Pacific Journal of Mathematics

ON SYSTEMS OF GENERATORS OF ARITHMETIC SUBGROUPS OF HIGHER RANK GROUPS

T. N. VENKATARAMANA

Volume 166 No. 1 November 1994

PACIFIC JOURNAL OF MATHEMATICS
Vol. 166, No. 1, 1994

ON SYSTEMS OF GENERATORS OF ARITHMETIC SUBGROUPS OF HIGHER RANK GROUPS

T.N.VENKATARAMANA

We show that any two maximal disjoint unipotent subgroups of an irreducible non-cocompact lattice in a Lie group of rank atleast two generates a lattice. The proof uses techniques of the solution of the congruence subgroup problem.

We show that any two maximal opposing unipotent subgroups of an irreducible lattice in a higher rank Lie Group, generate a lattice in the Lie Group. The method of proof is to use certain techniques of the solution of the congruence subgroup problem of arithmetic lattices in higher rank groups.

We freely use the notation and results of [**3**] without giving explicit references therein.

Let G be a simply connected absolutely almost simple linear algebraic group defined and isotropic over a global field K. Let U^+ be the unimpotent radical (which is defined over K) of a minimal parabolic K-subgroup P^+ of G. Let U^- be the unipotent radical of another minimal parabolic K-subgroup P^- of G which is *opposed* to P^+ in the sense that $U^+ \cap U^- = \{1\}$. Let S be a finite set of places of K including all the archimedian ones, if any. We call thering $A = O_S = \{x \in K; |x|_v \leq 1$ for all places v of K, *not* in $S\}$ the *ring of S-integers* in K. Choose a faithful representation $G \hookrightarrow GL_N$ defined over K and define $G(O_S) = \{g \in G; g_{ij} \in O_S, 1 \leq i,j \leq N\}$. The subgroups in G which are of finite index in $G(O_S)$ are called *S-arithmetic* groups. Define the S-rank of G to be the sum $\sum_{v\in S} K_v - rank(G)$. Given a non-zero ideal $\mathfrak{a}$ of A and an algebraic K-subgroup H of G define $H(\mathfrak{a}) = \{h \in H; h_{ij} \equiv \delta_{ij} (\mathrm{mod}\, \mathfrak{a})$, where $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j\}$. Let $\mathbf{A}(S)$ denote the ring of$S$-adélès of K.

THEOREM . *With the notation as above, let $E(\mathfrak{a})$ denote the group generated by $U^+(\mathfrak{a})$ and $U^-(\mathfrak{a})$. Then $E(\mathfrak{a})$ is an S-arithmetic subgroup of $G(\mathfrak{a})$* provided *$S - rank(G) \geq 2$ and $K - rank(G) = 1, Char(K) \neq 2$.*

REMARK. The theorem holds also when $K - rank(G) \geq 2$ and is proved for G a classical group of $K - rank(G) \geq 2$ in [**17**], G is a Chevalley group of $K - rank(G) \geq 2$ [**15**] and for G an arbitrary group of $K - rank(G) \geq 2$ [**11**].

The theorem is proved for $G = SL_2$ in [**18**] and Vaserstein has informed us that he has a proof (unpublished) of the theorem when $G = SU(2,1)$.

We now give an outline of the proof. The proposition of Section 1 says: a subgroup $F(\mathfrak{a})$ which is closely related to $E(\mathfrak{a})$ (and normalises $E(\mathfrak{a})$) has the property that given $g \in G(K)$ there exists a nonzero ideal $\mathfrak{a}$ of A such that $gF(\mathfrak{b})g^{-1} \subset F(\mathfrak{a})$. This is used to show that there is a completion $\widetilde{G}$ of $G(K)$ with respect to which the subgroups $G(\mathfrak{a})$ have open closures in $\widetilde{G}$. We then show that there is a continuous surjection π from $\widetilde{G}$ onto $G(\mathbf{A}(S))$ where $(\mathbf{A}(S))$ is the ring of S-adélès of K. The main point is then to show that the kernel C of π is central in $\widetilde{G}$. Then by appealing to [**13**], we are done.

In Section 2, we show that C is central when the semi-simple part of the Levi component of the minimal parabolic subgroup P^+ of G is isotropic over K_v for some $v \in S$. In Section 3, we prove the same when $G = SU(2,1)$ and in Section 4, by looking at suitable embeddings of $G = SU(2,1)$ and SL_2 in G, we prove that C is central even in the case of G for which the semisimple part mentioned above is anisotropic over K_v for all $v \in S$.

1. Construction of a completion $\widetilde{G}$ of $G(K)$.

NOTATION 1.1. Let $G, E(\mathfrak{a})$ be as in the introduction. Assume that $S - rank(G) \geq 2$ and that $K - rank(G) = 1$. Let $F(\mathfrak{a})$ denote the group generated by $U^+(\mathfrak{a}), U^-(\mathfrak{a})$, and $M(\mathfrak{a})$ where $M + P^+ \cap P^-$.

LEMMA 1.2.

(i) The group $F(\mathfrak{a})$ is Zariski dense in G.

(ii) More generally, if $\rho : G(K) \to GL_n(C)$ or if $\rho : G(K)^+ \to GL_n(C)$ is a homomorphism of abstract groups (C is algebraically closed), then the Zariski closure of $\rho(F(\mathfrak{a}) \cap G(K)^+$ is equal to the Zariski closure of $\rho(G(K)^+))$.

(iii) The Zariski closure of $\rho(G(K)^+)$ is connected.

Proof. The proof of (i) is easy: the Zariski closure of $F(\mathfrak{a})$ in G contains $U^+(\mathfrak{a})$ and $U^-(\mathfrak{a})$, therefore contains U^+ and U^- and therefore equals G.

Given a non-zero ideal $\mathfrak{f}$ of A, let $U_\mathfrak{f}^+$ denote the Zariski closure of $\rho(U^+(\mathfrak{f}))$. Clearly, if $\mathfrak{f} \subset \mathcal{C}$ and c is a nonzero ideal of A then $U_c^+ \subset U_b^+$. Since U_A^+ is Noetherian, there exists a nonzero ideal $\mathfrak{f}$ of A such that U_b^+ is minimal. Given any nonzero ideal c of A, we have $c \cap b \subset c$ and by minimality of U_b^+ , we have $U_b^+ = U_{c\cap b}^+ \subset U_c^+$. If $a \in P^+(K)$ is given, then there exists a nonzero ideal c of A such that $c \subset b$ and $aU^+(c)a^{-1} \subset U^+(b)$. Taking Zariski closures in $GL_n(C)$, we obtain: $\rho(a)U_c^+\rho(a)^+ \subset U_b^+ \subset U_c^+ = U_b^+$ which means that U_b^+ is normalised by $\rho(P^+(K))$. It is easy to show that

$$\bigcup_{a\in P^+(K)} aU^+(b)a^{-1} = U^+(K),$$

using the facts that for any nonzero integer m,

$$\bigcup_{\lambda\in K^*} \lambda^m b = K$$

and that P^+ contains a K-split torus. Therefore U_b^+ contains $\rho(U^+(K))$. We thus get: the Zariski closure of $\rho(F()) \cap G(K)^+)$ contains $U^+ \supset U_{\cap b}^+ = U_b^+$ which contains $\rho(U^+(K))$ and by symmetry the Zariski closure of $\rho(F() \cap G(K)^+)$ contains $\rho(U^-(K))$. This proves part (ii). Now (iii) follows from the fact that $(G(K)^+/$ centre) is an abstract *simple* group [**16**]. □

DEFINITION 1.3. Let L/K be an algebraic extension and $k \subset L$ a subfield. Suppose $f : G(K)^+ \to k$ is a function whose $G(K)^+$-translates on the left (or right) span a finite dimensional vector space (over k). We call f a $G(K)^+$-finite function.

COROLLARY 1.4. *Let L, k be as above, $f : G(K)^+ \to k$ a $G(K)^+$-finite function. Suppose f vanishes on $F(\mathfrak{a}) \cap G(K)^+$. (A) Then f vanishes on $G(K)^+$. (B) Moreover, $G(K)^+$-finite functions with values in k form an* integral domain.

Proof. (A) Immediate from (II) of Lemma 1.2. (B) Follows from (iii) of Lemma 1.2. □

LEMMA 1.5. *The group $M(A)$ is infinite.*

Proof. Suppose $Card(S) \geq 2$. The group M contains a K-split torus G_m since $1 = K - rank(M)$, and $G_m(A)$ contains, by the Dirichlet unit theorem, a free abelian group of $rank = (Card(S) - 1) \geq 1$.

