Finitely Generated Profinitely Dense Free Groups in Higher Rank Semi–simple Groups.

by

G.A. Soifer[1]
Math. and Computer Sciences Dept.
University of Bar–Ilan
Ramat–Gan, Israel
e-mail: soifer@sunlight.cs-ac.il

T.N. Venkataramana
School of Mathematics
Tata Institute of
Fundamental Research
Homi Bhabha Road, Colaba
Bombay 400 005, India
e-mail: venky@math.tifr.res.in

Introduction

We recall the main result from [Mar–Soi]. There it is proved that if Γ is a finitely generated linear group which is not an extension of a solvable group by a finite group, then Γ contains (uncountably) many maximal subgroups of infinite index. The strategy there is to produce free (*infinitely* generated) subgroups F_∞ of Γ which are "profinitely dense" in Γ (i.e. map *onto* every finite quotient of Γ). Any maximal subgroup of Γ which contains such an F_∞ must then necessarily be of infinite index.

Aner Shalev has asked the following question: can one obtain *finitely* generated free subgroups F of Γ which are profinitely dense in Γ (we will refer to such groups as $f \cdot g \cdot p \cdot d \cdot f$ subgroups).

A result of [Scott] says that if Γ is a "Surface group" (i.e. the fundamental group of a compact Riemann surface of genus $\geqq 2$) then *any* finitely generated subgroup of Γ is contained in a *proper* subgroup of finite order in Γ . Thus the above question has a negative answer for general subgroups of $GL_n(\mathbb{C})$.

[1]Partially supported by GIF grant No. G–454–213.06/95

In this paper we prove (see *Theorem* (3.1)) that if Γ is an arithmetic subgroup of a non–compact linear semisimple group G such that the associated simply connected algebraic group over $\mathbb{Q}$ has the congruence subgroup property (see (1.2) for the relevant definition), then Γ contains a finitely generated profinitely dense free subgroup. As a corollary (see (3.3)) we obtain a $f \cdot g \cdot p \cdot d \cdot f$ subgroup of $SL_n(\mathbb{Z})$ ($n \geqq 3$) . More generally, we prove that if Γ is an irreducible arithmetic non–cocompact lattice in a higher rank group (see (3.2)) then Γ contains $f \cdot g \cdot p \cdot d \cdot f$ groups.

A Theorem of [Nori] and [Weisfeiler], together with a Theorem of [Tits 1] on the existence of free groups in linear groups already implies the existence of $f \cdot g \cdot p \cdot d \cdot f$ subgroups of *some subgroup* of finite index in our group Γ . We use the methods of [Mar–Soi] to construct a free group of this type and *extend* this free group to the full group Γ . More precisely, we construct, following [Mar–Soi], certain "free–systems" which can be extended to larger free systems (see (2.3)); these can be exploited to prove Theorem (3.1).

According to the general strategy of [Mar–Soi] these finitely generated profinitely dense free subgroups F of Γ can be embedded in maximal subgroups of infinite index in Γ . It would be of interest to know if these maximal subgroups are finitely generated. In contrast, maximal subgroups of infinite index in lattices of $SL_2(\mathbb{R})$ are infinitely generated ([Soifer]).

We are very grateful to Professor G.A. Margulis for helpful conversations and to Professor H. Abels and the department of Mathematics of Bielefeld University for their warm hospitality. We also thank Professor L. Potyagailo for useful references and comments.

§ 1. Preliminary Reductions and A Theorem of [Nori] [Weisfeiler].

(1.1) Notation: Let G be a real non–compact semi–simple linear Lie group and $\Gamma \subset G$ an *arithmetic* lattice. By definition this means the following. There exists a connected simply connected semi–simple algebraic group $\mathcal{G}$ defined over

$\mathbb{Q}$ such that if $\mathcal{G}(\mathbb{R})$ (resp. $\overline{G}$) denotes the quotient of $\overline{\mathcal{G}(\mathbb{R})}$ (resp. of G) by the maximal compact normal subgroup of $\mathcal{G}(\mathbb{R})$ (resp. of G) then

1) there exists an isomorphism Φ of $\overline{\mathcal{G}(\mathbb{R})}$ with the connected component of identity of $\overline{G}$ (note: $\mathcal{G}(\mathbb{R})$ is connected since $\mathcal{G}$ is simply connected, see [Borel–Tits 2], (4.7)).

