United Nations Educational Scientific and Cultural Organization and International Atomic Energy Agency THE ABDUS SALAM INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

A NOTE ON FINITELY GENERATED NILPOTENT GROUPS

Nguyên Q. Thăng¹ Institute of Mathematics, P.O. Box 631, Bo Ho, Hanoi, Vietnam and The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

Abstract

We discuss a general approach to the proof of a theorem of Pickel on the finiteness of the number of isomorphism classes of finitely generated nilpotent groups with isomorphic finite quotients, which is applicable to handle other cases of finitely generated groups.

> MIRAMARE – TRIESTE August 2000

Introduction. In the study of discrete groups one often has to deal with various topologies and two of the most important of them are the profinite topology and the congruence topology, both of which turn out to be uniform. The profinite topology on a group G is defined by the collection of all subgroups of finite index in G, and we can define the profinite completion \hat{G} with respect to the profinite topology also as the projective limit of finite quotient subgroups of G. To define congruence topology we assume for simplicity that $G \hookrightarrow \operatorname{GL}_n(\mathbf{Z})$. The principal congruence subgroup of level m (denoted by $\operatorname{GL}_n(\mathbf{Z}, m)$) is defined as the kernel of the canonical projection $\operatorname{GL}_n(\mathbf{Z}) \to \operatorname{GL}_n(\mathbf{Z}/m\mathbf{Z})$ induced from the projection $\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$. The topology on $\operatorname{GL}_n(\mathbf{Z})$ defined by principal congruence subgroups $\operatorname{GL}_n(\mathbf{Z}, m)$ is called *congruence topology* and the congruence topology on G is the induced one. Denote by \tilde{G} the completion of G with respect to congruence topology. Thus G is a dense subgroup of the compact topological group \hat{G} (or \tilde{G}).

There are two natural questions. First, how one can distinguish these two topologies, i.e., one asks when they do coincide. If the answer is affirmative, one says that the congruence subgroup problem has positive solution for G. For solvable subgroups of $\operatorname{GL}_n(\mathbf{Z})$, the congruence subgroup problem is known to have positive solution, and we refer, say, to [DDMS, Ch. VI] for a survey of the problem. Second, it is natural to ask how strongly the groups G and \hat{G} (or \tilde{G}) are related, for example, to what extent the group \hat{G} (or \hat{G}) is determined by G. This kind of question was well-known and considered by many authors and in connection with algebraic geometry it was first explicitly stated by A. Grothendieck in [Gro]. If G is a finitely generated nilpotent group it was Pickel [Pi] who first showed that there exists only a finite number of isomorphic classes of finitely generated nilpotent groups which have isomorphic profinite completions. Subsequently, this important result has been used, among the others, in order to give an extension of this result for polycyclic groups, which is the main result of [GPS]. Notice that the proof given by Pickel in [Pi] makes essential use of (in fact is reduced to) some finiteness results regarding the commensurable finitely generated nilpotent groups due to Borel, and has more or less purely group-theoretic flavour, so it is very hard to extend this method to cover other classes of groups (especially non-solvable groups).

It is our objective to explore another approach to this result, which tends to be more arithmetic and algebraico - geometric and does not rely on this result of Borel. We make use of some results due to Hochschild and Mostow about the structure of the groups of automorphisms of solvable algebraic groups, finiteness theorems due to Borel and Serre, and also p-adic Lie theory. The purpose of the approach considered here is to pave a way for the case of discrete subgroups of other types (e.g. semisimple or solvable types) of algebraic groups (treated in [T]).

Notations. We keep the following notation and convention throughout the paper. $\mathbf{Z} =$ integers, $\mathbf{Q} =$ rational numbers, $\mathbf{R} =$ real numbers, $\mathbf{C} =$ complex numbers, $\mathbf{\Omega} =$ a fixed universal domain, $\mathbf{Z}_p = p$ -adic integers, $\mathbf{Q}_p = p$ -adic numbers, $\mathbf{A} =$ adèle ring of \mathbf{Q} . Algebraic groups under consideration are identified with their points over a certain fixed universal domain, say

 Ω . $\mathbf{G}(\mathbf{B}) = \text{the } \mathbf{B}\text{-points of a linear algebraic group } \mathbf{G}$, with respect to some matrix realization of $\mathbf{G} \hookrightarrow \operatorname{GL}_n$ and for some ring \mathbf{B} ; $Lie(\mathbf{G})$ denotes the Lie algebra of a Lie (resp. *p*-adic or algebraic) group \mathbf{G} ; *inv.lim* means inverse limit. If G is a group, \hat{G} denotes the profinite completion of G, \bar{G}^p denotes the pro-*p*-completion of G, and $\mathbf{G} = \bar{G}$ denotes the Zariski closure of G, where G is considered as a subgroup of some algebraic group. For a finitely generated group G, $\mathcal{B}(G)$ will denote the set of isomorphic classes of finitely generated groups H with $\hat{H} \simeq \hat{G}$.

1 Some Reductions

We need some preliminary results which reduce our problem to simpler case. The Proposition 1. 4 below is crucial, which enables one to replace the group G by its suitable torsion-free verbal subgroup (see Lemma 1.5). The following two lemmas are well-known.

1.1. Lemma. Let H be a normal subgroup of a group G. Then \hat{H} is a normal subgroup of \hat{G} and we have

$$(\widehat{G/H}) \simeq \widehat{G}/\widehat{H}.$$

In particular, if K is a subgroup of finite index in G, then $[G:K] = [\hat{G}:\hat{K}]$.

Recall that a polycyclic group is a group with a finite normal chain of normal subgroups such that each successive factor is cyclic. In particular, any finitely generated nilpotent group is polycyclic. For some other useful related notions and results we refer to [Ra, Ch. IV]. The following lemma was proved there. It provides us, as we will see later, many subgroups of finite index of a polycyclic group G with good properties.

1.2. Lemma. [Ra, 4.4] For a polycyclic group G, $[G : G^k] < \infty$, where G^k denotes the subgroup of G generated by k-powers in G.