Suppose $Card(S) = 1$, $S = \{v\}$. We have a nontrivial K-homomorphism $M \to G_m$, with kernel M_0. Now, $S - rank(M_0) = S - rank(M) - S - rank(G_m) \geq 2 - 1 = 1$. Therefore $M_0(K_v)$ is not compact; but, (by [**2**] and [**4**]), $M_0(A)$ is a cocompact lattice in $M_0(K_v)$ and so $M_0(A)$ is infinite. In particular $M(A)$ is infinite. □

We now state the main result of this section. We will prove it later in the section after proving some preliminary results.

PROPOSITION 1.6. *Given a nonzero ideal $\mathfrak{a}$ of A and an element of $g \in G(K)$, there exists a nonzero ideal b of A such that*

$$gF(b)g^{-1} \subset F(\mathfrak{a}).$$

NOTATION 1.7. The map $U^- \times M \times U^+ \to G$ given by $(u^-, m, u^+) \mapsto u^- m u^+$ is a K-isomorphism onto an open subset Ω of G. Given $x \in \Omega$, we may write $x = u_x^- m_x u_x$ with $u_x^- \subset U^-$, $m_x \in M$, $u_x \in U^+$ and $x \mapsto u_x$ is a K-rational function from Ω into U^+.

Given a nonzero ideal $\mathfrak{a}$ of A and $g \in G(K)$, consider the conjugate $g^{-1}F(\mathfrak{a})g = g^{-1}h^{-1}F(\mathfrak{a})hg$ for all $h \in F(\mathfrak{a})$. By Lemma 1.2, there exists an $h \in F(\mathfrak{a})$ such that $hg \in \Omega$ and so, by replacing g by hg if necessary we assume, as we may, that $g \in \Omega$, while looking at $g^{-1}F(\mathfrak{a})g$. Let b_1 be a nonzero ideal of A such that $g^{-1}G(a)g \supset G(b_1)$. Then for any $h \in F(\mathfrak{a}) \cap g^{-1}$ we have

$$g^{-1}h^{-1}F(\mathfrak{a})\,h\,g \supset g^{-1}h^{-1}P^{-}(\mathfrak{a})\,h\,g \cap P^{+} \supset (g^{-1}h^{-1}P^{-}\,h\,g \cap P^{+})(b_1)$$

$$= (u_{hg}^{-1}P^{-}u_{hg} \cap P^{+})(b_1) = (u_{hg}^{-1}P^{-}u_{hg} \cap P^{+})(b_1) = (u_{hg}^{-1}Mu_{hg})(b_1).$$

For $x \in \Omega$ denote by M_x the group $x^{-1}P^{-}x \cap P^{+} = u_x^{-1}MU_x$. Then $g^{-1}f(\mathfrak{a})g$ contains $\{M_{hg}(b_1); h \in F(\mathfrak{a}) \cap \Omega g^{-1}\}$. Denote by Δ_g the subgroup of $P^{-}(b)$ generated by $\{M_{hg}(b_1); h \in F(\mathfrak{a}) \cap \Omega g^{-1}\}$. We aim to show that Δ_g contains $P^{+}(b_g)$ for some nonzero ideal b_g of A, with $b_g \subset b$.

Let $h \in \{F(\mathfrak{a}) \cap \Omega g^{-1}\}$, with $M_{hg}(b_1) = (u_{hg}^{-1}Mu_{hg})(b_1), v_h = u_{hg}^{-1}u_g$ whence $M_{hg}(b_1) = (v_h M_g V_h^{-1})(b_1)$. There exists a nonzero ideal b_h of A such that $b_h \subset b_1$ and such that $\Delta_g \supset (v_h M_g v_h^{-1})(b_1) \supset v_h M_g(b_h)v_h^{-1}$. We also have $M_g(b_h) \subset M_g(b_1) \subset \Delta_g$. Denote by $[M_g(b_h), v_h]$ the subgroup of Δ_g generated by $\{mv_hm^{-1}m_h^{-1};\ m \in M_g(b_h)\}$. Then Δ_g contains $[M_g(b_H), v_h]$. Observe that $M_g(b_h)$ is normalised by $M_g(b_1) \subset \Delta_g$. Denote by $M_g(b_1)(v_h)$ the set $\{mv_hm^{-1};\ m \in M_g(b_1)\}$. Then we get: $\Delta_g \supset [M_g(b_k), M_g(b_1)(v_h)]$, and therefore $\Delta_g \supset [M_g(b_h), [M_g(b_1), v_h]]$. Let H_g be the subgroup generated by $\{[M_g(b_1), v_h]; h \in F(\mathfrak{a}) \cap \Omega g^{-1}\}$. Define $V^{+} = [U^{+}, U^{+}], W^{+} = U^{+}/V^{+}$ and $pr : U^{+} \to W^{+}$ the quotient map. Then V^{+} and W^{+} are finite dimensional K-vector spaces, on which $M(K)$ acts by K-linear transformations. We have the unique quotient $\pi : M_g \to \mathbf{G}_m$ defined over K. Let

$$M_g^0 = \left\{x = (x_v)_{v\in S} \in \prod_{v\in S} M(K_v);\ \prod_{v\in S} |\pi(x_v)| = 1\right\}$$

. Then (i) by [**2**] and [**4**], we have: $M_g(b_1)$ is a cocompact lattice in M_g^0; (ii) M_g^0 is compactly generated [**1**]; (iii) $M_g(b_1)$ is a finitely generated group. (This follows from (i), (ii) and [**5**].) Moreover every element of $M_g(b_1)$ is semisimple.

We assume, as we may, that b_1 is an ideal so deep that no nontrivial element of $M_g(b_1) - \{1\}$ has a nontrivial root of unity as an eigenvalue in its action on W^{+}. Let $\{\gamma; \gamma \in F\}$ be a finite nontrivial set of generators of $M_g(b_1)$. For $\theta \in M_g(b_1)$ let θ_* denote the linear transformation induced by θ on W^{+}.

If $\gamma \in F$, write $W_\gamma = (\gamma_* - 1)W^+$. Then $w \mapsto (\gamma_* - 1)w$ is a K-linear map of W^+ onto W_γ. Since γ is semisimple; (i) $w \mapsto (\gamma_* - 1)w$ is an isomorphism of W_γ onto itself (ii); W_γ is a direct sum of irreducible $K[\gamma]$-modules: $W_\gamma = \oplus W_j$; (iii) if $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$ denotes the subring generated by γ_* and γ_*^{-1} in $End_K(W_\gamma)$, then $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$ is a ring without nilpotent elements. By Schur's lemma, the commutant of the image of $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$ in $End_K(W_j)$ is a division algebra over K and therefore $\Im m\{\mathbf{F}_p[\gamma_*, \gamma_*^{-1}] \xrightarrow{p_j} End(W_j)\}$ is an integral domain and thus defines a prime ideal $\mathfrak{p}_j$ of $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$: $\mathfrak{p}_j = Ker(p_j)$. We thus get a finite set $X(\gamma)$ of prime ideals $\mathfrak{p}$ of $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$ and a decomposition $W_\gamma = \bigoplus_{\mathfrak{p} \in X(\gamma)} W_\mathfrak{p}$ of $K[\gamma_*, \gamma_*^{-1}]$-modules such that the homomorphism $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}] \to End_K(W_\mathfrak{p})$ has kernel $\mathfrak{p}$. Moreover, $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$ is a reduced ring acting faithfully on W_γ whence $\bigcap_{\mathfrak{p} \in X(\gamma)} \mathfrak{p} = (0)$. Let $\pi_\mathfrak{p} \in \mathfrak{p} - \bigcup_{\mathfrak{p} \in X(\gamma) - \{\mathfrak{p}\}} q; p\gamma_\mathfrak{p} : W_\gamma \to W_\mathfrak{p}$ denote the map $w \mapsto \left(\prod_{q \neq \mathfrak{p}} \pi_q\right) w$. Then $pr_\mathfrak{p} | W_\mathfrak{p} : W_\mathfrak{p} \to W_\mathfrak{p}$ is nonsingular. We also denote by $pr_\mathfrak{p}$ the composite $U^+ \xrightarrow{pr} W^+ \xrightarrow{(\gamma - 1} W_r \xrightarrow{pr_\mathfrak{p}} W_\mathfrak{p}$.

