GENERATORS FOR ARITHMETIC GROUPS

R. SHARMA AND T. N. VENKATARAMANA

Abstract. We prove that any non-cocompact irreducible lattice in a higher rank real semi-simple Lie group contains a subgroup of finite index which is generated by **three** elements.

1. Introduction

In this paper we study the question of giving a small number of generators for an arithmetic group. The question of a small number of generators is also motivated by the congruence subgroup problem (abbreviated to CSP in the sequel). Our main theorem says that if Γ is a higher rank arithmetic group, which is non-uniform, then Γ has a finite index subgroup which has at most THREE generators.

Our proof makes use of the methods and results of [T] and [R 4] on certain unipotent generators for non-uniform arithmetic higher rank groups, as also the classification of absolutely simple groups over number fields.

Let G be a connected semi-simple algebraic group over $\mathbb{Q}$. Assume that G is $\mathbb{Q}$-simple i.e. that G has no connected normal algebraic subgroups defined over $\mathbb{Q}$. Suppose further, that $\mathbb{R}$-$rank(G) \geq 2$. Let Γ be a subgroup of finite index in $G(\mathbb{Z})$. We will refer to Γ as a "higher rank" arithmetic group. Assume moreover, that Γ is non-uniform, that is, the quotient space $G(\mathbb{R})/\Gamma$ is not compact. With this notation, we prove the following theorem, the main theorem of this paper.

Theorem 1. *Every higher rank* **non-uniform** *arithmetic group* Γ *has a subgroup* Γ' *of finite index which is generated by at the most* **three** *elements.*

1991 *Mathematics Subject Classification.* Primary 20F05, 11F06; Secondary 22E40

R.Sharma. School of Mathematics, Homi Bhabha Road,Colaba, Mumbai 40005, India. ritumony@math.tifr.res.in

T.N.Venkataramana. School of Matematics, Homi Bhabha Road, Colaba, Mumbai 400005, India. venky@math.tifr.res.in.

The proof exploits the existence of certain unipotent elements in the arithmetic group. The higher rank assumption ensures that if U^+ and U^- are opposing unipotent radicals of some maximal parabolic $\mathbb{Q}$-subgroups of the semi-simple algebraic group G, and M is their intersection (note that M normalises both U^+ and U^-), then $M(\mathbb{Z})$ will have a "sufficiently generic" semi-simple element. There are generic elements in $U^{\pm}(\mathbb{Z})$ which together with this generic element in $M(\mathbb{Z})$ will be shown to generate, **in general**, an arithmetic group. This is already the case for the group $SL(2, O_K)$ where $K/\mathbb{Q}$ is a non-CM extension of degree greater than one (see section 2).

If γ is the above "generic" element, and $u^+ \in U^+$ and $u^- \in U^-$ are also "generic", then let Γ be the group generated by the n-th powers γ^n, $(u^+)^n$ and $(u^-)^n$ for some integer n. Clearly, Γ is generated by three elements. It is easy to show that any arithmetic subgroup of $G(\mathbb{Z})$ contains a group of the form Γ for some integer n. The genericity assumption will be shown to imply that for **most groups** G, Γ intersects $U^+(\mathbb{Z})$ and $U^-(\mathbb{Z})$ in subgroups of finite index. Then a Theorem of Tits ([T]) for Chevalley Groups and its generalisation to other groups of $\mathbb{Q}$-rank ≥ 2 by Raghunathan [R 4] (see also [V] for the case when $\mathbb{Q}$-rank (G)=1), implies that Γ is of finite index in $G(\mathbb{Z})$.

The proof that Γ intersects $U^{\pm}(\mathbb{Z})$ in a lattice for most groups, is reduced (see Proposition 15) to the existence of a torus in the Zariski closure M_0 of $M(\mathbb{Z})$ -the group M_0 is not equal to M- whose eigenspaces (with a given eigenvalue) on the Lie algebra $Lie(U^{\pm})$ are one dimensional. The existence of such a torus for groups of $\mathbb{Q} - rank \geq 3$ is proved by a case by case check, using the Tits diagrams (classification) of simple algebraic groups over number fields. It turns out that in the case of exceptional groups (of $\mathbb{Q}$-rank ≥ 2), the existence of such a torus is ensured by the results of Langlands [L] and Shahidi [Sh] who (in the course of their work on the analytic continuation of certain intertwining operators) analyse the action of the Levi subgroup L on the Lie algebra $Lie(U^+)$ of the unipotent radical.

However, this approach fails for many groups of $\mathbb{Q}$-rank one or two; in these cases, we will have to examine the individual cases (i.e. their Tits diagram), to produce an explicit system of three generators. Thus, a large part of the proof (and a sizable part of the paper), involves, in low rank groups, a case by case consideration of the Tits diagrams. In many of these cases, the explicit system of generators is quite different from the general case (see sections 4 and 5).

We end this introduction with some notation and remarks. Given a $\mathbb{Q}$-simple semi-simple algebraic group, there is an absolutely almost simple algebraic group $\mathcal{G}$ over a number field K such that $G = R_{K/\mathbb{Q}}(\mathcal{G})$ where $R_{K/\mathbb{Q}}$ is the Weil restriction of scalars. Moreover, $\mathbb{Q}-rank(G) = K-rank(\mathcal{G})$ and $G(\mathbb{Z})$ is commensurate to $\mathcal{G}(O_K)$ where O_K is the ring of integers in the number field. For these reasons, we use interchangeably, the group G over $\mathbb{Q}$ and an absolutely simple group (still denoted G by an abuse of notation), defined over a number field K.

Given a group G, and element $g, h \in G$ and a subset $S \subset G$, denote by ${}^g(h)$ the conjugate ghg^{-1}, and ${}^g(S)$ the set of elements ghg^{-1} with $h \in S$. Denote by $< S >$ the subgroup of G generated by the subset S.

If Γ_0 is a group, Γ, Δ are subgroups, one says that Γ **virtually contains** Δ and writes $\Gamma \geq \Delta$ if the intersection $\Gamma \cap \Delta$ has finite index in Δ. One says that Γ is **commensurate** to Δ and writes $\Gamma \simeq \Delta$ if Γ virtually contains Δ (i.e. $\Gamma \geq \Delta$) and vice versa (i.e. $\Delta \geq \Gamma$).

Remark 1. The assumption on higher rank is necessary. To see this, supppose that G is any semi-simple group over $\mathbb{Q}$; note that for all arithmetic groups Γ with Γ' of finite index in Γ, we have the inclusion of the first cohomology groups $H^1(\Gamma) \subset H^1(\Gamma')$ (the cohomology with $\mathbb{Q}$ coefficients). Suppose that the conclusion of Theorem 1 holds. Since Γ' is three-generated, it follows that $H^1(\Gamma)$ is at most three dimensional over $\mathbb{Q}$ for **all** arithmetic groups. However, as is well known, once the first Betti number is non-zero for a congruence subgroup Γ, it grows to infinity for a suitable family of congruence subgroups of Γ. This shows that $H^1(\Gamma) = 0$ if Theorem 1 holds. Now, for many rank one groups (the group of whose real points is isomorphic to SO(n,1) or SU(n,1)- up to compact factors), there exist arithmetic groups whose first Betti number is non-zero, by results of Millson, Kazhdan and Li. Also, any lattice Γ in $SL_2(\mathbb{R})$ has a subgroup of finite index whose first Betti number is arbitrarily large (the first Betti number grows to infinity with the index of the subgroup).

Remark 2. We do not know if Theorem 1 holds even when Γ is a **uniform** higher rank arithmetic group (i.e. $G(\mathbb{R})/\Gamma$ is compact). The method of proof in the present paper uses the existence of unipotent elements and hence works only for non-uniform higher rank arithmetic groups. One can show that if there exists an integer k such that every congruence subgroup Γ_0 contains a **congruence** subgroup Γ' which is k-generated, then the congruence subgroup property (CSP) holds for G.

Remark 3. By the results of [T], [R 4] and [V], it follows that given a semi-simple algebraic group G over $\mathbb{Q}$ as in Theorem 1, there exists an integer k (in fact k may be taken to be $2dim(U^+)$) such that every higher rank non-uniform arithmetic group $\Gamma \subset G(\mathbb{Q})$, contains a subgroup Γ'' of finite index which is generated by k elements. This is because $\Gamma \cap U^{\pm}(\mathbb{Z})$ is generated by $dim(U^+)$ elements and by the results cited above, Γ'' may be taken to be the group generated by $\Gamma \cap U^+$ and $\Gamma \cap U^-$. Thus the point of Theorem 1 is that the number of generators for a subgroup of finite index can be as small as 3. It seems imposible to cut this number down to two (it is trivial to see that no subgroup of finite index is one -generated).

Note. A sizeable part of this paper forms the thesis of R.Sharma, submitted in April, 2004 to the Tata Institute of Fundamental Research, Mumbai for the award of a Ph.D. degree.

2. Preliminary results on Rank one groups

2.1. **The Group SL(2).** In this subsection we prove Theorem 1 for the case $G = SL(2)$ over a number field E. The assumption of higher rank translates into the condition that E has infinitely many units. That is, E is neither $\mathbb{Q}$ nor an imaginary quadratic extension of $\mathbb{Q}$. It turns out that if E is not a CM field, that is, E is not a totally imaginary quadratic extension of a totally real number field, then, the proof is easier. We will therefore prove this part of the theorem first.

Proposition 2. *Let E be a number field, which is not $\mathbb{Q}$ and which is not a CM field. Let $G = R_{E/\mathbb{Q}}(SL(2))$. Then, any arithmetic subgroup of $G(\mathbb{Q})$ has a subgroup of finite index which has three generators.*

Before we begin the proof of Proposition 2 , we prove a few Lemmata. We will first assume that E is a non-CM number field with infinitely many units. Let O_E denote the ring of integers in the number field and O_E^* denote the multiplicative group of units in the ring O_E.

Lemma 3. *Let Δ be a subgroup of finite index in O_E^* and F the number field generated by Δ. Then $F = E$.*

Proof. If $r_1(K)$ and $r_2(K)$ are the number of inequivalent real and complex embeddings of a number field K, then, by the Dirichlet Unit Theorem, the rank of O_K^* is $r_1(K) + r_2(K) - 1$.

Let d be the degree of E over F. Let A be the set of real places of F. To each $a \in A$, let $x(a)$ be the number of real places of E lying above a and $y(a)$ the number of non-conjugate complex places of E lying above a. Then, for each $a \in A$ we have $x(a) + 2y(a) = d$, the degree of E over F. Clearly, $x(a) + y(a) \geq 1$ for each a.

Let B be the number of non-conjugate complex places of F. Then all places of E lying above a place $b \in B$ are imaginary. If their number is $y(b)$, then we have $y(b) = d$ for each b.

The rank of the group of units O_F^* of the number field F is, by the Drichlet Unit Theorem, $Card(A) + Card(B) - 1$. That of O_E^* is

$$-1 + \sum_{a\in A}(x(a) + y(a)) + \sum_{b\in B} y(b).$$

By assumption, O_F^* and O_E^* have the same rank, since O_F^* contains Δ, a subgroup of finite index in O_E^*. We thus have the equation

$$(2.1)\ Card(A) + Card(B) = \sum_{a\in A}(x(a) + y(a)) + \sum_{b\in B} y(b).$$

Since $x(a)+y(a)\geq 1$ and $y(b)=d\geq 1$, equation 2.1 shows that if B is non-empty, then $d=1$ and $E=F$.

If B is empty, then F has no complex places, and so F is totally real. Moreover, since $x(a)+y(a)\geq 1$, equation 2.1 shows that for each $a\in A$, $x(a)+y(a)=1$. Thus, either $x(a)=0$ or $y(a)=0$. If, for some a, $y(a)=0$ then the equation $d=x(a)+2y(a)$ shows that $d=1$ and $E=F$.

The only possibility left is that $x(a)=0$ and $y(a)=1$ for each $a\in A$, and F is totally real. Therefore, for each archimedean (necessarily real) place a of F, we have $y(a)=1$ and $d=2y(a)=2$, that is there is only one place of E lying above the place a of F and is a complex place, whence E/F is a quadratic extension, which is totally imaginary. Hence E is a CM field, which is ruled out by assumption. $\square$

The field extension E over $\mathbb{Q}$ has only finitely many proper sub fields $E_1, E_2, \cdots, E_m$ (this follows trivially from Galois Theory, for example).

Lemma 4. *Suppose that E is a number field which is not a CM field. Then There exists an element $\theta\in O_E^*$ such that for any integer $r\geq 1$, the sub ring $\mathbb{Z}[\theta^r]$ of O_E generated by θ^r is a subgroup of finite index in the additive group O_E. In particular, $\mathbb{Z}[\theta^r]\supset NO_E$ for some integer N. Consequently, there exists an element $\theta\in O_E^*$ which does not lie in any of the subfields $E_1,\cdots,E_m$ as above, and for every such θ, the sub-ring $\mathbb{Z}[\theta^r]$ is a subgroup of of finite index in O_E.*

Proof. By Lemma 3 the intersection $\Delta_i=O_E^*\cap E_i$ is of **infinite index** in O_E^*. Let us now write the abelian group O_E^* additively. Then, we have the $\mathbb{Q}$ -subspaces $W_i=\mathbb{Q}\otimes\Delta_i$ of the vector space $W=\mathbb{Q}\otimes O_E^*$ (the latter of dimension $r_1(E)+r_2(E)-1$ over $\mathbb{Q}$). Since W_i are finitely many proper subspaces of W, it follows that there exists an element of W (hence of the subgroup O_E^*) no rational multiple of which lies in W_i for any i. Interpreting this statement multiplicatively, there exists an element θ of O_E^* such that no integral power of θ lies in the sub fields E_i for any i. Consequently, for any integer $r\neq 0$, the subfield $\mathbb{Q}[\theta^{r\mathbb{Z}}]$ is all of E. In particular, the sub ring $\mathbb{Z}[\theta^r]$ generated by θ^r is of finite index in the ring O_E. $\square$

We now begin the proof of Proposition 2. Consider the matrices $u_+=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $u_-=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$. Abusing notation, denote by θ the matrix $\begin{pmatrix}\theta & 0\\ 0 & \theta^{-1}\end{pmatrix}$, where $\theta\in O_E^*$ is as in Lemma 4. Then, the group

$\Gamma =< u_+^r, u_-^r, \theta^r >$ generated by $u_\pm^r$ and θ^r contains, for integers $m_1, m_2, \cdots m_l$, and $n_1, n_2, \cdots n_l$, the element

$$^{\theta^{m_1 r}}(u_+^{rn_1})^{\theta^{m_2 r}}(u_+^{rn_2})\cdots^{\theta^{m_l r}}(u_+^{rn_l}).$$

This element is simply the matrix $\begin{pmatrix} 1 & r\sum n_i\theta^{2m_i r} \\ 0 & 1 \end{pmatrix}$. Picking suitable m_i, n_i, we get from Lemma 4, an integer N such that $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \Gamma$ for all $x \in NO_E$. Similarly, all lower triangular matrices of the form $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ are in Γ for all $x \in NO_E$. But the two subgroups $U^+(NO_E) = \begin{pmatrix} 1 & NO_E \\ 0 & 1 \end{pmatrix}$ and $U^-(NO_E) = \begin{pmatrix} 1 & 0 \\ NO_E & 1 \end{pmatrix} \subset \Gamma$ generate a subgroup of finite index in $SL_2(O_E)$ (by [Va]). Hence Γ is of finite index in $SL_2(O_E)$. It is clear that any subgroup of finite index in $SL_2(O_E)$ contains a three generated group $\Gamma =< u_+^r, \theta^r, u_-^r >$ for some r. This completes the proof of Proposition 2.

2.2. **The CM case.** Suppose that F is a totally real number field of degree $k \geq 2$ and suppose that E/F is a totally imaginary quadratic extension of F. There exists an element $\alpha \in E$ such that $\alpha^2 = -\beta \in F$ where β is a totally positive element of F (that is, β is positive in all the archimedean (hence real) embeddings of F). Let θ be an element of infinite order in O_F^* as in Lemma 4, so that for any integer r, the sub-ring $\mathbb{Z}[\theta^r]$ of O_F is a subgroup of finite index in O_F (in Lemma 4, replace E by the totally real field F). We have thus the following analogue of Lemma 4, in the CM case.

Lemma 5. *Suppose that E is a CM field and is a totally imaginary quadratic extension of a totally real number field F. There exists an element $\theta \in O_E^*$ such that for any integer $r \neq 0$, the ring $\mathbb{Z}[\theta^r]$ generated by θ^r is a subgroup of finite index in O_F.*

Proof. By the Dirichlet Unit Theorem, the groups O_E^* of units of E and the group of units O_F^* of F have the same rank. Hence O_E^* contains O_F^* as a subgroup of finite index. Therefore, we may apply the previous lemma (Lemma 4), with E replaced by F (the latter is not a CM field). □

Consider the elements $h = h(\theta) = \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}$, $u_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $u_- = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$ of $SL(2, O_E)$. Given an arithmetic subgroup Γ_0 of

$SL(2, O_E)$, there exists an integer r such that the group $\Gamma = < h^r, u_+^r, u_-^r >$ generated by the r-th powers h^r, u_+^r and u_-^r lies in Γ_0.

Proposition 6. *For every integer r, the group Γ in the foregoing paragraph is arithmetic (i.e. is of finite index in $SL(2, O_E)$). In particular, every arithmetic subgroup of $SL(2, O_E)$ is virtually 3-generated.*

Proof. Write the Bruhat decomposition for the element

$$u_-^r = \begin{pmatrix} 1 & 0 \\ r\alpha & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{r\alpha} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\frac{1}{r\alpha} & 0 \\ 0 & -r\alpha \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{r\alpha} \\ 0 & 1 \end{pmatrix}$$

By the choice of the element θ, the group generated by $h(\theta)^r$ and u_+^r contains, for some integer $N > 0$, the subgroup $U^+(NO_F) = \{u = \begin{pmatrix} 1 & Nb \\ 0 & 1 \end{pmatrix} : b \in O_F\}$. Clearly, $\Gamma \supset U^+(NO_F)$. Define $U^-(NO_F)$ similarly. Since α^2 lies in the smaller field O_F, a computation shows that the conjugate ${}^{u_-^r}(U^+(NO_F))$ contains the subgroup ${}^{v_+}(U^-(N'O_F))$ for some integer N', where v_+ is the element $\begin{pmatrix} 1 & \frac{1}{r\alpha} \\ 0 & 1 \end{pmatrix}$. Thus the group ${}^{v_+}(U^-(N'O_F)) \subset \Gamma$. Since the group U^+ is commutative, we have ${}^{v_+}(U^+(N'O_F)) = U^+(N'O_F) \subset \Gamma$. Thus, ${}^{v_+}(U^-(NO_F)) \subset \Gamma$ and ${}^{v_+}(U^+(NO_F)) \subset \Gamma$.

By a Theorem of Vaserstein ([Va]), the group generated by $U^+(NO_F)$ and $U^-(N'O_F)$ is a subgroup of finite index in $SL(2, O_F)$. In particular, it contains some power $h^M = h(\theta)^M$ of h. Hence, by the last paragraph, ${}^{v_+}(h^M) \in \Gamma$.