Let us be given an alphabet \mathcal{X} and let M be a set of words from this alphabet, $M = \{m_{\alpha} : \alpha \in A\}$, with $m_{\alpha} := x_{1\alpha}^{n_{1\alpha}} \cdots x_{p\alpha}^{n_{p\alpha}}, x_i \in \mathcal{X}$. The subgroup of G generated by the set

$$\{g_{1\alpha}^{n_{1\alpha}}\cdots g_{p\alpha}^{n_{p\alpha}}: g_{i\alpha}\in G, \alpha\in A\}$$

is called the *verbal subgroup* of G corresponding to M, and will be denoted by M_G . We have the following general result.

1.3. Lemma. Let M be a set of words, G (resp. H) be a group with a family of normal subgroups $\{N_{\alpha}\}_{\alpha \in \Lambda}$ (resp. $\{K_{\alpha}\}_{\alpha \in \Lambda}$), where Λ is a filtered set of indices by means of inclusion relation among subgroups N_{α} (resp. K_{α}). Assume there is an isomorphism of projective systems

(1)
$$(\phi_{\alpha}): (G_{\alpha}, \psi_{\alpha\beta}) \simeq (H_{\alpha}, \theta_{\alpha\beta}),$$

where $G_{\alpha} = G/N_{\alpha}, H_{\alpha} = H/K_{\alpha}$. Then (1) induces an isomorphism

$$\phi: inv.lim \ G_{\alpha} \simeq inv.lim \ H_{\alpha}$$

such that

$$\phi(inv.lim M_{G_{\alpha}}) = inv.lim M_{H_{\alpha}}.$$

b) In particular, if $\{N_{\alpha}\}_{\alpha \in \Lambda}$ (resp. $\{K_{\alpha}\}_{\alpha \in \Lambda}$) is the set of all normal subgroups of finite index in G (resp. H), then

$$\phi(M_G) = M_H.$$

Proof. a) Denote by $\mathcal{G} = inv.lim \ G_{\alpha}, \ \mathcal{H} = inv.lim \ H_{\alpha}$. Then we have the following commutative diagram

where p_{α} (resp. q_{α}) denotes canonical homomorphisms $\mathcal{G} \to \mathcal{G}_{\alpha}$ (resp. $\mathcal{H} \to \mathcal{H}_{\alpha}$). Since ϕ_{α} is an isomorphism, then

$$\phi_{\alpha}(M_{G_{\alpha}}) = M_{H_{\alpha}}.$$

But $G_{\alpha} = G/N_{\alpha}, H_{\alpha} = H/K_{\alpha}$, so we have

$$M_{G_{\alpha}} = M_G N_{\alpha} / N_{\alpha}, M_{H_{\alpha}} = M_H K_{\alpha} / K_{\alpha},$$

and one checks that $\{M_{G_{\alpha}}, \psi_{\alpha\beta}|_{M_{G_{\alpha}}}\}$ and $\{M_{H_{\alpha}}, \theta_{\alpha\beta}|_{M_{H_{\alpha}}}\}$ form projective systems of groups. Denote their limits respectively by \mathcal{M}_{G} and \mathcal{M}_{H} . Then $\mathcal{M}_{G} \subset \mathcal{G}$ and $\mathcal{M}_{H} \subset \mathcal{H}$ and we have the following commutative diagram

$$\begin{array}{cccc} \mathcal{M}_G & \stackrel{\tau}{\to} & \mathcal{M}_H \\ & & & \downarrow p_\alpha & & \downarrow q_\alpha \\ \\ \mathcal{M}_{G_\alpha} & \stackrel{\phi_\alpha}{\to} & \mathcal{M}_{H_\alpha} \end{array}$$

We show that $\phi|_{\mathcal{M}_G} = \tau$. Let $x \in \mathcal{M}_G$. From the first diagram we have

$$(\phi_{\alpha}p_{\alpha})(x) = q_{\alpha}(\phi(x)),$$

and from the second one we have

$$(\phi_{\alpha}p_{\alpha})(x) = q_{\alpha}(\tau(x)).$$

From these equalities one sees that the α -coordinates of $\phi(x)$ and $\tau(x)$ coincide, thus $\phi(x) = \tau(x)$, hence $\phi(\mathcal{M}_G) = \mathcal{M}_H$.

b) By the assumption, \mathcal{G} is \hat{G} (resp. \mathcal{H} is \hat{H}) up to an isomorphism. It is known that the induced topology on M_G (resp. M_H) is the profinite topology, hence

$$\phi(\hat{M}_G) = \hat{M}_H$$

and the proposition is proved. \blacksquare

The following proposition makes it possible to substitute G by its suitable verbal subgroup.

1.4. Proposition. Let G be a polycyclic group, M_G a verbal subgroup of finite index in G corresponding to a set of words M. If the number of isomorphism classes in $\mathcal{B}(M_G)$ is finite then the same is true for $\mathcal{B}(G)$.

Proof. Let $\{H_{\alpha}\}$ be a complete set of representatives of isomorphism classes in $\mathcal{B}(G)$. Let $\phi_{\alpha}: \hat{G} \simeq H_{\alpha}$ be corresponding isomorphisms. Lemma 1.3 shows that $\phi_{\alpha}(\hat{M}_G) = \hat{M}_{H_{\alpha}}$, hence by Lemma 1.1 one has

$$\hat{G}/\hat{M}_G \simeq \hat{H}_\alpha/\hat{M}_{H_\alpha}$$

thus $[H_{\alpha} : M_{H_{\alpha}}] < \infty$ (by Lemma 1.1), and $G/M_G \simeq H_{\alpha}/M_{H_{\alpha}}$. By assumption, there are only finitely many non-isomorphic groups among $M_{H_{\alpha}}$, $\alpha \in \Lambda$ (up to isomorphism). From a theorem of Segal [Seg1] (that there is only a finite number of extensions of given degree n of a given polycyclic group, where $n = [G : M_G]$) we conclude that there is only a finite number of non-isomorphic groups H_{α} .

1.4.1. Remarks. a) According to Lemmas 1.4 and 1.2, in order to prove the finiteness of the number of non-isomorphic classes in $\mathcal{B}(G)$ with G polycyclic, we may pass to subgroups of finite index in G of the form G^k .

b) Recall that a polycyclic G is called *strong* if there is a normal chain

$$G = G_0 > G_1 > \cdots > G_n = \{e\},\$$

where all the factors G_i/G_{i+1} are infinite cyclic. It is known that in any polycyclic group G there exists a strong polycyclic subgroup G' of finite index, which we may assume to be normal in G (see [Ra], Ch. IV). If |G/G'| = t then it is clear that $G^t \subset G'$, i.e., G^t is also a strong polycyclic group. This means that in order to prove the finiteness of the cardinality of $\mathcal{B}(G)$ we may substitute G by its suitable verbal strong polycyclic subgroup of finite index.