REMARK 1.8. Let $H \subset U^+(K)$ be a subgroup normalised by $M_g(b)$. Then $pr_\mathfrak{p}(H) \subset W_\mathfrak{p}$ is an $(\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]/\mathfrak{p})$-module. Moreover, $pr(H)$ contains $pr_\mathfrak{p}(H)$.

Proof. Clearly $pr(H)$ is a subgroup of W^+, is therefore $\mathbf{F}_p$-stable and hence $pr(H)$ is an $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$-module. Since $pr_\mathfrak{p} : W_\gamma \to W_\mathfrak{p}$ and $W^+ \to W_\gamma$ are given by multiplication by elements of $\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]$, we have: $pr_\mathfrak{p}(H) \subset \mathbf{F}_p[\gamma_*, \gamma_*^{-1}](pr_\mathfrak{p}(H)) \subset \mathbf{F}_p[\gamma_*, \gamma_*^{-1}](pr(H)) \subset pr(H)$. □

NOTATION 1.9. Let k_p denote the quotient field of the domain $A_p = \mathbf{F}_p[\gamma_*, \gamma_*^{-1}]/\mathfrak{p}$. Now, $W_\mathfrak{p}$ is an $(\mathbf{F}_p[\gamma_*, \gamma_*^{-1}]/\mathfrak{p})$-module and hence is a $k_\mathfrak{p}$-vector space as well as a K-vector space. [We use the fact that $W_\mathfrak{p}$ splits as a direct sum of irreducible $K[A_\mathfrak{p}]$ modules W_i and $A_\mathfrak{p}$ acts faithfully on each W_i (γ does not have roots of unity as eigenvalue) and by Schur's lemma, the commutant of $A_\mathfrak{p}$ is a *division ring* D whence $k_\mathfrak{p} \subset D$ and acts on W_i. Thus $k_\mathfrak{p}$ acts on $W_\mathfrak{p}$ too.] Let $R_\mathfrak{p}$ be the subring of $End_K(W_\mathfrak{p})$ generated by $k_\mathfrak{p}$

and K. Then $R_{\mathfrak{p}}$ is a finite dimensional K-vector space and since γ acts semisimply on $W_{\mathfrak{p}}, R_{\mathfrak{p}}$ is a product of finite field extensions of K. Now K is a global field and $k_{\mathfrak{p}}$ is an infinite field (again, $k_{\mathfrak{p}}$ is infinite because γ has no root of unity as an eigenvalue) and so $k_{\mathfrak{p}}$ is also a global field, whence $R_{\mathfrak{p}}$ is finite dimensional over $k_{\mathfrak{p}}$. Now $W_{\mathfrak{p}} = \oplus W_i \cong \oplus \Im m(R_{\mathfrak{p}})$ and so $W_{\mathfrak{p}}$ is finite dimensional over $R_{\mathfrak{p}}$ and therefore $W_{\mathfrak{p}}$ is a finite dimensional $k_{\mathfrak{p}}$-vector space.

LEMMA 1.10. *Given $\gamma \in F$ and $\mathfrak{p} \in X(\gamma)$, there exists a finite set $\{v_h\}$ of elements of $U^+(K)$, for $h \in F(\mathfrak{a}) \cap \Omega g^{-1} \cap G(K)^+$, such that the $k_{\mathfrak{p}}$-span of $\{pr_{\mathfrak{p}}[\gamma, v_h]\}$ is all of $W_{\mathfrak{p}}$.*

Proof. Let $\lambda : W_{\mathfrak{p}} \to k_{\mathfrak{p}}$ be a linear form over $k_{\mathfrak{p}}$ which vanishes on all $\{pr_{\mathfrak{p}}[\gamma, v_h];\ h \in F(\mathfrak{a}) \cap \Omega g^{-1}\}$. Then $\varphi(h) = \lambda \circ pr_{\mathfrak{p}}[\gamma, v_h]$ (for $h \in \Omega g^{-1}$) has the property: $\varphi(h) = 0$ for $h \in F(\mathfrak{a}) \cap \Omega g^{-} \cap G(K)^+$. Now $pr_{\mathfrak{p}}[\gamma, v_h] = pr_{\mathfrak{p}}[\gamma_*, pr(v_h)]$ and $pr(v_h) = \dfrac{A(h)}{B(h)}$ with $A(h) \in W^+$ and $B(h) \in K$; both $A(h)$ and $B(h)$ are polynomial functions on $G(K)$ with $B(h) \neq 0$ for all $h \in \Omega g^{-1}$. We think of K as embedded in $R_{\mathfrak{p}}$. Let $\{\in\}$ be a $k_{\mathfrak{p}}$-basis of $R_{\mathfrak{p}}$ and write $B(h) = \sum_{\in} B_{\in}(h) \in$. The function $B(h)$ is polynomial on $G(K)^+$ and hence the $k_{\mathfrak{p}}$-valued function $B_{\in}(h)$ is a $G(K)^+$-finite function. Now $B(h)^{-1} \in K$ hence $B(h)^{-1} = \sum X_{\in}(h) \in, X_{\in}(h) \in k_{\mathfrak{p}}$. Thus $\{X_{\in}(h)\}$ are solutions of linear equations whose coefficients are $k_{\mathfrak{p}}$-valued $G(K)^+$-finite functions on $G(K)^+$, and by Corollary 1.4, such functions form a domain. We may thus assume that $X_{\in}(h)$ belong to the quotient field of $R_{\mathfrak{p}}$, and write $x_{\in}(h) = \dfrac{Y_{\in}(h)}{Z(h)}$, where $Y_{\in}, Z : G(K)^+ \to k_{\mathfrak{p}}$ are $G(K)^+$-finite functions. We finally get

$$\varphi(h) = \lambda \circ pr_{\mathfrak{p}}[\gamma_* - 1][pr(v_h)] = \lambda \circ pr_{\mathfrak{p}}[\gamma_* - 1].\left[\frac{A(h)}{B(h)}\right] =$$

$$\lambda \circ pr_{\mathfrak{p}}(\gamma_* - 1)\left(\frac{C(h)}{Z(h)}\right) = \frac{\lambda \circ pr_{\mathfrak{p}}((r_* - 1)C(h))}{Z(h)}$$

(since λ is $k_{\mathfrak{p}}$-linear) and $\varphi(h)$ vanishes on $F(\mathfrak{a}) \cap \Omega g^{-} \cap G(K)^+$. Therefore $\lambda \circ pr_{\mathfrak{p}}(\gamma_* - 1)C(h) = \psi(h)$ is a $G(K)^+$-finite function which vanishes on $F(\mathfrak{a}) \cap \Omega g^{-} \cap G(K)^+$, and $G(K) - \Omega g^{-1}$ is the set of zeros of a polynomial $\eta(h) = \sum \eta_{\in}(h) \in$. Thus, for all $\in \psi(h)\eta_{\in}(h) \equiv 0$ on $G(K)^+ \cap F(\mathfrak{a})$ and by Corollary 1.4, part (ii), $\psi(h) \equiv 0$ on $G(K)^+$. This means that $\varphi(h) = \lambda \circ (pr_{\mathfrak{p}}(\gamma_* - 1)pr(v_h)) = 0$ for all $h \in G(K)^+ \cap \Omega g^{-1}, v_h = u_{h_g}^{-1} u_g$. Taking $h = Zg^{-1}, Z \in U^+(K)$, we get: $V_h = Z^{-1}u_g$ represents an arbitrary element of $U(K)^+$, and

$$0 = \lambda \circ (pr_{\mathfrak{p}}(\gamma_* - 1)pr(U^+(K))) = \lambda \circ (pr_{\mathfrak{p}}(\gamma_* - 1)W^+) = \lambda(W_{\mathfrak{p}}).$$

Thus $\lambda = 0$ on $W_{\mathfrak{p}}$ whenever $0 = \lambda \circ (pr_{\mathfrak{p}}[\gamma, u_h], (h \in F(\mathfrak{a}) \cap \Omega g^{-1} \cap G(K)^+))$. Hence $\{pr_{\mathfrak{p}}[\gamma, V_h]; h \in F(\mathfrak{a}) \cap \Omega g^{-1}\}$ contains a $k_{\mathfrak{p}}$-basis of $W_{\mathfrak{p}}$, but $W_{\mathfrak{p}}$ is finite dimensional, whence the lemma follows. □