Since a power of h already lies in Γ, we see that for some integer r', the commutator u_1 of $h^{r'}$ and ${}^{v_+}(h^{r'})$ lies in Γ. This commutator is nothing but the matrix $\begin{pmatrix} 1 & (\theta^{2r'} - 1)(\frac{1}{r\alpha}) \\ 0 & 1 \end{pmatrix}$. Now, $\frac{1}{\alpha} = \frac{-\alpha}{\beta}$, with $\beta \in F$. Therefore, by Lemma 4, the subgroup generated by $\theta^{r'}$ and u_1 contains, for some M', the subgroup $U^+(M'O_F\alpha)$ consisting of elements of the form $\begin{pmatrix} 1 & xM'\alpha \\ 0 & 1 \end{pmatrix}$. Hence, $U^+(M'O_F\alpha) \subset \Gamma$. We have already seen that $U^+(MO_F) \subset \Gamma$. Now, up to a subgroup of finite index, O_E is the sum of O_F and $O_F\alpha$ since E/F is a quadratic extension generated by α. This shows (after changing M' if necessary by a suitable multiple), that $U^+(M'O_E) \subset \Gamma$. The conjugate of U^+ by the *lower triangular* matrix $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$ is a unipotent group V opposed to U^+. By Vaserstein's Theorem in [Va] (replacing U^- by our opposite unipotent group V) we see that Γ contains an arithmetic subgroup of $SL(2, O_E)$ and is hence itself arithmetic. $\square$

Note that in Proposition 6, α was assumed to be an element whose square lies in F; that is the trace of α over F is zero. For handling some $\mathbb{Q}$-rank one groups, we will need a more general version of Proposition 6, where α is replaced by an element with non-zero trace. Let $x \in E \backslash F$ be an integral element divisible by $N!$ (the product of the first N integers) for a large rational integer N. Denote by $U^-(xO_F)$ the set of matrices of the form $\begin{pmatrix} 1 & 0 \\ xa & 0 \end{pmatrix}$ with $a \in O_F$. Denote by $U^+(rO_F)$ the group of matrices of the form $\begin{pmatrix} 1 & ra \\ 0 & 1 \end{pmatrix}$ with $a \in O_F$.

Proposition 7. *The group generated by $U^+(rO_F)$ and $U^-(xO_F)$ is of finite index in $SL(2, O_E)$.*

Proof. Denote by Γ the group in the proposition. We first find an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in Γ such that $ac \neq 0$ and c lies in the smaller field F. To do this, we use the existence of infinitely many units in F. Write $x^2 = tx - n$ with $t (= tr_{E/F}(x))$ and $n (= N_{E/F}(x))$ in F. Assume that $t \neq 0$ since $t = 0$ has already been covered in Proposition 6. Given a unit $\theta \in O_E^*$ consider the product element $g \in SL(2, E)$ given by $g = \begin{pmatrix} 1 & 0 \\ -x\theta^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{\theta-1}{t} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$.

Now, normal subgroups of higher rank arithmetic groups are again arithmetic ([M], [R 1], [R 2]). Since $T(O_F)(= T(O_E))$ normalises the groups $U^+(rO_F)$ and $U^-(xO_F)$, it follows that to prove the arithmeticity of Γ, it is enough to prove the arithmeticity of the group generated by Γ and $T(O_F)$. We may thus assume that Γ contains $T(O_E) = T(O_F)$. Here the equality is up to subgroups of finite index.

If θ is a unit such that $\theta \equiv 1 \pmod{tO_F}$, then from the definition of g and Γ it is clear that $g \in \Gamma$. Write $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. A computation shows that $a = 1 + \frac{\theta-1}{t}x$, $c = \frac{1-\theta^{-1}}{t}n$. Since x and 1 are linearly independent over F ($x \notin F$), it follows that $a \neq 0$ and in fact that $a \notin F$. The expression for c shows that $c \neq 0$. It also shows that c lies in the smaller field F.

The Bruhat decomposition for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & ac^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c^{-1} & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & dc^{-1} \\ 0 & 1 \end{pmatrix}.$$

Thus, $\Gamma \supset {}^{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}\begin{pmatrix} 1 & rO_F \\ 0 & 1 \end{pmatrix} = {}^{\left(\begin{smallmatrix} 1 & ac^{-1} \\ 0 & 1 \end{smallmatrix}\right)}\begin{pmatrix} 1 & 0 \\ c^2 rO_F & 1 \end{pmatrix}$. Moreover $\Gamma \supset \begin{pmatrix} 1 & rO_F \\ 0 & 1 \end{pmatrix} = {}^{\left(\begin{smallmatrix} 1 & ac^{-1} \\ 0 & 1 \end{smallmatrix}\right)}\begin{pmatrix} 1 & rO_F \\ 0 & 1 \end{pmatrix}$. The group Δ generated by $\begin{pmatrix} 1 & rO_F \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ c^2 rO_F & 1 \end{pmatrix}$ contains, for some integer r', $U^+(r'O_F)$ and $U^-(r'O_F)$ (since c and hence c^2 lie in the field F) Hence, by Vaserstein's Theorem ([Va]) Δ is an arithmetic subgroup of $SL(2, O_F)$.

In particular, Γ contains the subgroup ${}^{\left(\begin{smallmatrix} 1 & ac^{-1} \\ 0 & 1 \end{smallmatrix}\right)}(\theta^{r''\mathbb{Z}})$ for some integer r''. By enlarging r'' if necessary, assume that $\theta^{r''\mathbb{Z}} \subset \Gamma$. Thus Γ contains the commutator group

$$[\begin{pmatrix} 1 & ac^{-1} \\ 0 & 1 \end{pmatrix}, \theta^{r''\mathbb{Z}}] = \begin{pmatrix} 1 & ac^{-1}(\sum \mathbb{Z}(\theta^{r''k} - 1)) \\ 0 & 1 \end{pmatrix}$$

where the sum is over all integers k. By the properties of the element θ, the sum is a subgroup of finite index in the ring O_F, whence, we get an integer r_0 such that $\Gamma \supset \begin{pmatrix} 1 & ac^{-1} r_0 O_F \\ 0 & 1 \end{pmatrix}$. Since Γ already contains $\begin{pmatrix} 1 & rO_F \\ 0 & 1 \end{pmatrix}$, a does not lie in F, c lies in F, and O_E contains $O_F \oplus r_0 ac^{-1} O_F$ for a suitable r_0, it follows that for a suitable integer r_1, the subgroup $\begin{pmatrix} 1 & r_1 O_E \\ 0 & 1 \end{pmatrix}$ lies in Γ. Now Γ is obviously Zariski dense in $SL(2, O_E)$; moreover it intersects the unipotent radical U^+ is an arithmetic group. Hence it intersects some opposite unipotent radical also in an arithmetic group; but two such opposing unipotent arithmetic groups generate an arithmetic group ([Va]). Therefore, Γ is arithmetic. $\square$

2.3. **the group SU(2,1).** In this section, we prove results on the group $SU(2, 1)$ (with respect to a quadratic extension L/K of a number field K), analogous to those in the section on SL_2. These will be needed in the proof of Theorem 1, in those cases where a suitable $SU(2, 1)$ embeds in G.

Suppose that $E/\mathbb{Q}$ is a **real** quadratic extension, $E = \mathbb{Q}(\sqrt{z})$ with $z > 0$. Denote by $x \mapsto \overline{x} = x^*$ the action of the non-trivial element of the Galois group of $E/\mathbb{Q}$. Let $h = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. We will view h as a form in three variables on E^3 which is hermitian with respect to this non-trivial Galois automorphism. Set

$$G = SU(h) = SU(2,1) = \{g \in SL_3(E) : \overline{{}^tg}hg = h\}.$$

Then G is an algebraic group over $\mathbb{Q}$.

Define the groups

$$U^+ = \{\begin{pmatrix} 1 & z & -\frac{z\overline{z}}{2} \\ 0 & 1 & -\overline{z} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & w \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : w + \overline{w} = 0\},$$

$U^- =^t (U^+)$, the subgroup of $SU(2,1)$ which is an opposite of U^+ consisting of matrices which are transposes of those in U^+ and let T be the diagonals in $SU(2,1)$. Then, up to subgroups of finite index, we have $T(\mathbb{Z}) = \{\begin{pmatrix} \theta & 0 & 0 \\ 0 & \theta^{-2} & 0 \\ 0 & 0 & \theta \end{pmatrix} : \theta \in O_E^*\}$. Note that for a unit $\theta \in O_E^*$, we have $\theta\overline{\theta} = \pm 1$.

Suppose that $F/\mathbb{Q}$ is imaginary quadratic, $t \in O_F \setminus \mathbb{Z}$ and **define** the group $U^+(t\mathbb{Z})$ as the one generated by the matrices $\begin{pmatrix} 1 & 0 & tx\sqrt{z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & tux & -\frac{t^2x^2u\overline{u}}{2} \\ 0 & 1 & -t\overline{u}x \\ 0 & 0 & 1 \end{pmatrix}$ with $x \in \mathbb{Z}$ and $u \in O_E$. Denote by $U_{2\alpha}$ the root group corresponding to the root 2α, where α is the simple root for $\mathbf{G}_m (\subset T)$ occurring in $LieU^+$. Here, the inclusion of $\mathbf{G}_m$ in T is given by the map $x \mapsto \begin{pmatrix} x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^{-1} \end{pmatrix}$. Note that the commutator $[U^+(t\mathbb{Z}), U^+(\mathbb{Z})]$ is $U_{2\alpha}(t\mathbb{Z}) \subset U^+(t\mathbb{Z})$. Hence $U^+(\mathbb{Z})$ normalises $U^+(t\mathbb{Z})$. Note moreover that $U^+(t\mathbb{Z})$ contains the subgroup $U_{2\alpha}(t^2\mathbb{Z} + t\mathbb{Z}))$; now, the elements t and t^2 are linearly independent over $\mathbb{Q}$, hence $t\mathbb{Z} + t^2\mathbb{Z}$ contains $r\mathbb{Z}$ for some integer $r > 0$.

Proposition 8. *If $\Gamma \subset G(O_F)$ is such that for some $r \geq 1$, the group Γ contains the group generated by $U^+(rt\mathbb{Z})$ and $U^-(r\mathbb{Z})$, then Γ is of finite index in $G(O_F)$.*

Proof. By the last remark in the paragraph preceding the proposition, there exists an integer, we denote it again by r, such that the group Γ contains $U_{2\alpha}(r\mathbb{Z})$ and $U^-(r\mathbb{Z})$. Thus, by [V] (note that $\mathbb{R}-rank(G) = 2$ since $E/\mathbb{Q}$ is real quadratic and $G(\mathbb{R}) = SL(3,\mathbb{R})$), Γ contains a subgroup of $SU(2,1)(\mathbb{Z})$ of finite index. Therefore, Γ contains the group generated by $U^+(rt\mathbb{Z})$ and $U^+(r\mathbb{Z})$ for some integer r. The group generated contains $U^+(r'O_F)$ for some integer r' (since $F/\mathbb{Q}$ is quadratic and t and 1 are linearly independent over $\mathbb{Q}$). Clearly Γ is Zariski dense in the group $SU(2,1)$ thought of as a group over F. Therefore, by [V] again, we get: Γ is an arithmetic subgroup of $G(O_F)$. $\square$

We now prove a slightly stronger version of the foregoing proposition.

Proposition 9. *Suppose that E and F are as before, $E = \mathbb{Q}\sqrt{z}$ and $F = \mathbb{Q}(t)$ with $t^2 \in \mathbb{Q}$, but $t \notin \mathbb{Q}$. Let $\Gamma \subset G(O_F)$ be such that for some integer r, Γ contains the groups $U^-(r\mathbb{Z})$ and $U_{2\alpha}(rt\mathbb{Z})$. Then, Γ is of finite index in $G(O_F)$.*

Proof. Consider the map $f : SL(2) \to SU(2,1)$ given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 & b\sqrt{z} \\ 0 & 1 & 0 \\ \frac{c}{\sqrt{z}} & 0 & d \end{pmatrix}$. The map f is defined over $\mathbb{Q}$, takes the upper triangular matrices with 1s on the diagonal to the group $U_{2\alpha}$ and takes the Weyl group element w into the 3×3 matrix w' which has non-zero entries on the anti-diagonal and zeros elsewhere. Under conjugation action by the element $f(h)$ with $h = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, the group $U^+(r\mathbb{Z})$ is taken into $U^+(ra\mathbb{Z})$. Under conjugation by w', U^- is taken into U^+ and vice versa.

Write the Bruhat decomposition of $u_+ = \begin{pmatrix} 1 & rt \\ 0 & 1 \end{pmatrix}$, with respect to the lower triangular group. We get $u_+ = v_1^- h_1 w u_1^-$. Here, $h_1 = \begin{pmatrix} -rt & 0 \\ 0 & -\frac{1}{rt} \end{pmatrix}$. If r is suitably large, then Γ contains u_+ by assumption. To prove arithmeticity, we may assume (see the proof of Proposition

7) that $\Gamma \supset T(r\mathbb{Z})$. Then,

$$\Gamma \supset^{u_+} (U^-(r\mathbb{Z})) \supset^{v_1^-} (U_\alpha(rt\mathbb{Z})) \supset^{v_1^-} (U_{2\alpha}(r^2t^2\mathbb{Z})).$$

The last inclusion follows by taking commutators of elements of $U_\alpha(rt\mathbb{Z})$ where, $U_\alpha(rt\mathbb{Z})$ is the group generated by the elements $\begin{pmatrix} 1 & rtx & -\frac{r^2t^2x\overline{x}}{2} \\ 0 & 1 & -rt\overline{x} \\ 0 & 0 & 1 \end{pmatrix}$ with $x \in O_{\mathbb{Q}(\sqrt{z})}$. Note that $t^2 \in \mathbb{Q}$ by assumption. Hence $\Gamma \supset^{v_1^-} (U_{2\alpha}(r'\mathbb{Z}))$ for some integer r'.

Since v_1^- centralises all of U^-, we obtain $\Gamma \supset U^-(r\mathbb{Z}) \supset^{v_1^-} (U^-(r\mathbb{Z}))$.

The conclusions of the last two paragraphs and [V] shows that there exists a subgroup Δ of finite index in $SU(2,1)(\mathbb{Z})$ such that $\Gamma \supset^{v_1^-} (\Delta)$. In particular, for some integer r', the group ${}^x(\Gamma)$ with $x^{-1} = v_1^-$ contains *both* the groups $U_\alpha(r't\mathbb{Z})$ and $U_\alpha(r\mathbb{Z})$. Consequently, it contains $U^+(r'O_F)$, a subgroup of finite index in the integral points of the unipotent radical of a minimal parabolic subgroup of $SU(2,1)$ over F (note that up to subgroups of finite index, $t\mathbb{Z} + \mathbb{Z} = O_F$). Note also that the real rank of $SU(2,1)(F \otimes \mathbb{R}) = SL(3,\mathbb{C})$ is at least two. Now, Γ is clearly Zariski dense in $SU(2,1)$ regarded as a group over F. Therefore, by [V], ${}^x(\Gamma)$ is arithmetic, and hence Γ is arithmetic. $\square$

2.4. **Criteria for Groups of Rank One over Number Fields.** Suppose that K is a number field. Let G be an absolutely almost simple algebraic group with K-rank $(G) \geq 1$. Let $S \simeq \mathbf{G}_m$ be a maximal K-split torus in G, P a parabolic subgroup containing S, and U^+ the unipotent radical of P. Let $M \subset P$ be the centraliser of S in G. Let M_0 be the connected component of identity of the Zariski closure of $M(O_K)$ in M. Write $\mathfrak{g}$ for the Lie algebra of G. We have the root space decomposition $\mathfrak{g} = \mathfrak{g}_{\pm\alpha} \oplus \mathfrak{g}_0$, where $\mathfrak{u} = \oplus_{\alpha>0}\mathfrak{g}_\alpha$ is a decomposition of $LieU^+$ for the adjoint action of S. Denote by $log : U^+ \to \mathfrak{u}$ the log mapping on the unipotent group U^+. It is an isomorphism of K-varieties (not of groups in general). Define similarly U^- to be the unipotent K-group group with Lie algebra $\mathfrak{u}^- = \oplus_{\alpha>0}\mathfrak{g}_{-\alpha}$. This is the "opposite" unipotent group. There exists an element $w \in N(S)/Z(S)$ in the Weyl group of G ($N(S)$ and $Z(S)$ being the normaliser and the centraliser of S in G), which conjugates U^+ into U^-. Further, the map $(u,m,v) \mapsto umwv = g$ maps $U^+ \times M \times U^+$ isomorphically onto a Zariski open subset of G.

The following technical proposition will be used repeatedly in the sequel.

Proposition 10. *Suppose that K is any number field. Let G be of K-rank ≥ 1. Let $\Gamma \subset G(O_K)$ be Zariski dense, and assume that $\mathbb{R}$-rank $(G_\infty) \geq 2$. Suppose that there exists an element $m_0 \in M(O_K)$ of infinite order such that 1) all its eigenvalues are of infinite order in its action on $LieU^+$, 2) if $g = umwv \in \Gamma$, then there exists an integer $r \neq 0$ such that ${}^u(m_0^r) \in \Gamma$. Then, Γ is arithmetic.*

Proof. Let V be the Zariski closure of the intersection of U^+ with Γ. View U^+ as a $\mathbb{Q}$-group, be restriction of scalars. By assumption, for a Zariski dense set of elements $u \in U^+(\mathbb{Q})$, there exists an integer $r = r(u)$ such that the commutator $[m_0^r, u]$ lies in Γ. If $\mathfrak{v}$ denotes the $\mathbb{Q}$-Lie algebra of V, then, this means that, $\mathfrak{v}$ contains vectors of the form $(Ad(m_0^r) - 1)(logu)$ with $logu$ spanning the $\mathbb{Q}$-vector space $\mathfrak{u}$. By fixing finitely many u' which give a basis of $\mathfrak{u}$ (as a $\mathbb{Q}$-vector space), we can find a common integer r such that $(Ad(m_0^r) - 1)logu \in \mathfrak{v}$, for all u; in other words, $(Ad(m_0^r) - 1)(\mathfrak{u}) \subset \mathfrak{v}$. The assumption on m_0 now implies that $\mathfrak{v} = \mathfrak{u}$. Hence $V = U^+$, which means that $\Gamma \cap U^+ \subset U^+(O_K)$ is Zariski dense in U^+. By [R 5], Theorem (2.1), it follows that $\Gamma \cap U^+(O_K)$ is of finite index in $U^+(O_K)$.

Similarly, Γ intersects $U^-(O_K)$ in an arithmetic group. Hence by [R 4] and [V], Γ is arithmetic. $\square$

From now on, in this section, we will assume that K-rank of G is ONE. Consequently, $\mathfrak{u}$ has the root space decomposition $\mathfrak{u} = \mathfrak{g}_\alpha \oplus \mathfrak{g}_{2\alpha}$. Assume that $\mathfrak{g}_{2\alpha} \neq 0$. Denote by $U_{2\alpha}$ the subgroup of G whose Lie algebra is $\mathfrak{g}_{2\alpha}$. This is an algebraic subgroup defined over K.

It is easy to see that the group G_0 whose Lie algebra is generated by $\mathfrak{g}_{\pm 2\alpha}$ is necessarily semi-simple and K-simple. Moreover, it is immediate that $S \subset G_0$. Note the Bruhat decomposition of G: $G = P \cup UwP$ where $w \in N(S)$ is the Weyl group element such that conjugation by w takes U^+ into U^- and $U_{2\alpha}$ into $U_{-2\alpha}$. It is clear that $UwP = UwMU$ is a Zariski open subset of G.