The following lemma allows us, instead of groups in $\mathcal{B}(G)$ to consider their subgroup of finite index, which are *torsion-free*.

1.5. Lemma. Let G be a strong polycyclic torsion-free group. Then all groups in $\mathcal{B}(G)$ are also torsion-free.

Proof. First we claim that if a sequence $\{x_i\}$ in G converges to $x \in \hat{G}$, and for some $n \in \mathbb{N}$, $x_i^n \to 1$ (in profinite topology), then $x_i \to 1$ (in profinite topology). We proceed by induction on rank r = rk(G) of G. It is trivial if r = 0, 1. Let

$$1 \to G_1 \to G \xrightarrow{\pi} \mathbf{Z} \to 1$$

be an exact sequence of groups, where the multiplication in \mathbb{Z} is denoted additively. Since $x_i \to x$ we have $\pi(x_i^n) = n\pi(x_i) \to 0$, hence $\pi(x_i) \to 0$, thus $x_i \to x \in \hat{G}_1$. Since $x^n = 1$ and $rk(G_1) < rk(G)$, by induction hypothesis we have x = 1. If for a group $H_\alpha \in \mathcal{B}(G)$ there is $h \in \hat{H}_\alpha$ such that $h^n = 1$ then $\phi_\alpha^{-1}(h)^n = 1$, where $\phi_\alpha : \hat{G} \simeq \hat{H}_\alpha$ is an isomorphism, and we conclude that $\phi_\alpha^{-1}(h) = 1$, i.e., h = 1.

1.5.1. Remarks. From 1.4, 1.5 and from the Remarks 1.4.1 above we see that, for a polycyclic group G, in order to prove the finiteness of the $\mathcal{B}(G)$, one may substitute G by its strong polycyclic torison-free subgroup of the form G^t , and all groups H from $\mathcal{B}(G)$ by its torsion-free subgroups. Thus from now on we may assume that all finitely generated nilpotent groups under consideration are torsion-free. Moreover, we may further assume that they are given in the matrix form, such that for every $H \in \mathcal{B}(G)$ (including G) there is a faithful representation $H \to \operatorname{GL}_n(\mathbb{Z})$ for some n, according to a well-known theorem of Malcev [Ma]. Then with respect to this representation $H \subset \mathbf{H}(\mathbb{Z})$ and $\mathbf{H}(\mathbb{Z})$ is Zariski dense in \mathbf{H} , where \mathbf{H} is the Zariski closure of H in $\operatorname{GL}_n(\Omega)$. Denote by \overline{G}^p the pro-p-completion of G, i.e., $\overline{G}^p := inv.lim_i (G/\Delta_i)$, where Δ_i run over subgroups of index equal to powers of a prime p. Since finite nilpotent groups are direct products of their Sylow-subgroups, or more generally, for solvable integral matrix groups the congruence subgroup problem has an affirmative solution, i.e., the profinite topology coincides with the topology defined by congruence subgroups (see [Cha]), we conclude that

$$\hat{G} = \prod_{p} \bar{G}^{p}$$

where p runs over all prime numbers. Therefore from above remarks we have

1.6. Proposition. With the assumptions made above (1.5.1) regarding the finitely generated nilpotent group G and $H \in \mathcal{B}(G)$ we have for all primes p

$$\bar{G}^p \simeq \bar{H}^p$$

2 Finitely Generated Nilpotent Groups

In this section we will prove the finiteness of the set $\mathcal{B}(G)$ of a finitely generated nilpotent group G. According to Section 1, we may assume that G and all groups $H \in \mathcal{B}(G)$ are torsion-free. Then by a theorem of Malcev [Ma], each group H possesses a faithful matrix representation

$$H \to U_n(\mathbf{Z})$$

to the group of upper triangular unipotent integral matrices $U_n(\mathbf{Z})$. Denote by $\mathbf{H} := \overline{H}$ the Zariski closure of H in $U_n(\Omega)$. Then \mathbf{H} is a unipotent group defined over \mathbf{Q} . We will make essential use of the structure of linear algebraic group on the group of rational automorphisms of unipotent algebraic groups and also of a fundamental theorem of Borel [Bor] on the finiteness of the number of double coset classes of $Aut(\mathbf{G})(\mathbf{A})$, where $Aut(\mathbf{G})$ denotes the \mathbf{Q} -algebraic group of rational automorphisms of \mathbf{G} and \mathbf{A} will denote the adèle ring of \mathbf{Q} .

Via the matrix realization of G above, it is clear that \overline{G}^p is the *p*-adic closure of G in the *p*-adic topology induced from $\operatorname{GL}_n(\mathbb{Z}_p)$. By Proposition 1.6, for all prime numbers p we have $\overline{G}^p \simeq \overline{H}^p$ and it is well-known (see e.g. [La, Ch. III], [Bou, Ch. III], [DDMS, Ch. I]) that any such isomorphism is a continuous isomorphism. The following lemma shows that this isomorphism is in fact a *polynomial* isomorphism.

2.1. Lemma. Let $f_p : \overline{G}^p \simeq \overline{H}^p$ be an isomorphism of pro-p-groups. Then f is uniquely extended to a \mathbf{Q}_p -polynomial isomorphism $\overline{f}_p : \mathbf{G} \to \mathbf{H}$.