2) $\Phi(\overline{\mathcal{G}(\mathbb{Z})}) \cap \overline{\Gamma}$ has finite index in $\overline{\Gamma}$ (where $\overline{\Gamma}$ is the image of Γ in $\overline{G}$; for a fixed linear imbedding $\mathcal{G} \hookrightarrow SL_N$ defined over $\mathbb{Q}$, $\mathcal{G}(\mathbb{Z}) = SL_N(\mathbb{Z}) \cap \mathcal{G}$: $\mathcal{G}(\mathbb{Z})$ may vary with respect to this imbedding but its commensurability class does not. Finally, $\overline{\mathcal{G}(\mathbb{Z})}$ is the image of $\mathcal{G}(\mathbb{Z})$ in $\overline{\mathcal{G}(\mathbb{R})}$).

Now $\mathcal{G}(\mathbb{Z})$ is finitely generated, whence by commensurability, Γ is finitely generated. $\blacksquare$ Since Γ is contained in G and G is linear, by a theorem of Selberg, Γ contains a subgroup (Γ_0) of finite index which is torsion free, and may be assumed to be normal in Γ . Consider the diagonal map $\Gamma \to \overline{\Gamma} \times \Gamma/\Gamma_0$ (where the projections are the natural quotient maps from Γ to $\overline{\Gamma}$ and to Γ/Γ_0). The kernel of this map is contained in $\Gamma_0 \cap \mathrm{Ker}\,(G \to \overline{G})$. The latter kernel is compact, and Γ_0 is torsion-free, whence $\Gamma_0 \cap \mathrm{Ker}\,(G \to \overline{G}) = \{1\}$ and Γ is a *subgroup* of $\overline{\Gamma} \times \Gamma/\Gamma_0$. We may thus replace G by $\overline{G} \times Q$, Q a finite group ($= \Gamma/\Gamma_0$ in our case) and Γ by its image in $\overline{\Gamma} \times Q$, without changing the associated simply connected group $\mathcal{G}$, or the lattice Γ . The group $\overline{G} \times Q$ has the property that its connected component of identity is a product of connected simple *non–compact* Lie groups.

Write $G = \overline{G} \times Q$. Clearly $\overline{G}$ is contained in $\mathrm{Aut}\,(\mathfrak{g})$ where $\mathfrak{g}$ is the Lie algebra of $\overline{G}$ (or of G). We thus get a linear embedding of G in $\mathrm{Aut}\,(\mathfrak{g}) \times Q$ (by fixing any linear embedding of the finite group Q). Let $\mathbb{G}$ be the Zariski closure of G and $\mathbb{G}^0$ its connected component of 1 . Let G^0 be the connected component of 1 of G . Clearly $G^0 \subset \mathbb{G}^0(\mathbb{R})$.

We now assume that Γ is an *irreducible* lattice in G . Therefore $\Phi(\mathcal{G}(\mathbb{Z}))$ is also an irreducible lattice. However, $\mathcal{G}$, being a simply connected semisimple $\mathbb{Q}$–algebraic group, is a product of simply connected $\mathbb{Q}$–simple algebraic semisimple groups: $\mathcal{G} = \mathcal{G}_1 \times \cdots \times \mathcal{G}_h$. Up to commensurability we obtain $\mathcal{G}(\mathbb{Z}) = \mathcal{G}_1(\mathbb{Z}) \times \cdots \times \mathcal{G}_h(\mathbb{Z})$, and $\mathcal{G}(\mathbb{Z}) \to \Phi(\mathcal{G}(\mathbb{Z}))$ has finite kernel. The irreducibility of $\Phi(\mathcal{G}(\mathbb{Z}))$ thus implies that exactly one of the groups $\mathcal{G}_1(\mathbb{Z}), \ldots, \mathcal{G}_h(\mathbb{Z})$ is infinite, say $\mathcal{G}_1(\mathbb{Z})$. Since $\mathcal{G}_i(\mathbb{Z})$ is a lattice in $\mathcal{G}_i(\mathbb{R})$, this means that $\mathcal{G}_2(\mathbb{R}), \ldots, \mathcal{G}_h(\mathbb{R})$ are all compact, and $\overline{\mathcal{G}_1(\mathbb{R})} = \overline{\mathcal{G}(\mathbb{R})}$. We may thus assume (and we do from now on) that $\mathcal{G} = \mathcal{G}_1$ is a $\mathbb{Q}$–simple simply connected group. Now $\overline{\mathcal{G}_1(\mathbb{R})} = G^0$, hence $\overline{\mathcal{G}_1(\mathbb{R})}$ has $\mathbb{G}^0$ as the Zariski closure. From now on, denote $\mathcal{G}$ by G (when there is no danger of confusion with the real linear semisimple Lie group G).