Proposition 11. *Suppose that K has infinitely many units, and that K-rank $(G) = 1$. Suppose that $\Gamma \subset G(O_K)$ is a Zariski dense subgroup such that $\Gamma \supset U_{2\alpha}(rO_K)$ for some integer $r > 0$. Suppose that rank-$(G_\infty) = \sum_{v \in S_\infty} K_v$-rank$(G) \geq 2$. Then, Γ is of finite index in $G(O_K)$.*

Proof. Let $g = uwmv$ be an element in $\Gamma \cap UwP$. We obtain, $\Gamma \supset <^g (U_{2\alpha}(rO_K)),\ U_{2\alpha}(rO_K) >$. The Bruhat decomposition for g and the fact that u centralises $U_{2\alpha}$ shows that $\Gamma \supset^u < U_{-2\alpha}(r'O_K), U_{2\alpha}(r'O_K) >$ for some integer r'. The group G_0 is also of higher real rank, since $S \subset G_0$ and K has infinitely many units. Therefore by [V], the group generated by $U_{\pm 2\alpha}(r'O_K)$ is of finite index in $G_0(O_K)$ and in particular, contains $S(r''O_K)$ for some $r'' > 0$.

We have thus seen that $\Gamma \supset^u (S(r''O_K))$ for some integer r''. Since K-rank of G is one, the weights of S acting on $\mathfrak{u}$ are α and 2α. Since $S(r''O_K)$ is infinite, there are elements in $S(r''O_K)$ none of whose eigenvalues (in their action on $\mathfrak{u}$) is one. Therefore, Proposition 10 implies that Γ is arithmetic. $\square$

We continue with the notation of this subsection. There exists an integer N such that the units θ of the number field K which are congruent to 1 modulo N, form a torsion-free abelian group. Let F be the field generated by these elements. There exists an element $\theta \in O_K^*$ such that for all integers $r > 0$, the field $\mathbb{Q}[\theta^r] = F$ (see Lemma 5). Moreover, $S(O_F)$ is of finite index in $S(O_K)$. We also have, 1) $F = K$ if K is not CM. 2) F is totally real, K totally imaginary quadratic extension of F otherwise.

Given an element $u_+ \in U_{2\alpha}(O_K) \setminus \{1\}$, consider the subgroup V^+ generated by the conjugates ${}^{\theta^j}(u_+)$ of u_+, as j varies over all integers. By Lemma 4, there exists an integer r such that $V^+ \supset u_+^{rO_F} \overset{def}{=} Exp(rO_F log(u_+))$. Here Exp is the exponential map from $Lie(U^+)$ onto U^+ and log is its inverse map. By the Jacobson-Morozov Theorem, there exists a homomorphism $f : SL(2) \to G$ defined over K such that $f\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = u_+$. The Bruhat decomposition shows that the image of the group of upper triangular matrices lies in P. Since all maximal K-split tori in P are conjugate to S by elements of $P(K)$, it follows that there exists a $p \in P(K)$ such that $pf(D)p^{-1} = S$, where D is the group of diagonals in $SL(2)$. Write $p = um$ with $u \in U$ and $m \in M$. Now, M centralises S and u centralises u_+ (since u_+ lies in $U_{2\alpha}$). Therefore, after replacing f by the map $f' : x \mapsto u(f(x)u^{-1}$, we see that $f'(D) = S$ and $f'\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = u_+$. We denote f' by f again, to avoid too much notation.

Proposition 12. *Suppose that K has infinitely many units, and G an absolutely almost simple group over K of K-rank one. Suppose that $\mathfrak{g}_{2\alpha}$ is one dimensional over K. Then every arithmetic subgroup of $G(O_K)$ is virtually three generated.*

Proof. Let $u_+ \in U_{2\alpha}(O_K)$ and $\theta \in S(O_K)$ be as above. Suppose that $\gamma \in G(O_K)$ is in general position with respect to u_+. Then, for every $r \geq 1$, the group $\Gamma = < u_+^r, \theta^r, \gamma^r >$ is Zariski dense. It is enough to prove that Γ is arithmetic.

By replacing r by a bigger integer if necessary, and using the fact that $\mathbb{Z}[\theta^r]$ has finite index in O_F, we see that $f\begin{pmatrix} 1 & rO_F \\ 0 & 1 \end{pmatrix} = u_+^{rO_F} \subset \Gamma$. Write w for the image of $f\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = f(w_0)$. Then, w takes U^+ into U^- under conjugation. Write u_- for wu_+w^{-1}. Now, $M(K)$ normalises $U_{2\alpha}$ and the latter is one dimensional. Therefore, ${}^m(u_+^{rO_F}) = f\begin{pmatrix} 1 & 0 \\ \xi rO_F & 1 \end{pmatrix} \stackrel{def}{=} u_-^{\xi rO_F}$, for some element ξ of the larger field K. If $\xi \notin F$, then by Proposition 7, the group generated by $u_+^{rO_F}$ and $u_-^{\xi rO_F}$ contains $f(\Delta)$ for some subgroup of finite index in $SL(2, O_K)$.

Pick an element $g \in \Gamma$ of the form $g = uwmv$ with $u, v \in U^+$ and $m \in M$. Then,

$$\Gamma \supset <^g (u_+^{rO_F}), u_+^{rO_F} > \supset^u <^m (u_-^{rO_F}), u_+^{rO_F} > =^u < u_-^{\xi rO_F}, u_+^{rO_F} >$$

If g is "generic", then m is sufficiently generic, so that $\xi \notin F$ (otherwise, ${}^m(u_-)$ is always F-rational i.e. is in the image of $SL(2, F)$ under f, which lies in a smaller algebraic group namely the image of $R_{F/\mathbb{Q}}(SL(2))$, and genericity implies that this is not possible for all m). Then, by the conclusion of the last paragraph, $\Gamma \supset^u f(S(rO_F))$ for some integer r. Since u's run through a Zariski dense subset of U, Proposition 10 implies that Γ is arithmetic. $\square$

3. Some General Results

In the following, we will, by restricting scalars to $\mathbb{Q}$, think of the group G as an algebraic group over $\mathbb{Q}$. Thus, when we say that $G(O_K)$ is Zariski dense in G, we mean that $G(O_K)$ is Zariski dense in $G(K \otimes \mathbb{C}) = R_{K/\mathbb{Q}}(\mathbb{C})$. With this understanding, we prove the following slight strengthening of the Borel density theorem.

Lemma 13. *Let G be a connected semi-simple K-simple algebraic group, and that $G(O_K)$ is infinite. Then, the arithmetic group $G(O_K)$ is Zariski dense in the complex semi-simple group $G(K \otimes \mathbb{C})$.*

Proof. By restriction of scalars, we may assume that $K = \mathbb{Q}$. Suppose that H is the connected component of identity of the Zariski closure of $G\mathbb{Z})$ in $G(\mathbb{C})$. Then, as $G(\mathbb{Q})$ commensurates $G(\mathbb{Z})$, it follows that $G(\mathbb{Q})$ normalises H. The density of $G(\mathbb{Q})$ in $G(\mathbb{R})$ (weak approximation) shows that $G(\mathbb{R})$ normalises H. Clearly, $G(\mathbb{R})$ is Zariski dense in $G(\mathbb{C})$; hence $G(\mathbb{C})$ normalises H. The definition of H shows that H is defined over $\mathbb{Q}$. Now, the $\mathbb{Q}$-simplicity of G implies (since $G(\mathbb{Z})$ is infinite and hence H is non-trivial) that $H = G$. □

Remark 4. Since, $G(O_K)$ is a lattice in $G(K \otimes \mathbb{R})$, the Borel density Theorem implies that the Zariski closure of $G(O_K)$ maps onto the quitient of $G(K \otimes \mathbb{R})$ by a maximal **normal** compact subgroup. The point of Lemma 13 is that the Zariski closure is $G(K \otimes \mathbb{C})$ i.e. includes the compact factors of $G(K \otimes \mathbb{R})$ as well. Moreover, the proof does not use the deep fact that $G(O_K)$ is a lattice (the Borel-HarishChandra Theorem), but depends only on the fact that arithmetic groups have a large commensurator.

The following is repeatedly used in the sequel.

Lemma 14. *Let U be a unipotent group over a number field K. Then, $U(O_K)$ is Zariski dense in $U(K \otimes \mathbb{C})$; moreover, if $\Delta \subset U(O_K)$ is a subgroup which is Zariski dense in $U(K \otimes \mathbb{C})$ then, Δ is of finite index in $U(O_K)$.*

Proof. The proof is essentially given in Theorem (2.1) of [R 5], provided $K = \mathbb{Q}$. But, by restriction of scalars, we may assume that $K = \mathbb{Q}$. □

3.1. **Notation.** Suppose G is a semi-simple linear algebraic group which is absolutely almost simple and defined over a number field K, with K-rank$(G) \geq 1$ and *rank*- $(G_\infty) \overset{def}{=} \sum_{v \in S_\infty} K_v$-rank $(G) \geq 2$ (the last condition says that $G(O_K)$ is a "higher rank lattice"). Let $P \subset G$ be a proper parabolic K-subgroup, U its unipotent radical, $S \subset P$ a maximal K-split torus in G, and $\Phi^+(S, P)$ the roots of S occurring in the

Lie algebra $\mathfrak{u}$ of U. Let Φ^- be the negative of the roots in $\Phi^+(S,P)$, and $\mathfrak{u}^- = \oplus \mathfrak{g}_{-\alpha}$ be the sum of root spaces with $\alpha \in \Phi^+(S,P)$. Then, $\mathfrak{u}^-$ is the Lie algebra of a unipotent algebraic group U^- defined over K, called the "opposite" of U. Write the Levi decomposition $P = MU$ with $S \subset M$.

In the following, we will, by restricting scalars to $\mathbb{Q}$, think of all these groups G, M, $U^\pm$ as algebraic groups over $\mathbb{Q}$. Thus, for example, when we say that $U^+(O_K)$ is Zariski dense in U^+ we mean that $U^+(O_K)$ is Zariski dense in the complex group $U^+(K \otimes \mathbb{C}) = (R_{K/\mathbb{Q}}(U^+))(\mathbb{C})$.

Denote by M_0 the connected component of identity of the Zariski closure of $M(O_K)$ in M, and let $T_0 \subset M_0$ be a maximal torus defined over K. The groups M, M_0 and T_0 are all defined over $\mathbb{Q}$ and act on the $\mathbb{Q}$-Lie algebra $\mathfrak{u}$ of $R_{K/\mathbb{Q}}U^+$ by inner conjugation in G. Write the eigenspace decomposition $\mathfrak{u} \otimes \mathbb{C} = \oplus_{\chi \in X^*(T_0)} \mathfrak{u}_\chi$ for the action of T_0 on the complex lie algebra $\mathfrak{u} \otimes \mathbb{C}$.

Proposition 15. *Suppose that each of the spaces $\mathfrak{u}_\chi$ is one dimensional. Then every arithmetic subgroup of $G(O_K)$ is virtually three generated.*

Proof. Let $\mathcal{U}$ be the set of pairs $(m,v) \in M_0 \times \mathfrak{u}$ such that the span $\sum_{k \in \mathbb{Z}} \mathbb{C}({}^{m^k}(v))$ is all of $\mathfrak{u}$. Then, $\mathcal{U}$ is a Zariski open subset of $M_0 \times \mathfrak{u}$. For, the condition says that if $dim \mathfrak{u} = l$, then there exist integers $k_1, k_2, \cdots, k_l$ such that the wedge product

$$ {}^{m^{k_1}}(v) \wedge \cdots \wedge {}^{m^{k_l}}(v) \neq 0, $$

which is a Zariski open condition for $(m,v) \in M_0 \times \mathfrak{u}$.

Let Γ_0 be an arithmetic subgroup of $G(K)$. Then, the intersection $\Gamma_0 \cap U$ is Zariski dense in $R_{K/\mathbb{Q}}U$. Now, the map $log : U \to \mathfrak{u}$ is an isomorphism of varieties over $\mathbb{Q}$.

By assumption on M_0, the group $\Gamma_0 \cap M_0$ is Zariski dense in M_0 (the Zariski closure of $\Gamma_0 \cap M_0$ is of finite index in M_0 since Γ_0 is of finite index in $M(O_K)$, and M_0 is connected).

By the foregoing, we thus get elements $m \in \Gamma_0 \cap M_0$ and $u \in U \cap \Gamma_0$ such that $(m, logu) \in \mathcal{U}$. This means that the $\mathbb{Z}$-span of ${}^{m^k}(logu)$ as k varies, is Zariski dense in $\mathfrak{u}$. Therefore, the group U_1 generated by the elements ${}^{m^k}(u)$ with $k \in \mathbb{Z}$ is a Zariski dense subgroup of $U \cap \Gamma_0$. Hence, by Lemma 14, U_1 is of finite index in $U \cap \Gamma_0$.

Similarly, we can find an element $u^- \in U^- \cap \Gamma_0$ such that the group U_1^- generated by the conjugates ${}^{m^k}(u^-)$ with $k \in \mathbb{Z}$, is of finite index in $U^- \cap \Gamma_0$. Set

$$\Gamma = < m, u, u^- > \subset \Gamma_0.$$

Now, Γ contains $< U_1, U_1^- >$. By [R 4] and [V], the latter group is of finite index in Γ_0, hence so is Γ. But Γ is three generated by construction. □

Remark 5. The criterion of Proposition 15 depends on the group M_0 (which is the connected component of identity of the Zariski closure of $M(O_K)$) and hence on the K-structure of the group. But, this dependence is a rather mild one. However, the verification that the conditions of Proposition 15 are satisfied is somewhat complicated, and is done in the next few sections by using the Tits classification of absolutely simple groups over number fields. Somewhat surprisingly, the criterion works directly when K-rank $(G) \geq 3$ or for groups of exceptional type, thanks to the analysis of the representations of M occurring in the Lie algebra $\mathfrak{u}$ carried out by Langlands and Shahidi (see [L] and [Sh]).

However, there are some classical groups of K-rank ≤ 2 (notably, if G is of classical type A, C or D but is not of Chevalley type over the number field), for which the criterion of Proposition 15 fails. To handle these cases, we prove below some more lemmata of a general nature.

3.2. **Notation.** Let F be a field of characteristic zero, and G an absolutely simple algebraic group over F. Let $x \in G(F)$ be an element of infinite order. Fix a maximal torus $T \subset G$ defined over F and Φ the roots of T occurring in the Lie algebra $\mathfrak{g}$ of G. We have the root space decomposition $\mathfrak{g} = \mathfrak{t} \oplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$ with $\mathfrak{t}$ the Lie algebra of T. Now $T(F)$ is Zariski dense in T, hence there exists a Zariski open set $\mathcal{V} \subset T$ such that for all $v \in T(F) \cap \mathcal{V}$, the values $\alpha(v)$ $(\alpha \in \Phi)$ are all different and distinct from 1. Fix $y \in T(F) \cap \mathcal{V}$.

Lemma 16. *There is a Zariski open set $\mathcal{U}$ of G such that the group generated by x and gyg^{-1} is Zariski dense in G for all $g \in \mathcal{U}$.*

Proof. Let H be a proper connected Zariski closed subgroup of G containing (or normalised by) the element y. Then, the Lie algebra $\mathfrak{h}$ splits into eigenspaces for the action of y. Since the values $\alpha(y)$ are all different (and distinct from 1), it follows that $\mathfrak{h} = \mathfrak{t} \cap \mathfrak{h} \oplus \mathfrak{g}_\alpha \cap \mathfrak{h}$. Moreover, $\mathfrak{g}_\alpha = \mathfrak{h} \cap \mathfrak{g}_\alpha$ if the latter is non-zero. Therefore, there exists a proper connected subgroup H' containing T which also contains H (e.g. the one with Lie algebra $\mathfrak{t} \oplus \mathfrak{g}_\alpha$ for all α such that $\mathfrak{h} \cap \mathfrak{g}_\alpha \neq 0$).

The collection of connected subgroups of G containing the maximal torus T is finite since such subgroups are in one to one correspondence with certain subsets of the finite set of roots Φ. Let $H_1, \cdots, H_n$ be the set of **proper** connected subgroups of G containing T. By replacing x by a power of it, we may assume that the Zariski closure Z of the group generated by x is connected. Since G is simple, the group generated by $< gZg^{-1} : g \in G >$ is all of G. Hence, for each μ, the set $Z_\mu = \{g \in G : gZg^{-1} \subset H_\mu\}$ is a **proper** Zariski closed set, whence its complement U_μ is open. Therefore, $\mathcal{U} = \cap_{1 \leq \mu \leq n} U_\mu$ is also Zariski open.

Let $g \in \mathcal{U}$ and H be the connected component of the Zariski closure of the group generated by x and gyg^{-1}. If $H \neq G$, then by the first paragraph of the proof, there exists a proper connected subgroup H' containing H and the torus T. By the foregoing paragraph, H' must be one of the H_μ whence, $g \notin U_\mu$, and so $g \notin \mathcal{U}$, a contradiction. Therefore, $H = G$ and the lemma is proved. $\square$

3.3. **Notation.** Suppose that G is an absolutely simple algebraic group over a number field K, with K-rank $(G) \geq 2$. Let S be a maximal split torus, and $\Phi(G, S)$ the root system. Let Φ^+ be a system of positive roots, $\mathfrak{g}$ the L:lie algebra of G. Let U_0 be the subgroup of G whose Lie algebra is $\oplus_{\alpha > 0} \mathfrak{g}_\alpha$, and P_0 the normaliser of U_0 in G; then $P_0 = Z(S)U_0$ where $Z(S)$ is the centraliser of S in G. Moreover, P_0 is a minimal parabolic K-subgroup of G.

Let $\alpha \in \Phi^+$ be the highest root and $\beta > 0$ a "second-highest" root. Then, $\gamma = \alpha - \beta$ is a simple root. Let U_α and U_β be the root groups corresponding to α and β.

Proposition 17. *Let $\Gamma \subset G(O_K)$ be a Zariski dense subgroup. Suppose that there exists an integer $r > 0$ such that $\Gamma \supset U_\alpha(rO_K)$ and $\Gamma \supset U_\beta(rO_K)$. Then, Γ has finite index in $G(O_K)$.*

Proof. This is proved in [V2]. We sketch the proof, since we will use this repeatedly in the case of the groups of K-rank ≥ 2, for which the criterion of Proposition 15 fails. If w denotes the longest Weyl group element, then the double coset $P_0 w U_0$ is a Zariski open subset of G. Hence its intersection with Γ is Zariski dense in G. Fix an element $g_0 = p_0 w u_0 \in \Gamma \cap P_0 w U_0$ and consider an arbitrary element $g = pwu \in PwU \cap \Gamma$.

The subgroup $V = U_\alpha U_\beta$ is normalised by all of P. By assumption, there exists an integer r such that $\Gamma \supset V(rO_K)$. Hence Γ contains the group $<^g (V(rO_K)), V(rO_K) >$. By the Bruhat decomposition of g, and the fact that V is normalised by P, we find an integer r' such that ${}^g(V(rO_K)) \supset^p (V^-(r'O_K))$ where $V^- = U_{-\alpha}U_{w(\beta)}$ is the conjugate of V by w. Note that $-w(\beta)$ is again a second highest root. Write $\gamma = \alpha + w(\beta)$. Then γ is a simple root. Moreover, it can be proved that the commutator subgroup $[U_\alpha, U_{w(\beta)}]$ is not trivial and is all of U_γ. Therefore, we get ${}^p(U_\gamma(rO_K)) \subset \Gamma$ for a Zariski dense set of $p's$ (r depends on the element p). It can be proved that the group generated by ${}^p(U_\gamma)$ is all of the unipotent radical U_1 of the maximal parabolic subgroup corresponding to the simple root γ. Consequently, for some integer r, $U_1(rO_K) \subset \Gamma$, and by [V2], a Zariski dense subgroup of $G(O_K)$ which intersects the unipotent radical of a K-parabolic subgroup in an arithmetic group, it itself arithmetic. Therefore, Γ is arithmetic. □

We will now deduce a corollary to Lemma 16 and Proposition 17.

