. Denote by $R_l(a, b)$ the infimum of $R_l(a + bx) : x = 0, 1, 2, 3, \dots$. The l -exponent of the quotient $M(\mathbb{Z})/\Delta$ where Δ is the group generated by $\{M(a + bx); x \in \mathbb{Z}\}$ is clearly no bigger than the

l -exponent $R_l(a + bx)$ of $M(\mathbb{Z}/(a + bx)\mathbb{Z})$ for each x . Therefore the l exponent of $M(\mathbb{Z})/\Delta$ is $\leq R_l(a, b)$.

Proposition 8. *There is an integer R_l depending only on n and not on a, b such that $R_l(a, b) \leq R_l$.*

Proof. Let l^m be the largest power of l dividing b ; hence $b = l^m c$ with c coprime to l . We find a prime p such that p generates the unit group $(\mathbb{Z}/l^m\mathbb{Z})^*$. Thus $p \in S$ of the preceding lemma. Suppose $a = p^h$ modulo l^m . By Dirichlet's theorem, we can find primes p_1, \dots, p_{h-1} such that $p_j \equiv 1 \pmod{c}$, and $p_j \equiv p \pmod{l^m}$ ($j \leq h-1$). We also choose $p_h \equiv a \pmod{c}$ and $p_h \equiv p \pmod{l^m}$. Then $p_1 p_2 \cdots p_h \equiv a \pmod{b}$. Now $GL_n(\mathbb{Z}/p_1 p_2 \cdots p_h \mathbb{Z})$ is the product of $GL_n(\mathbb{F}_{p_i})$, and the l exponent of the product is the supremum of the exponents of $GL_n(\mathbb{F}_{p_i})$. The latter is, by the lemma, bounded only by an integer R_l depending on n : $R_l \leq l^{2n} \leq (n+1)^{2n}$ (Corollary 1). The proposition follows. □

We are now in a position to prove Theorem 2. We restate it (to save notation, we replace bm by b , as we may, since a is still coprime to bm) as follows.

Proposition 9. *Let $M \subset GL_n$ be a linear algebraic group defined over \mathbb{Q} , and a, b two coprime integers. Let $M(\mathbb{Z})$ be fixed, and denote by N the (normal) group generated by the congruence subgroups $M(ax + b)$ with $x \in \mathbb{Z}$ of $M(\mathbb{Z})$. There exists an integer R depending only on n such that the exponent of every element of $M(\mathbb{Z})/N$ divides R ; in particular, the group $\Delta = M(\mathbb{Z})^R$ generated by R -th powers of $M(\mathbb{Z})$ lies in N .*

Proof. This is a simple application of the preceding lemma. We first prove this for elements whose exponents are a power of the prime l . In that case, the integer R is the $R_l \leq (n+1)^{2n}$ of the preceding lemma. Moreover, by Corollary 1, the l -exponent is 1 unless l is a prime with $l \leq n+1$. Hence the exponent of M/N is

$$R = \prod_{l \leq n+1} R_l \leq \prod_{l \leq n+1} (n+1)^{2n} = [(n+1)^{2n}]^{\pi(n+1)},$$

where $\pi(n+1)$ is the number of primes $l \leq n+1$. This proves the proposition and equivalently Theorem 2. □

5. PROOF OF CENTRALITY WHEN $\mathbb{Q} - \text{rank}(G) = 1$ AND $M_0(\mathbb{Z})$ IS VIRTUALLY ABELIAN

5.1. generalities.

Notation 5. We assume that $\mathbb{Q} - \text{rank}(G) = 1$. Then the proper maximal parabolic subgroup $P = P_0$ is a minimal parabolic subgroup defined over \mathbb{Q} , U the unipotent radical of P , and $P = LU$ a Levi decomposition of P . Take $S \subset L$ a maximal \mathbb{Q} -split torus in L (and in G since $\mathbb{Q} - \text{rank}(G) = 1$). Since $\mathbb{Q} - \text{rank}(G) = 1$, the group $L(\mathbb{Q})$ consists entirely of semisimple elements.