1.2 Definition: Let $\mathbb{A}_f$ be the ring of finite adéles over $\mathbb{Q}$ with its usual topology. Then $G(\mathbb{A}_f)$ is a locally compact totally disconnected group containing $G(\mathbb{Q})$. Subgroups of $G(\mathbb{Q})$ of the form $\Gamma_U = G(\mathbb{Q}) \cap U$ (U a compact open subgroup of $G(\mathbb{A}_f)$) are called *congruence* subgroups. It is clear that congruence subgroups are commensurable with $G(\mathbb{Z})$. Fix such a congruence subgroup Γ_U and $\overline{\Gamma_U}(c)$ its closure in $G(\mathbb{A}_f)$ (since $G(\mathbb{R})$ is non–compact and G is simply connected, $\overline{\Gamma_U}(c) = U$ by strong approximation, but this is irrelevant to our discussion). Let $\widehat{\Gamma}_U$ denote the profinite completion of Γ_U . We then get a natural exact sequence $1 \to C \to \widehat{\Gamma}_U \to \overline{\Gamma}_U(c) \to 1$ of totally disconnected topological groups. It is well known (and easily proved) that C is independent of the congruence subgroup chosen. We will say that G has the *congruence subgroup property* if C is *finite* (C is called the congruence subgroup kernel).

If $\mathbb{R}$–rank $(G) \geqq 2$, $G(\mathbb{R})/G(\mathbb{Z})$ is not compact (and G is $\mathbb{Q}$–simple, as we have assumed), then by [Raghunathan 1,2], G has the congruence subgroup property (for reference to earlier works e.g. [Mennicke], [Serre], [Bass–Milnor–Serre], [Matsumoto], see [ibid]). For most groups which are not of type (A_n) , even if $G(\mathbb{R})/G(\mathbb{Z})$ is compact, but $\mathbb{R}$–rank $(G) \geqq 2$, the congruence subgroup property is true (see [Kneser], [Rapinchuk], ... ; for references, see[Pl–Ra]).

Before we go on, we record a result of [Nori] and [Weisfeiler]. Under our assumption that G is simply connected, $\mathbb{Q}$–simple and $G(\mathbb{R})$ is not compact, this result says that any subgroup Δ of $G(\mathbb{Z})$ which is Zariski dense in G has open closure in the group $G(\mathbb{A}_f)$ (or in the group $\overline{G(\mathbb{Z})}(c)$). Using this we prove

(1.3) Lemma: Let G be a linear semisimple Lie group as in (1.1) . Suppose that the associated simply connected algebraic group $\mathcal{G}$ (which will sometimes be denoted by G) has the congruence subgroup property. Let $\Delta \subset \Gamma$ be a subgroup whose Zariski closure in $\mathbb{G}$ contains $\mathbb{G}^0$. Then the closure $Cl(\Delta)$ (of Δ) in the profinite completion $\widehat{\Gamma}$ (of Γ), is open.

Proof: Note that Δ may be replaced by a subgroup of finite index without altering the hypotheses of the Lemma. We may thus assume that Δ is the isomorphic image under Φ of a subgroup, also denoted Δ, of $G(\mathbb{Z})$. If $G = R_{K/\mathbb{Q}}(G_0)$, where $R_{K/\mathbb{Q}}$ denotes the Weil restriction of scalars $K/\mathbb{Q}$ is a finite extension and G_0 is an absolutely simple simply connected group over $\mathbb{Q}$ (this is possible since G is $\mathbb{Q}$–simple, see [Tits 2]), then $G(\mathbb{Z}) \cong G_0(O_K)$ upto commensurability (here, O_K is the ring of integers in K). Now $G(\mathbb{R}) = G_0(K \bigotimes_{\mathbb{Q}} \mathbb{R})$. Let $G_0^{nc} = \prod_{v\in\infty'} G_0(K_v)$, where ∞' is the set of archimedean primes of K such that $G_0(K_v)$ is not compact. By our assumption ($G(\mathbb{R}) \xrightarrow{\Phi} G$ has compact kernel, hence) the Zariski closure $\mathcal{H}$ of Δ in G contains G_0^{nc}, and $\Phi : \mathcal{H}(\mathbb{R}) \to G^0$ also has compact kernel, and is *surjective*. Since $\Delta \subset \mathcal{H} \cap G(\mathbb{Z}) = \mathcal{H}(\mathbb{Z})$, $\mathcal{H}$ is the Zariski closure of $\mathcal{H}(\mathbb{Z})$ as well. Therefore $\mathcal{H}(\mathbb{R})/\mathcal{H}(\mathbb{Z})$ has finite volume (by [Borel–Harish–Chandra]) and $\Phi(\mathcal{H}(\mathbb{Z}))$ is also a lattice in G^0. However, $\Gamma \cap G^0$ is a lattice in G^0 commensurate with $\Phi(G(\mathbb{Z}))$ which shows that $\mathcal{H}(\mathbb{Z})$ and $G(\mathbb{Z})$ are commensurate, i.e. $\mathcal{H} = \mathcal{G}$ by the Borel density theorem. We may thus assume in the Lemma (after replacing Δ by a subgroup of finite index if necessary) that $\Delta \subset \mathcal{G}$ is Zariski dense in $\mathcal{G}$. Now our assumption that $\mathcal{G}$ has congruence subgroup property and the theorem of [Nori] and [Weisfeiler] mentioned above says that $Cl(\Delta)$ is open in $\widehat{G(\mathbb{Z})}$ (the profinite completion of $G(\mathbb{Z})$). As $G(\mathbb{Z})$ and Γ are commensurate, this is equivalent to saying that the closure $Cl(\Delta)$ in $\widehat{\Gamma}$ is open. This completes the proof of the Lemma.

