Journal of Lie Theory
Volume **13** (2003) 13–20

Zariski Dense Subgroups of Semisimple Algebraic Groups with Isomorphic p-adic Closures

Nguyễn Quốc Thắng[*]

Communicated by G. A. Margulis

Abstract. We prove under certain natural conditions the finiteness of the number of isomorphism classes of Zariski dense subgroups in semisimple groups with isomorphic p-adic closures.

1. Introduction.

The present paper was inspired by the work of Mazur [Ma], in which he considered various types of *local-global priciples* in number theory and also the problem, for a given number field k, to determine the *companions* of a given algebraic k-variety V (i.e., those k-forms of V, which are locally everywhere k_v-isomorphic to V). He also conjectured that for projective smooth varieties V over k, there are, up to k-isomorphism, only a finite number of companions of V. For algebraic groups which are not necessarily linear, the corresponding conjecture was confirmed by Borel and Serre [BS]. We consider here an analog in the case of Zariski dense subgroups of semisimple groups. The following remarks provide a connection with similar question. Let k be a number field, S a finite set of valuations of k, containing the set ∞ of archimedean ones. Let $\mathcal{O} = \mathcal{O}(S)$ be the ring of S-integers of k, $\mathbf{\Omega}$ be a fixed universal domain containing k. For a valuation v of k we denote by k_v the v-adic completion of k, and by $\mathcal{O}_v$ the ring of v-adic integers of k_v. The algebraic groups under consideration are identified with their points over $\mathbf{\Omega}$. Assume that $G \subset \mathbf{G}(\mathcal{O})$, $\mathbf{G} \hookrightarrow \mathrm{GL}_n(\mathbf{\Omega})$, where $\mathbf{G}$ denotes the Zariski-closure of G in GL_n and $\mathbf{G}(\mathbf{B})$ denotes the $\mathbf{B}$-points of a linear algebraic group $\mathbf{G}$, with respect to the above the matrix realization and for some ring $\mathbf{B}$. Also, $\mathrm{Cl}_v(G)$ denotes the (v-adic) closure of G in $\mathbf{G}(\mathcal{O}_v)$ with respect to the v-adic topology on $\mathbf{G}(k_v)$. So, attached to a given G, there is a collection $(\mathrm{Cl}_v(G))_v$ of v-adic closures of G, which measures how big G is locally. One may ask the following natural question:
($*$) *To what extent does the collection* $(\mathrm{Cl}_v(G))_v$ *determine the group* G *up to isomorphism? Failing that, is the number of isomorphism classes finite?*

[*] Regular Associate of the Abdus Salam I.C.T.P.

ISSN 0949–5932 / $2.50

We are most interested in the finiteness aspect of above question, i.e., given topological isomorphisms $\mathrm{Cl}_v(G) \simeq \mathrm{Cl}_v(G_i)$ for all v, where i runs over a set of indices I, we ask whether the set of isomorphism classes of $\{G_i\}_{i\in I}$ is finite.

These questions are closely related also to the congruence subgroup problem and strong approximation in simply connected algebraic groups in its wide sense.

It is our objective to establish the finiteness of the number of isomorphism classes in the case of Zariski-dense subgroups of almost simple simply connected groups, which are big in certain sense.

In general, this is a difficult question and we will show the finiteness to hold under certain restrictions. The first restriction is to require the groups G_i to be "big" in the following sense. For simplicity we restrict ourselves to the case $k = \mathbf{Q}$. Let G_i be a Zariski dense subgroup of a simply connected absolutely almost simple $\mathbf{Q}$-group $\mathbf{G}_i \hookrightarrow \mathrm{GL}_{n_i}$, such that $G_i \subset \mathbf{G}_i(\mathbf{Z})$, for each i in certain set of indices I, and $G_i \not\simeq G_j$ if $i \neq j$. Assume that each G_i satisfies the condition

$$\bigcap_p (\mathbf{G}_i(\mathbf{Q}) \cap \mathrm{Cl}_p(G_i))) = G_i. \qquad (B)$$

This condition means that the groups G_i are "big" so that one can recover the group G_i from local closures. As it follows from Nori's Theorem [No], these groups are arithmetic subgroups in $\mathbf{G}_i(\mathbf{Z})$. A Zariski dense subgroup $G_i \subset \mathbf{G}_i$ satisfying this condition (B) such that all closures $\mathrm{Cl}_p(G_i)$ are open and compact subgroups of $\mathbf{G}_i(\mathbf{Q}_p)$ will be called *big*.