Proof. Since f_p is continuous, it is also an analytic isomorphism of *p*-adic Lie groups (see [DDMS, Ch. X], [La]). For a *p*-adic Lie group *P* we denote by Lie(P) the Lie algebra of *P*. It is well-known ([Bou, Ch. III], [La], [DDMS, Ch. VII]) that there exists a open neighbourhood *V* of zero in $Lie(\bar{G}^p)$ such that the following diagram is commutative :

$$V \xrightarrow{exp} exp(V)$$

$$\downarrow df_p \qquad \qquad \qquad \downarrow f_p$$

$$df_p(V) \xrightarrow{exp} f_p(exp(V))$$

So we can take exp(V) in the form $(\bar{G}^p)^{p^s}$, where $(\bar{G}^p)^{p^s}$ is the subgroup of \bar{G}^p generated by p^s -powers in \bar{G}^p , such that the logarithm map log (which is inverse to exp) is defined on exp(V). Since G and H have faithful unipotent representation, we may assume that both of them are subgroups of $U_n(\mathbf{Z})$ for some n. Then the maps log and exp are given explicitly as follows

$$log(x) = (x \Leftrightarrow E) \Leftrightarrow (x \Leftrightarrow E)^2/2 + \dots + (\Leftrightarrow 1)^n (x \Leftrightarrow E)^{n-1}/(n \Leftrightarrow 1), x \in \bar{G}^p$$
$$exp(X) = E + X + X^2/2! + \dots + X^{n-1}/(n \Leftrightarrow 1)!, X \in Lie(\bar{G}^p),$$

where E denotes the $n \times n$ identity matrix. Now we know that log and exp are defined over all \bar{G}^p and $Lie(\bar{G}^p)$, respectively, hence we have

$$f_p = exp \circ df_p \circ log,$$

i.e., f_p is a \mathbf{Q}_p -polynomial map, thus it is uniquely extended to a \mathbf{Q}_p -isomorphism $\bar{f}_p : \mathbf{G} \simeq \mathbf{H}$.

We see that under our assumption made above, \mathbf{G} and \mathbf{H} are linear algebraic \mathbf{Q} -groups which are isomorphic locally everywhere. From [BS, Thm. 7.1] it follows that such groups lie in finitely many \mathbf{Q} -isomorphic classes. Thus we have

2.1.1. Corollary. For any finitely geberated torsion free nilpotent group G, the set $\mathcal{B}(G)$ of G is a disjoint union of finitely many classes of groups H with \mathbf{Q} -isomorphic Zariski closures.

It follows that we need only to prove the finiteness of any set of those groups in $\mathcal{B}(G)$ which have **Q**-isomorphic Zariski closures. We consider any one of these, say with a representative Gand by abuse of notation we denote it again by $\mathcal{B}(G)$.

The following result shows the adèle nature of the family (f_p) of Lemma 2.1.

2.2. Lemma. With notation as in Lemma 2.1, for almost all p, \bar{f}_p is a \mathbb{Z}_p -polynomial isomorphism with respect to the given matrix realization of the groups G and H.

Proof. Since f_p is an isomorphism of p-adic analytic Lie groups, it maps a uniform subgroup² of finite index S_G in \overline{G}^p onto a uniform subgroup of finite index $S_H < \overline{H}^p$ (see [DDMS, Ch. IV], [La, Ch. III], for more details). But $Lie(S_G) \simeq Lie(S_H)$ as \mathbb{Z}_p -Lie algebras (loc. cit.) so df_p must be a \mathbb{Z}_p -linear map. Denote by \mathbb{G} (resp. \mathbb{H}) the Zariski closure of G (resp. H) in $U_n(\Omega)$. Since \mathbb{G} and \mathbb{H} are unipotent algebraic groups, they are connected. Thus $f_p|_{S_G}$ can be extended to a rational homomorphism

$$\bar{f}_p: \bar{S}_G = \mathbf{G} \to \mathbf{H} = \bar{S}_H.$$

 But

$$f_p = exp \circ df_p \circ \log g$$

thus f_p will be \mathbb{Z}_p -polynomial map for those p not lying in the set T of primes dividing $(n \Leftrightarrow 1)!$. Therefore \bar{f}_p is defined over \mathbb{Z}_p for all $p \notin T$.

 $^{^{2}}p$ -saturable subgroup in terminology of [La]

We need the following technical lemma in the sequel.

2.3. Lemma. With above notation, let f_1, \ldots, f_N be Q-rational functions over Gwhich are linearly independent over Q. Then there exists $x_1, \ldots, x_N \in \mathbf{G}(\mathbf{Z})$ such that

$$det(f_i(x_j))_{1 < i,j, < N} \in \mathbf{Q} \setminus \{0\},\$$

where $\mathbf{G}(\mathbf{Z})$ denotes the subgroup of \mathbf{Z} -points of \mathbf{G} with respect to the given matrix realization.

Proof. We prove by induction on N. The case N = 1 is trivial. Notice that $\mathbf{G}(\mathbf{Z})$ is Zariski dense in \mathbf{G} . Denote

$$f(x_1, ..., x_n) := det(f_i(x_j))_{1 < i, j, < N}.$$

Let N > 1 and assume that we have found $N \Leftrightarrow 1$ points x_1, \ldots, x_{N-1} such that

$$c = det(f_i(x_j)_{1 \le i,j \le N-1}) \neq 0$$

Consider the following Q-rational function g(z) on G defined as follows

$$g(z) := f(x_1, ..., x_{N-1}, z),$$

and decompose the matrix g(z) after the last row we have

$$g(z) = a_1 f_1(z) + \dots + a_{N-1} f_{N-1}(z) + c f_N(z).$$

If for all $z \in \mathbf{G}(\mathbf{Z})$ we had g(z) = 0, then due to the Zariski density of $\mathbf{G}(\mathbf{Z})$ in \mathbf{G} , it would follow that g(z) = 0. Hence c = 0 since $f_1, ..., f_N$ are \mathbf{Q} -linearly independent, which contradicts the choice of c.

Denote by $M = \operatorname{Aut}(\mathbf{G})$ the group of rational automorphisms of \mathbf{G} . It is well-known that M has a natural structure of linear \mathbf{Q} -algebraic group (see, e.g., [BS], or just look at the diagram in the proof of Lemma 2.1). We need a specific realization of the group M, which plays a crucial role in our arguments, as follows. Recall that \mathbf{A} denotes the adèle ring of \mathbf{Q} .

2.4. Proposition. With above notation there is a realization of M as a linear algebraic \mathbf{Q} -group such that for every $H \in \mathcal{B}(G)$ and for any \mathbf{Q} -isomorphism $g : \mathbf{H} \to \mathbf{G}$, the family $(g \circ f_p)$ (p runs over all prime numbers) is belong to $M(\mathbf{A})$.