§ 2. Construction of A Representation of G and related free systems.

(2.1) Notation: Fix a maximal unipotent subgroup $\mathcal{U}$ of $G(\mathbb{R})$. By [Borel–Tits 1] *Théorème (8.2)*, all the maximal unipotent subgroups of $G(\mathbb{R})$ are conjugate under $G(\mathbb{R})$. Moreover, $\Phi : G(\mathbb{R}) \to G$ is injective on $\mathcal{U}$, let U be its image (Φ as in the beginning of (1.1)). Let A be the connected component of identity of a maximal $\mathbb{R}$–split torus $\widetilde{A}$ in $G(\mathbb{R})$, normalizing U (we identify $\mathcal{U}$ with U).

Let $\mathcal{P} = N_{G(\mathbb{R})}(\mathcal{U})$, $P = N_G(U)$ (where $N_?$, denotes the normalizer in ?). Then $\mathcal{P}$ is a minimal parabolic subgroup of $G(\mathbb{R})$. Let $M_0 \subset Z_{G(\mathbb{R})}(A)$ be the maximal compact subgroup (of the centralizer $Z_{G(\mathbb{R})}(A)$ of A in $G(\mathbb{R})$). We have the Langlands decomposition $\mathcal{P} = M_0 \cdot A \cdot U$. Note that A maps isomorphically onto its image under Φ , so we identify $\Phi(A)$ with A . Now all maximal $\mathbb{R}$–split tori in $\mathcal{P}$ are conjugate in $\mathcal{P}$ to $\widetilde{A}$ (by an element of U , in fact). We may thus assume that every element of G/G^0 is represented by an element x such that $x\,U\,x^{-1} = U$, $x\,A\,x^{-1} = A$. Let $W_0 \in N_G(\widetilde{A})/\widetilde{A}$ be the "*longest element*" of the Weyl group, and put $U^- = w_0 U w_0^{-1}$. Now $w_0 \in G(\mathbb{R})$ and identify its image under Φ again with w_0 : then $w_0 \in G^0$. If x is fixed as above, then the action of x on the character group of $\widetilde{A}$ takes the positive roots of $\widetilde{A}$ (i.e. the roots of $\widetilde{A}$ occurring in the Lie algebra Lie (U) of U) into themselves. Let Φ^+ denote the positive roots of $\widetilde{A}$, and α the highest root in Φ^+ , $\mathfrak{g}_\alpha \subset$ Lie (U) the corresponding root space. We have: $x\,U^- x^{-1} = U^-$ for the choice of x above.

Let $d = \dim(\mathfrak{g}_\alpha)$ and W the G–span of the line $L = \overset{d}{\wedge}\mathfrak{g}_\alpha$ in $\overset{d}{\wedge}\mathfrak{g}$ ($\mathfrak{g} =$ Lie (G)). Denote by ρ the representation of G on W . Let X be a *finite* set of representatives of G/G^0 chosen so that for $x \in X$, $x\,A\,x^{-1} = A$, $x\,U^+ x^{-1} = U^+$, $x\,U^- x^{-1} = U^-$. Then $P = X \cdot \Phi(M_0) \cdot A \cdot U$, hence $P(L) = L$. Let $\mathbb{P}(W)$ be the projective space of W . Now $W = G$–span of L , $G = G^0 \cdot X$, $X(L) = L$ whence W is the G^0–span of $L = G(\mathbb{R})$–span of L . By highest weight theory, L is *absolutely* irreducible for $G(\mathbb{R})$, hence for G^0 .