2. The Theorem.

Our main result can be stated as follows.

Theorem 2.1. *Let G_i be Zariski-dense subgroups in simply connected absolutely almost simple $\mathbf{Q}$-groups $\mathbf{G}_i$ $(i \in I)$, such that $G_i \subset \mathbf{G}_i(\mathbf{Z})$, and that all G_i are big in $\mathbf{G}_i$; assume further that they are mutually non-isomorphic, while their p-adic closures are topologically isomorphic for all primes p. Then the set $\{G_i\}_{i\in I}$ is the disjoint union of a finite number of isomorphism classes.*

The proof of the theorem will be given in several steps.

We fix two groups G, H from the set $\mathcal{B}(G) := \{G_i\}_{i\in I}$. The Lie algebra of a Lie (resp. p-adic or algebraic) group $\mathbf{G}$ will be denoted by $L(\mathbf{G})$. We fix once for all a matrix realization of $\mathbf{G}$ into $\mathrm{GL}_n(\mathbf{\Omega})$. The adjoint group of $\mathbf{G}$ will be denoted by $\mathrm{Ad}(\mathbf{G})$.

Lemma 2.2. *The set $\mathcal{B}(G)$ is a disjoint union of finitely many classes of groups G_i with $\mathbf{Q}$-isomorphic Zariski closures.*

Proof. By our assumption, each p-adic closure $\mathrm{Cl}_p(G_i)$ is an open and compact subgroup of $\mathbf{G}_i(\mathbf{Q}_p)$ and they are isomorphic to each other as topological groups. Denote by $f_p : \mathrm{Cl}_p(G) \simeq \mathrm{Cl}_p(H)$ the given topological isomorphism, where G and H are two fixed groups from $\{G_i\}_{i\in I}$. By [Pi], Corollary 0.3, f_p can be extended uniquely to a $\mathbf{Q}_p$-isomorphism $\bar{f}_p : \mathbf{G} \simeq \mathbf{H}$, so $\mathbf{G}$ and $\mathbf{H}$ are $\mathbf{Q}$-linear algebraic groups which are $\mathbf{Q}_p$-isomorphic for all p. By Borel - Serre [BS], Théorème 7.1, it follows that such groups lie in finitely many $\mathbf{Q}$-isomorphic classes. ∎

From now on we assume that all groups G_i have **Q**-*isomorphic Zariski closures.*

The following lemma shows the adele nature of the family (f_p).

Lemma 2.3. *With the notation as in the proof of Lemma 2.2, for almost all p, $\bar{f}_p$ is a $\mathbf{Z}_p$-polynomial isomorphism with respect to the given matrix realization of the groups* **G** *and* **H**.