As a module over $S \simeq \mathbb{G}_m$ the Lie algebra \mathfrak{u} of U^+ decomposes as $\mathfrak{u} = \mathfrak{g}_\alpha \oplus \mathfrak{g}_{2\alpha}$; similarly the Lie algebra \mathfrak{u}^- of U^- decomposes as $\mathfrak{u}^- = \mathfrak{g}_{-\alpha} \oplus \mathfrak{g}_{-2\alpha}$. Since S is in the centre of L , these decompositions are stable under the adjoint action of L . If we denote by \mathfrak{l} the Lie algebra of L then we have the decomposition

$$\mathfrak{g} = \mathfrak{u}^- \oplus \mathfrak{l} \oplus \mathfrak{u} = \mathfrak{g}_{-2\alpha} \oplus \mathfrak{g}_{-\alpha} \oplus \mathfrak{l} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{2\alpha}.$$

As before, denote by $M = ZCl(L(\mathbb{Z}))^0$ the connected component of identity of the Zariski closure of the group $L(\mathbb{Z})$ of integer points of L .

In this section, we assume that M is abelian i.e. that $L(\mathbb{Z})$ is virtually abelian.

Lemma 10. *M is in the centre of L .*

Proof. Since $L(\mathbb{Q})$ commensurates $L(\mathbb{Z})$, it follows that the identity component M of the Zariski closure of $L(\mathbb{Z})$ is normal in L . Now L is reductive and hence so is M . Since M is abelian, M is a torus of dimension d say. Therefore the automorphism group M is a discrete group, namely $GL_d(\mathbb{Z})$. The conjugation action of L on M yields a homomorphism $L \rightarrow GL_d(\mathbb{Z})$; but since L is connected and $GL_d(\mathbb{Z})$ is discrete, it follows that this homomorphism is trivial. That is, L centralises M . \square

Lemma 11. [1] *The Lie algebra generated by $\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}$ is all of \mathfrak{g} .*

[2] *We have $[\mathfrak{g}_\alpha, \mathfrak{g}_\alpha] = \mathfrak{g}_{2\alpha}$.*

Proof. We first prove that \mathfrak{g} is generated as a Lie algebra by the subspaces $\mathfrak{g}_\alpha, \mathfrak{g}_{2\alpha}, \mathfrak{g}_{-\alpha}, \mathfrak{g}_{-2\alpha}$. Denote temporarily, the Lie algebra generated by these subspaces as \mathfrak{g}' ; this is normalised by \mathfrak{l} , since each of these spaces is. Hence all of \mathfrak{g} normalises \mathfrak{g}' . The \mathbb{Q} -simplicity of \mathfrak{g} now ensures that $\mathfrak{g}' = \mathfrak{g}$.

Under the Lie bracket, the subspace $\mathfrak{g}_{2\alpha}$ takes $\mathfrak{g}_{-\alpha}$ into \mathfrak{g}_α , and \mathfrak{g}_α into 0; consequently, by the Jacobi identity, the Lie algebra \mathfrak{g}'' generated by $\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}$ is normalised by the adjoint action of $\mathfrak{g}_{2\alpha}$ (and similarly by the action of $\mathfrak{g}_{-2\alpha}$); hence \mathfrak{g}'' is normalised by \mathfrak{g}_β with $\beta \in \{\pm\alpha, \pm 2\alpha\}$; by the preceding paragraph, \mathfrak{g}'' is normalised by \mathfrak{g} ; the \mathbb{Q} -simplicity of \mathfrak{g} now implies that $\mathfrak{g}'' = \mathfrak{g}$. This proves [1].