In (1.1), we considered a subgroup Γ_0 of finite order in Γ . We may assume that Γ_0 is the isomorphic image under Φ , of an arithmetic subgroup of $G(\mathbb{Z})$ which is torsion free. Let $A^+ = \{a \in A;\ \ \alpha(a) > 1 \ \text{ for all } \ \alpha \in \Phi^+\}$, and let $\gamma \in M_0 A^+$. The weights of $\widetilde{A}$ on W are of the form $\mu = d\alpha - (\alpha_1 + \cdots + \alpha_h)$, $\alpha_i \in \Phi^+$, α the highest root (because W contains $\overset{d}{\wedge}\mathfrak{g}_\alpha$ as a highest weight line with highest weight $d\alpha$). Moreover, the weights $\pm(d\alpha)$ occur with multiplicity one. Therefore, if $\Omega_0(G)$ is the set of g in G such that $\rho(g)$ is semisimple, and such that , over $\mathbb{C}$, $\rho(g)$ can be conjugated into a diagonal matrix

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \quad \text{with} \quad \begin{array}{ll} \lambda_1 > |\lambda_i| & (i \geq 2) \\ \lambda_n < |\lambda_i| & (i \leq n-1) \end{array}$$

then $M_0 A^+ \subset \Omega_0(G) \neq \emptyset$. Now $\Gamma_0 \cap \Omega_0(G) \neq \emptyset$. This follows, for example from the existence of hyper–regular elements (see [Prasad–Raghunathan]) in lattices. Fix $\gamma \in \Gamma$. Then, by Lemma 9 of [MS] $\Omega_0(G) \cap \gamma N \neq \emptyset$ for *every* subgroup N of finite index in Γ . Given $g \in \Omega_0(G)$, let $A^+(g)$ (resp. $A^-(g)$) denote the unique line spanned by the eigenvector with the unique highest eigenvalue (resp.

lowest eigenvalue). Let $B^+(g)$ (resp. $B^-(g)$) denote the sum of eigenspaces of g excluding $A^-(g)$ (resp. $A^+(g)$), and let $B(g) = B^+(g) \cup B^-(g)$.

(2.2) Definitions: If $b_0, b_q, \ldots, b_m \in \Omega_0(G)$, we say that $b_0, b_q, \ldots, b_m$ are in *good position* if for each i, j , $i \neq j$, $0 \leq i, j \leq m$, we have

$$A^{\pm}(b_i) \subset \mathcal{C}\, B(b_j).$$

Here $\mathcal{C}$ denotes the complement of the set involved .

We say that $a_0, \ldots, a_m \in \Omega_0(G)$ form a *free system* $\delta = \langle a_0, a_1, \ldots, a_m \rangle$, if for each i, j , $i \neq j$, $0 \leq i, j \leq m$, there exist compact neighbourhoods K_i of $A^{\pm}(a_i)$ such that

$$\begin{aligned} &1) \quad K_i \cap K_j = \emptyset \\ &2) \quad K_i \subset \textstyle\bigcap_{j \neq i} \mathcal{C}\, B(b_j) \\ &3) \quad a_i^m (\textstyle\bigcup_{j \neq i} K_j) \subset K_i \ (m \in \mathbb{Z},\ m \neq 0). \end{aligned}$$

Let $a_0, a_1, \ldots, a_m \in \Gamma \cap \Omega_0(G)$ be in good position. Then there exists a $\gamma \in \Gamma$ such that, for any $0 \leq k \leq m$,

(1) $\quad a_0, a_1, \ldots, a_m$, $\gamma a_k \gamma^{-1}$ are in good position.