LEMMA 1.11. *There exists a finite set $\{v_h\} = X$ of elements of $U^+(K)$ with $h \in F(\mathfrak{a}) \cap G(K)^+ \cap \Omega g^{-1}$ such that (i) for every $\gamma \in F$ and $\mathfrak{p} \in X(\gamma)$, we have, the $k_{\mathfrak{p}}$-span of $pr_{\mathfrak{p}}[\gamma, v_h]$ is all of $W_{\mathfrak{p}}$ (ii) $[\gamma, v_h] \in H_g$ for all $\gamma \in F, v_h \in X$. We denote by H_X the group generated by $\{[\theta, v_h] : v_h \in X\theta, \in M_g(b_1)\}$.*

Proof. We get a finite set $X_{\gamma,\mathfrak{p}} = \{v_h\}$ satisfying the conditions of Lemma 1.10. Take $X = UX_{\gamma,\mathfrak{p}}$. □

LEMMA 1.12. *Let c be a nonzero ideal of A, contained in b. Then there exist a nonzero ideal $c_{\mathfrak{p}}$ of $(\mathbf{F}_{\mathfrak{p}}[\gamma_*, \gamma_*^{-1}]/\mathfrak{p})$ and a subgroup $H_c \subset U^+_{(c)} \cap H_X$ such that*

$$pr_{\mathfrak{p}}(H_c) \supset \sum_{v_h \in X} c_{\mathfrak{p}}(pr_{\mathfrak{p}}[\gamma, v_h]).$$

Proof. We have $pr_{\mathfrak{p}}[\gamma, v_h] = (\gamma_* - 1)pr_{\mathfrak{p}}(v_h)$. Now, for any integer $N, pr_{\mathfrak{p}}[\gamma^N, v_h] = (1 + \gamma_* + \cdots + \gamma_*^{N-1})pr_{\mathfrak{p}}[\gamma, \gamma_h] \in k_{\mathfrak{p}}^* pr_{\mathfrak{p}}[\gamma, v_h]$ because γ_* has no torsion eigenvalues. Therefore the $k_{\mathfrak{p}}$-span of $\{pr_{\mathfrak{p}}[\gamma^N, v_h]; v_h \in X\} = k_{\mathfrak{p}}$-span of $\{pr_{\mathfrak{p}}[r; v_h]; v_h \in X\}$ which by Lemma 1.11 is all of $W_{\mathfrak{p}}$. Choose now an integer N such that $[\gamma^N, v_h] \in U^+(c)$ for all $v_h \in X$. Let $c_{\mathfrak{p}} \subset \mathbf{F}_{\mathfrak{p}}[\gamma_*, \gamma_*^{-1}]/\mathfrak{p}$ be the ideal generated by $(1 + \gamma_* + \cdots + \gamma_*^{N-1})$. Let H_c be the smallest subgroup of $U^+(c)$ containing $\{[\gamma^N, v_h]; v_h \in X\}$ and normalised by

$M_g(b)$. Then H_c is clearly contained in $U^+(c) \cap \Delta_g(\gamma^{-1}v_h\gamma v_h^{-1} \in \Delta_g$ for $\gamma \in M_g(b_1))$. Moreover, by Remark 1.8,

$$pr_{\mathfrak{p}}(H_c) \supset \sum_{v_h \in X} (\mathbf{F}_{\mathfrak{p}}[\gamma_*, \gamma_*^{-1}]/\mathfrak{p}) \cdot (1 + \gamma_* + \cdots + \gamma_*^{N-1}) pr_{\mathfrak{p}}[\gamma, v_h] \supset$$

$$\supset \sum_{v_h \in X} c_{\mathfrak{p}} pr_{\mathfrak{p}}[\gamma, v_h].$$

□

LEMMA 1.13. *Given a nonzero ideal C of A contained in b, there is a subgroup $H_c \subset U^+(c) \cap H_X$ such that $pr(H_c)$ contains $W^+(b_3)$ where b_3 is a nonzero ideal of A contained in c.*

Proof. We have: $R_{\mathfrak{p}} \bigotimes_K \left(\prod_{v \in S} K_v\right)$ is a product of local fields L_w. Let

$$S_1 = \{w; |\gamma|_{L_w} < 1\}, S_2 = \{w; |\gamma|_{L_w} > 1\}, \text{ and } S_3 = \{w; |\gamma|_{L_w} = 1\}.$$

Let k_1(resp. k_2) be the closure of $k_{\mathfrak{p}}$ in $\prod_{w \in S_1} L_w$ $\left(\text{resp. in } \prod_{w \in S_2} L_w\right)$. Now $\mathbf{F}_{\mathfrak{p}}[\gamma_*, \gamma_*^{-1}]/\mathfrak{p}$ is a lattice in $k_1 \times k_2$. Since $_{\mathfrak{p}}$ is a (faithful) $R_{\mathfrak{p}}$-module, the module $W_{\mathfrak{p}} \otimes_K \prod_{v \in S} K_v$ is a direct sum of $\{L_w\}$, with multiplicity m_w. Let U_3 be a compact open subgroup of $\oplus_{w \in S_3} m_w L_w$. Then $\sum_{v_h \in X} c_{\mathfrak{p}} pr_{\mathfrak{p}}[\gamma, v_h]$ contains a lattice in

$$U_p = \sum k_1 pr_{\mathfrak{p}}[\gamma, v_h] + \sum k_2 pr_{\mathfrak{p}}[\gamma, v_h] + U_3.$$

Now $\{pr_{\mathfrak{p}}([\gamma, v_h]) : v_h \in X\}$ contains a $k_{\mathfrak{p}}$-basis of $w_{\mathfrak{p}}$ and since k_i is a local field ($i = 1, 2$), each $\{L_w; w \in S_i\}$ is a finite dimensional vector space over k_i and $\sum k_i pr_{\mathfrak{p}}[\gamma, v_h] = \sum_{w \in S_i} m_w L_w$. Thus, $U_{\mathfrak{p}}$ contains the nonzero $\prod_{v \in S} K_v$-submodule $\sum_{w \in S_1 U S_2} m_w L_w = E_{\mathfrak{p}}$. Write $E_g = \sum_{\mathfrak{p} \in X(\gamma)} \sum_{x \in M_g(b)} x_*(E_{\mathfrak{p}})$. This is also a $\left(\prod_{v \in S} K_v\right)$-submodule of

$W \bigotimes_K \prod_{v \in S} K_v$, which is stable under M_g^0 (since it is stable under the Zariski closure of $M_g(b)$: by finite dimensionality, the sum over $x \in M_g(b)$ is really a finite sum). We look at the action of γ on $(W^+ \otimes \prod K_v)/E_\gamma$. By the definition of S_1 and S_2, γ has only bounded eigenvalues in its action on W^+/E_γ. Now the space $\sum_{\gamma \in F} E_\gamma$ is also M_g^0 stable and on $\left(W^+ \otimes \prod K_v\right)/\sum_{\gamma \in F} E_\gamma$, every element γ of f acts with bounded eigenvalues. We now use the fact that $\left(\prod_{v \in S} U^+(K_v)\right) \rtimes M_g^0$ is compactly generated, to conclude $\left((W^+ \otimes \prod K_v) \rtimes M_g^0 \text{ and therefore}\right) \left(\prod_{v \in S} K_v \otimes W^+\right) / \sum_{\gamma \in F} E_\gamma \rtimes M_g^0$ is compactly generated. On the other hand, the image og M_g^0 in $Aut\left[(\prod K_v) \otimes W^+ / \sum_{\gamma \in F} E_\gamma\right]$ is bounded, as we have just observed. This implies that

$$W^+ \otimes \prod_{v \in S} K_v = \sum_{\gamma \in F} E_\gamma = \sum_{\gamma \in F} \sum_{\mathfrak{p} \in X(r)} \sum_{x \in M_g(b)} x_*(E_\mathfrak{p}) = \sum_{\gamma, \mathfrak{p}, x} x_*(U_\mathfrak{p})$$

$$\left(E_\mathfrak{p} \subset U_\mathfrak{p} \subset W \otimes \prod K_v\right).$$