Corollary 1. *Under the notation and assumptions of this subsection, suppose that every arithmetic subgroup Γ_0 of $G(O_K)$ contains a 2 generated subgroup $< a, b >$ which* **contains** *a group of the form*

$$U_\alpha(rO_K)U_\beta(rO_K)$$

for some second highest root β. Then, every arithmetic subgroup of $G(O_K)$ is virtually three-generated.

Proof. Given $a, b \in \Gamma_0$ such that $< a, b >$ contains the group $(U_\alpha U_\beta)(rO_K)$ for some integer r, Lemma 16 implies the existence of an element $c \in \Gamma$ such that the group $\Gamma =< a, b, c >$ generated by a, b, c is Zariski dense in G (Γ_0 itself is Zariski dense in G by the Borel density theorem). Then, by Lemma 17, Γ is of finite index in Γ_0. □

4. Groups of K-rank ≥ 2

In this section, we verify that all arithmetic groups of K-rank at least two are virtually three-generated. The proof proceeds case by case, using the Tits classification of algebraic groups over a number field K. In most cases, we check that the hypotheses of criterion of Proposition 15 are satisfied. In the sequel, G is an absolutely almost simple group defined over a number field K, with K-rank $(G) \geq 2$. The degree of $K/\mathbb{Q}$ is denoted k.

The classical groups over $\mathbb{C}$ come equipped with a natural (irreducible) representation, which we refer to as the **standard** representation, and denote it St.

4.1. **Groups of Inner Type A.** In this subsection, we consider all groups which are inner twists of $SL(n)$ over K. By [T2], the only such groups are SL(n) over number fields or SL(m) over central division algebras over number fields.

4.1.1. *SL(n) over number fields.* G is SL(n) over the number field K. The rank assumption means that $n \geq 3$. Take P to be the parabolic subgroup of SL(n) consisting of matrices of the form $\begin{pmatrix} g & x \\ 0 & detg^{-1} \end{pmatrix}$, where $g \in GL(n-1)$, $x = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_{n-1} \end{pmatrix}$ is a column vector of size $n-1$, and 0 is the $1 \times (n-1)$ matrix whose entries are all zero. The Levi part M of P may be taken to be $GL(n-1) = \{ \begin{pmatrix} g & 0 \\ 0 & det(g^{-1}) \end{pmatrix} : g \in GL(n-1)\}$. Recall that M_0 is the connected component of identity of the Zariski closure of $M(O_K)$. Hence M_0 contains the subgroup $H = SL(n-1)$, by Lemma 13. Take T_0 to be the diagonals in $SL(n-1)$. The unipotent radical of P is the group $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ with x a column vector as before. As a representation of $GL(n-1)(\mathbb{C})$ (and therefore of $H(\mathbb{C}) = SL(n-1)(\mathbb{C})$), the Lie algebra $\mathfrak{u}$ is nothing but $St \otimes det$, the standard representation twisted by the determinant. Restricted to the torus T_0, thus $\mathfrak{u}$ is the standard representation, and is hence multiplicity free. By Proposition 15, it follows that every arithmetic subgroup of $G(O_K)$ is virtually three-generated.

4.1.2. *SL(m) over division algebras.* $G = SL_m(D)$ where D is a central division algebra over the number field K, of degree $d \geq 2$. The rank assumption means that $m \geq 3$. Consider the central simple algebra $D \otimes_{\mathbb{Q}} \mathbb{R}$, denoted $D \otimes \mathbb{R}$ for short. Then, $D \otimes \mathbb{R}$ is a product of copies of $M_d(\mathbb{C})$, $M_{d/2}(\mathbf{H})$, and $M_d(\mathbb{R})$ where $\mathbf{H}$ is the division algebra of Hamiltonian quaternions. We consider four cases.

Case 1. $D \otimes \mathbb{R} \neq \mathbf{H} \times \cdots \mathbf{H}$.

Then, $SL_1(D \otimes \mathbb{R})$ is a non-compact semi-simple Lie group with either $SL_d(\mathbb{C})$ or $SL_d(\mathbb{R})$ or $SL_{d/2}(\mathbf{H})$ (the last can happen only if $d \geq 3$ is even) as a non-compact factor. Then, the Zariski closure of the arithmetic subgroup $SL_1(O_D)$ of $SL_1(D)$ (for some order O_D of D) is the noncompact group $SL_1(D \otimes \mathbb{R})$ by Lemma 13.

Take P to be the parabolic subgroup (with the obvious notation) $P = \begin{pmatrix} GL_1(D) & * \\ 0 & GL_{m-1}(D) \end{pmatrix}$, with unipotent radical $U = \begin{pmatrix} 1 & M_{1\times m}(D) \\ 0 & 1 \end{pmatrix}$ where $M_{1\times m}(D)$ denotes the spaces of $1 \times m$ matrices with entries in the division algebra D. The group M_0 obviously contains (from the observation in the last paragraph) the group $H = \begin{pmatrix} SL_1(D) & 0 \\ 0 & SL_{m-1}(D) \end{pmatrix}$, with $H(K \otimes \mathbb{C}) = [SL_d(\mathbb{C}) \times SL_{d(m-1)}(\mathbb{C})]^k$. Let T_0 be the product of the diagonals in each copy of $SL_d \times SL_{d(m-1)}$. As a representation of H, the Lie algebra $\mathfrak{u}$ of U is the direct sum $\oplus \mathbb{C}^d \otimes (\mathbb{C}^{(m-1)d})^*$, where the sum is over each copy of $SL_d \times SL_{(m-1)d}$. $\mathbb{C}^d$ is the standard representation of SL_d and $*$ denotes its dual. It is then clear that as a representation of the (product) diagonal torus T_0, $\mathfrak{u}$ is multiplicity free. Hence the criterion of Proposition 15 applies. Every arithmetic subgroup of $G(O_K)$ is virtually three-generated.

Case 2. $D \otimes \mathbb{R} = \mathbf{H} \times \cdots \times \mathbf{H}$ *but* $m \geq 4$.

This can happen only if $d = 2$, and $D \otimes \mathbb{R} = \mathbf{H}^k$. Take P to be the parabolic subgroup $P = \begin{pmatrix} SL_{m-2}(D) & * \\ 0 & SL_2(D) \end{pmatrix}$ and denote its unipotent radical by U, with $U = \begin{pmatrix} 1 & M_{(m-2)\times 2}(D) \\ 0 & 1 \end{pmatrix}$. Then, as before, M_0 contains $H = \begin{pmatrix} SL_{m-2}(D) & 0 \\ 0 & SL_2(D) \end{pmatrix}$. Then, $H(K \otimes \mathbb{C}) = [SL_{(m-2)2}(\mathbb{C}) \times SL_4(\mathbb{C})]^k$. As a representation of $H(K \otimes \mathbb{C})$, $\mathfrak{u}$ is the k-fold direct sum $\mathbb{C}^{(m-2)2} \otimes (\mathbb{C}^4)^*$. Let T_0 be the product of the diagonals in $H(K \otimes \mathbb{C})$. Then, it is clear that $\mathfrak{u}$ is multiplicity free as a representation of T_0. By Proposition 15 every arithmetic subgroup of $G(O_K)$ is virtually three-generated.

Case 3. $D\otimes\mathbb{R}=\mathbf{H}\times\cdots\times\mathbf{H}$, $m=3$ *but* $k\geq 2$.

In this case it turns out that the criterion of Proposition 15 fails (we will not prove that it fails), so we give an ad hoc argument that every arithmetic subgroup of $SL_3(D)$ is virtually three-generated.

Since $D\otimes\mathbb{R}=\mathbf{H}^k$, it follows that K is totally real. Since $k\geq 2$, K has infinitely many units. By lemma 3, for every subgroup Δ of finite index in O_K^*, $\mathbb{Q}[\Delta]=K$. By Lemma 4, there exists an element $\theta\in\Delta$ such that $\mathbb{Q}[\theta^r]=K$ for all $r\geq 1$. Consider the 3×3 - matrix $m=\begin{pmatrix}\theta^{k_1} & 0 & 0\\ 0 & \theta^{k_2} & 0\\ 0 & 0 & \theta^{-k_1-k_2}\end{pmatrix}$ which lies in $SL_3(O_D)$ for some order O_D in D.

Consider the following matrices in $SL_3(D)$ given by $u=\begin{pmatrix}1&1&1\\0&1&x\\0&0&1\end{pmatrix}$, and $u^-=\begin{pmatrix}1&0&0\\y&1&0\\z&t&1\end{pmatrix}$, where x,y,z,t are elements of the division algebra such that no two of x,y,z,t,tx commute. We may assume that they lie in the order O_D. We will prove that for every $r>0$, the group $\Gamma=<m^r,u^r,(u^-)^r>$ generated by the r-th powers of m,u,u^- is arithmetic. This will prove that every arithmetic subgroup of $GO_K)$ is virtually three generated. We use the following notation. If $i,j\leq 3$, $i\neq j$ and w is an element of O_D, denote by $x_{ij}^{O_Kw}$ the subgroup $1+cwE_{ij}$ where, c runs through elements of O_K; E_{ij} is the matrix whose ij-th entry is 1 and all other entries are zero. We also write $x_{ij}^{O_Kw}\leq\Gamma$ to say that for some integer r', the subgroup $x_{ij}^{r'O_Kw}$ is contained in Γ.

For ease of notation, we replace the r-th powers of m,u,u^- by the same letters m,u,u^-; this should cause no confusion. Then, the group $<^{m^l}(u):l\in\mathbb{Z}>$ virtually contains the subgroups (by the choice of θ; see Lemma 4) $x_{12}^{O_K}$, $x_{13}^{O_K}$ and $x_{23}^{xO_K}$. Similarly, $<m^l(u^-):l\in\mathbb{Z}>$ virtually contains $x_{21}^{O_Ky},x_{31}^{O_Kz}$ and $x_{32}^{O_Kt}$. Since Γ contains all these groups, by taking commutators, we get $x_{12}^{O_Kt}=[x_{13}^{O_K},x_{32}^{tO_K}]\leq\Gamma$. Similarly, $x_{13}^{O_Kx}=[x_{12}^{O_K},x_{23}^{O_Kx}]\leq\Gamma$, and $x_{13}^{O_Ktx}=[x_{12}^{O_Kt},x_{23}^{xO_K}]\leq\Gamma$. By taking suitable repeated commutators, we obtain

$$x_{13}^{O_K+O_Ktx+O_Kx+O_Ky}\leq\Gamma.$$

Since up to subgroups of finite index $O_D = OK + O_K tx + O_K x + O_K y$, we see that $x_{13}^{O_D} \leq \Gamma$, and similarly, $x_{ij}^{O_D}$ for all ij with $i \neq j$. Therefore, $\Gamma \supset U(O_K)$ and $U^-(O_K)$ for two opposing maximal unipotent subgroups of G. By [R 4], Γ is then an arithmetic group.

Case 4. $D \otimes \mathbb{R} = \mathbf{H}^k$, $m = 3$ and $k = 1$.

The assumptions mean that $K = \mathbb{Q}$, and $D \otimes \mathbb{R} = \mathbf{H}$. Consider the elements $m_0 = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $u_0 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = x_{13}$, $u_0^- = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = x_{32}$. We assume that the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is "generic". In particular, assume that $c \notin \mathbb{Q}$ and that $e = ca + dc$ does not commute with c. Fix $r \geq 1$ and put $\Gamma = < m_0^r, u_0^r, (u_0^-)^r >$. By arguments similar to the last case, it is enough to prove that Γ is an arithmetic subgroup of $SL_3(O_D)$ for some order O_D of the division algebra D.

We have $x_{13}^{\mathbb{Z}} \leq \Gamma$ and $x_{32}^{\mathbb{Z}} \leq \Gamma$. By taking commutators, we get $x_{12}^{\mathbb{Z}} \leq \Gamma$.

The conjugate ${}^{m^0}(u_0) = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$. Hence we get $\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{\mathbb{Z}} \leq \Gamma$. By taking commutators with $x_{12}^{\mathbb{Z}}$, we then get $x_{13}^{\mathbb{Z}[c]} \leq \Gamma$. Taking commutators with $x_{32}^{\mathbb{Z}} \leq \Gamma$, we obtain $x_{12}^{\mathbb{Z}[c]} \leq \Gamma$ as well.

Consider $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} a^2 + bc \\ ca + dc \end{pmatrix} = \begin{pmatrix} a' \\ e \end{pmatrix}$. Clearly, ${}^{m_0^2}(u_0) = \begin{pmatrix} 1 & 0 & a' \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix}$. By the argument of the last paragraph, taking commutators of its conjugates with $x_{12}^{\mathbb{Z}[c]}$ we obtain $x_{13}^{\mathbb{Z}[e]\mathbb{Z}[c]} \leq \Gamma$. Since e and c do not commute and D has dimension 4 over $\mathbb{Q}$, it follows that the additive group $\mathbb{Z}[e]\mathbb{Z}[c]$ is of finite index in an order O_D of D. Therefore, $x_{13}^{O_D} \leq \Gamma$. Taking commutators with $x_{32}^{\mathbb{Z}} \leq \Gamma$, we obtain $x_{12}^{O_D} \leq \Gamma$ (and $x_{13}^{O_D} \leq \Gamma$). Thus, Γ intersects the unipotent radical (consisting of x_{12} and x_{13} root groups) of a parabolic subgroup of G. Clearly, Γ is Zariski dense. Therefore by [V2] (see also [O]), Γ is arithmetic.

4.2. **Groups of outer type A.** Suppose that K is a number field of degree $k \geq 1$ over $\mathbb{Q}$. Let E/K be a quadratic extension and $\sigma \in Gal(E/K)$ be the non-trivial element. Suppose that D is a central division algebra over E of degree $d \geq 1$ (as usual d^2 is the dimension of D as a vector space over E). Assume there is an involution $*$ on D such that its restriction to the centre E coincides with σ. If $N \geq 1$ is an integer, and $g \in M_N(D)$, with $g = (g_{ij})$ is an $N \times N$ matrix with entries in D, then define g^* as the matrix with ij-th entry given by $g^*_{ij} = (g_{ij})^*$. Thus, $M_N(D)$ gets an involution $g \mapsto ({}^t g)^*$.

Fix an integer $m \geq 0$. Consider the $(m+4) \times (m+4)$-matrix $h = \begin{pmatrix} 0_{2\times 2} & 0_{2\times m} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 0_{m\times 2} & h_0 & 0_{m\times 2} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 0_{2\times m} & 0_{2\times 2} \end{pmatrix}$, where $0_{p\times q}$ denotes the zero matrix of the relevant size. Here h_0 is a non-singular $m \times m$ matrix with entries in D such that $({}^t h_0)^* = h_0$. Then h defines a Hermitian form with respect to $*$ on the $m+4$ dimensional vector space over D. The algebraic group we consider is of the form

$$G = SU_{m+4}(h, D) = \{g \in SL_{m+4}(D) : ({}^t g)^* h g = h\}.$$

Then G is an absolutely simple algebraic group over K. Since h contains **two** copies of the "hyperbolic" Hermitian form $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ it follows that K-rank $(G) \geq 2$. From the classification tables of [T2], these G are the only outer forms of type A of K-rank at least two.

Arithmetic subgroups Γ_0 of G are commensurate to $G \cap GL_{m+4}(O_D)$ for some order O_D of the division algebra D. Consider the subgroup

$$H = \{\begin{pmatrix} g & 0 & 0 \\ 0 & 1_m & 0 \\ 0 & 0 & J[({}^t g)^*]^{-1} J^{-1} \end{pmatrix} : g \in SL_2(D)\}.$$

Since $\Gamma_0 \cap H$ is an arithmetic subgroup of H, it follows that $\Gamma_0 \cap H \simeq SL_2(O_D)$. Since $H(K \otimes \mathbb{R}) = SL_2(D \otimes \mathbb{R})$ is non-compact, it follows from the Borel density theorem (see Lemma 13) that $\Gamma_0 \cap H$ is Zariski dense in the group $H(K \otimes \mathbb{C}) = [SL_{2d}(\mathbb{C}) \times SL_{2d}(\mathbb{C})]^k$. The intersection of G with diagonals is at least two dimensional, and is a maximal K-split torus S, if h_0 is suitably chosen (that is, split off all the hyperbolic forms in h_0 in the same way as was done for *two* hyperbolic forms for h).

With respect to S, the intersection of unipotent upper triangular matrices with G yields a maximal unipotent subgroup U_0 of G and the roots of S occurring in the Lie algebra $\mathfrak{u}_0$ of U_0 form a system Φ^+ of positive roots. If α and β are the highest and a second highest root in Φ^+, then the group $U_\alpha(O_K)U_\beta(O_K)$ is contained in the group $U = \{\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : x \in M_2(O_D), ({}^t x)^* + JxJ = 0\}$. Now, as a module over $H(K \otimes \mathbb{C}) = [SL_{2d}(\mathbb{C}) \times SL_{2d}(\mathbb{C})]^k$, the Lie algebra $LieU(\mathbb{C})$ is isomorphic to $[\mathbb{C}^{2d} \otimes (\mathbb{C}^{2d})^*]^k$ and has distinct eigenvalues for the diagonals T_H in $H(K \otimes \mathbb{C})$ (thought of as a product of copies of $SL_{2d}(\mathbb{C})$). Therefore, by section 3 (cf. the proof of Proposition 15), there exist $m_0 \in \Gamma_0 \cap H$, $u_0 \in U \cap \Gamma_0$ such that the group generated by the conjugates $\{{}^{m_0^j}(u_0) : j \in \mathbb{Z}\}$ contains the group $U(rO_K)$ for some integer r. Now the criterion of Proposition 17 says that there exists a $\gamma_0 \in \Gamma_0$ such that the three-generated group $\Gamma =< \gamma_0, m_0, u_0 >$ is of finite index in Γ_0.

4.3. **Groups of type B and inner type D.** (i.e. type ${}^1D^1_{n,r}$). In this subsection, we consider groups of the form $G = SO(f)$ with f a non-degenerate quadratic form in n variables over K, $n \geq 5$ (and $n \geq 8$ if n is even). Assume that f is a direct sum of two copies of a hyperbolic form and another non-degenerate form f_2: $f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus f_2$.

Put $f_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus f_2$. Then $f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus f_1$. Then, K-rank $(G) \geq 2$. Consider the subgroup $P = \{\begin{pmatrix} a & x & -\frac{x{}^t x}{2} \\ 0 & SO(f_1) & -{}^t x \\ 0 & 0 & a^{-1} \end{pmatrix} : a \in \mathbf{G}_m, x \in K^{n-2}\}$. Then P is a parabolic subgroup of G with unipotent radical $U = \{\begin{pmatrix} 1 & x & -\frac{x{}^t x}{2} \\ 0 & 1 & -{}^t x \\ 0 & 0 & 1 \end{pmatrix} : x \in K^{n-2}\}$. Now, the group $SO(f_1)$ is isotropic over K since f_1 represents a zero. Moreover, since $n-2 \geq 3$, $SO(f_1)$ is a semi-simple algebraic group over K. Hence by lemma 13 $SO(f_1)(O_K)$ is Zariski dense in $SO(f_1)(K \otimes \mathbb{C})$. Consequently, M_0 contains the subgroup $SO(f_1)$. Moreover, as a representation of $SO(f_1)(K \otimes \mathbb{C}) = SO(n-2)(\mathbb{C})^k$, the Lie algebra $\mathfrak{u}(K \otimes \mathbb{C})$ of U is the standard representation St^k. Clearly, for a maximal torus in $SO(n-2)(\mathbb{C})$, the standard representation is multiplicity free. Therefore, the criterion of Proposition 15 applies: every arithmetic subgroup of $G(O_K)$ is virtually three-generated.