Proof. First we fix a universal domain Ω . It follows from results of [HM] (see the discussion before Lemma 3.1 there), that **G** is a conservative **Q**-group, i.e., the group M acts locally finitely on the **Q**-algebra **Q**[**G**] of regular functions defined over **Q** on **G**. As before, we fix an embedding $G \hookrightarrow U_n(\mathbf{Z})$ and let $x_{ij} (1 \le i, j \le n)$ be the coordinate matrix functions on **G**. Let

V be the smallest finite dimensional **Q**-vector subspace of $\mathbf{Q}[\mathbf{G}]$ containing $x_{ij}, 1 \leq i, j \leq n$, which is *M*-invariant (i.e. V is generated by x_{ij} and their images under the action of M). Let $\{f_1, ..., f_N\}$ be **Q**-regular functions over **G** which form a **Q**-basis of V containing all x_{ij} (notice that all x_{ij} are **Q**-linearly independent). By multiplying f_k with a suitable integer, we may assume that f_k are all **Z**-polynomial functions. For $\phi \in M$ let the action of ϕ be given as follows

$$\phi: f_i \mapsto f_i \circ \phi = \sum_{1 \le j \le N} a_{ij}^{(\phi)} f_j,$$

where $a_{ij}^{(\phi)} \in \Omega$ (=universal domain). Since the **Q**-basis $\{f_1, ..., f_N\}$ contains all coordinate functions, it follows that the mapping

$$\Phi:\phi\mapsto (a_{ij}^{(\phi)})$$

is a faithful **Q**-representation of M into $\operatorname{GL}(V)$, where the latter is identified with $\operatorname{GL}_N(\Omega)$ by means of the basis $\{f_1, ..., f_N\}$. Further we will identify M with a closed **Q**-subgroup of $\operatorname{GL}_N(\Omega)$. Thus

$$\phi \in M(\mathbf{Z}_p) \Leftrightarrow a_{ij}^{(\phi)} \in \mathbf{Z}_p, \ \forall i, j.$$

Now let

$$\bar{f}_p:\mathbf{G}\simeq\mathbf{H}$$

be the isomorphism extending the isomorphism $f_p: \bar{G}^p \simeq \bar{H}^p$ (so \bar{f}_p is defined over \mathbf{Q}_p) and let $g: \mathbf{H} \simeq \mathbf{G}$ be any **Q**-isomorphism.

We now choose elements $x_1, ..., x_N$ as in Lemma 2.3. For the convenience, we denote $a_{ij} = a_{ij}^{(f_p)}$, where p is fixed. Then we have the following systems of equations

$$(A_1) \begin{cases} f_1(g \circ \bar{f}_p(x_1)) = a_{11}f_1(x_1) + \dots + a_{1N}f_N(x_1) \\ \vdots \\ \vdots \\ f_1(g \circ \bar{f}_p(x_N)) = a_{11}f_1(x_N) + \dots + a_{1N}f_N(x_N) \end{cases}$$

$$(A_N) \begin{cases} f_N(g \circ \bar{f}_p(x_1)) = a_{N1} f_1(x_1) + \dots + a_{NN} f_N(x_1) \\ \cdot \\ \cdot \\ \cdot \\ f_N(g \circ \bar{f}_p(x_N)) = a_{N1} f_1(x_N) + \dots + a_{NN} f_N(x_N) \end{cases}$$

Denote

$$r := det(f_i(x_j)) \ (1 \le i, j \le N).$$

By our choice of f_i , we have $r \in \mathbf{Z}$. By solving the system A_t above with respect to $a_{t1}, ..., a_{tN}$, we have

$$a_{ij} = (1/r)d_{ij}, \forall i, j,$$

where $d_{ij} \in \mathbf{Q}_p$. Denote

 $S:=\{ \text{ prime numbers } q \text{ such that } g \text{ is not defined over } \mathbf{Z}_q$

(i.e.,
$$g$$
 is not a \mathbf{Z}_q -polynomial map) }

and

$$T := \{ \text{ primes divisors of } (n \Leftrightarrow 1)! \} .$$

It is clear that S and T are finite, so for $p \notin S \cup T$ we have $g \circ f_p \in M(\mathbb{Z}_p)$ as required.

The following is a well-known result of Malcev (see [Ma], [Ra, Ch. VI]).

2.5. Proposition. With notation as above, the group G has finite index in $\mathbf{G}(\mathbf{Z})$, i.e., G is an arithmetic subgroup.

The following statement shows that the groups $H \in \mathcal{B}(G)$ are uniquely determined by their Zariski-closure and *p*-adic closures.

2.6. Proposition. For any $H \in \mathcal{B}(G)$ we have

$$\mathbf{H}(\mathbf{Q}) \cap (\cap_p \bar{H}^p) = H.$$

Proof. Denote the above intersection by R. It is clear that $R \subset \mathbf{H}(\mathbf{Z}), H \subset R \subset \bar{H}^p$, hence for all p we have $\bar{R}^p = \bar{H}^p$. As consequence of the congruence-subgroup property, we deduce that $\hat{R} = \hat{H}$. From Lemma 1.1 and Proposition 2.5 we derive that R = H.

Remark. It is interesting to note that the question of whether the similar property as in 2.6 holds for arithmetic subgroups of almost simple simply connected groups over number fields is a partial case of Platonov - Margulis conjecture.

We will need the following important property of finitely generated torsion-free nilpotent groups [Ma].

2.7. Proposition. With above notation let $f : G \simeq H$ be an isomorphism. Then f can be uniquely extended to a Q-polynomial isomorphism $\mathbf{G} \simeq \mathbf{H}$.