We have: $pr_\mathfrak{p}(H_c) \cap U_\mathfrak{p} (\subset pr(H_c) \cap U_\mathfrak{p})$ contains a *lattice* in $U_\mathfrak{p}$ whence $pr(H_c)$ contains a lattice L_c in $W^+ \otimes \prod_{v \in S} K_v$, such that (i) $L_c \subset \sum_{\gamma, \mathfrak{p}} pr_\mathfrak{p}(H_c) \cap U_\mathfrak{p} \subset W^+(c\lambda)$ by Lemma 1.12. (Here $\lambda \in K^*$ is such that for all ideals $\mathfrak{a}$ of A, $pr(U^+(\mathfrak{a})) \subset W^+(\mathfrak{a}, \lambda)$), (ii) L_c is $M_g(b)$-stable. It can then be shown easily (see [**13**], Section (2.10)) that $\overline{L}_c \supset W^+(b_2)$, whenever $L_c \subset W^+ \otimes \prod_{v \in S} K_v$ is a *lattice* satisfying (i) and (ii), where $b_2 \subset A$ is a nonzero ideal. Take $b_3 = b_2 \cap \mathcal{C}$. The proof of the lemma is over. □

LEMMA 1.14. *There exists a non-zero ideal b_4 of A such that Δ_g contains $U^+(b_4)$.*

Proof. From Lemma 1.13, we have any nonzero ideal $\mathcal{C}$ of A, an H_c such that $H \supset H_c, H_c \subset U^+(c)$ and $pr(H_c) \supset W^+(b_3)$, with

$\mathfrak{b}_3 \subset \mathcal{C} \subset \mathfrak{b}$. Now, $[W^+(\mathfrak{a}), W^+(\mathfrak{a})]$ contains $V^+(\mathfrak{a}^2\mu)$ for a fixed $\mu \in K^*$ and varying nonzero ideals $\mathfrak{a}$ of A. In particular, $[H_c, H_c]$ contains $[W^+(\mathfrak{b}_3), W^+(\mathfrak{b}_3)] \supset V^+(\mathfrak{b}_3^2\mu)$, whence $H_X \supset V^+(\mathfrak{b}_3^2\mu)$. Let $\mathfrak{b}_4 \subset \mathfrak{b}_3^2\mu \cap \mathfrak{b}_3\lambda^{-1} \cap A$. Then for $x \in U^+(\mathfrak{b}_4)$ we have $pr(x) \in W^+(\mathfrak{b}_3)$ (by definition of λ) $\subset pr(H_c)$ and so (14) there exists an $h \in H_c$ such that $xh^{-1} \in V^+(c)$. Thus $U^+(\mathfrak{b}_4) \subset H_cV^+(c) \subset H_XV^+(c)$. Now we replace c by $c \cap \mathfrak{b}_3\mu = c'$. Then for the corresponding ideals $\mathfrak{b}_3'$, $\mathfrak{b}_3'$ we have: $U^+(\mathfrak{b}_4') \subset H_XV^+(c') \subset H_XV^+(\mathfrak{b}_3\mu) \subset H_X$. We recall that $\Delta_g = [M_g(\mathfrak{b}_h), [M_g(\mathfrak{b}_1), v_h]]$ and that for $v_h \in X$, we have $[M_g(\mathfrak{b}_1), v_h] \in H_X$. Therefore if $\mathfrak{b}_5 = \cup_{v_h \in X} \mathfrak{b}_h$, then $\Delta_g \supset [M_g(\mathfrak{b}_5), H_X]$ and we have just shown that $H_X \supset U^+(\mathfrak{b}_4)$. Thus $\Delta_g \supset [M_g(\mathfrak{b}_5), U^+(\mathfrak{b}_4)]$. Again, by argumments similar to (2.10) of [**13**], it is easy to show that $[M_g(\mathfrak{b}_5), U^+(\mathfrak{b}_4)] \supset U^+(\mathfrak{b}_6)$, for a nonzero ideal $\mathfrak{b}_6$ of A. This proves the lemma. □

We now complete the proof of Proposition 1.6: we have seen that $g^{-1}F(\mathfrak{a})g \supset \Delta_g \supset U^+(\mathfrak{b}_6)$ and $\Delta_g \supset M_g(\mathfrak{b}_1)$. The group generated by $U^+(\mathfrak{b}_6)$ and $M_g(\mathfrak{b}_1)$ contains $P^+(\mathfrak{b}_+)$ for some nonzero ideal $\mathfrak{b}_+$ of A, hence $g^{-1}F(\mathfrak{a})g \supset P^+(\mathfrak{b}_+)$. By symmetry $g^{-1}F(\mathfrak{a})g \supset P^-(\mathfrak{b})$ for a nonzero ideal $\mathfrak{b}$ of A whence $g^{-1}F(\mathfrak{a})g \supset F(\mathfrak{b})$, with $\mathfrak{b} = \mathfrak{b}_- \cap \mathfrak{b}_+$.

NOTATION AND DEFINITIONS 1.15. We construct $\mathcal{G}$. Consider the group $G(K)^+$ (instead of $G(K)$). By [7], $G(K)/G(K)^+$ is finite and therefore we may (and we do) replace $G(A), G(\mathfrak{a})$ and $F(\mathfrak{a})$ by their intersections with $G(K)^+$ without affecting questions of S-arithmeticity. We denote the intersections by $G(A), G(\mathfrak{a})$ and $F(\mathfrak{a})$. Define a topology on $G(K)^+$ by taking the sets $\{gF(\mathfrak{a}); g \in G(K)^+$, a nonzero ideal of $A\}$ to be open. We then get a left uniform structure and a right uniform structure on $G(K)^+$. We now call a sequence $\{x_n\}$ in $G(K)^+$ to be Cauchy if and only if $\{x_n\}$ is Cauchy with respect to both the uniform structures on $G(K)^+$ i.e. if and only if for every non-zero ideal $\mathfrak{a}$ of A, there exists an integer $l = l(\mathfrak{a}) \geq 0$ such that $x_n^{-1}x_m \in F(\mathfrak{a}), x_mx_n^{-1} \in F(\mathfrak{a})$ for all $m, n \geq l$. Define two Cauchy sequences $\{x_n\}, \{y_n\}$ to be *equivalent* if and only if for every nonzero ideal $\mathfrak{a}$ of A, there exists an integer $l = l(\mathfrak{a}) \geq 0$ such that $x_n^{-1}y_n \in F(\mathfrak{a}), x_ny_n^{-1} \in F(\mathfrak{a})$ for all $n \geq l$. It is now routine to check that equivalence classes of Cauchy sequences in $G(K)^+$ form a topological group $\mathcal{G}$ with $G(K)^+$ being a dense subgroup. Let C be the kernel of the map $\mathcal{G} \to G(\mathbf{A}(S))$. By [**12**] ,Lemma

(2.10), the map is surjective. Clearly C is a closed normal subgroup og $\mathcal{G}$. We also observe that $U^+(\mathbf{A}(S))$ and $U^-(\mathbf{A}(S))$ are embedded in $\mathcal{G}$ (as closures of $U^+(K)$ and $U^-(K)$ respectively).

LEMMA 1.16. *Suppose C is centralised by $G(K)^+$. Then C is centralised by $G(K)^+$. Then C is finite and $F(\mathfrak{a})$ is an S-arithmetic subgroup of $\mathcal{G}(K)^+$.*

Proof. Let $\overline{F(\mathfrak{a})}$ be the closure of $F(\mathfrak{a})$ in $\mathcal{G}$. Then $\overline{F(\mathfrak{a})}$ is open in $\mathcal{G}$ and therefore $C \cap \overline{F(\mathfrak{a})}$ is open in C. By assumption, and density of $G(K)^+$ in $\mathcal{G}$, we see that C is central in $\mathbf{G}$ and so we get a central extension

$$1 \to C/C \cap \overline{F(\mathfrak{a})} \to \mathcal{G}/C \cap \overline{F(\mathfrak{a})} \to G(\mathbf{A}(S)) \to 1,$$

where $C/C \cap \overline{F(\mathfrak{a})}$ is a *discrete* group. Thus $\mathcal{G}/C \cap \overline{F(\mathfrak{a})}$ is a locally compact central extension of $G(\mathbf{A}(S))$, split over $G(K)^+$ and by [**10**], $C/C \cap \overline{F(\mathfrak{a})}$ is a quotient of $\mu(K)$ the group of n^{th}-roots of unity in K for all n. This shows that C itself is finite, and so, $F(\mathfrak{a})$ is S-arithmetic (see proof of (1.10) in [**11**]). □

NOTATION 1.17. Let $G_\mathfrak{a}$ denote the closure of $F(\mathfrak{a})$ in $G(K)^+$ in the S-congruence topology on $G(K)^+$. Then, by [**12**], $G_\mathfrak{a}$ is a congruence subgroup. Since $F(\mathfrak{a})$ is stable under conjugation by $M(A)$, we see that $M(A)$ acts by conjugation on the double coset $F(\mathfrak{a})\backslash G(\mathfrak{a})/F(\mathfrak{a})$. Let H be a K-isotropic K-simple algebraic K-subgroup of G, let $\mathcal{H}$ be the closure of $H \cap G(K)^+$ in $\mathcal{G}, H_0$ the closure of $H \cap G(K)^+$ in $G(\mathfrak{a}(S)), H_0$ is the closure of $H \cap F(\mathfrak{a})$ in the S-congruence topology on $G(K)^+$. We get an extension $1 \to C \cap \mathcal{H} \to \mathcal{H} \to H_0 \to 1$.