Denote by \mathfrak{g}^* the direct sum subspace

$$\mathfrak{g}^* = [\mathfrak{g}_\alpha, \mathfrak{g}_\alpha] \oplus \mathfrak{g}_\alpha \oplus \mathfrak{l} \oplus \mathfrak{g}_{-\alpha} \oplus [\mathfrak{g}_{-\alpha}, \mathfrak{g}_{-\alpha}].$$

By examining the brackets of each of the individual terms in this direct sum, we see that \mathfrak{g}^* is a Lie subalgebra defined over \mathbb{Q} . Further it is normalised by the subspaces $\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}$ (since it contains them); by part [1], \mathfrak{g}^* is therefore normalised by all of \mathfrak{g} . The \mathbb{Q} -simplicity of \mathfrak{g} then implies that $\mathfrak{g}^* = \mathfrak{g}$. This proves [2] and in particular, proves that $[\mathfrak{g}_\alpha, \mathfrak{g}_\alpha] = \mathfrak{g}_{2\alpha}$. □

Lemma 12. *If $t \in M$ is not in the centre of G , then the element t does not have a non-zero fixed point in \mathfrak{g}_α . That is, all the eigenvalues of the linear transformation $Ad(t)$ acting on \mathfrak{g}_α are different from 1.*

Proof. : Since M is a torus, every element of M is semisimple. Split the space \mathfrak{g}_α into eigenspaces for t : $\mathfrak{g}_\alpha = \bigoplus_{\lambda \neq 1} (\mathfrak{g}_\alpha)_\lambda \oplus (\mathfrak{g}_\alpha)_1 = W \oplus (\mathfrak{g}_\alpha)_1$. Similarly there is a decomposition for $\mathfrak{g}_{-\alpha}$. If possible, let $X \in (\mathfrak{g}_\alpha)_\lambda$ and $Y \in (\mathfrak{g}_{-\alpha})_1$ be both nonzero. We will show that this leads to a contradiction. The bracket $[X, Y]$ is in $\mathfrak{g}^S \simeq \mathfrak{l}$. This is impossible since the action of t on X is multiplication by λ and on Y and X it is multiplication by 1. Therefore, $[X, Y] = 0$, and hence, by taking the sum over all the λ , $[W, Y] = 0$. Note that W is defined over \mathbb{Q} .

Now take $X \in W(\mathbb{Q}) \setminus \{0\}$; then $u = \exp(X)$ is a unipotent element commuting with the unipotent element $v = \exp(Y) \in U^-$. Hence u, v generate a unipotent group E . However, in the \mathbb{Q} -rank one group G , every nontrivial unipotent element belongs to a unique maximal unipotent group; hence $u \in U^+$ and hence $E \subset U^+$; similarly, $v \in U^-$ and hence $E \subset U^-$; this means that $E = \{1\}$ i.e. $X = 0$ and $Y = 0$, a contradiction.

This means that either $X = 0$ or $Y = 0$; in other words, \mathfrak{g}_α is either fixed pointwise by t , or $\mathfrak{g}_\alpha = W$ has no fixed points. Suppose $\mathfrak{g}_\alpha = \mathfrak{g}_\alpha^t$. By considering orthogonal decomposition (with respect to the Killing form κ) of \mathfrak{g} as a module over $t \in SO(\kappa)$, one sees that $\mathfrak{g}_{-\alpha} = \mathfrak{g}_{-\alpha}^t$ is

also pointwise fixed by t . Since \mathfrak{g} is generated by $\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}$ by lemma 11, it follows that all of \mathfrak{g} is pointwise fixed by t ; that is, t is in the centre of G . \square

Corollary 2. *Let $V = \{\exp(tX); t \in \mathbb{G}_a \subset U^+\}$ be the subgroup generated by the exponentials of an element $X \in \mathfrak{g}_\alpha$. Suppose $t \in M$ is not in the centre of G . The commutator subgroup $[t^{\mathbb{Z}}, V]$ contains V .*

Proof. The Cayley-Hamilton theorem and the fact that 1 is not an eigenvalue of $Ad(t)$ (lemma) show that the matrix $Ad(t) - 1$ is invertible on \mathfrak{g}_α and the inverse is a polynomial in $Ad(t) - 1$. Hence X is in the span of the vectors $(Ad(t) - 1)^k(X)$.