2.8. Proposition. With above notation \overline{G}^p is of finite index in $\overline{\mathbf{G}(\mathbf{Z})}^p$ and for almost all p we have

$$\bar{G}^p = \overline{\mathbf{G}(\mathbf{Z})}^p.$$

Proof. By Lemma 1.1 and Proposition 2.5 we have $[\widehat{\mathbf{G}(\mathbf{Z})}: \hat{G}] = [\mathbf{G}(\mathbf{Z}): G] < \infty$, and from

$$\widehat{\mathbf{G}(\mathbf{Z})} = \prod_{p} \overline{\mathbf{G}(\mathbf{Z})}^{p}, \ \hat{G} = \prod_{p} \bar{G}^{p},$$

we derive the desired result. \blacksquare

Denote by

 $\mathcal{C}(G) = \{(f_p) \in \prod_p M(\mathbf{Q}_p) : f_p(\bar{G}^p) = \bar{G}^p, \text{ for all } p, \text{ and} \\ \bar{f}_p \in M(\mathbf{Z}_p) \text{ for almost all } p\}.$

It is clear that $\mathcal{C}(G)$ is a subgroup of $M(\mathbf{A})$. Next we want to parametrize the set $\mathcal{B}(G)$ by assigning to each $H \in \mathcal{B}(G)$ a double coset class in $M(\mathbf{Q}) \setminus M(\mathbf{A}) / \mathcal{C}(G)$ defined as follows :

If $g : \mathbf{H} \simeq \mathbf{G}$ is a **Q**-isomorphism, $\bar{f}_p : \mathbf{G} \simeq \mathbf{H}$ is the isomorphism extending $f_p : \bar{G}^p \simeq \bar{H}^p$ for all p, then we set

$$a(G,H) := M(\mathbf{Q})(g \circ \overline{f}_p)\mathcal{C}(G).$$

According to Proposition 2.4, $(g \circ \bar{f}_p) \in M(\mathbf{A})$ so a(G, H) is an element of the set of double coset classes $M(\mathbf{Q}) \setminus M(\mathbf{A}) / \mathcal{C}(G)$.

2.9. Proposition. The correspondence defined above is a well-defined map which is constant on isomorphism class of H, i.e., if $H \simeq K$ then a(G, H) = a(G, K).

Proof. First we have to show that the class $M(\mathbf{Q})(g \circ \bar{f}_p)\mathcal{C}(G)$ does not depend on the choice of g and (\bar{f}_p) .

Let $g' : \mathbf{H} \simeq \mathbf{G}$ be another **Q**-isomorphism, $f'_p : \overline{G}^p \simeq \overline{H}^p$ be an isomorphism with the extension $\overline{f}'_p : \mathbf{G} \to \mathbf{H}$ for all p. Then we have

$$(*) g \circ \bar{f}_p = (g \circ g'^{-1}) \circ (g' \circ \bar{f}'_p) \circ (\bar{f}'_p^{-1} \circ \bar{f}_p).$$

Since $g \circ g'^{-1}$ is a **Q**-isomorphism of **G**, $g \circ g'^{-1} \in M(\mathbf{Q})$. For all p we have

$$(\bar{f'_p}^{-1} \circ \bar{f}_p)(\bar{G}^p) = \bar{G}^p.$$

Hence for all p we have $\bar{f'_p}^{-1} \circ \bar{f_p} \in M(\mathbf{Q}_p)$ and thus for almost all $p, \bar{f'_p}^{-1} \circ \bar{f_p} \in M(\mathbf{Z}_p)$, because $\bar{f'_p}$ and $\bar{f_p}$ are so. Hence $(\bar{f'_p}^{-1} \circ \bar{f_p}) \in \mathcal{C}(G)$. Thus

$$M(\mathbf{Q})(g \circ \bar{f}_p)\mathcal{C}(G) = M(\mathbf{Q})(g' \circ \bar{f}'_p)\mathcal{C}(G).$$

To show that this map is constant on isomorphism classes, we let $s : H \simeq K$ be any isomorphism of groups, i. e. H, K belong to the same isomorphism class in $\mathcal{B}(G)$. Let $f_p : \bar{G}^p \simeq \bar{H}^p$ (resp. $g_p : \bar{G}^p \simeq \bar{K}^p$) be isomorphisms with extensions $\bar{f}_p : \mathbf{G} \simeq \mathbf{H}$ (resp. $\bar{g}_p : \mathbf{G} \simeq \mathbf{K}$). Moreover, s can be extended to $s_p : \overline{H}^p \simeq \overline{K}^p$, which in turn can be extended to $\overline{s}_p : \mathbf{H} \simeq \mathbf{K}$. It is clear that \overline{s}_p are all equal to the same $\overline{s} : \mathbf{H} \simeq \mathbf{K}$ due to the uniquenes of the extension by Proposition 2.7 and \overline{s} is defined over \mathbf{Q} . Let $f : \mathbf{H} \simeq \mathbf{G}$ (resp. $g : \mathbf{K} \simeq \mathbf{G}$) be a \mathbf{Q} -isomorphism. Then we may argue as above (use (*)) to obtain the following

$$M(\mathbf{Q})(f \circ \bar{f}_p)\mathcal{C}(G) = M(\mathbf{Q})((f \circ \bar{s}^{-1} \circ g^{-1})) \circ (g \circ \bar{g}_p) \circ (\bar{g}_p^{-1} \circ \bar{s} \circ \bar{f}_p)\mathcal{C}(G)$$

 $= M(\mathbf{Q})(g \circ \bar{g}_p)\mathcal{C}(G).$

Proposition 2.9 is proved.

The injectivity of the map $H \mapsto a(G, H)$ now follows from the following

2.10. Proposition. If (G, H) and (G, K) have the same double coset class then $H \simeq K$.

Proof. With notation as in the proof of Proposition 2.9, we have for all p

$$f \circ f_p = g_{\mathbf{Q}}(g \circ \bar{g}_p)h_p,$$

where $g_{\mathbf{Q}} \in M(\mathbf{Q})$ and $(h_p) \in \mathcal{C}(G)$ by the assumption. Denote $f' = g_{\mathbf{Q}}^{-1} \circ f$, $\bar{g}'_p = \bar{g}_p \circ h_p$. Then for all p we have

$$f' \circ \bar{f}_p = g \circ \bar{g}'_p,$$

 \mathbf{or}

$$g^{-1} \circ f' = \bar{g}'_p \circ \bar{f}_p^{-1},$$

i.e., $g^{-1} \circ f'$ is a Q-isomorphism $\mathbf{H} \simeq \mathbf{K}$, mapping \bar{H}^p onto \bar{K}^p for all primes p.

For $h \in H \subset \mathbf{H}(\mathbf{Q})$ we have $(g^{-1} \circ f')(h) \in \mathbf{K}(\mathbf{Q})$, and $(g^{-1} \circ f')(h) \in \overline{K}^p$ for all p. Thus

$$(g^{-1} \circ f')(h) \in \mathbf{K}(\mathbf{Q}) \cap (\cap_p \bar{K}^p) = K$$

by Lemma 2.6. Hence $(g^{-1} \circ f')(H) \subset K$. Similarly we have

$$(f'^{-1} \circ g)(K) \subset H,$$

i.e., $(f^{-1} \circ f')(H) = K$, and $H \simeq K$. The Proposition 2.10 is proved.