For, consider the set $Z = \{g \in \mathbb{G}^0$; $a_0, a_1, \ldots, a_m$, $g\, a_k g^{-1} = a'$ are *not* in good position$\}$. This means either that $A^{\pm}(a') \in B(a_i)$ for some i or that $A^{\pm}(a_i) \in B(a')$ for some i (by $A^{\pm}(a') \in B(a_i)$ we mean either $A^+(a') \in B(a_i)$ or $A^-(a_i) \in B(a_i)$). However, $g\, A^{\pm}(a_k) = A^{\pm}(a'), B(a') = g\, B(a_i)$. If the connected algebraic group $\mathbb{G}^0$ acts irreducibly on (ρ, W) , then $\mathbb{G}^0 \cdot (p)$ cannot be contained in a finite union $W_1 \cup \cdots \cup W_m$ of *proper* subspaces, for any $p \in \mathbb{P}(W)$. To see this, note that by the connectedness of $\mathbb{G}^0$, $\mathbb{G}^0(p) \subset W_i$ for some i , and by irreducibility, $W =$ span of $G^0(p) (\subset W_i)$ which is impossible. Therefore $\{g : g\, A^{\pm}(a_k) \in B(a_i)\}$ is a proper closed subset Z_1 of $\mathbb{G}^0$. Similarly, the $\mathbb{G}^0$–irreducibility of ρ implies that $\{g ; g^{-1}(A^{\pm}(a_i)) \in B(a_i)$ for some $i\}$ is a proper closed subset Z_2 of $\mathbb{G}^0$, whence $Z = Z_1 \cup Z_2$ is proper and $\mathbb{G}^0 - Z$ is a nonempty Zariski open subset of $\mathbb{G}^0$. Now $\Gamma \cap \mathbb{G}^0$ is Zariski dense in $\mathbb{G}^0$ by the Borel density theorem, whence $\Gamma \cap (\mathbb{G}^0 - Z)$ is non–empty. This proves (1).

We now claim that if $\langle a_0, a_1, \ldots, a_m \rangle$ are in good position, then there exists an integer $k \geqq 1$ such that

(2) $\langle a_0^{k_1}, a_1^{k_1}, \ldots, a_m^{k_1} \rangle$ form a free system $(|k_1| \geqq k)$.

The claim is easily proved once one notices that if $g \in \Omega_0(G)$, $K \subset \mathbb{P}(W) - B(g)$ is a compact set and $|k|$ is sufficiently large, then $g^k(K)$ lies in an arbitrarily small neighbourhood of $\{A^+(g), A^-(g)\}$. The details are in [Tits].

Note also that if

(3) $S = \langle a_0, \ldots, a_m \rangle$ form a free system, then the group generated by $\langle a_1, \ldots, a_m \rangle$ is free.

The proof of (3) is immediate from the Ping–Pong Lemma of [Tits 1].

§ 3. Proof of The Main Theorem.

(3.1) Theorem: Let Γ be an irreducible arithmetic lattice in a linear real semi–simple non–compact Lie group G . Assume that the simply connected algebraic semi–simple $\mathbb{Q}$–group associated to the arithmetic group Γ has the congruence subgroup property. Then Γ contains a finitely generated profinitely dense free subgroup.

Proof: By (1.1) we may assume that G^0 is a product of non–compact simple Lie groups. Let (ρ, W) be the representation of G constructed in (2.1). Pick elements $\{a_0, \ldots, a_r\}$ of Γ , such that they form a free system. By section (2.1) $\Gamma \cap \Omega_0(G) \neq \emptyset$. Then by (1) of (2.2), we may assume that $r \geqq R$ for *any* R .

Given a free system $S = \langle a_0, a_1, \ldots, a_{r-1}, a_r \rangle$ of elements of Γ , we associate a connected algebraic subgroup $G(S)$ of $\mathbb{G}$: *fix* the ordering $\langle a_0, \ldots, a_r \rangle$ of S . For $1 \leq i \leq r-1$, let $\mathcal{H}_i$ denote the connected component of identity of the Zariski closure of $a_i^{\mathbb{Z}}$, and let $G(S)$ be the algebraic subgroup of $\mathbb{G}$ generated by $\langle \mathcal{H}_1, \ldots, \mathcal{H}_{r-1} \rangle$.

Let $d = \sup\{\dim G(S) : S$ is a finite free system in $\Gamma\}$.

Claim 1: $d = \dim \mathbb{G}$.