If \mathcal{G} is a group, $R = \mathbb{Z}[\mathcal{G}]$ its integral group ring and $a, b \in \mathcal{G}$, then $a - 1, b - 1, ab - 1$ are elements of R . We have the identity

$$(a - 1)(b - 1) = (ab - 1) - (a - 1) - (b - 1),$$

in R ; this shows that the span of $Ad(t^k) - 1$ contains the span of $(Adt - 1)^k$ for all integers $k \geq 1$. This and the preceding paragraph show that X is a linear combination of $(Ad(t^k) - 1)(X)$.

Since the Lie algebra of the commutator group $[t^{\mathbb{Z}}, V]$ contains the span of $(Ad(t^k) - 1)(X)$ for $k \geq 1$, the conclusion of the preceding paragraph shows that X lies in this Lie algebra; that is, V lies in $[t^{\mathbb{Z}}, V]$. \square

Notation 6. Let $\theta : H = SL_2 \rightarrow G$ be a non-trivial morphism of algebraic \mathbb{Q} -groups. Denote by U_H^+ (resp. U_H^-) the group of upper triangular (resp. lower triangular) unipotent matrices in SL_2 . Assume θ is such that $\theta(U_H^\pm) \subset U^\pm$, and that the image under θ of the group D of diagonals in H is the torus S in G .

Corollary 3. *If $\Delta \subset M$ is an infinite subgroup, then the commutator group $[\Delta, \theta(SL_2)]$ contains $\theta(SL_2)$:*

$$[\Delta, \theta(SL_2)] \supset \theta(SL_2) \quad \text{and} \quad [D, \theta(SL_2(\mathbb{Q}))] \supset SL_2(\mathbb{Q}).$$

Proof. By the preceding corollary, the commutator subgroup $[\Delta, \theta(U_H^+)]$ contains $\theta(U_H^+)$; similarly, $[\Delta, \theta(U_H^-)]$ contains $\theta(U_H^-)$. Since SL_2 is generated by U_H^\pm the corollary follows. \square

5.2. Some consequences of Proposition 9. In this subsection, we derive some consequences of Proposition 9 for $\theta(SL_2)$ and the results of the preceding subsection.

Corollary 4. *If $\theta : SL_2 \rightarrow G$ is a nontrivial morphism, and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Dm\mathbb{Z})$, then the conjugate $t\theta(g)t^{-1} \in \theta(g)E(m\mathbb{Z})$ for all $m \in M(Da^N\mathbb{Z})$. That is, $M(Da^N\mathbb{Z})$ acts trivially on $\theta(g)$ viewed as an element of $\Gamma(m)/E(m)$.*

Proof. Write

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{pmatrix} = u^- z v$$

with $u^- \in U_H^-$, $z \in \text{diagonals}$ and $v \in U_H^+$. Thus u^-, v are matrices of the form $1 + \frac{Dm}{a}x$ with $x \in M_2$. By equation (4) there exist integers D, N such that $\theta(u^-) \in 1_B + \frac{m}{Da^N}M_B(\mathbb{Z})$. Suppose $t \in M(Da^N\mathbb{Z})$; then by equation (7),

$$t\theta(g)t^{-1} = \theta(g)E(m),$$

preserves the coset of $E(m)$ in $\Gamma(m)$ through the element $\theta(g)$. \square

Corollary 5. *The isotropy of $\theta(g) \in \Gamma(m)/E(m)$ with $g \in SL_2(Dm\mathbb{Z})$ as in the preceding corollary, contains the group generated by the congruence groups $M(D(a+bx)^N\mathbb{Z})$, with $x \in Dm\mathbb{Z}$.*