LEMMA 1.18. *Suppose a subgroup B of $M(A)$ acts trivially on the* subset *$F(\mathfrak{a})\backslash F(\mathfrak{a})H_\mathfrak{a}F(\mathfrak{a})/F(\mathfrak{a})$ of the double coset $F(\mathfrak{a})\backslash F(\mathfrak{a})\mathcal{H}F(\mathfrak{a})/F(\mathfrak{a})$, for all but finitely many nonzero ideals $\mathfrak{a}$ of A. Then $C \cap \mathcal{H}$ is centralised by B.*

Proof. Let $c \in C \cap \mathcal{H}$ and $b \in B$. Then $c = \lim_{m\to\infty}(h_m)$ for a Cauchy sequence $\{h_m\}$ in H. Since $c \in C$, its image in $G(\mathbf{A}(S))$ is

1, i.e. $h_m \in H$ if $m \geq l(\mathfrak{a})$, for any fixed nonzero ideal $\mathfrak{a} \subset A$ which is sufficiently deep. Therefore $bh_m b^{-1} = \xi_m h_m \eta_m$ (by assumption) where $\xi_m, \eta_m \in F(\mathfrak{a})$. This shows that $\xi_m \to 1$ and $\eta_m \to 1$ in $\mathbf{G}$, which implies that $bcb^{-1} = c$. □

2. Centrality of C when M_0 is not abelian.

NOTATION 2.1. We denote by M_0, the connected component of identity of the Zariski closure M_1 of $M(A)$. We assume in this section that $[M_0, M_0]$ is not trivial. Therefore $[M_0, M_0]$ is a semisimple K-group, let $\widetilde{M}_1$ denote the simply connected cover of $[M_0, M_0]$. Now, $\widetilde{M}_1(A)$ is Zariski dense in $\widetilde{M}_1$ since $M_1(A) \cap M_0$ is Zariski dense in M_0. Since $\widetilde{M}_1$ is simply connected, by [**8**] and [**9**], $\widetilde{M}_1(A)$ has strong approximation.

LEMMA 2.2. *There exists a congruence subgroup B of $\widetilde{M}_1(A)$ such that for any two nonzero ideals $\mathfrak{a}$ and b of A with $\mathfrak{a} + b = A$, the group generated by $\widetilde{M}_1(\mathfrak{a})$ and $\widetilde{M}_1(b)$ contains B.*

Proof. This is an easy consequence of strong approximation. For details see [**12**], Section (4.12). □

2.3. PROOF OF CENTRALITY. We borrow the notation of (4.8) of [**12**]. Let $f(g)$ be the function defined there. Write, as in (1.5), $g = u_g^- m_g u_g$ for $g \in G_{\mathfrak{a}}$. This can be done if $\mathfrak{a}$ is a sufficiently deep ideal. With respect to the representation W in (4.8) of [**12**], $f(g)$ is defined, and u_g^-, m_g, u_g have the properties: $f(g) \equiv 1 (mod\ \mathfrak{a})$,

$$f(g)^N((u_g^-)_{ij} - \delta_{ij}), f(g)^N[(m_g)_{ij} - \delta_{ij}], f(g)^N[(u_g)_{ij} - \delta_{ij}] \in$$

where N is a large integer depending only on (G, W) and if $T \in End(W), T_{ij}$ denotes its $(ij)^{th}$ entry of viewed as a matrix, with respect to the basis defined in (4.8), [**12**]. Let B be as in (2.2). Take $\theta \in \widetilde{M}_1(f(g)^{2N})$. Then $\theta g \theta^{-1} = (\theta u_g^- \theta^{-1})(\theta m_g \theta^{-1})(\theta u_g \theta^{-1}) = [\theta, u_g^-] u_g^- m_g u_g [(m_g u_g)^{-1}, \theta]$ and $[\theta, u_g^-]$ and $[(m_g u_g)^{-1}, \theta]$ lie in $F(\mathfrak{a})$. This shows that in $F(\mathfrak{a}) \backslash G(\mathfrak{a}) / F(\mathfrak{a})$, $\widetilde{M}_1(f(g)^{2N})$ acts trivially on g. Since $F(\mathfrak{a})$ is dense in G_a in the S-congruence topology on $G(K)^+$, one can find $h \in F(\mathfrak{a})$ such that $gh \equiv 1 \ mod(f(g)^{2N})$, and therefore $f(g)^{2N}$ and $f(gh)^{2N}$ are coprime. We have proved that $\widetilde{M}_1(f(gh)^{2N})$ fixes $gh \equiv g$ in the double coset. Apply Lemma 2.2 to conclude that B fixes every g in the double coset $F(\mathfrak{a})\backslash G(\mathfrak{a})/F(\mathfrak{a})$. Now , by Lemma 1.18, C is centralised by $B \subset G(K)^+$, and since $G(K)^+$ is simple modulo its centre, $G(K)^+$ centralises C.

3. Centrality of C when $G = SU(2,1)$. We first prove a lemma which is very similar to Lemma (2.1) of [**14**].

LEMMA 3.1. *Suppose a and b are two elements of A such that $aA + bB = A$. Let L/K be a finite separable extension. Consider the K-group $T = R_{L/K}(\mathbf{G}_m)$ where $R_{L/K}$ is the Weil restriction of scalars, let N be a positive integer and consider the group $T_{a,b,N}$ in $T(A)$ generated by $\{T((a+bx)^N); x \in A\}$. Then the index $f_{a,b,N}$ of $T_{a,b,N}$ in $T(A)$ is bounded by a constant independent of a, b.*

Proof. It is easy to reduce to the case when L/K is a Galois extension. Let $d =$ degree of (L/K). We will show that $f_{a,b,N} \le G(d,N,K)$ where G is a function of d, N and K. Let $\widetilde{S}$ be the places of L lying above the places of S. Then $T(A) = T(O_S)$ is commensurable with $O^*_{\widetilde{S}} = \mathbf{G}_m(O_{\widetilde{S}})$. Moreover if $\mathfrak{a} \subset A$ is a nonzero ideal and $\widetilde{\mathfrak{a}} = \mathfrak{a} \otimes_{O_S} O_{\widetilde{S}}$ denotes the ideal in $O_{\widetilde{S}}$ generated by $\mathfrak{a}$, then $T(\mathfrak{a}) = \mathbf{G}_m(\widetilde{\mathfrak{a}})$. Now $T(A)/T_{a,b,N}$ is a quotient of $T(A)/T[(a+bx)^N] = \mathbf{G}_m(O_{\widetilde{S}})/\mathbf{G}_m[(\widetilde{a+bx})^N]$ and the latter is a subgroup of $(O_{\widetilde{S}}/(\widetilde{a+bx})^N)^*$ the group of units in $(O_{\widetilde{S}}/(\widetilde{a+bx})^N)$. This shows that if $\varphi[(a+bx)^N]$ denotes the cardinality of $(O_{\widetilde{S}}/(\widetilde{a+bx})^N)^*$, then $f_{a,b,N}$ divides $\varphi[(a+bx)^N]$ for all $x \in A$. We have, therefore:

$$f_{a,b,N} \le gcd\{\varphi(a+bx)^N : x \in A\}.$$

Write $a + bx = \mathfrak{p}_1 \cdots \mathfrak{p}_k$, a product of primes of A. Each $\mathfrak{p}_i$ decomposes as a product of primes $\mathcal{B}$ of $O_{\widetilde{S}}$. Hence

$$\left(\widetilde{a+bx})^N = \prod_{i=1}^{k}(\prod_{\beta|\mathfrak{p}}\beta\right)^N.$$

Therefore

$$\varphi[(a+bx)^N] = \prod_{i=1}^{k} \prod_{\beta|\mathfrak{p}_i}^{k} (Norm\,\beta)^{N-1}(Norm\beta - 1).$$