Preceding observations show that the number of isomorphism classes in $\mathcal{B}(G)$ is not greater than the cardinality of $M(\mathbf{Q}) \setminus M(\mathbf{A}) / \mathcal{C}(G)$. We want to show that the latter is finite. Define

$$\mathcal{D} = \mathcal{D}(G) := \{ (a_p) \in \mathcal{C}(G) : a_p \in M(\mathbf{Z}_p) , \forall p \},\$$

i.e, $\mathcal{D} = \mathcal{C}(G) \cap M(\mathbf{A}(\infty))$, where $\mathbf{A}(\infty)$ denotes the subring of finite adèles of \mathbf{A} . In particular we have

$$Card(M(\mathbf{Q})\backslash M(\mathbf{A})/\mathcal{C}(G)) \leq Card(M(\mathbf{Q})\backslash M(\mathbf{A})/\mathcal{D}).$$

Next we need the following

2.11. Proposition. With above notation the group G(Z) satisfies integral approximation in p for all p, i.e., we have

$$\overline{\mathbf{G}(\mathbf{Z})}^p = \mathbf{G}(\mathbf{Z}_p).$$

Proof. It is well-known (see [Bor]) that any \mathbf{Q} -unipotent group \mathbf{G} has strong approximation property. In particular we have

$$\overline{\mathbf{G}(\mathbf{Z}_{(p)})}^p = \mathbf{G}(\mathbf{Q}_p),$$

where $\mathbf{Z}_{(p)}$ denotes the localization of \mathbf{Z} at $p\mathbf{Z}$. Then for $x \in \mathbf{G}(\mathbf{Z}_p)$ there exists a sequence $\{x_i\}, x_i \in \mathbf{G}(\mathbf{Z}_{(p)})$, such that $x = \lim x_i$ in the *p*-adic topology. Since $x \in \mathbf{G}(\mathbf{Z}_p)$ and $x_i \in \mathbf{G}(\mathbf{Z}_{(p)})$, there is N such that for n > N we have $x_n \in \mathbf{G}(\mathbf{Z})$.

The following proposition plays a crucial role in the proof of the finiteness of $Card(M(\mathbf{Q}) \setminus M(\mathbf{A}) / \mathcal{D})$.

2.12. Proposition. There is only a finite number of subgroups of a given finite index m in $\mathbf{G}(\mathbf{Z}_p)$.

Proof. Let R be a subgroup of index m in $\mathbf{G}(\mathbf{Z}_p)$. First we assume that R is a normal subgroup. Then by considering the factor group $\mathbf{G}(\mathbf{Z}_p)/R$ we conclude that R contains the subgroup $\mathbf{G}(\mathbf{Z}_p)^m$ of $\mathbf{G}(\mathbf{Z}_p)$ generated by the m-powers. Then it suffices only to prove that

$$[\mathbf{G}(\mathbf{Z}_p):\mathbf{G}(\mathbf{Z}_p)^m]<\infty.$$

We will proceed by induction on $dim(\mathbf{G})$. If $dim(\mathbf{G}) = 1$ then $G \simeq \mathbf{G}_a$ and the assertion is true. Assume that the above inequality holds true for $dim(\mathbf{G}) \leq s \Leftrightarrow 1$. Now let $dim(\mathbf{G}) = s$. Since **G** is unipotent, there exists an exact sequence giving the "splitting" of **G**:

$$1 \to \mathbf{G}_1 \to \mathbf{G} \xrightarrow{\pi} \mathbf{G}_a \to 1.$$

Here \mathbf{G}_1 is a normal \mathbf{Q} -subgroup of \mathbf{G} , and π is defined over \mathbf{Q} . We deduce from this the following exact sequence

$$1 \to \mathbf{G}_1(\mathbf{Q}_p) \to \mathbf{G}(\mathbf{Q}_p) \xrightarrow{\pi'} \mathbf{G}_a(\mathbf{Q}_p) \to \mathrm{H}^1(\mathbf{Q}_p, \mathbf{G}_1).$$

Since 1-Galois cohomology of \mathbf{G}_1 is trivial (see e.g. [BS]), π' is surjective. Since \mathbf{G}_a is commutative, it is clear that $[\pi'(\mathbf{G}(\mathbf{Z}_p)) : \pi'(\mathbf{G}(\mathbf{Z}_p)^m)] < \infty$, so from this it follows that

$$[\mathbf{G}_1(\mathbf{Q}_p)\mathbf{G}(\mathbf{Z}_p):\mathbf{G}_1(\mathbf{Q}_p)\mathbf{G}(\mathbf{Z}_p)^m]<\infty,$$

or

$$[\mathbf{G}(\mathbf{Z}_p):\mathbf{G}(\mathbf{Z}_p)^m(\mathbf{G}_1(\mathbf{Q}_p)\cap\mathbf{G}(\mathbf{Z}_p))]<\infty$$

$$[\mathbf{G}(\mathbf{Z}_p):\mathbf{G}(\mathbf{Z}_p)^m\mathbf{G}_1(\mathbf{Z}_p)]<\infty.$$

But we have

 $[\mathbf{G}(\mathbf{Z}_p)^m \mathbf{G}_1(\mathbf{Z}_p) : \mathbf{G}(\mathbf{Z}_p)^m] = [\mathbf{G}_1(\mathbf{Z}_p) : \mathbf{G}_1(\mathbf{Z}_p) \cap \mathbf{G}(\mathbf{Z}_p)^m]$

$$\leq [\mathbf{G}_1(\mathbf{Z}_p):\mathbf{G}_1(\mathbf{Z}_p)^m] < \infty$$

by induction hypothesis. The proposition is proved in this case.

Now we assume that R is not normal in $\mathbf{G}(\mathbf{Z}_p)$. Then it is well-known that R contains a subgroup R_0 normal in $\mathbf{G}(\mathbf{Z}_p)$ and of index $[\mathbf{G}(\mathbf{Z}_p): R_0]$ dividing m!, hence R_0 contains $\mathbf{G}(\mathbf{Z}_p)^{m!}$. Then the above proof shows that $[\mathbf{G}(\mathbf{Z}_p): \mathbf{G}(\mathbf{Z}_p)^{m!}] < \infty$, therefore the proposition follows.