Proof. The preceding Corollary 4 says that $M(Da^N)$ stabilises the element $\theta(g) \in \Gamma(m)/E(m)$. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Dm)$ and $x \in Dm$, we may apply the corollary to the element $g' = gu$ with $u = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$; then $a(gu) = a + bx$ and $\theta(g') \in \theta(g)E(m)$. Now the preceding Corollary 4 says that $M(D(a+bx)^N)$ also stabilises $\theta(g) = \theta(g')$ in $\Gamma(m)/E(m)$. This proves the corollary. \square

Corollary 6. *In the notation of Proposition 9, denote by Δ the normal subgroup generated by the congruence subgroups $M(D(ax+b)^N)$ for some **fixed** integers D, N . The exponent of $M(\mathbb{Z})/\Delta$ depends only on integer D and not on a, b .*

Proof. This is immediate from Corollary 5 and Proposition 9. \square

Corollary 7. *There exists a fixed infinite subgroup $\Delta \subset M(\mathbb{Z})$ such that Δ acts trivially on the image C' of the congruence subgroup kernel of SL_2 under the map $\theta : SL_2 \rightarrow G$.*

Proof. By Proposition 9 (and its consequence, namely Corollary 6), there exists a *fixed* infinite subgroup Δ in $M(D\mathbb{Z})$, which acts trivially on $\theta(g)$ for **all** $g \in SL_2(Dm\mathbb{Z})$. Since C' is the inverse limit of $\theta(SL_2(Dm)/E_2(Dm))$, it follows that Δ acts trivially on C' as well. \square

Proposition 13. *Let $\theta : SL_2 \rightarrow G$ be as in the paragraph preceding Corollary 3. Denote again by θ the map induced at the level of congruence subgroups kernels: $\theta : C_H \rightarrow C$ with image C' say.*

The action of $SL_2(\mathbb{Q})$ on C' is trivial.

Proof. We know that $\Delta \subset M(\mathbb{Z})$ acts trivially on C' . But the group $SL_2(\mathbb{Q})$ acts on the kernel C' ; hence the commutator $[\Delta, SL_2(\mathbb{Q})]$ acts trivially on C' . By Corollary 3, $SL_2(\mathbb{Q}) \subset [\Delta, SL_2(\mathbb{Q})]$ and hence acts trivially on C' . \square

5.3. Proof of Theorem 1 when $\mathbb{Q} - \text{rank}(G) = 1$ and $L(\mathbb{Z})$ is virtually abelian.

Theorem 14. *Let $\mathbb{Q} - \text{rank}(G) = 1$, $\mathbb{R} - \text{rank}(G) \geq 2$ and assume that $M_0(\mathbb{Z})$ is virtually abelian. Then the congruence subgroup kernel C is central in \widehat{G} .*

Proof. Fix $X \in \mathfrak{g}_\alpha(\mathbb{Q})$ be such that over the algebraic closure $\overline{\mathbb{Q}}$, the projection of X to each root space (occurring in \mathfrak{g}_α) of a maximal torus in G containing the product torus MS is nonzero. Since L (being the centraliser of the split torus S) contains this maximal torus, it follows that the space generated by the conjugates ${}^t(X); t \in L(\mathbb{Q})$ is all of \mathfrak{g}_α . The Lie algebra generated by \mathfrak{g}_α is all of $\text{Lie}U^+$ by part 2 of Lemma 11. Denote by $\exp : \mathfrak{g}_\alpha \rightarrow U^+ \subset G$ the exponential map on the elements (which are of course, nilpotent matrices) of \mathfrak{g}_α .