4.4. **Groups of type C and the rest of the Groups of type D.**

4.4.1. *$G = Sp_{2n}$ over K with $n \geq 3$.* Denote by

$$\kappa = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

the $n \times n$ matrix all of whose entries are zero, except for the anti-diagonal ones, which are all equal to one. Let $J = \begin{pmatrix} 0_n & \kappa \\ -\kappa & 0_n \end{pmatrix}$ be the non-degenerate $2n \times 2n$ skew symmetric matrix. Define the symplectic group $G = Sp_{2n} = \{g \in SL_{2n} :^t gJg = J\}$. The group $P = \{\begin{pmatrix} g & 0 \\ 0 & \kappa^t g\kappa^{-1} \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x + \kappa^t x\kappa = 0, g \in GL_n\}$ is a parabolic subgroup. Denote by M the Levi subgroup of P such that $x = 0$. Then, by Lemma 13, $M_0 \supset H \simeq SL_n = \{\begin{pmatrix} g & 0 \\ 0 & \kappa^t g\kappa^{-1} \end{pmatrix}\}$. As a representation of H, the Lie algebra $\mathfrak{u}$ of the unipotent radical U of P is seen to be isomorphic to $S^2(\mathbb{C}^n)$, the second symmetric power of the standard representaqtion of $H = SL_n$. Therefore, with respect to the diagonal torus T_H of H, the representation $\mathfrak{u}$ is multiplicity free. Therefore, by Proposition 15, every arithmetic subgroup of $Sp_{2n}(O_K)$ is three-generated.

4.4.2. *Other Groups of type C and D.* In this subsection, we will consider all groups of type C or D, which are not covered in the previous subsections. Let D be a **quaternionic** division algebra over the number field K. Let σ be an involution (of the first kind) on D. In the case of type C (resp. type D), assume that the space D^σ of σ-invariants in D is one dimensional (resp. three dimensional) over K. Let $m \geq 0$ be an integer. Consider the $m+4$ dimensional matrix $h = \begin{pmatrix} 0_2 & 0 & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 0 & h_0 & 0 \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 0 & 0 \end{pmatrix}$, where h_0 is a non-singular matrix with entries in D, such that ${}^t\sigma(h_0) = h_0$. We will view h as a non-degenerate form on $D^{m+4} \times D^{m+4}$ with values in D, which is hermitian with respect to the involution σ. The algebraic group which we consider is the special unitary group of this hermitian form: $G = SU(h)$ - an algebraic group over K (if D^σ is three dimensional, then G is of type ${}^1D$ or ${}^2D$ according as the discriminant of h is 1 or otherwise). With this choice of h, it is immediate that K-rank $(G) \geq 2$ (h has two copies of the hyperbolic form: cf. the subsection on groups of outer type A).

Since We needed K-rank $(G) \geq 2$ we had split off two hyperbolic planes from h. The form h_0 may have more hyperbolic planes in it; after splitting these off in a manner similar to that for h, we obtain a form h_1 which is anisotropic over K. We will assume that h_0 is of this type. Then, the intersection of G with the diagonals is a maximal K-split torus S in G. The roots of S occurring in the group of unipotent upper triangular matrices in G form a positive system Φ^+. Choose α the highest root and a second highest root β in Φ^+.

The group $U_\alpha U_\beta$ is contained in the unipotent group $U = \{ \begin{pmatrix} 1_2 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} :$ x *suitable*$\}$ which is the unipotent radical of a parabolic subgroup. Set $H = \{ \begin{pmatrix} g & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & J^t g J^{-1} \end{pmatrix} : g \in SL_2(D)\}$. Then, M_0 contains H. Let $\Gamma_0 \subset G(O_K)$ be an arithmetic subgroup. Then, there exist $m_0 \in H(O_K) \cap \Gamma_0$ and $u \in U(O_K) \cap \Gamma_0$ such that the group generated by m_0 and u (denoted as usual by $< m_0, u >$) intersects $(U_\alpha U_\beta)(O_K)$ in a subgroup of finite index. By Lemma 16, there exists an element $\gamma \in \Gamma_0$ such that $\Gamma =< m_0, u, \gamma >$ is Zariski dense in $G(K \otimes \mathbb{C})$. By Proposition 17, Γ has finite index in Γ_0: Γ_0 is virtually three-generated.

4.5. **The Exceptional Groups.** In this subsection, we prove Theorem 1 for all groups G of exceptional type of K-rank ≥ 2. In each of these cases, we will locate a simple K-root in the Tits -Dynkin diagram of G, such that the Levi subgroup (actually the group M_0 contained in the Levi) of the parabolic group corresponding to the simple root contains a subgroup H with the following property. $H(K \otimes \mathbb{C})$ has a maximal torus T_H whose action on the Lie algebra $\mathfrak{u} = Lie(U)(K \otimes \mathbb{C})$ is multiplicity free. By Proposition 15, this implies that every arithmetic subgroup of $G(K)$ is virtually three-generated. The notation is as in [T2].

4.5.1. *the groups* ${}^3D_{4,2}^2$ *and* ${}^6D_{4,2}^2$. In the Tits diagram, there is one simple circled root α, and three other simple roots which are circled together. The semi-simple part M_{ss} of the Levi is therefore K-simple, and hence contains (over $\mathbb{C}$), the group $SL_2(\mathbb{C})^3$ (three-fold product of $SL(2)$). Moreover, by Lemma 13, $M_{ss}(O_K)$ is Zariski dense in $M_{ss}(K \otimes \mathbb{C})$. Thus, $M_{ss} \subset M_0$. According to [L] and [Sh], the representation $\mathfrak{u}$

is the direct sum of $St \otimes St \otimes St$ and $1 \otimes St \otimes 1$ (St is the standard representation and 1 is the trivial one). This is multiplicity free for the product of the diagonals in the group $SL(2)^3$.

4.5.2. *Groups of type E_6.* There are three groups of inner type E_6 with K-rank ≥ 2.

Case 1. $G = {}^1E_{6,2}^{28}$. The extreme left root in the diagram is circled. Since its K-rank is ≥ 1, the group M_{ss} of the Levi of the corresponding maximal parabolic subgroup is non-compact. Then, as in (4.5.3), M_0 contains $M_{ss} = SO(10)$ over $\mathbb{C}$. According to [L], the representation on $\mathfrak{u}$ is one of the $\frac{1}{2}$-spin representation of $SO(10)$ and has distinct characters for the maximal torus.

Case 2. $G = {}^1E_{6,2}^{16}$. Over the number field K, the diagram is that of ${}^1E_{6,2}^{16}$. The root in the middle of the diagram is circled. However, over any archimedean completion, the diagram can only be the split form (${}^1E_{6,2}^{16}$ can not transform into ${}^1E_{6,2}^{28}$ over $\mathbb{R}$ or $\mathbb{C}$). Consequently, $M(K \otimes \mathbb{R})$ contains $SL_3 \times SL_2 \times SL_3$, whence , by Lemma 13, $M_0 \supset SL_3 \times SL_2 \times SL_3$. According to [Sh], the representation of $M_0(\mathbb{C})$ on $\mathfrak{u}$ is the direct sum of $St_{SL_3} \otimes St_{SL_2} \otimes \wedge^2 St_{SL_3}$ (from now on we will drop the subscript SL_3 or SL_2 for ease of notation), $\wedge^2 St \otimes Triv \otimes St$ and $Triv \otimes St \otimes Triv$. It is clear that restricted to the product of the diagonals in $SL_3 \times SL_2 \times SL_3$, the representation $\mathfrak{u}$ has multiplicity one.

Case 3. $G = {}^1E_{6,6}^{0}$. The same M_0 as in Case 2 works, to prove multiplicity one for the torus.

Now consider the groups of outer type E_6 of K-rank ≥ 2. These are ${}^2E_{6,2}^{16'}$, ${}^2E_{6,2}^{16''}$, and ${}^2E_{6,4}^{2}$. In all these, the root at the extreme left is circled. Then, since K-rank $(M) \geq 1$, it follows that $M_0(\mathbb{C}) \supset SL_6$. The representation on $\mathfrak{u}$ is (by [L], page 49, (x)) the direct sum of $Triv$ and $\wedge^3(St)$ and the diagonal torus in SL_6 has multiplicity one for its action on $\mathfrak{u}$.

4.5.3. *Groups of type E_7.* There are four groups of type E_7 over a number field K with K-rank ≥ 2. They are $E_{7,2}^{31}$, $E_{7,3}^{28}$, $E_{7,4}^{9}$ and $E_{7,7}^{0}$. In all these, the root on the extreme right is circled, and M has K-rank ≥ 1. Hence $M_0(\mathbb{C})$ contains the semi-simple part of the Levi group M. This is $SO(12)$. According to [L], the representation $\mathfrak{u}$ of $SO(12)$ is $triv \oplus \frac{1}{2}spin$ which has distinct eigenvalues for the torus in $SO(12)$.

4.5.4. *Groups of type E_8.* The groups with K-rank ≥ 2 are $E_{8,4}^{28}$ and $E_{8,8}^{0}$. Consider the root on the extreme right in the diagram. The corresponding M has semi-simple (actually simple) part $SO(14)$ which is isotropic over K. The representation $\mathfrak{u}$, according to [L], is $\frac{1}{2}$-spin $\oplus St$ and has multiplicity one for the maximal torus of $SO(14)$.

4.5.5. *The groups F_4.* There is only one K-rank ≥ 2 group, namely the split one, denoted $F^0_{4,4}$. Take the root on the extreme left. Then $M_0 \supset SO(7)$. The representation is $triv \oplus \frac{1}{2}spin$ and is multiplicity free for the action of the maximal torus in $SO(7)$.

4.5.6. *Groups of type G_2.* . The only group is $G^0_{2,2}$, the split form. For the root on the extreme left, the group M_0 contains $SL(2)$ and the representation $\mathfrak{u}$ is $Triv \oplus Sym^3$ which has distinct eigenvalues for the action of the maximal torus in $SL(2)$.

This completes the proof of Theorem 1 for groups of K-rank ≥ 2.

5. Classical Groups of Rank One

The case of groups G such that K-rank $(G) = 1$ and $\mathbb{R}-rank(G_\infty) \geq 2$ is much more involved. We will have to consider many more cases, both for classical and exceptional groups. In some cases, we will have to supply ad hoc proofs, because the general criteria established in the previous sections do not apply.

5.1. **Groups of inner type A.** The assumptions imply that $G = SL_2(D)$ where D is a central division algebra over the number field K.

Case 1. $D = K$. Thus, $G = SL_2$ over K. The assumption that $\mathbb{R}-rank(G_\infty) \geq 2$ is equivalent to $r_1 + r_2 \geq 2$. Therefore, K has infinitely many units. This case has been covered in Section (2.1) on $SL(2)$.

Case 2. $D \neq K$, $D \otimes_{\mathbb{Q}} \mathbb{R} \neq \mathbf{H} \times \cdots \times \mathbf{H}$. Here $\mathbf{H}$ denotes the algebra of Hamiltonian quaternions. Consider the parabolic subgroup $P = \{\begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : g, h \in GL_1(D), Det(gh) = 1, x \in D\}$. Let U be its unipotent radical. The assumption on D means that $SL_1(D \otimes \mathbb{R})$ is not compact, and $SL_1(D \otimes_{\mathbb{Q}} \mathbb{C})$ contains $SL_1(O_D)$ as a Zariski dense subgroup (Lemma 13). Therefore, M_0 contains the subgroup M_1 with $M_1(K \otimes \mathbb{C}) = [SL_2(\mathbb{C}) \times SL_2(\mathbb{C})]^k$. As a representation of $M_1(\mathbb{C})$, the Lie algebra $\mathfrak{u} = (LieU)(K \otimes \mathbb{C})$ is $[St \otimes St^*]^k$ and is multiplicity free for the action of the maximal torus ($2k$-fold product of the diagonals in $SL_2(\mathbb{C})$). Therefore, every arithmetic subgroup of $G(K)$ is virtually three-generated.

Case 3. $D \neq K$ and $D \otimes_{\mathbb{Q}} \mathbb{R} = \mathbf{H}^k$. Therefore, K is totally real of degree k over $\mathbb{Q}$. The assumption $\mathbb{R}-rank(G_\infty) \geq 2$ means that $K \neq \mathbb{Q}$. Let P, M be the parabolic subgroup and its Levi subgroup in Case 2 of the present subsection. Fix $m = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in M(K)$ such that $\delta = \alpha\beta^{-1}$ does not lie in K. Since $D \otimes \mathbb{R} = \mathbf{H}^k$, it follows that the extension $K(\delta)/K$ is a CM extension. Fix $u_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $m_0 = \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}$ where $\theta \in O_K^*$ is chosen as in Lemma 4. Fix $\gamma \in G(O_K)$ in general position with respect to u_+ and m_0. Then, for every integer r, the group $\Gamma = < u_+^r, m_0^r, \gamma^r >$ generates a Zariski dense subgroup of G (see Lemma 16). We will show that Γ is arithmetic, proving that every arithmetic subgroup of $G(K)$ is virtually 3-generated (since arithmetic groups contain a group of the form $<\gamma^r, m_0^r, u_+^r>$ for some integer r).

Since Γ contains θ^r and u_+, it follows that for some integer r', Γ contains the group $V^+ = \begin{pmatrix} 1 & r'O_K \\ 0 & 1 \end{pmatrix}$. Pick a generic element $g \in \Gamma$, with Bruhat decomposition of the form $g = umwv$, where $m = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ may be assumed to be as in the foregoing paragraph. Then, $\Gamma \supset <^g (V^+), V^+>$. Note that u, v centralise the group V^+; put $V^- =^w (V^+)$. One sees that $\Gamma \supset^u <^m (V^-), V^+> =^u < \begin{pmatrix} 1 & 0 \\ \alpha^{-1}\beta r'O_K & 1 \end{pmatrix}, \begin{pmatrix} 1 & r'O_K \\ 0 & 1 \end{pmatrix} >$. By the result on SL(2) over CM fields (Proposition 7), $\Gamma \supset^u (\Delta)$ for some subgroup Δ of finite index in $SL_2(O_E)$, where $E = K(\alpha^{-1}\beta)$ a CM extension of K. In particular, there exists an integer r'' such that $\Gamma \supset^u (\theta^{r''\mathbb{Z}})$. By Proposition 10, it follows that Γ is arithmetic.

5.2. **Groups of outer type A.**

5.2.1. **The Groups SU(h) over fields.** In this subsection, K is a number field, E/K a quadratic extension whose non-trivial Galois automorphism is denoted σ. Let $h : E^{n+1} \times E^{n+1} \to E$ denote a σ-hermitian form which is isotropic over K, and write $h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus h_0$ where h_0 is **anisotropic** over K. Let $G = SU(h)$ be the special unitary group of this hermitian form. Then, K-rank (G)=1. The positive roots are α and 2α. Assume that $\mathbb{R}$-rank $(G_\infty) \geq 2$. Therefore, $\mathbb{R}$-rank $(SU(h_0))_\infty \geq 1$. The arguments are general when K has infinitely many units or when n is large (i.e. $n \geq 4$). But for small n and small fields, the proofs become more complicated, and we give ad hoc arguments. We thus have 5 cases to consider.

Case 1. K has infinitely many units. Note that the 2α root space is one dimensional. Therefore, by the criterion of Proposition 12, every arithmetic group is virtually 3 generated.

Case 2. K is $\mathbb{Q}$ or is an imaginary quadratic extension of $\mathbb{Q}$ but $n \geq 4$. Take P (resp. M) to be the parabolic subgroup of G (resp. Levi subgroup of P), consisting of matrices of the form $\begin{pmatrix} a & * & * \\ 0 & b & * \\ 0 & 0 & \sigma(a)^{-1} \end{pmatrix}$

(resp. $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & \sigma(a)^{-1} \end{pmatrix}$). Then, $(M \supset) M_0 \supset M_1 = SU(h_0)$. The last inclusion holds since the latter group is semi-simple (because $n-2 \geq 2$; we only use the hypothesis that $n \geq 3$, so these observations apply to the next two cases as well) and is non-compact at infinity, and therefore contains an arithmetic subgroup as a Zariski dense subgroup (Lemma 13). Moreover, $SU(h_0)(\mathbb{C}) = SL_{n-1}(\mathbb{C})$, and its representation on the Lie algebra $\mathfrak{u}$ of the unipotent radical of P, is simply $St \oplus St^* \oplus triv$. Since $M_1(\mathbb{C}) = SL_{n-1}(\mathbb{C})$ with $n-1 \geq 3$, the standard representation is not equivalent to its contragredient. Thus the diagonal torus T_1 of M_1 has one dimensional eigenspaces in $\mathfrak{u}$. Hence arithmetic subgroups of $G(K)$ are virtually three- generated.

Case 3. $n = 3$, either $K = \mathbb{Q}$ and $E/\mathbb{Q}$ is real quadratic or K is an imaginary quadratic extension of $\mathbb{Q}$. Then, $SU(h_0)(\mathbb{C}) = SL_2(\mathbb{C})$, but the torus T_1 of the last case does not have multiplicity one in its action on $\mathfrak{u}$. However, observe that M_0 of the last case contains in addition the torus T_2 consisting of matrices $\begin{pmatrix} u & 0 & 0 & 0 \\ 0 & u^{-1} & 0 & 0 \\ 0 & 0 & u^{-1} & 0 \\ 0 & 0 & 0 & u \end{pmatrix}$ with u a unit in the real quadratic extension E (E has infinitely many units). Put $T_0 = T_1 T_2$. Now, $T_0 \subset M_0$ is a torus consisting of matrices of the form $\begin{pmatrix} u & 0 & 0 & 0 \\ 0 & u^{-1}v & 0 & 0 \\ 0 & 0 & u^{-1}v^{-1} & 0 \\ 0 & 0 & 0 & u \end{pmatrix}$ with $u, v \in \mathbf{G}_m$, and has (as may be easily seen) distinct eigenvalues in $\mathfrak{u} : St \oplus St^* \oplus triv = \mathfrak{u}$, where $\mathfrak{u}$ is as in the previous case. Thus, arithmetic subgroups of $G = SU(h)$ are virtually three-generated.

Case 4. $K = \mathbb{Q}$, $n = 3$ and $E/\mathbb{Q}$ is imaginary quadratic. Then, $U(h_0)$ is not contained in M_0 (of course, $SU(h_0) \subset M_0$). We give an ad hoc argument in this particular case.

Write $h_0 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ with $\lambda_1, \lambda_2 \in \mathbb{Q}$ (every Hermitian form in two variables is equivalent to one of this type). Now, $h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus h_0$ is viewed a **hermitian** (with respect to σ) form from $E^4 \times E^4 \to E$.

Consider $f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ as a **quadratic** form on $\mathbb{Q}^4$. Now, the $\mathbb{Q}$-group $SU(h)$ contains the group $H = SO(f)$ as a $\mathbb{Q}$-subgroup. Since $SU(h_0)_\infty = SU(1,1)$ is non-compact (as we have seen before, this follows from the fact that the real rank of G_∞ is ≥ 2), it follows that $SO(f_0)_\infty = SO(1,1)$ is also non-compact. Here $f_0 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ is viewed as a quadratic form. Consequently, the group $SO(f)(\mathbb{R}) \supset SO(1,1) \times SO(1,1)$ and therefore has real rank ≥ 2.