The same proof of Proposition 2.12 gives the following (compare with [Seg2])

2.12.1. Proposition. There is only a finite number of subgroups of $\mathbf{G}(\mathbf{Q}_p)$ containing $\mathbf{G}(\mathbf{Z}_p)$ with given index m.

Now we set

$$M(\mathbf{Z}_p, \bar{G}^p) := \{ f \in M(\mathbf{Z}_p) : f(\bar{G}^p) = \bar{G}^p \}.$$

From Propositions 2.8 and 2.11 we know that $\bar{G}^p = \mathbf{G}(\mathbf{Z}_p)$ for almost all p (say, for all p outside a finite set W of primes). By the choice of the functions f_j (in the proof of 2.4), they are \mathbf{Z} -polynomial functions. So if $f \in M(\mathbf{Z}_p)$ then we have $f(\mathbf{G}(\mathbf{Z}_p)) = \mathbf{G}(\mathbf{Z}_p)$. Hence for $p \notin W$ we have

$$M(\mathbf{Z}_p, \bar{G}^p) = M(\mathbf{Z}_p).$$

We need also the following

2.13. Proposition. $M(\mathbf{Z}_p, \bar{G}^p)$ is of finite index in $M(\mathbf{Z}_p)$.

Proof. Let

$$t = [\mathbf{G}(\mathbf{Z}_p) : \bar{G}^p] < \infty,$$

and $\overline{G}^p = A_1, \ldots, A_k$ be all subgroups of $\mathbf{G}(\mathbf{Z}_p)$ of index t (see Prop. 2.12). Then for any $f \in M(\mathbf{Z}_p)$ we have

$$[\mathbf{G}(\mathbf{Z}_p):f(A_j)] = [f(\mathbf{G}(\mathbf{Z}_p)):f(A_j)] = [\mathbf{G}(\mathbf{Z}_p):A_j] = t,$$

thus f acts transitively on the set $\{A_1, \ldots, A_k\}$. Therefore we obtain a homomorphism

 $\psi: M(\mathbf{Z}_p) \to S_k,$

where S_k denotes the symmetric group on k symbols. Consequently we have

$$[M(\mathbf{Z}_p) : \operatorname{Ker} \psi] < \infty$$

It is obvious that Ker $\psi \subset M(\mathbf{Z}_p, \overline{G}^p)$ and the proposition follows.

Now we are able to show

2.14. Proposition. With above notation we have

$$Card(M(\mathbf{Q})\backslash M(\mathbf{A})/\mathcal{D}) < \infty.$$

Proof. We have

$$Card(M(\mathbf{Q})\backslash M(\mathbf{A})/\mathcal{D}) =$$

$$= Card(M(\mathbf{Q})\backslash M(\mathbf{A})/(\prod_{p\notin W} M(\mathbf{Z}_p) \times \prod_{p\in W} M(\mathbf{Z}_p, \bar{G}^p)))$$

$$\leq Card(M(\mathbf{Q})\backslash M(\mathbf{A})/M(\mathbf{A}(\infty))) \times \prod_{p\in W} [M(\mathbf{Z}_p) : M(\mathbf{Z}_p, \bar{G}^p)]$$

$$< \infty$$

by the main theorem of Borel [Bor] and by Proposition 2.13. \blacksquare

Summing up we have proved the following

2.15. Theorem. [Pi] For any finitely generated nilpotent group G the number of isomorphism classes in $\mathcal{B}(G)$ is finite.

Remark. In [T] we give some applications of the method treated here to other class of discrete subgroups of Lie groups and prove a similar finiteness result.

A cknowledgments

This work was done within the Associateship Scheme of the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy. Financial support from the Swedish International Development Cooperation Agency (SIDA) is acknowledged. The author would like to thank Dr. A. Sharomet for helpful suggestions regarding the preliminary version of the results presented here.

References

- [Bor] A. Borel, Some finiteness properties of adèle groups over number fields, Pub. Math. I.
 H. E. S. v. 16 (1963), 101 126.
- [BS] A. Borel et J. -P. Serre, Théorèmes de finitufe en cohomologie galoisienne, Comm. Math. Helv. v. 39 (1964), 111 - 164.
- [Bou] N. Bourbaki, Groupes et algèbrs de Lie, Ch. I III, Hermann Paris, 1974.
- [Cha] J. Chahal, Solution of the congruence subgroup problem for solvable algebraic groups, Nagoya Math. J. v. 79 (1980), 141 - 144.
- [DDMS] J. D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, Analytic pro-p-groups, London Math. Soc. Lec. Note Ser. 157, Cambridge, 1991.
- [Gro] A. Grothendieck, Représentations linéaires et compactification profinie des groupes discrets, Manuscripta Math. 2 (1970), 375 396.
- [GPS] F. Grünewald, P. Pickel and D. Segal, On polycyclic groups with isomorphic finite quotients, Annals of Math. v. 111 (1980), 155 195.
- [HM] G. Hochschild and G. Mostow, Automorphisms of algebraic groups, J. Algebra v. 23(1969), 435 - 443.
- [La] M. Lazard, Groupes analytiques *p*-adiques, Pub. Math. I. H. E. S. t. 26 (1965), 5 250.
- [Ma] A. Malcev, On a class of homogeneous spaces, Izv. Acad. USSR Sci., Ser. Math. t. 13 (1949), 9 - 32.
- [Pi] P. Pickel, Finitely generated nilpotent groups with isomorphic finite quotients, Trans. Amer. Math. Soc. 160 (1971), 327 - 341.
- [Ra] M. S. Raghunathan, *Discrete subgroups of Lie groups*, Springer-Verlag, 1972.
- [Seg1] D. Segal, Two theorems on polycyclic groups, Math. Z. Bd.164 (1978), 185 187.
- [Seg2] D. Segal, Some remarks on p-adic analytic groups, Bull. London Math. Soc. v. 31 (1999), 149 - 153.
- [T] N. Q. Thang, On the finiteness of isomorphism classes of arithmetic subgroups with isomorphic *p*-adic closures, Preprint, 2000.