Since L/K is Galois, for a given $\mathfrak{p}_i$, we have $Norm\,\beta = (Norm\,\mathfrak{p}_i)^{f_i}$ for some integer f_i dividing d, for each $\beta|\mathfrak{p}_i$. Moreover the number f_i of β lying above $\mathfrak{p}_i$ also divides d (in fact $f_i r_i$ divides d). We thus get:

$$\text{(1)} \quad \varphi[(a+bx)^M] = \prod_{i=1}^{k} (Norm\,\mathfrak{p}_i)^{(N-1)f_i r_i}[(Norm\,\mathfrak{p}_i)^{f_i} - 1]^{r_i}.$$

Let $l > 1$ be a prime and suppose $l^e | gcd\{\varphi[(a+bx)^N]; x \in O_S\}$. Then by (1) we have:

$$\text{(2)} \qquad l^e | \prod_i (N\mathfrak{p}_i)^{(N-1)f_i r_i}((Norm\,\mathfrak{p}_i)^{f_i} - 1)^{r_i}.$$

Case 1: $Char(K) = 0$ or $N = 1$:

Let e' be the smallest integer such that $4de' \geq e$. Then $e' = [\frac{e}{4d} - 1] + 1$, where $x \mapsto [x]$ is the "integral part" function. Let $q > 1$ be a prime, suppose q^h divides the degree $d(e')$ of $K(\sqrt[l^{e'}]{1})/K$. We may write

$$\text{(3)} \qquad (a, K(\sqrt[l^{e'}]{1})/K) = \sigma^m$$

where $(a, K(\sqrt[l^{e'}]{1})/K)$ is the Artin symbol and $\sigma \in Gal(K(\sqrt[l^{e'}]{1})/K)$ is a generator. Let K_b/K be the classifield corresponding to (b) in **A**. Let E be the compositum of K_b and $K(\sqrt[l^{e'}]{1})/K$ is σ.

(A) If q is odd or if q is 2 and m even, then $x(m-x) \not\equiv 0 \pmod q$ has solutions. We write

$$\text{(4)} \qquad (a, E/K) = (\tilde{\sigma}^x)(\tilde{\sigma}^{(m-x)})(\tilde{\sigma}^{-1}\xi)(\tilde{\sigma})$$

where ξ restricted to $K(\sqrt[l^{e'}]{1}/K)$ is trivial. This can be done by (3). We may represent each of the bracketed terms in (4) by (an infinite family of) prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ by the Cebotarev density theorem. Then from (4) we get:

$$\text{(5)} \qquad (a, K_b/K) = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4, K_b/K)$$

and so there exists $\lambda \in K^*$ such that $\lambda \equiv 1 \pmod b$ and $a' = a\lambda = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ (by Artin Reciprocity) i.e. $a' \in A$ and $a' \equiv a \pmod b$, therefore $a' = a\lambda = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$. This shows from (2), that

$$\varphi[(a+bx)^N] = \prod_{i=1}^{4}(Norm\,\mathfrak{p}_i)^{(N-1)r_if_i}((Norm\,wp_i)^{f_i} - 1)^{r_i}.$$

We have $l^e|\varphi(a+bx)^N$. We are in the case 0 =Char(K) or $N = 1$. If Char $(K) = p > 0$ then $N = 1$, whence $l^e|\prod_{i=1}^{4}((N\,\mathfrak{p}_i)^{f_i} - 1)^{r_i}$. If Char $(K) = 0$, we use the infinitude of the solutions $\{\mathfrak{p}_i\}$ to (4), to pick $\mathfrak{p}_i$ such that Norm$(\mathfrak{p}_i)$ is a power of a prime $p_i > l$. Then again $l^e|\prod_{i=1}^{4}((N\,\mathfrak{p}_i)^{f_i} - 1)^{r_i}$. Let e_2 be the largest power of l dividing $(N\,\mathfrak{p}_i)^{f_i} - 1$. We have $e \le r_2e_1 + r_1e_2 + r_3e_3 + r_4e_4$. Let e_M be the maximum of e_1, e_2, e_3, e_4. Then $e \le 4e_Md$ (since $r_i \le d$) which shows that $e_M \ge e'$. Therefore, for some $i, l^{e'}$ divides $(N\,\mathfrak{p}_i)^{f_i} - 1$. But $(\mathfrak{p}_i, K(\sqrt[l^{e'}]{1})/K)$ sends $\sqrt[l^{e'}]{1}$ into $(\sqrt[l^{e'}]{1})^{Norm(\mathfrak{p}_i)}$, therefore the order of $(\mathfrak{p}_i^{f_i}, K(\sqrt[l^{e'}]{1})/K)$ is equal to 1. From (4) and the fact that $\tilde{\sigma}|K(\sqrt[l^{e'}]{1}) = \sigma$, we know that

$$(\mathfrak{p}_i, K(\sqrt[l^{e'}]{1})/K) = \sigma^x \text{ or } \sigma^{m-x} \text{ or } \sigma^{-1} \text{ or } \sigma.$$

We therefore get: one of the numbers $xf_1, (m-x)f_2, -f_3$ or f_4 is divisible by the degree $d(e)$ of $K(\sqrt[l^{e'}]{1})/K$ and hence by q^h. By the choice of $x(x(m-x) \not\equiv 0)$, this means that $d(e)$ divides f_i for some i and $f_i|d$ for each i. Therefore q^h divides d if q is an odd prime or else if $(a, K(\sqrt[l^{e'}]{1})/K) = \sigma^m$ where m is *even.*

(B) If $q = 2$ but m is odd, and

$$(a, K(\sqrt[l^{e'}]{1})/K) = \sigma^m,$$

we write

$$(a, E/K) = (\tilde{\sigma}^m)(\tilde{\sigma}^{-1}\xi)(\tilde{\sigma}) \tag{6}$$

and represent $\tilde{\sigma}^m, \tilde{\sigma}^{-1}\xi$ and $\tilde{\sigma}$ by primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$. Then $(\mathfrak{p}_1, K(\sqrt[l^{e'}]{1})/K) = \sigma^m$, $(\mathfrak{p}_2, K(\sqrt[l^{e'}]{1})/K) = \sigma^{-1}$, $(\mathfrak{p}_3, K(\sqrt[l^{e'}]{1})/K) = \sigma$.

By (2), we have $l^e | \prod_{i=1}^{3}((N\mathfrak{p}_i)^{f_i} - 1)^{r_i}$ (we use an argument similar to the one in (A) to choose $\mathfrak{p}_i$ such that $l|(Norm\ \mathfrak{p}_i))$. If e_i is the largest power of l dividing $(N\mathfrak{p}_i)^{f_i} - 1$ and $e_M = \max\{e_1, e_2, e_3\}$, then $e \le \sum r_i e_i \le 3de_M \le 4de_M$ whence $e' \le e_M$, i.e. $l^{e'}$ divides $(N\mathfrak{p}_i)^{f_i} - 1$ for some i. Now (6) shows that one of the numbers $f_1 m, -f_2, f_3$ is divisible by q^h, and since m is odd and $q = 2$, this means $q^h | f_1$ or f_2 or f_3 and each f_i divides d. We have thus proved in all cases that if q^h is a prime power dividing the degree $d(e')$, then q^h divides by a constant depending only on (K, d) provided O $=$ Char (K) or $N = 1$. Now $l^{e'} = l^{[e/4d-1]+1}$ is bounded which means that l^e is bounded by $G(K, d, 1)$ whenever $l^e | gcd\{\varphi(a+bx)^N; x \in A\}$ and we are in case 1. Thus in Case 1, $f_{a,b,1}$ is bounded by $G(K, d, 1)$ and if Char $(K) = 0$ then $f_{a,b,N}$ is bounded by $G(K, d, 1)$.