Claim: $H = SO(f)$ is a $\mathbb{Q}$-simple group. For, if $SO(f)$ is not $\mathbb{Q}$-simple, (since it is isogenous over $\mathbb{C}$ to the product $SL_2(\mathbb{C}) \times SL_2(\mathbb{C})$) then it is isogenous to $SL_2 \times SL_2$ or $SL_2 \times SL_1(D)$ over $\mathbb{Q}$ (with D a quaternionic division algebra over $\mathbb{Q}$). Now, the only four dimensional representations of $SL_2(\mathbb{C}) \times SL_2(\mathbb{C})$ are $St \otimes St$, or $St \oplus St$, or $Triv \otimes Triv \oplus Triv \otimes S^2(St)$, or $Triv^2 \oplus Triv \otimes St$. Thus, if both the factors have to act non-trivially, then the only possible four dimensional representations are $St \oplus St$ and $St \otimes St$. But, $St \oplus St$ does not have a quadratic form invariant under $SL_2 \times SL_2$. Thus, the only possible representation (over $\mathbb{C}$), of $SL_2 \times SL_2$ onto $SO(4)$ is $St \otimes St$.

It follows that the group $SL_2 \times SL_1(D)$ cannot have a four dimensional representation defined over $\mathbb{Q}$ with image $SO(f)$. Thus, $SO(f)$ must be isogenous to $SL_2 \times SL_2$. But then, the $\mathbb{Q}$-rank of $SO(f)$ is two, whereas $SO(f)$ has $\mathbb{Q}$-rank one, being a subgroup of G. This proves the claim.

Choose an element $\theta \in SO(h_0)$ of infinite order. Pick non-trivial elements $u_0 \in (SO(f) \cap U^+)(\mathbb{Z})$ and $v_0 \in U_{2\alpha}(\mathbb{Z})$. Then, the group $< \theta, u_0 v_0 >$ generated by θ and $u_0 v_0$ contains $\theta^{\mathbb{Z}}$, and (since θ acts by different characters on $Lie U_{2\alpha}$ and $U^+ \cap SO(f)$) also contains the product unipotent group $V^+ = V^+(r\mathbb{Z}) = [SO(f) \cap U^+(r\mathbb{Z})] U_{2\alpha}(r\mathbb{Z})$ for some integer r. Let $\gamma \in G(\mathbb{Z})$ be an element in general position with respect to θ and $u_0 v_0$ as in Lemma 16. For an integer r, consider the group $\Gamma =< \theta^r, (u_0 v_0)^r, \gamma^r >$. Then Γ is Zariski dense. By arguments similar to the previous cases, to prove that every arithmetic group in $G(\mathbb{Z})$ is virtually three-generated, it is enough to show that Γ is arithmetic for every r. Pick an element $g \in \Gamma$ with Bruhat decomposition $g = umwv$, say. Then, there exists an integer r' such that u and v, under conjugation, take $V^+(r'\mathbb{Z})$ into $V^+(r\mathbb{Z})$ (since the commutator of u and v with V^+ lands inside $U_{2\alpha}$). Thus, $\Gamma \supset^u <^m (V^-), V^+ >$ where

$V^- =^w (V^+)$ as before. Hence, we get $\Gamma \supset^u < U_{-2\alpha}(r\mathbb{Z}), V^+(r\mathbb{Z}) >$.

Consider the group $< U_{-2\alpha}(r\mathbb{Z}), U_H^+(r\mathbb{Z}) >$. An element in $U_{-2\alpha}(r\mathbb{Z})$ has the Bruhat decomposition $u_1m_1wv_1$ where $u_1, v_1 \in U_{2\alpha}(\mathbb{Q})$ *commute with* U_H^+. Therefore, $< U_{-2\alpha}(r\mathbb{Z}), U_H^+(r\mathbb{Z}) >$ contains

$$<^{u_1m_1wv_1} (U_H^+(r\mathbb{Z})), U_H^+(r\mathbb{Z}) >=^{u_1}<^{m_1} (U_H^-(r\mathbb{Z})), U_H^+(r\mathbb{Z}) >$$

and the latter contains $^{u_1} < U_H^-(r'\mathbb{Z}), U_H^+(r'\mathbb{Z}) >$ for some integer r'. Now, H is $\mathbb{Q}$-simple by the claim above, and has $\mathbb{R}$-rank two. Hence, by [V], the latter group is of finite index in $H(\mathbb{Z})$. It follows, in particular, that $< U_{-2\alpha}(r\mathbb{Z}), U_H^+(r\mathbb{Z}) >\supset^{u_1} (\theta^{r\mathbb{Z}}) = \theta^{r\mathbb{Z}}$ for some integer r. Therefore, from the foregoing paragraph, we get $\Gamma \supset^{uu_1} (\theta^{r\mathbb{Z}}) =^u (\theta^{r\mathbb{Z}})$. Then, Γ contains the commutator $[^u(\theta^r), \theta^r]$, with u running through generic elements of U^+ whence, $\Gamma \supset U^+(r\mathbb{Z})$ for some integer r. By [V], Γ is arithmetic.

Case 5. $n = 2$, K is either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$.

We can take $h = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ as a Hermitian form over a quadratic extension E/K and $G = SU(h)$ over K.

If $K = \mathbb{Q}$, and E is imaginary quadratic, then the real rank of $SU(h)$ is one (the group of real points is $SU(2,1)$), and in Theorem 1 we have assumed that $\mathbb{R} - rank(G_\infty) \geq 2$. Hence, E is real quadratic and has infinitely many units. If K is imaginary quadratic, then any quadratic extension E of K has infinitely many units. We can therefore assume that E has infinitely many units.

If P is the parabolic subgroup of $G = SU(h)$ consisting of upper triangular matrices in G, then it follows from the conclusion of the last paragraph, that $M_0(\mathbb{C}) = \mathbb{C}^*$ since $M_0(O_K)$ contains the group of matrices $h = \begin{pmatrix} u & 0 & 0 \\ 0 & u^{-2} & 0 \\ 0 & 0 & u \end{pmatrix}$ where u is a unit in E. The action of $M_0(\mathbb{C}) = \mathbb{C}^*$ on the Lie algebra $\mathfrak{u}$ of the unipotent radical of P is given by $\mathfrak{u} = \mathbb{C}(3) \oplus \mathbb{C}(-3) \oplus \mathbb{C}(0)$ where $\mathbb{C}(m)$ is the one dimensional module over $M_0(\mathbb{C}) = \mathbb{C}^*$ on which an element $z \in \mathbb{C}^*$ acts by z^m. Hence $\mathfrak{u}$ is multiplicity free for the $M_0(\mathbb{C})$ action, and we have proved Theorem 1 in this case.

5.2.2. **The Groups SU(h) over division algebras.** In this subsection, K is a number field, E/K a quadratic extension, D a central division algebra over E with an involution $*$ of the second kind, degree (D)=$d \geq 2$, $k = [K : \mathbb{Q}]$. $h : D^{m+2} \times D^{m+2} \to D$ is a $*$-hermitian form in $m+2$ variables over D. h is of the form

$$h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus h_m$$

where h_m is an anisotropic hermitian form in m variables. The special unitary group $G = SU(h)$ of the hermitian form h is an absolutely simple algebraic group over K, and under our assumptions, K-rank(G) $= 1$.

Case 1. $D \otimes \mathbb{R} \neq \mathbf{H} \times \cdots \times \mathbf{H}$.

Then, the group $SL_1(D \otimes \mathbb{R})$ is not compact, and is semi-simple. If $U^+ = \{\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}\}$, $U_{2\alpha} = \{\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : x + x^* = 0\}$ and P is the normaliser of U^+ in G (then P is a parabolic subgroup of G), there is the obvious Levi subgroup M of P. Since $SL_1(D)$ is non-compact at infinity, it follows that $M_0 \supset M_1$, where, $M_1 = R_{E/K}(SL_1(D))$. Moreover, $M_1(\mathbb{C}) = SL_d(\mathbb{C}) \times SL_d(\mathbb{C})$, and as a module over $M_1(\mathbb{C})$, the Lie algebra $\mathfrak{u}_{2\alpha}$ of $U_{2\alpha}$ is $\mathbb{C}^d \otimes (\mathbb{C}^d)^*$. Thus, the weight spaces of the torus T= diagonal$\times$ diagonal of $SL_d \times SL_d$, on $\mathfrak{u}_{2\alpha}$ are all one dimensional. Hence, there exist $m_0 \in M_1(O_K)$, $u_0 \in U_{2\alpha}(O_K)$ such that for every integer $r \geq 1$, there exists an integer r_0 with $< m_0^r, u_0^r > \supset U_{2\alpha}(r_0 O_K)$.

By Lemma 16, there exists an element $\gamma \in G(O_K)$ such that for any integer r, the group $\Gamma = < m_0^r, u_0^r, \gamma^r >$ is Zariski dense in $G(K \otimes \mathbb{C})$. As in the previous sections, it suffices to prove that Γ is arithmetic. Pick $g = umwv \in \Gamma$. Then, Γ contains for some integers r', r'' the groups ${}^g(U_{2\alpha}(r'O_K)) \supset {}^u(U_{-2\alpha}(r"O_K))$ as well as $U_{2\alpha}(r'O_K) = {}^u(U_{2\alpha}(r'O_K)$.

Consider the group $H = SU(J, D)$, where J is the hyperbolic hermitian (with respect to $*$) form in two variables given by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. H is absolutely simple over K. Moreover, it contains as a K-subgroup, the group $M_H = R_{E/K}(GL_1(D))$, the embedding given by $g \mapsto \begin{pmatrix} g & 0 \\ 0 & (g^*)^{-1} \end{pmatrix}$. Now, $M_H(K \otimes \mathbb{R}) = GL_1(D \otimes \mathbb{R}) \supset \mathbb{R}^* \times SL_1(D \otimes \mathbb{R})$. Since $SL_1(D \otimes \mathbb{R})$ is not compact by assumption, it follows that $M_H(K \otimes \mathbb{R})$ has real rank ≥ 2. The groups $U_{\pm 2\alpha}$ are maximal opposing unipotent subgroups of H, and hence by [V], the group $< U_{2\alpha}(r'O_K), U_{-2\alpha}(r''O_K) >$ is an arithmetic subgroup of $H(O_K)$. Therefore, we get from the last paragraph, that $\Gamma \supset^u (\Delta')$ for some subgroup $\Delta' \subset H(O_K)$ of finite index, which implies that $\Gamma \supset^u (\Delta)$ for some subgroup Δ of finite index in $SL_1(O_D)$ for some order O_D in D. Since $SL_1(O_D)$ contains elements which do not have eigenvalue 1 in their action on $LieU^+$, it follows from Proposition 10 that Γ is arithmetic.

Case 2. $D \otimes \mathbb{R} = \mathbf{H} \times \cdots \times \mathbf{H}$ and $m \geq 2$.

Then E is totally real (and so is K), and D must be a quaternionic division algebra over E. Moreover, $SU(h_m)(K \otimes \mathbb{R}) = \{g \in SL_m(D \otimes \mathbb{R}) : g^* h_m g = h_m\} = \{g = (g_1, g_2) \in SL_m(\mathbf{H})^k \times SL_m(\mathbf{H})^k : (g_2^\iota, g_1^\iota(h_m, h_m)(g_1, g_2) = (h_m, h_m)\}$ where ι is the standard involution on $\mathbf{H}$ induced to $SL_m(\mathbf{H})^k$. Thus, $SL_m(K \otimes \mathbb{R})$ is isomorphic to $SL_m(\mathbf{H})^k$. Since $m \geq 2$, the group $SL_m(\mathbf{H})^k$ is semi-simple and non-compact, and contains a Zariski dense set of integral points , which are $SU(h_m)(O_K) = M_1(O_K)$. Take P to be the standard parabolic subgroup of $G = SU(h)$. Hence $M_0(\mathbb{C}) \supset M_1(\mathbb{C}) = SL_{2m}(\mathbb{C})^k$. As a module over $M_1(\mathbb{C})$, the Lie algebra $LieU^+(\mathbb{C}) = [\mathbb{C}^2 \otimes (\mathbb{C}^{2m})^* \oplus \mathbb{C}^{2m} \otimes (\mathbb{C}^2)^* \oplus triv^4]^k$. Choose a generic toral element $m_0 \in M_1(O_K)$, and an element $u_0 = u_1 u_1 \in U^+(O_K)$ with $u_1 \in Exp(\mathfrak{g}_\alpha)$ and $u_2 \in Exp(\mathfrak{g}_{2\alpha})$. Choose an element $\gamma \in G(O_K)$ of infinite order, in general position with respect to u and m (Lemma 16). Then, for every integer r, the group $\Gamma =< u_0^r, \gamma^r, m_0^r >$ is Zariski dense.

Let $\Delta \subset U^+$ be the group generated by ${}^{m_0^{jr}}(u_0^r) : j \in \mathbb{Z}$ and $Log : U^+ \to \mathfrak{u}$ the log mapping. Then, $log(\Delta)$ contains elements of the form $v_1, \cdots, v_N$ with each v_i an eigenvector for $m_0 \in \prod SL_{2m}(\mathbb{C}) = M_1(\mathbb{C})$. For the generic toral element m_0, the number of distinct *eigenvalues* on $V_1 = (\mathbb{C}^2)^* \otimes \mathbb{C}^{2m} \oplus \cdots \oplus (\mathbb{C}^2)^* \otimes \mathbb{C}^{2m}$ (the direct sum taken k times) is $2mk$. Fix corresponding eigenvectors $v_1^i, \cdots, v_{2m}^i$ $(1 \leq i \leq k$ in V_1. Pick similarly, $2mk$ eigenvectors $(v_1^i)^*, \cdots (v_{2m}^I)^*$ $(1 \leq i \leq k$ in $V_1^* = (\mathbb{C}^2) \otimes (\mathbb{C}^{2m})^* \oplus \cdots \oplus (\mathbb{C}^2) \otimes (\mathbb{C}^{2m})^*$ (the direct sum taken k times) for m_0. The trivial $M_1(\mathbb{C})$ module $\mathfrak{g}_{2\alpha}$ is the k fold direct sum of $M_2(\mathbb{C})$ with itself. Denote the ith component of this direct sum $M_2(\mathbb{C})_i$ $(1 \leq i \leq k)$. By general position arguments (since the toral element m_0 is generic) it can be proved that for each i, the $2m - 1 (\geq 3)$ vectors $v_1^i(v_2^i)^* - v_2^i(v_1^i)^*, \cdots, v_1^i(v_{2m}^i)^* - v_{2m}^i(v_1^i)^*$ together with the vector $v_2^i(v_3^i)^* - v_3^i(v_2^i)^*$, span all of the i-th component $M_2(\mathbb{C})_i$. We choose u_1 such that the element $log(u_1)$ has non-zero projections into each of the eigenspaces of m_0 in $V_1 \oplus V_1^*$, and its projections $v_\mu^i, (v_\mu^i)^*$ are as in the foregoing.

Therefore, $\Gamma \supset Exp(\Delta) \supset U_{2\alpha}(r'O_K)$ for some integer r'. To prove Theorem 1 in this case, by standard arguments, it is enough to prove that Γ is arithmetic. Take a generic element $g = umwv \in \Gamma$. Then, Γ contains the group $<^g (U_{-2\alpha}(r'O_K)), U_{2\alpha}(r'O_K)u_1^{r'\mathbb{Z}}>$ (recall that $u_1 \in Exp(\mathfrak{g}_\alpha)$). Thus, for some other integer (denoted again by r' to save notation), Γ contains $^u < U_{-2\alpha}(r'O_K), u_1^{r'\mathbb{Z}}U_{2\alpha}(r'O_K)>$.

Let us view $h_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ as a Hermitian form for E/K. Set $H = SU(h_0) \simeq SU(2,1)$. This is an algebraic group over K, and has corresponding upper triangular unipotent group U_H^+. The Lie algebra spanned by $Elog(u_1)$ and $Elog(^w(u_1)$ is easily seen to be isomorphic to that of H with $Lie(U_H^+) = Elog(u_1) \oplus [Elogu_1, Elogu_1]$ (the square bracket denotes the commutator). From the conclusion of the last paragraph, we get $\Gamma \supset <^u (U_{-2\alpha}(r'O_K), u_1^{r'\mathbb{Z}}U_{2\alpha}(r'O_K)>$. By [V], the latter group contains $^u(SU(2,1)(r'O_K))$. Hence Γ contains $^u(SU(2,1)(r'O_K))$ as $g = umwv$ varies, and for some fixed $g' = u'm'wv'$, contains $^{u'}(SU(2,1)(r'O_K))$ as well.

The toral element $h \in SU(2,1)$ of the form $h = \begin{pmatrix} \theta & 0 & 0 \\ 0 & \theta^{-2} & 0 \\ 0 & 0 & \theta \end{pmatrix}$ acts on the root space $\mathfrak{g}_\alpha$ by the eigenvalues $\theta, \cdots, \theta$ and θ^3 (as may be easily seen). Therefore, h has no fixed vectors in $\mathfrak{g}_\alpha$. Now, by the last paragraph, Γ contains the group $^u(h)$ (u generic). Hence, by Proposition 10, Γ is arithmetic.

Case 3. $D \otimes \mathbb{R} = \mathbf{H}^{2k}$ *and* $m \leq 1$, *but* $k \geq 2$.

Again, E and K are totally real. $G = SU(h)$ with $G(K \otimes \mathbb{R}) = SL_3(\mathbf{H})^k$ if $m = 1$ and $SL_2(\mathbf{H})^k$ if $m = 0$. Fix $\theta \in O_K^*$ such that $\mathbb{Z}[\theta^r]$ is a subgroup of finite index in O_K for all $r \neq 0$ (Lemma 4). Let α be a totally positive element such that $E = K(\sqrt{\alpha})$. Denote by $t(\theta)$ (resp. u_+) the matrix $\begin{pmatrix} \theta & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \theta^{-1} \end{pmatrix}$ (resp. $\begin{pmatrix} 1 & 0 & \sqrt{\alpha} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$) if $m = 1$ and the matrix $\begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}$ (resp. $\begin{pmatrix} 1 & \sqrt{\alpha} \\ 0 & 1 \end{pmatrix}$) if $m = 0$. By the choice of θ, the group $<\theta^r, u_+^r>$ contains, for every r, $u_+^{r'O_K}$ for some integer

r'. Pick an element $\gamma \in G(O_K)$ in general position as in Proposition 16. Then for every $r \neq 0$, $\Gamma =< t^r, u_+^r, \gamma^r >\subset G(O_K)$ is Zariski dense in $G(K \otimes \mathbb{C})$. Pick a generic element $g = um_0wv \in \Gamma$. Then,

$$\Gamma \supset <^g (u_+^{rO_K}), u_+^{rO_K} >=^u <^{m_0} ((u_-)^{rO_K}, u_+^{rO_K} > .$$

The element m_0 is of the form $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & (a^*)^{-1} \end{pmatrix}$ with $b \in SU(h_m)$ if $m = 1$ and $\begin{pmatrix} a & 0 \\ 0 & (a^*)^{-1} \end{pmatrix}$ if $m = 0$ for some $a \in D^*$. Hence ${}^{m_0}(u_-^{rO_K})= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \sqrt{\alpha}(aa^*)^{-1}r'O_K & 0 & 1 \end{pmatrix}$, $u_+^{rO_K} = \begin{pmatrix} 1 & 0 & r'O_K \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ if $m = 1$ (and ${}^{m_0}(u_-^{r'O_K}) = \begin{pmatrix} 1 & 0 \\ (aa^*)^{-1}r'O_K & 1 \end{pmatrix}$, $u_+^{r'O_K} = \begin{pmatrix} 1 & r'O_K \\ 0 & 1 \end{pmatrix}$ if $m = 0$). These two groups ${}^{m_0}(u_-)$ and u_+ generate SL_2 over $K(c)$ if $m = 1$ and SL_2 over K if $m = 0$.