Proof of Claim 1: Suppose $S = \langle a_0, a_1, \ldots, a_r \rangle$ is a free system such that $d = \dim G(S)$. Let $\gamma \in \Gamma$ $(j \leq r-1)$ be such that $\langle a_0, a_1, \ldots, a_r, \ \gamma^{-1} a_j \gamma \rangle$ are in good position. (Its existence is assured by (1) of (2.2)). Then there exists $k \geqq 1$ such that

$$S' = \langle a_0^k, a_1^k, \dots, a_{r-1}^k, \gamma^{-1} a_j^k \gamma, a_r^k \rangle$$

form a free system (the existence of k is assured by (2) of (2.2)). Consider the group $G(S')$. Clearly $G(S')$ contains the connected component of identity of the Zariski closure of $a_i^{k\mathbb{Z}}$, but this is the same as $\mathcal{H}_i$ $(1 \le i \le r-1)$. Hence $G(S') \supset G(S)$. By the maximality of the dimension of $G(S)$, and connectedness of $G(S')$, we must have $G(S) = G(S')$. However, $(G(S) =) G(S') \supset \gamma^{-1}\mathcal{H}_j\gamma$ by construction. Therefore, $\gamma^{-1}\mathcal{H}_j\gamma \subset G(S)$ $(\forall j \le r-1)$ i.e. $G(S)$ is normalized by Γ , hence by $\mathbb{G}^0$. The irreducibility of the lattice Γ implies now that $G(S) \cap \Gamma$ is either finite or commensurable with Γ . $G(S) \cap \Gamma$ cannot be finite because it contains the free group generated by $\langle a_1^k, \dots, a_{r-1}^k \rangle$ for some $k (r \geqq 2)$. Therefore $\Gamma \cap G(S)$ is commensurate to Γ . By the Borel density theorem, $G(S) = \mathbb{G}^0$. The claim follows.

We now consider any finite free system S such that $G(S) = \mathbb{G}^0$. Put $\Delta =$ the group generated by $\langle a_1, \dots, a_{q-1} \rangle$ in Γ_0 . Now the Zariski closure of Δ in $\mathbb{G}$ contains $\mathbb{G}^0 = G(S)$, by the definition of $G(S)$. By Lemma (1.2) ([Nori], [Weisfeiler]), $Cl(\Delta)$ is open in $\widehat{\Gamma}$. Let $\Gamma(S) = \Gamma \cap Cl(\Delta)$ (Γ is naturally included in $\widehat{\Gamma}$ since Γ is residually finite). Define the integer $i(S) = \mathrm{Card}\,(\Gamma/\Gamma(S))$.

Claim 2: $\inf\{i(S) : S$ a finite free system such that $G(S) = \mathbb{G}^0\} = 1$.

Proof of Claim 2: Suppose i denotes this infimum. Let S be so that $G(S) = \mathbb{G}^0$ and $i(S) = i$. Put $N = \Gamma(S)$. Let $x \in \Gamma - N$ (if possible). Then by Lemma 9 of [Margulis–Soifer], $x\,N \cap \Omega_0(G) \neq \emptyset$. As in the proof of (1) of (2.2), we may assume after a conjugation by $\gamma \in N$ (such that $x^{-1}\gamma x \in N$) , that $\langle a_0, a_1, \dots, a_r, g \rangle$ are in good position for some $g \in x\,N \cap \Omega_0(G)$. If g is replaced by $g^{1+ki!}$ for some large k (note: since $\mathrm{Card}\,(\Gamma/N) = i$, $g^{1+ki!} \in \gamma N$) , then by (2) of (2.2), $\langle a_0^{k\cdot i!}$, $g' = g^{1+ki!} \rangle$ form a free system. Consider the set $S' = \langle a_0^k, a_1, a_2, \dots, a_{n-1}, a_{n+1} = a_0^{k(i!)} g' a_0^{-k(i!)}, a_n \rangle$. If k is large, then $A^{\pm}(a_0^k g' a_0^{-k}) = a_0^k(A^{\pm}(g')) \subset K_0$ where $K_0, K_1, \dots, K_{n-1}$ are chosen as in the beginning of (2.2). Also, for *every* $m \neq 0$, $(g')^m(K_i) \subset K_{g'}$ if $\underset{=}{k}$ is sufficiently large . (Here $K_{g'}$ is a small neighbourhood of $A^+(g') \cup A^-(g')$ such that $K_0, \cdots K_{n-1}, K_{g'}$ satisfy the conditions of (2.2)). Thus, for every $m \neq 0$, provided k is large $a_0^{ki!}$ $g^{[1+k(i!)]m}$ $a_0^{-ki!}(K_i) \longrightarrow A^+(a_0)(k \to \infty)$ i.e. $a_0^{ki!}$ $g^{(1+k(i!))m}$ $a_0^{-ki!}(K_i) \subset$

K_0 . Thus $\langle a_i, a_{n+1} \rangle$ form a free system $(k \gg 0)$. Now $\langle a_0^k, a_{n+1} \rangle$ is conjugate to $\langle a_0^k, g' \rangle$ which is already a free system. Whence S' is a free system. Consider the group $\Gamma(S')$. It contains $\Gamma(S) = N$. It also contains a_{n+1} . However, $x\,N = a_0^{ki!} x\,N$ and so, $a_{n+1}N = a_0^{ki!} x \theta a_0^{-ki!} N \quad (\theta \in N) = x\,N$. Thus $i(S') < i(S)$, contradicting the minimality of $i(S)$. Therefore $i(S) = 1$.