Case 2: $Char(K) = p > 0$, and $N > 1$. Let $p^M \ge N$ $\left(\text{choose } M = 1 + \left[\dfrac{\log N}{\log p}\right]\right)$. Then $T_{a,b,1}^{p^M} \subset T_{a,b,N}$, because $(T(a + bx))^{p^M} \subset T((a + bx)^N)$ which shows that Card $(T(A)/T_{a,b,N}) \le p^{M(Card(\widetilde{S})-1)}$ Card $(T(A)/T_{a,b,N})$ i.e. $f_{a,b,N} \le p^{M(Card(\widetilde{S})-1)} f_{a,b,1}$ and we have shown in Case 1 that $f_{a,b,1} \le G(d, K, 1)$. Therefore $f_{a,b,N} \le G(K, d, N)$ in all cases. □

NOTATION 3.2. We observe that for $G = SU(2,1)$, for any K-algebra A, we have

$$G(A) = \left\{ g \in SL_3(L \otimes A); \quad \sigma({}^t g) \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} g \right\} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

where L/K is a Galois extension of degree 2 whose Galois group is generated by σ, σ acts on $L \otimes A$ by its action on L and on the group $SL_3(L \otimes A)$ by acting entrywise, ${}^t g$ is the transpose of the matrix g. Then

$$U^+(K) = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & (-\bar{x}) \\ 0 & 0 & 1 \end{pmatrix}; \quad N(x) = tr_{L/K}(y), \quad x, y \in L \right\},$$

$$U^-(K) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & -\bar{x} & 1 \end{pmatrix}; \quad N(x) = tr_{L/K}(y), \quad x, y \in L \right\},$$

$$M(K)=\left\{\begin{pmatrix} a & 0 & 0\\ 0 & \bar{a}/a & 0\\ 0 & 0 & \bar{a}^{-1}\end{pmatrix};\quad a\in L^*\right\}.$$

Thus, $M = R_{L/K}(\mathbf{G}_m)$. Take W to be the standard representation of G on L^3 and $f(g) = a_{11}(g)$ i.e. the $(1,1)$-th entry of g. Look at the action of $M(O_S)$ on $F(\mathfrak{a})\backslash G(\mathfrak{a})/F(\mathfrak{a})$, one can write

$$(*)\quad g=\begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}=\begin{pmatrix} 1 & 0 & 0\\ a_{21}/a_{11} & 1 & 0\\ a_{31}/a_{11} & -\overline{(a_{21}/a_{11})} & 1\end{pmatrix}$$

$$\times\begin{pmatrix} a_{11} & 0 & 0\\ 0 & \bar{a}_{11}/a_{11} & 0\\ 0 & 0 & \bar{a}_{11}^{-1}\end{pmatrix}\begin{pmatrix} 1 & a_{12}/a_{11} & a_{13}/a_{11}\\ 0 & 1 & -\overline{a_{12}/a_{11}}\\ 0 & 0 & 1\end{pmatrix}.$$

Suppose $\rho : SL_2 \to SU(2,1)$ is a K-representation (nontrivial) such that

$$\rho\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix};x\in\mathbf{G}\right\}\subset U^+,\quad \rho\left\{\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix};x\in\mathbf{G}\right\}\subset U^+$$

$\left(\text{then } \rho\left\{\begin{pmatrix}t & 0\\ 0 & t^{-1}\end{pmatrix};t\in\mathbf{G}\right\}\subset M\right)$. Moreover, $f\left[\rho\begin{pmatrix}a & 0\\ 0 & a^{-1}\end{pmatrix}\right] = a$ or a^2 as can be easily seen. If $g \in [\rho(SL_2)]$, then (*) shows that $M(a^2)$ acts trivially on $g = \rho\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Therefore $M((a+bx)^2)$ acts trivially on $\bar{g}$ in $F(\mathfrak{a})\backslash F(\mathfrak{a})\rho(SL_2)F(\mathfrak{a})/F(\mathfrak{a})$. Now Lemma 2.2 shows that there is a fixed subgroup T_0 of $M(O_S)$ such that T_0 acts trivially on $F(\mathfrak{a})\backslash F(\mathfrak{a})[\rho(SL_2)]_{\mathfrak{a}}F(\mathfrak{a})/F(\mathfrak{a})$. Hence, if $H_\rho = \rho(SL_2)$, then by Lemma 1.18, T_0 acts trivially on $C \cap \mathcal{H}_\rho$.

Then T_0 acts trivially on $\mathcal{H}_\rho \cap C$, and $H_\rho(K)$ acts on $C\cap\mathcal{H}_\rho$. But, if $2 \neq \text{Char}(K)$ then T_0 and $\mathcal{H}_\rho(K)$ generate $G(K)^+$, which shows that $G(K)^+$ acts, and acts trivially on $C \cap \mathcal{H}_\rho$. Thus $\mathcal{H}_\rho(K) \cap U^+(K_w)$ and $H_\rho(K) \cap U(\overline{K_{w'}})$ commute if $w, w' \notin S$, $w \neq w'$. By **[12]**, this implies $U^+(K_w)$ and $U(K_w)$ commute, whence C is centralised by $G(K)^+$.

4. The case when M_0 is abelian. In this case we have emb eddings of $H = R_{L/K}SU(2,1)$ or of $H = SL_2$ in G where $R_{L/K}(SU(2,1))$

of SL_2 has S-rank at least 2 ([**12**]). Therefore $(U^+ \cap H)(K_v)$ and $(U^- \cap H)(K_w)$ commute if $v \neq w, v, w \notin S$. By Lemma (2.1) of [**12**], this means that $[U^+(K_v), \ U^-(K_w)] = 1$ in $\mathcal{G}$ for all $v, w \in S$, $v \neq w$, i.e. C is *central.*

CONCLUSION. We have shown that

$$1 \to C \to \mathcal{G} \to G(\mathbf{A}(S)) \to 1$$

is a central extension in all cases, whence C is finite by [**11**], i.e. $\underline{F(\mathfrak{a})}$ is a subgroup of finite index in $G(\mathfrak{a})$. Now $F(\mathfrak{a})$ normalises $\overline{E(\mathfrak{a})}$. Hence, again by [**12**], $E(\mathfrak{a})$ has finite index in $G(\mathfrak{a})$. This completes the proof of the theorem of the introduction.

Acknowledgement. I thank M. S. Raghunathan for many helpful conversations. I also thank M. K. Priyan for typing this manuscript excellently.

REFERENCES

[1] Borel, Harder, *Existence of discrete cocompact subgroups of reductive groups over local fields*, J. Reine Angew. Math., **298** (1978), 53-64 .

[2] Borel, Harish, Chandra, *Arithmetic subgroups of Algebraic Groups*, Ann. of Math., **75** (1965) 485-535.

[3] Borel, Tits, *Groupes Réductifs*, Publ. Math. IHES, **27** (1965), 55-150.

[4] Harder, *Über die Galoiskohomologie des halbeinfacher algebraischer gruppen III*, J. Reine Angew. Math., **274/275**(1975), 125-138.

[5] Kneser, *Erzeugende und Relationen Verallgemeinerter Einheitengruppen*, Crelle's J., **214/215** (1964), 345-349.

[6] Margulis, *Arithmeticity of the irreducible lattices in semisimple groups of rank greater than 1*, Invent. Math., **76** (1984), 93-120.

[7] Margulis, *Finiteness of quotient groups of discrete groups, Funct. Anal. Appl.*, **13** (1979), 178-187.

[8] Platonov, *The Problem of Strong Approximation and the Kneser-Tits Hypothesis for Algebraic Groups*, Math. USSR, Izv., **3** (1970), 1139-1147.

[9] G.Prasad, *Strong Approximation for semisimple groups over function fields*, Ann. of Math., **105** (1977), 553-572.

[10] Prasad, Raghunathan, *On the Congruence subgroup problem: determination of the metaplectic kernel*, Invent. Math., **71** (1983), 21-42.

[11] Raghunathan, *On the Congruence Subgroup Problem*, Publ. Math. IHES, **46** (1976), 107-161.

[12] Raghunathan, *On the congruence subgroup problem II*, Invent. Math., **85** (1986), 73-117.

[13] Raghunathan, *A note on generators for arithmetic subgroups of algebraic groups*, Pacific J. Math., **152** (1991), 365-373.

[14] Serre, *Le problem de groupes de congruence pour SL_2*, Ann. Math., **92** (1970), 489-527.

[15] Tits, *Systems Generatteurs de Groupes de Congruence*, C.R. Acad. Sci., Paris, Serie A 283 (1976), 693.

[16] Tits, *Algebraic and abstract simple groups*, Annals of Math., **80** (1964), 313-329.

[17] Vaserstein, *The Structure of Classical Arithmetical Groups of rank greater than one*, (English translation) Math. USSR; Sbornik, **20** (1973), 465-492.

[18] Vaserstein, *On the group SL_2 over Dedekind rings of arithmetic type*, Math. USSR Sbornik, **18** (1972),no.2.

Received March 2, 1992 and accepted for publication July 27, 1992

TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD, COLABA,
BOMBAY 400 005, INDIA

PACIFIC JOURNAL OF MATHEMATICS

Volume 166 No. 1 November 1994