The element $c = aa^* \in D^*$ has its reduced norm and trace in E. But, in fact, $Tr(c)$ and $N(c)$ lie in K itself, as may be easily seen. Now, c being in the quaternionic division algebra D over E with $D \otimes \mathbb{R} = \mathbf{H}^{2k}$, generates a totally imaginary quadratic extension over the totally real E. Hence $K(c)/K$ is also totally imaginary quadratic extension. By the SL(2) result i.e. Proposition 7 (K is a totally real number field with infinitely many units), we get $<^{m_0} (u_-^{r'O_K}), u_+^{r'O_K} >$ is a subgroup of finite index in $SL_2(O_{K(c)})$ if $m = 1$ and $SL_2(O_K)$ if $m = 0$. In particular, the group $<^{m_0} (u_-^{r'O_K}), u_+^{r'O_K} >$ contains the group $t^{r'\mathbb{Z}} = t(\theta)^{r''\mathbb{Z}}$ for some $r'' \neq 0$.

Thus, Γ contains the group ${}^u(t^{r''\mathbb{Z}})$, u is generic and t does not have eigenvalue one in its action on the Lie algebra $Lie\ U^+$. Therefore, by Proposition 10, Γ is arithmetic.

Case 4. $D \otimes \mathbb{R} = \mathbf{H}^{2k}$, $m = 1$ and $k = 1$ (i.e. $K = \mathbb{Q}$). In this case, we will explicitly exhibit elements u_+, u_- and t in $G(O_K)$ such that for every $r \neq 0$, the group $\Gamma =< u_+^r, u_-^r, t^r >$ is arithmetic. This will prove Theorem 1 in this case. Since $D \otimes \mathbb{R}$ is a product of the Hamiltonian quaternions $\mathbf{H}$, it follows that $E/\mathbb{Q}$ is real quadratic. Fix a generic element $a \in D^*$. Then, the element aa^* generates as in the last case, an imaginary quadratic extension over $\mathbb{Q}$. Pick an element $t_2 \in \mathbb{Q}(aa^*) \setminus \mathbb{Q}$ such that $t_2^2 \in \mathbb{Q}$. Now choose $t_1 \in D$ such that $t_1^2 \in E$

but t_1 does not commute with t_2. Write $E = \mathbb{Q}(\sqrt{z})$ where $z \in \mathbb{Q}$ is positive. Pick a unit $\theta \in O_E^*$ of infinite order.

Write

$$u_+ = \begin{pmatrix} 1 & 1 & -\frac{1}{2} \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \sqrt{z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, u_- = \begin{pmatrix} 1 & 0 & 0 \\ t_1 & 1 & 0 \\ -\frac{t_1^2}{2} & -t_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ t_2\sqrt{z} & 0 & 1 \end{pmatrix},$$

and $t = \begin{pmatrix} \theta & 0 & 0 \\ 0 & \theta^{-2} & 0 \\ 0 & 0 & \theta \end{pmatrix}$. Now, the group $H = SU(2,1)$ associated to the extension $E/\mathbb{Q}$ embeds in G with the corresponding group of upper and lower triangular unipotent matrices denoted $U_H^{\pm}$.

Conjugating u_+ by powers of t and taking the group generated by these conjugates, we obtain that Γ intersects $U_H^+(r\mathbb{Z})$ in a subgroup of finite index. Conjugate u_- by powers of t and take the group generated by these conjugates. This is easily seen to contain $U_{-2\alpha}(rt_2\mathbb{Z})$ for some integer $r > 0$. Thus, $\Gamma \supset U_{-2\alpha}(rt_2\mathbb{Z})$. Then, by Proposition 9 applied to this SU(2,1), we see that Γ also contains $U_H^{\pm}(r'O_{\mathbb{Q}(t_2)})$ for some integer r'.

The group generated by the conjugates of u_- by powers of t also contains elements of the form $u_{-\alpha}(t_1x) = \begin{pmatrix} 1 & 0 & 0 \\ t_1x & 1 & 0 \\ -\frac{t_1^2xx^*}{2} & -t_1x^* & 1 \end{pmatrix}$. Hence $\Gamma \supset U_H^-(rt_1\mathbb{Z})$ with $x \in O_E$, the ring of integers in E. Taking commutators of these elements with $U_H^-(rO_{\mathbb{Q}(t_2)}) \subset \Gamma$ we obtain $U_{-2\alpha}(rt_1\mathbb{Z}) \subset \Gamma$ **and** $U_{-2\alpha}(rt_1t_2\mathbb{Z}) \subset \Gamma$ for some integer r. Since Γ, by the last paragraph, also contains $U_H^+(r\mathbb{Z})$, we get, by Proposition 9, that $\Gamma \supset SU(2,1)(O_{\mathbb{Q}(t_1)})$ **and** $\Gamma \supset SU(2,1)(O_{\mathbb{Q}(t_1t_2)})$.

The conclusions of the last two paragraphs imply that Γ contains the group U_1 generated by $U_H^+(rO_{\mathbb{Q}(\xi)})$ with $\xi \in \{t_1, t_2, t_1t_2\}$. Since D is a quaternionic division algebra over the quadratic extension E of $\mathbb{Q}$, it follows that the order O_D contains as a subgroup of finite index, the integral span of $O_{\mathbb{Q}(\xi)} \otimes O_E$ with $\xi \in \{t_1, t_2, t_1t_2\}$. Thus, U_1 contains $U^+(r''\mathbb{Z})$ for some integer r''. Hence Γ intersects U^+ in an arithmetic subgroup.

Then, by [V], Γ is an arithmetic subgroup of G.

Case 5. $D \otimes \mathbb{R} = \mathbf{H}^{2k}$, $m = 0$, $k = 1$ (i.e. $K = \mathbb{Q}$). Then, $G(\mathbb{R}) = SU(h)(\mathbb{R}) = SL_2(\mathbf{H})$. Therefore, $G(\mathbb{R})$ has real rank one, and in Theorem 1, this is excluded.

5.3. **Groups of type B.** $G = SO(f)$ with f a non-degenerate quadratic form in $2l+1 \geq 5$ variables over a number field K. f is the direct sum of a hyperbolic form and an anisotropic form in $2l-1$ variables:

$$f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus f_m$$

with $m = 2l - 1 \geq 3$. Assume that $\mathbb{R}$-rank $(G_\infty) \geq 2$, where $G_\infty = G(K \otimes \mathbb{R})$. Take P to be the parabolic subgroup $P = \{\begin{pmatrix} a & * & * \\ 0 & b & * \\ 0 & 0 & a^{-1} \end{pmatrix} \in G : a \in GL_1/K, b \in SO(f_m)\}$. The unipotent radical U^+ of P consists of matrices of the form $\begin{pmatrix} 1 & x & -\frac{\sum x_i^2}{2} \\ 0 & 1_m & -{}^t x \\ 0 & 0 & 1 \end{pmatrix}$ with 1_m the $m \times m$ identity matrix, and $x \in \mathbf{A}^{2l-1}$, the affine $2l-1$-space over K. Denote by $\mathfrak{u}$ the Lie algebra of U^+. Let U^- be the transpose of U^+ (it lies in G). Let M be the Levi subgroup of P given by $M = \{\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & a^{-1} \end{pmatrix} \in P : a \in GL_1/K, b \in SO(f_m)\}$. Put $H = SO(f_m)$.

Case 1. $H_\infty = H(K \otimes \mathbb{R})$ *is non-compact.* Then, H_∞ is a non-compact semi-simple group, hence $H(O_K)$ is Zariski dense in $H(K \otimes \mathbb{C})$. Therefore, $M_0 \supset H$. As a module over $H(\mathbb{C}) = SO(2l-1, \mathbb{C})$, $\mathfrak{u}(\mathbb{C}) = St = \mathbb{C}^{2l-1}$ is the standard representation, and the maximal torus T_H of $H(\mathbb{C})$ has distinct eigenvalues. Hence by Proposition 15, Theorem 1 is true for $G = SO(f)$ in this case.

Case 2. $H_\infty = H(K \otimes \mathbb{R})$ *is compact.* Then, K is totally real, and $(2 \leq)\mathbb{R}$-rank $(G_\infty) = \mathbb{R}$-rank $(GL_1(K \otimes \mathbb{R})) = [K : \mathbb{Q}]$, therefore $K \neq \mathbb{Q}$. Now, M_0 is rather small. $M(O_K)$ is commensurate to $GL_1(O_K) = O_K^*$, hence $M_0 = \{\begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a^{-1} \end{pmatrix} \in G : a \in GL_1/K\}$. In this case, we will use the fact that $SO(f)$ contains many $PSL_2(E)$ for totally *imaginary* quadratic extensions of the totally real number field K.

To see this, we first prove a lemma. Write the anisotropic form f_m as a direct sum $f_m = \phi \oplus \phi'$ with ϕ a quadratic form in **two** variables; here ϕ is the restriction of f_m to an **arbitrary** two dimensional subspace of the quadratic space associated to f_m. Write $\phi = 1 \oplus \lambda)$ with $\lambda \in K$. Form the quadratic forms $Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \phi$, and $Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus 1$. Then, for any archimedean completion K_v of K, $SO(Q)(K_v) = SO(3,1)(\mathbb{R}) \simeq SL_2(\mathbb{C})$. Let $Spin(Q)$ denote the simply connected two sheeted cover of $SO(f)$.

Lemma 18. *There exists a totally imaginary quadratic extension E/K such that $Spin(Q)$ is K-isomorphic to the group $R_{E/K}(SL_2)$ where $R_{E/K}$ denotes the Weil restriction of scalars.*

Proof. By the argument of Case 4 of the claim in subsection (5.2.1), $SO(Q)$ is K-simple. Hence $Spin(Q) = R_{E/K}(H_0)$ with H_0 an absolutely simple simply connected group over E, for some extension E/K, say of degree d. Since $SO(Q)$ is isotropic over K, so is H_0 over E. Since $dim(SO(Q)/K) = 6$, one sees that $dim(H_0) = \frac{6}{d}$. But $dim(H_0) \geq 3$ since it is absolutely simple, hence $d \leq 2$. Since Q is a form in four variables, $Spin(Q)$ is not absolutely simple. Therefore, $d = 2$ (i.e. E/K is a quadratic extension), and H_0 has dimension 3 (and is isotropic over E). Therefore, $H_0 = SL_2$. Since $SO(Q)(K_v) = PSL_2(\mathbb{C})$, it follows that $Spin(K_v) = SL_2(\mathbb{C}) = H_0(E \otimes K_v)$, for every archimedean (hence real) completion of K. Hence E is a totally imaginary. ☐

The inclusion of the quadratic spaces Q_1 and Q in f induce inclusions of $SO(Q_1)$ and $SO(Q)$ into $SO(f)$ defined over K. They further induce corresponding inclusions (defined over K) of the group of unipotent upper (and lower) triangular matrices $U^{\pm}_{Q_1}$ and $U^{\pm}_{Q}$ into the group $U^{\pm}$ defined at the beginning of this subsection. Let $v \in U^+_Q(O_K) \setminus U^+_{Q_1}(O_K)$ ($U^+_{Q_1}$ is one dimensional). Then the SL_2 result (Proposition 7) shows that $< v^{rO_K}, U^-(rO_K) >$ generates a subgroup of finite index in $SO(Q)(O_K)$ (which is commensurate to $SL_2(O_E)$).

Let $H = SO(Q_1) \subset SO(f)$, $U^+_H = U^+ \cap H$ be as in the last paragraph. Let $t = \begin{pmatrix} \theta & 0 & 0 \\ 0 & 1_m & 0 \\ 0 & 0 & \theta^{-1} \end{pmatrix}$ be in $M(O_K)$, $\theta \in O_K^*$ such that $\mathbb{Z}[\theta^r]$ of finite index in O_K (Lemma 4). Fix $u_+ \in U^+_H(O_K)$, $u_+ \neq 1$. Let γ be in general position with respect to t and u_+. Write, for an integer $r \neq 0$,

$$\Gamma =< u_+^r, t^r, \gamma^r > .$$

Then Γ is Zariski dense in $G(K \otimes \mathbb{C})$. Moreover, by the assumptions on θ, Γ contains the subgroup $V^+(r') = u_+^{r'O_K}$for some r'. Define $V^-(r')$ as the w-conjugate of $V^+(r')$. Pick a generic element $g = um'wv \in \Gamma$. Then, Γ contains the group $<^g (V^+(r')), V^+ >=^{um'w} (V^+(r''), V^+(r') >$ for some r''. The latter group contains $^u <^{m'} (V^-(r'')), V^(r'') >$ (replace r'' by a larger r'' if necessary).

If $logu_+ = X \in LieU^+ \simeq K^m$, then for the generic m', the vectors X and $^{m'}(X)$ span a two dimensional subspace W of the anisotropic quadratic space (K^m, f_m). Write the restriction of f_m to W as $\mu\phi$ for some $\mu \in K$, and ϕ as in the Lemma above, with $\phi(X, X) = 1$, say. Then, Γ contains $^u <^{m'w} (exp(r''O_K X), exp(r''O_K X) >$ which is $^u <^w (exp(r''O_K^m(X)), exp(r''O_K X) >$ (note that m' and w commute). By the last but one paragraph (essentially Proposition 7), the latter group contains $^u(\Delta)$ for some subgroup Δ of finite index in $SO(Q)(O_K)$, where Q is the four dimensional quadratic form as in the Lemma. Now, Δ contains $t^{r_0\mathbb{Z}}$ for some r_0. Hence Γ contains $^u(t^r)$, with $t \in M_0(O_K) \cap \Gamma$. By Proposition 10, Γ is arithmetic. This proves Theorem 1 for K-rank one groups of type B.

5.4. **Groups of type C.** The groups of type C are Sp_{2n} over K (which does not have K-rank 1), and certain special unitary groups over quaternionic division algebras. In the case of K-rank one groups, we need only consider the groups of the latter kind. Thus, let D be a quaternionic central division algebra over K, $\sigma : D \to D$ an involution of the *first* kind, such that the space of σ invariants in D is precisely K: $D^\sigma = K$. Suppose $h : D^n \times D^n \to D$ is a σ-hermitian form which is a sum of a hyperbolic form in two variables and an anisotropic form:

$$h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus h_{n-2}$$

with h_{n-2} an anisotropic hermitian form on D^{n-2}. The subgroup P of G consisting of matrices of the form $\begin{pmatrix} g & 0 & 0 \\ 0 & h & 0 \\ 0 & 0 & (g^\sigma)^{-1} \end{pmatrix} \begin{pmatrix} 1 & z & w \\ 0 & 1_{n-2} & 0 \\ 0 & -^t z & 1 \end{pmatrix}$ is a parabolic subgroup with unipotent radical U^+ consisting of matrices $\begin{pmatrix} 1 & z & w \\ 0 & 1_{n-2} & 0 \\ 0 & -^t z & 1 \end{pmatrix}$ with $w + w^\sigma = 0$. The commutator of U^+ is $U_{2\alpha}$ is the set of matrices $\begin{pmatrix} 1 & 0 & w \\ 0 & 1_{n-2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ with $w + w^\sigma = 0$ having dimension 3 over K. Then M is the Levi subgroup of P, with elements of the form $\begin{pmatrix} g & 0 & 0 \\ 0 & h & 0 \\ 0 & 0 & (g^\sigma)^{-1} \end{pmatrix}$.

Case 1. $D \otimes \mathbb{R} \neq \mathbf{H} \times \cdots \times \mathbf{H}$.

Then, $SL_1(D \otimes \mathbb{R})$ is a non-compact semi-simple group. Therefore, M_0 contains $SL_1(D)$, embedded as the subgroup of M of matrices of the form $\begin{pmatrix} g & 0 & 0 \\ 0 & 1_{n-2} & 0 \\ 0 & 0 & (g^\sigma)^{-1} \end{pmatrix}$ with $g \in SL_1(D)$. Note that for any embedding of K in $\mathbb{C}$, we have $SL_1(D \otimes_K \mathbb{C}) = SL_2(\mathbb{C})$. As a representation of $SL_2(\mathbb{C})$, the module $LieU_{2\alpha}$ is $Sym^2(\mathbb{C}^2)$ (since the space $w = -w^\sigma$ is 3-dimensional) which is multiplicity free for the diagonal torus in $SL_2(\mathbb{C})$. Therefore, there exists an $m_0 \in SL_1(O_D)$, and $u_0 \in U_{2\alpha}((O_K)$ such that the group generated by the elements ${}^{m_0^j}(u_0) : j \in \mathbb{Z}$ has finite index in $U_{2\alpha}(O_K)$.

Choose an element $\gamma \in G(O_K)$ in general position with respect to m_0, u_0 as in Lemma 16. Write, for an integer $r \neq 0$, $\Gamma =< m_0^r, u_0^r, \gamma^r >$. Then, Γ is Zariski dense in $G(K \otimes \mathbb{C})$. By the last paragraph, Γ intersects $U_{2\alpha}(O_K)$ in a subgroup V of finite index. Put ${}^w(V) = V^-$.

If H denotes the subgroup generated by $U_{\pm 2\alpha}$, then it is clear that H is semi-simple, K simple and contains the above copy of $SL(1, D)$. Hence H is of higher rank. Thus, V and V^- together generate an arithmetic subgroup of $H(K)$, by [V].

Let $g = umwv \in \Gamma$. Then, $\Gamma \supset <^g (V), V >=^u <^m (V), V >$. By the last paragraph, $\Gamma \geq^u (H(O_K)) \supset^u (m_0^{\mathbb{Z}})$. By Proposition 10, Γ is an arithmetic subgroup of $G(K)$, proving Theorem 1 in this case.

Case 2. $D \otimes \mathbb{R} = \mathbf{H}^k$, $k = [K : \mathbb{Q}] \geq 2$. Then K is totally real, and contains an element $\theta \in O_K^*$ such that the ring generated by θ has finite index in the integers O_K of K. Pick a non-trivial element $u_+ \in U_{2\alpha}(O_K)$ and let u_- denotes its conjugate by the Weyl group element w. Let $t = \begin{pmatrix} \theta & 0 & 0 \\ 0 & 1_{n-2} & 0 \\ 0 & 0 & \theta^{-1} \end{pmatrix} \in G(O_K)$. For $r \neq 0$, the group $< t^r, u_+^r >\supset u_+^{r' O_K} = V^+$ for some integer $R' \neq 0$. Choose $\gamma \in G(O_K)$ in general position with respect to t, u_0. Then, $\Gamma =< u_+^r, t^r, \gamma^r >$ is Zariski dense (Lemma 16). Then, $V^+ \subset \Gamma$. Pick a generic element

$g = umwv \in \Gamma$. Then, Γ contains the subgroup $<^g (V^+), V^+ >\supset^u<^m (u_+^{r''O_K}), u_+^{r'O_K} >$ for some other integer r''. If $u_+ = \begin{pmatrix} 1 & 0 & w \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ then

$$^m(u_+) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ (a^\sigma)^{-1}wa^{-1} & 0 & 1 \end{pmatrix} \text{ where } m = \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (a^\sigma)^{-1} \end{pmatrix}.$$

Since m is generic, the element $\xi = (a^\sigma)^{-1}wa^{-1}w^{-1} \in D$ generates a quadratic (totally imaginary, by the assumption on D in this case) extension of K. Therefore, by Proposition 7, the group $<^m (u_-^{r'O_K}), u_+^{r'O_K} >$ is an arithmetic subgroup of $SL_2(K(\xi))$. In particular, Γ contains $^u(t^{r_0\mathbb{Z}})$ for some integer r_0. The action of t on $LieU^+$ has no fixed vectors. By Proposition 10, Γ is arithmetic.