By the Jacobson-Morozov theorem, there exists a homomorphism $\theta' : H = SL_2 \rightarrow G$ defined over \mathbb{Q} , such that $u = \theta \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \exp(X) \in U^+$. Denote by B (resp. T) the group of upper triangular (resp. diagonal) matrices in H . Since $P = P_0$ is a minimal parabolic subgroup, it follows that there exists $g_1 \in G(\mathbb{Q})$ which conjugates $\theta(B)$ into P : ${}^{g_1}\theta'(B) \subset P$. The conjugacy of split tori in P shows that there exists $g_2 \in P$ which conjugates $\theta'(T)$ into S . The product $g = g_2g_1$ then conjugates $\theta'(B)$ into P and $\theta'(T)$ into S . Denote by θ the map $h \mapsto g\theta'(h)g^{-1}$. Since $\exp(X)$ lies in a unique maximal unipotent \mathbb{Q} -subgroup namely U^+ , the inclusions ${}^g(\exp(X)) \in U^+, \exp(X) \in U^+$

imply that $g \in P$. Write $g = mu$ with $m \in M_0(\mathbb{Q}), u \in U^+$.

Now ${}^g(\exp(X)) = \exp({}^g(X)) = \exp^m(u(X))$. Since u is unipotent, the element ${}^u(X)$ is of the form $X + Y$ with $Y \in \mathfrak{g}_{2\alpha}$. Since $S = \theta(T)$ acts by the eigencharacter α on ${}^u(X)$ it follows that $Y = 0$ and ${}^u(X) = X \in \mathfrak{g}_\alpha$. Hence ${}^u(X) = X$ also has nonzero projection to all the root spaces of T , and hence the set ${}^M({}^u(X))$ generates $Lie(U^+)$, and the set ${}^M(\exp(X))$ generates $U^+(\mathbb{Q})$. Moreover, ${}^\kappa(X) \in \mathfrak{g}_{-\alpha}$; hence ${}^M({}^\kappa(X))$ generates $\mathfrak{g}_{-\alpha}$ and ${}^M(U_H^-)$ generates U^- .

Lemma 15. *If K_p is a compact open subgroup in $M(\mathbb{Q}_p)$ then*

$${}^{K_p}(U_H^+(p)) = {}^{M_p}(U_H^+) = U^+(p).$$

Proof. It is enough to prove that the \mathbb{Q}_p Lie algebra \mathfrak{v} generated by ${}^{K_p}(U_H^+(p))$ is all of $\mathfrak{u} = Lie(U^+(p))$. Let $X \in Lie(U_H^+)$ as before. If $\mathfrak{v} \neq \mathfrak{u}$ then there exists an $m_0 \in M_0(\mathbb{Q})$ such that $Y = {}^{m_0}(X) \notin \mathfrak{v}$. Suppose $\lambda : \mathfrak{u} \rightarrow \mathbb{Q}_p$ is a linear form which is nonzero on Y but zero on \mathfrak{v} ; the function $\lambda_X : m \mapsto \lambda({}^m(X))$ is a polynomial function on M which is identically zero on the open subgroup K_p ; but K_p being open, is Zariski dense and hence λ_X is zero on all of M_p , a contradiction. Therefore, $\mathfrak{v} = \mathfrak{u}$. \square

We can now complete the proof of centrality for G .

Since C' is central in $\theta(\widehat{SL}_2)$ (Proposition 13), it follows from Proposition 6 that $U_H^+(p)$ and $U_H^-(q)$ commute. Conjugation by elements $m \in M(\mathbb{Q})$ shows that ${}^m(U_H(p))$ and ${}^m(U_H^-(q))$ commute for all $m \in M(\mathbb{Q})$. However, the action of $M(\mathbb{Q})$ on $U^+(p)$ and $U^-(q)$ factors via the map

$$M(\mathbb{Q}) \rightarrow M(\mathbb{Q}_p) \times M(\mathbb{Q}_q) \rightarrow Aut(U^+(p)) \times Aut(U^-(q)).$$