Thus $\Gamma = \Gamma(S) = \Gamma \cap Cl(\Delta)$, where Δ is the group generated by $\langle a_1, \ldots, a_{n-1} \rangle$. This group is free by (3) of (2.2), is finitely generated, and by definition, $Cl(\Delta) = \widehat{\Gamma}$. This completes the proof of Theorem (3.1).

(3.2) Corollary: Let G be a linear real semi–simple group with $\mathbb{R}$–rank $(G) \geqq 2$, let $\Gamma \subset G$ be an irreducible non–cocompact arithmetic lattice. Then Γ contains a finitely generated profinitely dense free subgroup.

By [R 1,2], the associated simply connected group has the congruence subgroup property. Then (3.2) follows from (3.1).

(3.3) Corollary: If $n \geqq 3$, then the group $SL_n(\mathbb{Z})$ contains a free finitely generated subgroup which maps onto every finite quotient of $SL_n(\mathbb{Z})$. In particular, $SL_n(\mathbb{Z})$ contains maximal subgroups of infinite index.

This is immediate from (3.1), since by a Theorem of Mennicke (see [R 1]), $SL_n(\mathbb{Z})(n \geq 3)$ satisfies the congruence subgroup property. Note that this gives another proof of Platonov's conjecture on existence of maximal subgroups in $SL_n(\mathbb{Z})(n \geq 3)$. Instead of an infinitely generated free group as in [M–S], we have produced a finitely generated free group in $SL_n(\mathbb{Z})$ which is profinitely dense. As in the introduction, this implies the existence of maximal subgroups of infinite index in $SL_n(\mathbb{Z})$.

(3.4) Corollary: If Γ is as in (3.1) and J is a finite group, then $\Gamma \times J$ contains a free profinitely dense finitely generated subgroup.

We may replace Γ and G in (3.1) by $\Gamma \times J$ and $G \times J$. The hypotheses of (3.1) are unaltered. So are the conclusions.

References

Tits 1, *Free subgroups in Linear Groups*, J. of Algebra **20** (1972), 250–272.

———2, *Classification of Algebraic Semi–simple Groups*, Proc. Symp. Pure. Math., Amer. Math. Soc. Providence **9** (1966).

Nori, M.V., *On Subgroups of* $GL_n(\mathbb{F}_p)$, Invent. Math. 88 **2** (1987), 257–275..

Weisfeiler, B., *Strong Approximation for Zariski Dense Subgroups of Semi–simple Algebraic Groups*, Ann. of Math. **120** (1984), 271–315.

Prasad, G. – Raghunathan, M.S., *Cartan Subgroups and Lattices in Semi–simple Lie Groups*, Ann. of Math. **64** (1972).

Raghunathan, M.S. 1, *On the Congruence Subgroup Probleme*, Publ. Math. I.H.E.S. **46** (1976), 107–161.

———2, *On the Congruence Subgroup Problem II*, Invent. Math. 85 **1** (1986), 73–117.

Margulis, G.A. – Soifer, G.A., *Maximal Subgroups of Infinite Index in finitely generated Linear Groups*, J. of Alg. **69** (1981), 1–23.

Borel, A. – Tits, J 1, *Groupes Reductifs, Publ. Math. IHES* **27** (1965), 55–150.

———2, *Complèménts à làrticle "Groupes Reductifs"*, Publ. Math. IHES **41** (1972), 253–276.

Soifer, G.A., *Maximal Subgroups of Lattices in* $SL_n(\mathbb{R})$ *(submitted to TIFR* ■ *)*.

Platonov, V.P. and Rapinchuk, A., *Algebraic Groups and Number Theory*, Academic Press **139** (Pure and Applied Math. Series).

Borel, A. and Harish–Cahndra, *Arithmetic Subgroups of Algebraic Groups*, Ann. of Math. **75** (1962), 485–535.

Scott, P., *Subgroups of surface groups are almost geometric*, J. London Math. Soc. **17** (1978), 555–565.

, corr. J. London Math. Soc. (2) **32** (1985), 217–220.