Case 3. $D \otimes \mathbb{R} = \mathbf{H}$, $k = 1$ *(i.e.* $K = \mathbb{Q}$*).*

Let $H = SU(h_{n-2})$. Since $\mathbb{R}$-rank $(G) \geq 2$, it follows that $\mathbb{R}$-rank $(H) \geq 1$. Thus, $n-2 \geq 2$. But then, $H(\mathbb{R}) = SU(h_{n-2}, \mathbf{H})$ is isotropic if and only if h_{n-2} represents a zero over $\mathbb{R}$. Since $n-2 \geq 2$, and a hermitian form in ≥ 2 variables over a quaternionic algebra (with respect to an involution of the first kind whose fixed points are of dimension one) represents a zero over $\mathbb{Q}_p$ for every prime p, it follows by the Hasse principle (see Ch 6, section (6.6), Claim (6.2) of [PR]) that h_{n-2} represents a a zero over $\mathbb{Q}$ as well, whence $\mathbb{Q}$-rank $(H) \geq 1$ and $\mathbb{Q}$-rank $(G) \geq 2$; this case is not under consideration in this section.

5.5. **Classical groups of type D.** *Case 1.* $G = SO(f)$. Here, $f = J \oplus f_{2n-2}$ with $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ being the hyperbolic form on Kr, f_{2n-2} an anisotropic quadratic form in $2n-2$ variables over K, and $n \geq 4$ (i.e. $n-1 \geq 3$). Now, the real rank of $SO(f)(K \otimes \mathbb{R})$ is ≥ 2. The argument for groups of type B applies without change.

We now assume that $G = SU_n(h, D)$. Here, D is a quaternionic central division algebra over K with an involution σ of the first kind such that the dimension of the set of fixed points D^σ is three (in the symplectic case, this dimension was one). $h = J \oplus h_{n-2}$, where $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the hyperbolic form on D^2 and h_{n-2} is an anisotropic hermitian form. Let P, U^+ and M be as in the symplectic case The only change from that case is that the involution σ has three dimensional fixed space, hence $U_{2\alpha}$ which consists of matrices of the form $\begin{pmatrix} 1 & 0 & w \\ 0 & 1_{n-2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ with $w + w^\sigma$ is one dimensional over K.

Case 2. K has infinitely many units. Then, by Proposition 12, Theorem 1 holds in this case.

Case 3. K is an imaginary quadratic extension of $\mathbb{Q}$. Then, $SL_1(D \otimes \mathbb{R}) = SL_2(\mathbb{C})$. Moreover, $SU(h_{n-2})(K \otimes \mathbb{R}) = SO_{2n-4}(\mathbb{C})$. Note that $n \geq 4$. Therefore, $SO_{2n-4}(\mathbb{C})$ is a semi-simple group. Hence, $M_0(K \otimes \mathbb{R}) = M_0(\mathbb{C}) \supset SL_2(\mathbb{C}) \times SO_{2n-4}(\mathbb{C})$. Then, the product of the diagonals in the latter group has multiplicity one in its action on the Lie algebra $LieU^+(\mathbb{C}) \simeq \mathbb{C}^2 \otimes \mathbb{C}^{2n-4} \oplus triv$. By Proposition 15, Theorem 1 holds.

Case 4. $K = \mathbb{Q}$ and $D \otimes \mathbb{R} \neq \mathbf{H}$. Then, $SL_1(D \otimes \mathbb{R})$ is non-compact and semi-simple. Now, the group $SL_1(D) \times SL_2/K$ is embedded in $SU(J, D)$ where $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the hyperbolic form in two variables. Therefore, the real rank of $SU(J, D)$ is ≥ 2.

Write $h_{n-2} = \lambda_1 \oplus h_{n-3}$ for some $\lambda \in D^\sigma - \setminus\{0\}$. After a scaling, we may assume that $\lambda = 1$. Consider the group $G_1 = SU_3(J \oplus 1, D)$. Let P_1, U_1 be the intersections of P and U with G_1. They are respectively a parabolic subgroup and its unipotent radical in H. By the last paragraph, it follows that $M_0 \simeq SL_1(D) \subset G_1$.

Now, the Tits diagram of G_1 is that of ${}^2A_3 \simeq SU(1, 3)$ over $\mathbb{Q}$, where $SU(1, 3)$ actually denotes the K-rank one group $SU(B)$ with B a hermitian form in four variables over a quadratic extension E of $\mathbb{Q}$, such that the maximal isotropic subspaces of E^4 for the form B are one dimensional. Thus, G_1 is as in Cases 3 or 4 of subsection (5.2.1). In Case 3 of (5.2.1), it is easy to see (and is observed there) that M_0 is not semi-simple. Therefore, only Case 4 of (5.2.1) applies. In this case (see (5.2.1), Case 4), there is an embedded $H = SO(1, 3)$ in this $G_1 \simeq SU(1, 3)$ of real rank two. Choose the unipotent element $u_0 \in H \cap U_1(\mathbb{Z}) \subset U^+(\mathbb{Z})$ and $v_0 \in (U_1)_{-2\alpha}(\mathbb{Z}) = U_{2\alpha}(\mathbb{Z})$ (the last equality holds since the space $\mathfrak{g}_{2\alpha}$ is one dimensional) and an element $\theta \in M_0 \cap H$ as in (5.2.1), Case 4. Set $V^+(r) = H \cap U^+(r\mathbb{Z})U_{2\alpha}(r\mathbb{Z})$. Then, by the argument of section (5.2.1), Case 4, $V^+(r)$ is contained in the two-generated group $< (\theta)^r, (u_0v_0)^r >$. Let $\gamma \in G(\mathbb{Z})$ be in general position with respect to u_0v_0 and θ. By Lemma 16, for each r, the group $\Gamma =< (u_0v_0)^r, \theta^r, \gamma^r >$ is Zariski dense. To prove Theorem 1, it is sufficient (by the now familiar arguments) to prove that Γ is arithmetic. Let $V^-(r)$ denote the w conjugate of $V^+(r)$.

Pick a generic element $g = umwv \in \Gamma$. Γ contains the group $<^g (V^+), V^+ >\supset^u<^m (V^-(r')), V^+(r') >$ for some r'. Thus, Γ contains the subgroup $^u < U_{-2\alpha}(r'\mathbb{Z}), U_H(r\mathbb{Z}) >$ where $U_H = U^+ \cap H$; it is proved in Case 4 of (5.2.1), that the group $< U_{-2\alpha}(r'\mathbb{Z}), U_H(r'\mathbb{Z}) >$ contains $\theta^{r''\mathbb{Z}}$ for some r''. Therefore, Γ contains $^u(\theta^{r''\mathbb{Z}})$. By Proposition 10, Γ is arithmetic.

Case 5. $K = \mathbb{Q}$ and $D \otimes \mathbb{R} = \mathbf{H}$.

If, as before, $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the hyperbolic form in two variables over the division algebra D, then, $SU(J, D)(\mathbb{R}) = \{g \in SL_2(\mathbf{H}) : g^\sigma J g = J\}$ has $\mathbb{R}$-rank 1. Recall that $h = J \oplus h_{n-2}$. Since R-rank $(SU(h)) \geq 2$, we must have $\mathbb{R}$-rank $(SU(h_{n-2})) \geq 1$. Hence h_{n-2} represents a zero over $\mathbb{R}$, and therefore, $n - 2 \geq 2$.

If $n-2 \geq 3$, then write $h_{n-2} = h_2 \oplus h_{n-4}$. Now, $G_0 = SU(J \oplus h_2, D)$ is an absolutely simple $\mathbb{Q}$-subgroup of G. We will show that $\mathbb{Q}$-rank $(G_0) \geq 2$, which will prove the same for G, and contradicts our assumption that $\mathbb{Q}$-rank of G is one.

The group G_0 is of type D_4, with $\mathbb{Q}$-rank one. Thus, In the diagram of G_0, there is one circled root.

[1]. If the anisotropic kernel M' is $\mathbb{Q}$-simple, then, $M'(\mathbb{C}) \supset SL_2^3$, and therefore, $< U^+_{G_0}(\mathbb{Z}), S_0(\mathbb{Z}) >$ (with S_0 a suitable torus in M'), is two generated: say by u_+ and θ. By considering an element $\gamma \in G(O_K)$, in general position it follows that $< \gamma^r, \theta^r, u_+^r >$ is Zariski dense. Write V^+ for the group generated by θ^r and u_+^r, and V^- for its conjugate by w. Since G_0 contains the 2α root group $U_{2\alpha}$ it follows that V^+ is normalised by the unipotent arithmetic group $U^+(r\mathbb{Z})$. Consequently, given $g = umwv \in \Gamma \cap U^+MwU^+$, Γ contains the group $<^g (V^+), V^+ >=^u<^m (V^-), V^+ >$. The latter contains $\Delta =^u< U_{-2\alpha}(r\mathbb{Z}), U^+_{G_0}(r\mathbb{Z}) >$. Since G_0 is of higher real rank (and of $\mathbb{Q}$-rank one), any Zariski dense subgroup of $G_0(\mathbb{Z})$ intersecting $U^+_{G_0}(\mathbb{Z})$ in an arithmetic group is of finite index in $G_0(\mathbb{Z})$ by [V]. Therefore, Δ is of finite index in $G_0(\mathbb{Z})$ and hence $\Gamma \supset^u (S_0(r'\mathbb{Z}))$ for some integer

r'. Now, non-trivial elements of $S_0(r'\mathbb{Z})$, act by eigenvalues $\neq 1$ on the α root space $\mathfrak{g}_\alpha$. An argument similar to the proof of Proposition 10 shows that the Zariski closure $\mathfrak{v}$ of $\Gamma \cap U^+$ has Lie algebra which contains $\mathfrak{g}_\alpha$. The latter *generates* $\mathfrak{u}$. Therefore, $\mathfrak{v} = \mathfrak{u}$ and $\Gamma \supset U^+(r''\mathbb{Z})$ for some r''. Thus, by [V], Γ is arithmetic, and Theorem 1 holds.

[2]. If the anisotropic kernel is not $\mathbb{Q}$-simple, then, there is at least one simple root connected to the above circled root, and the root groups corresponding to $\pm$ the simple roots connected to the circled root together generate a group G_1 isomorphic to SL_3 over $\mathbb{C}$. Over $\mathbb{R}$, G_1 cannot be outer type SL_3, since one root is already circled over $\mathbb{Q}$ (in outer type A_2, *two* roots over $\mathbb{R}$, are circled together). Therefore, G_1 is SL_3 over $\mathbb{R}$. Hence, over $\mathbb{Q}$, G_1 can only be $SU(2,1)$ with respect to a real quadratic extension. Then again, the group $< U^+_{G_1}(r\mathbb{Z}), \theta^{r\mathbb{Z}} >$ is virtually two generated (for any r), and a general-position argument as in the previous paragraph shows that Theorem 1 holds in this case too.

6. Exceptional groups of rank one

6.1. **Groups of type $^3D_4$ and $^6D_4$.** The only K-rank one groups (according to [T2], p.58) are $^3D^9_{4,1}$ and $^6D^9_{4,1}$. The simple root that is connected to all the others is circled. The anisotropic kernel M_1 is, over $\overline{K}$, SL_2^3. Moreover, the Galois group of $\overline{K}/K$ acts transitively on the roots connected to this simple root. Thus, the anisotropic kernel is an *inner twist* of the quasi-split group $M' = R_{E/K}(SL_2)$ with E/K either cubic ($^3D^9_{4,1}$) or sextic ($^6D^9_{4,1}$). M' is K-simple whence any inner twist is K-simple (inner twist of a product is a product of inner twists).

Now, G being an inner twist of the quasi-split group $\mathcal{G}$, is given by an element of the Galois cohomology set $H^1(K, \mathcal{G})$. However, this element is in the image of $H^1(K, M')$ (Proposition 4 (ii) of [T2]). Hence G contains the K-subgroup M_1 (inner twist of M'), whence M_1 is K-simple.

Since $\mathbb{R}$-rank $(M_1(K \otimes \mathbb{R})) \geq 1$ (it follows by looking at the Tits diagrams, that $G(K_v)$ has K_v-rank ≥ 2 for each archimedean place v of K, because these forms do not occur over real or complex numbers), that $M_1(K \otimes \mathbb{R})$ is non-compact and semi-simple. Hence it follows from Lemma 13 that the Zariski closure of $M_1(O_K)$ is M_1. Now, by [L], [Sh], as a module over $M_1(\mathbb{C}) = SL_2(\mathbb{C})^3$, $LieU^+ = St \otimes St \otimes St$. Therefore, the torus of $M_1(\mathbb{C})$ given by the product of diagonal tori in SL_2 acts by multiplicity one on $LieU^+$. By Proposition 15, Theorem 1 follows.

6.2. **Groups of type E_6.** We consider only those of K-rank one.

Case 1. There are no inner type groups of rank one.

Case 2. $G =^2 E^{35}_{6,1}$. The anisotropic kernel M_1 is K-simple (since its Tits diagram is connected). It is also non-compact at infinity, since $\mathbb{R}$-rank of any non-compact form of E_6 over K_v has K_v-rank ≥ 2 for any archimedean completion of K. Hence, by Lemma 13, $M_0 \supset M_1$. As a module over $M_1(\mathbb{C}) = SL_6(\mathbb{C})$, $LieU^+$ is $\wedge^3(\mathbb{C}^{10})$ ([L], [Sh]), and is multiplicity free for the diagonal torus in SL_6. This completes the proof.

Case 3. $G =^2 E^{29}_{6,1}$. The anisotropic kernel is non-compact at infinity for the same reason as above. Hence, by Lemma 13, $M_1 \subset M_0$, with $M_1 = SO(8)$. As an $M_1(\mathbb{C}) = SO(8, \mathbb{C})$ module, the space $LieU^+$ is (by p. 568, $^2E_6$-3 of [Sh]), $St \oplus \delta_3 \oplus \delta_5$ where St, δ_3 and δ_5 are respectively, the standard, and the two distinct spin modules. With respect to the maximal torus of $SO(8, \mathbb{C})$, the weights are $x_1, \cdots x_4$, $\frac{\epsilon_1 x_1 + \cdots + \epsilon_4 x_4}{2}$ with

$\epsilon_i = \pm 1$, each occurring with multiplicity one. Therefore, Theorem 1 follows from Proposition 15.

6.3. **Groups of type E_7 or E_8 or G_2.** There are no K-rank one forms over number fields.

6.4. **Groups of type F_4.** The K-rank one form is $F_{4,1}^{21}$. This is the only exceptional group which can have rank one over some archimedean completion of K.

Case 1. K is not totally real or $K = \mathbb{Q}$ or the anisotropic kernel is non-compact at infinity. Then, the anisotropic kernel M_1 is a form of $SO(7)$. Over $\mathbb{C}$ this is non-compact. In case $K = \mathbb{Q}$ again, this is non-compact over $\mathbb{R}$ since G is of real rank ≥ 2. If $K \neq \mathbb{Q}$ is totally real, then by *assumption*, M_1 is non-compact at infinity. Thus, $LieU^+ = St \oplus \wedge^3(\mathbb{C}^7)$ ([L], (xxii), p.52) is multiplicity free for the torus of $SO(7)$.

Case 2. $K \neq \mathbb{Q}$ totally real, and the anisotropic kernel is compact at infinity. let $\mathfrak{g}_{2\alpha}$ be the 2α root space. Then, the subgroup G_1 of G with Lie algebra $\mathfrak{g}_1 =< \mathfrak{g}_{-2\alpha}, \mathfrak{g}_{2\alpha} >$ must be locally isomorphic to $SO(1,8)$. For, $\mathfrak{g}_1$ has real rank one (since $\mathfrak{g}$ has), is semi-simple, and its obvious parabolic subgroup has abelian unipotent radical. Therefore, it can only be $SO(1,k)$. Since $dim(\mathfrak{g}_{2\alpha}) = 7$, it follows that $k - 1 = 7$ i.e. $k = 8$. Now, the anisotropic factor $SO(7)$ of $G_1 = SO(1,8)$ is an anisotropic factor of $F_{4,1}^{21}$ as well.

Fix $u_+ \in U_{2\alpha}(O_K)$, and $\theta \in \mathbf{G}_m(O_K)$ suitably chosen (as in Lemma 4). Fix $\gamma \in G(O_K)$ in general position with respect to u_+, θ (Proposition 16). For each r, write $\Gamma =< u_+^r, \theta^r, \gamma^r >$. Then, 1) Γ is Zariski dense in $G(K \otimes \mathbb{C})$ (Proposition 16). 2) $V^+ = V^+(r') == u_+^{r'O_K} \subset \Gamma$ for some integer r'. Put $V^- = V^-(r')$ for the w conjugate of $V^+(r')$. 3) If $g = umwv \in \Gamma$ is generic, then $\Gamma \supset <^g (V^+), V^+ > \supset ^u <^m (V^-), V^+ >$. By using the result proved for $SO(1,8)$ (it is important to note that $K \neq \mathbb{Q}$ is totally real, and that $m \in SO(7) \subset SO(1,8)$ to apply this result), we see that $^u(\theta^{r''\mathbb{Z}}) \subset \Gamma$ for some $r'' \neq 0$. Then, by Proposition 10, Γ is arithmetic.

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.

[BT] A.Borel and J.Tits, Groupes reductifs, Publ.Math. I.H.E.S., **27**, (1965) 55-150.

[L] R. Langlands, Euler Products, James Whittmore Lecture, Yale mathematical monographs, **1**, Yale University Press, New Haven, Conn.-London, 1971.

[M] J.Mennicke, Finite Factor Groups of the Unimodular Group, Annals of Math.(2), **81**, (1965) 31-37.

[O] H.Oh, On discrete subgroups containing a lattice in a horospherical subgroup, Israle J.Math., **110**, (1999) 333-340.

[PR] V. P. Platonov and A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, Vol 139.

[R 1] M. S. Raghunathan, On the congruence subgroup problem, Publ. Math. Inst. Hautes Etud. Sci. **46** (1976) 107-161.

[R 2] M. S. Raghunathan, On the congruence subgroup problem II, Invent. Math. **85** (1986) 73-117.

[R 3] 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.

[R 4] M.S.Raghunathan, A Note on Generators for Arithmetic Groups, Pacific J. Math. **152** (1972), no. 2 365-373.

[R 5] M.S.Raghunathan, Discrete subgroups of Lie Groups, Ergebnisse Math. Grenzgeb. (3), **68**, Springer-Verlag, New York, 1972.

[Sch] W.Scharlau, Quadratic and Hermitian Forms, Grundlehren der Mathematischen Wissenschaften, **270**, Springer-Verlag, Berlin, 1985.

[Sh] F. Shahidi, On the Ramanujan Conjecture and finiteness of poles of certain L-functions, Ann. of Math. (2)**127** (1988), **no. 3**, 547-584.

[T] J.Tits, "Systeḿes geńerateurs de groupes de congruence. C.R.Acad. Sci, Paris Seŕ. A-B, **283** (1976), no.9 Ai, A 693-A 695.

[T2] J.Tits, Classification of algebraic semi-simple groups, (1966) Algebraic Groups and Discontinuous Groups, Proc. Symp. Pure Math., Boulder, Colorado, 1965), 33-62 , Amer. Math. Soc. Providence, R.I.

[T3] J.Tits, Free subgroups in linear groups, Journal of Algebra **20** (1972) 250-270.

[Va] L.Vaserstein, Structure of the classical arithmetic groups of rank greater than one (in Russian) Math.Sb (N.S), **91** (**133**) (1973), 445-472.

[V] T.N.Venkataramana, On Systems of generators for higher rank arithmetic groups, Pacific Journal. **166** (1994), 193-212.

[V2] T.N.Venkataramana, Zariski dense subgroups of arithmetic groups, J. of Algebra, **108** (1987), 325-339.

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai 400005, India

E-mail address: `ritumony@math.tifr.res.in, venky@math.tifr.res.in`