(the maps given by $m \mapsto (m_p, m_q)$ and the conjugation by m becomes ${}^m(U^+(p)) = {}^{m_p}(U^+(p)), {}^m(U^-(q)) = {}^{m_q}(U^-(q))$). By a theorem of Sansuc (see Theorem 7.9 of [Pl-R]), the closure of $M(\mathbb{Q})$ in $M(\mathbb{Q}_p) \times M(\mathbb{Q}_q)$ is *open* of finite index. Hence the closure of $M(\mathbb{Q})$ contains a subgroup of the form $K_p \times K_q$ with $K_p \subset M(\mathbb{Q}_p), K_q \subset M(\mathbb{Q}_q)$ open. Consequently, ${}^{K_p}(U_H(p))$ commutes with ${}^{K_q}(U_H^-(q))$. Then Lemma 15 implies that $U^+(p)$ and $U^-(q)$ commute. By Proposition 6, this implies that C is central. \square

6. WHEN $\mathbb{Q} - \text{rank}(G) \geq 2$ OR $M(\mathbb{Z})$ IS NOT VIRTUALLY ABELIAN

6.1. **Centrality of C/C'_M .** Assume that $\infty - \text{rank}(G) \geq 2$. Suppose that $M_s(\mathbb{Z})$ is infinite. Now consider the quotient \widehat{G}/C'_M ; since (by Lemma 5) C'_M is a central and compact subgroup of \widehat{G} , it follows that this quotient is a locally compact and Hausdorff topological group.

As we already observed in the discussion preceding equation (6) the restriction to $P(\mathbb{Z}) \simeq U(\mathbb{Z})M(\mathbb{Z})$ of the topology induced on $G(\mathbb{Q})$ viewed as a subgroup of \widehat{G}/C'_M is simply the congruence topology. Thus, for $m \geq 1$ the groups $P(m\mathbb{Z})$ give a fundamental system of neighbourhoods of identity of $P(\mathbb{Q}) \subset \widehat{G}/C'_M$.

Let $F(m)$ denote the subgroup of $G(m\mathbb{Z})$ normalised by $G(\mathbb{Z})$ and generated as a normal subgroup by the two groups $P(m\mathbb{Z})$ and $P^-(m\mathbb{Z})$. Then the quotient \widehat{G}/C'_M maps onto $G(\mathbb{A}_f)$ with kernel $C/C'_M \simeq \varprojlim G(m\mathbb{Z})/F(m)$ (see equation (6)).

An element in the quotient group $G(m\mathbb{Z})/F(m)$ (after perhaps multiplying it on the right by an element of the Zariski dense subgroup $F(m)$) may be written in the form u^-p with $u^- \in U^-$, $p \in P$. Moreover, the denominators a of the entries of the matrices u^\pm and p are coprime to m . From equation (7), if $t \in M'(Da^N\mathbb{Z})$, then ${}^t(g) = g \in gF(m)$ for every $t \in M(a^N\mathbb{Z})$. On the other hand, $M(m\mathbb{Z})$ also acts trivially on $G(m\mathbb{Z})/F(m)$ since $M(m\mathbb{Z})$ is contained in $F(m)$.

If (D, m) denotes the g.c.d of D and m , then $M(m\mathbb{Z})$ and $M(Da^N\mathbb{Z})$ together generate the group $M((D, m)\mathbb{Z})$, since m and a are coprime (it follows from strong approximation that for two non-zero integers u, v with g.c.d. w , the group generated by $M'(u\mathbb{Z})$ and $M'(v\mathbb{Z})$ is all of $M'(w\mathbb{Z})$); therefore the infinite group $M'(D\mathbb{Z}) \subset M'(D, m)\mathbb{Z}$ acts trivially on $G(m\mathbb{Z})/F(m)$ and hence on C/C'_M .

Since all of $G(\mathbb{Q})$ operates on the quotient C/C'_M (recall that we have proved that C'_M is centralised by $G(\mathbb{Q})$ and hence, in particular, is stable under the action of $G(\mathbb{Q})$), and the infinite group $M'(D\mathbb{Z})$ acts trivially, it follows by the simplicity of $G(\mathbb{Q})$ modulo its centre, that $G(\mathbb{Q})$ acts trivially; hence C/C'_M is centralised by \widehat{G}/C'_M .

6.2. Centrality of C . Now let $g \in G(\mathbb{Q})$ and $c \in C$. From the preceding subsection, g acts trivially on C/C'_M and C'_M is central in \widehat{G} . Then $\psi(g) = gcg^{-1}c^{-1}$ is in C'_M and is central in \widehat{G} . Hence it follows that $\psi(g_1g_2) = \psi(g_1)\psi(g_2)$. Thus $\psi : G(\mathbb{Q}) \rightarrow C'_M$ is a homomorphism into the abelian group C'_M . Since $G(\mathbb{Q})$ is simple modulo centre, it follows that ψ is trivial and hence that C is central in \widehat{G} .

This and Theorem 14 together prove Theorem 1 in all cases.

REFERENCES

- [BMS] H. Bass, J. Milnor and J.-P. Serre, Solution of the congruence subgroup problem for $SL_n(n \geq 3)$ and $Sp_{2n}(n \geq 2)$, Publ. Math. I.H.E.S., **33** (1967) 59-137.
- [Gille] P. Gille, Le Probleme de Kneser-Tits, Seminaire Bourbaki, Vol. 2007-2008, Asterisque No. **326** (2009), Exp 983, vii, 39-81.
- [Pl-R] V. Platonov and A.Rapinchuk. Algebraic Groups and Number Theory, pure and applied math **139**, Academic Press Inc. Boston, MA (1994).
- [P] G. Prasad, On some work of Raghunathan, Algebraic Groups and Arithmetic, 25-40, Tata Inst. Fund. Res, Mumbai (2040).
- [Pr-R1] G.Prasad and M.S.Raghunathan On the Congruence Subgroup Problem: determination of the “metplectic kernel”. Invent math. 71 (1983), no.1 21-42.
- [Pr-R2] G.Prasad and M.S.Raghunathan Topological central extensions of semisimple groups over local fields I and II Ann of math (2) **119** (1984) **no.1** 143-201,**no. 2** 203-268.
- [Pr-Ra] G.Prasad and A.Rapinchuk Computation of the metaplectic kernel, I.H.E.S Publ. Math. **no 84** (1997), 91-187.
- [Pr-Ra2] G.Prasad and A.Rapinchuk On the congruence kernel for simple algebraic groups, Tr. Math Inst Steklova, **292** (2016) 224-254.
- [R1] M. S. Raghunathan, On the congruence subgroup problem, Publ. Math. Inst. Hautes Etud. Sci. **46** (1976) 107-161.
- [R2] M. S. Raghunathan, On the congruence subgroup problem II, Invent. Math. **85** (1986) 73-117.
- [R3] M. S. Raghunathan, The congruence subgroup problem, in Proceedings of the Hyderabad conference on algebraic groups, 465-494, ed. S. Ramanan, National Board for Higher Mathematics, Mumbai, 1991.
- [Ser] J-P.Serre, Le probleme de groupes de congruence pour SL_2 , Ann of Math. **92** (1970), 489-527.
- [Sury] B. Sury, Congruence Subgroup Problem for anisotropic groups over semilocal rings, Proc. Ind Acad.Sci. Math. **101** (1991), no. **2**, 87-110.
- [Tits] Algebraic and abstract simple groups, Ann of Math. **80** (1964) 313-329.

SCHOOL OF MATHEMATICS, TATA INSTITUTE OF FUNDAMENTAL RESEARCH,
HOMI BHABHA ROAD, BOMBAY - 400 005, INDIA.

Email address: `venky@math.tifr.res.in`