Proof. Recall that we have fixed an embedding $G \subset \mathrm{GL}_n(\mathbf{Q})$. Since f_p is an isomorphism of topological groups, it is also an isomorphism of p-adic analytic Lie groups (see e.g. [Se]. Ch. 5. Sec. 9, or [DDMS], Sec. 9.2), thus it maps a open standard subgroup S_G of $\mathrm{Cl}_p(G)$ onto a open standard subgroup S_H of $\mathrm{Cl}_p(H)$ (see [DDMS], Sec. 8. 4, [Se], Ch. 4, Sec. 8 for more details). From the definition of Lie algebras of standard groups ([Se], Ch. 5, Sec. 1, [DDMS], Sec. 4.5) and the construction of standard subgroups it follows that $L(S_G) \simeq L(S_H)$ as $\mathbf{Z}_p$-Lie algebras, i.e., as Lie algebras with structural constants belonging to $\mathbf{Z}_p$ ([Se], Ch. 5, Sec. 1) so that df_p must be a $\mathbf{Z}_p$-linear map with respect to the given matrix realization (which is always fixed). Since S_G is an open uniform subgroup of $\mathrm{Cl}_p(G)$, its Lie algebra $L(S_G)$ is a $\mathbf{Z}_p$-lattice of $L(\mathrm{Cl}_p(G))$ and in particular, $L(\mathrm{Cl}_p(G)) = L(S_G) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ by definition ([DDMS], Sec. 9.5). The same is true for H instead of G. Therefore $df_p : L(\mathrm{Cl}_p(G)) \simeq L(\mathrm{Cl}_p(H))$ is defined over $\mathbf{Z}_p$, thus the same is true for isomorphism $L(\mathbf{G}) \simeq L(\mathbf{H})$, and so also for $d_p : \mathrm{Aut}(L(\mathbf{G})) \simeq \mathrm{Aut}(L(\mathbf{H}))$. Since the map d_p is given by $d_p(\phi) = df_p \circ \phi \circ df_p^{-1}$, it follows that $\bar{f}'_p : \mathrm{Ad}(\mathbf{G}) \to \mathrm{Ad}(\mathbf{H})$ will be a $\mathbf{Z}_p$-polynomial isomorphism. Since f_p extends uniquely to $\mathbf{Q}_p$-isomorphism $\bar{f}_p : \mathbf{G} \to \mathbf{H}$ by [Pi], Corollary 0.3, the following diagram is commutative :

$$\begin{array}{ccc} \mathbf{G} & \xrightarrow{\bar{f}_p} & \mathbf{H} \\ \pi_1 \downarrow & & \pi_2 \downarrow \\ \mathrm{Ad}(\mathbf{G}) & \xrightarrow{\bar{f}'_p} & \mathrm{Ad}(\mathbf{H}); \end{array}$$

here π_i denotes the corresponding isogeny. It follows that for those p not lying in the set T of primes dividing $m = Card(\mathrm{Ker}\ (\pi_1))$, $\bar{f}_p$ is also defined over $\mathbf{Z}_p$. Therefore $\bar{f}_p$ is defined over $\mathbf{Z}_p$ for all p not belonging to T. ∎

In the sequel we need the following lemma in order to realize $\mathrm{Aut}(\mathbf{G})$ as linear algebraic group over $\mathbf{Q}$.

Lemma 2.4. *With above notation, let $f_1, \ldots, f_N$ be* **Q**-*rational functions over* **G** *which are linearly independent over* **Q**. *Then there exist $x_1, \ldots, x_N \in \mathbf{G}(\mathbf{Q})$ such that* $\det(f_i(x_j))_{1 \le i,j, \le N} \in \mathbf{Q} \setminus \{0\}$.

Proof. We prove the claim by induction on N. The case $N = 1$ is trivial. Recall that $\mathbf{G}(\mathbf{Q})$ is Zariski dense in $\mathbf{G}$. Define $f(x_1, ..., x_n) := \det(f_i(x_j))_{1 \le i,j, \le N}$. Let $N > 1$ and assume that we have found $N - 1$ 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 by $g(z) := f(x_1, ..., x_{N-1}, z)$, and expand the determinant $g(z)$ by the last row. We obtain $g(z) = a_1 f_1(z) + \cdots + a_{N-1} f_{N-1}(z) + c f_N(z)$. If for all

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

Denote by $M = \mathrm{Aut}(\mathbf{G})$ the group of rational automorphisms of $\mathbf{G}$. It is well-known that M has the natural structure of a linear $\mathbf{Q}$-algebraic group (see, e.g., [BS], [HM]). We need a specific realization of the group M, which plays a crucial role in our proof, as follows. Let $\mathbf{A}$ be the adele ring of $\mathbf{Q}$.

Proposition 2.5. *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 $(g \circ f_p)$, where p runs over all prime numbers, belongs to $M(\mathbf{A})$.*

Proof. First we fix a universal domain $\mathbf{\Omega}$. It follows from results of [HM] that $\mathbf{G}$ is a conservative $\mathbf{Q}$-group, i.e., the group M acts locally finitely on the $\mathbf{Q}$-algebra $\mathbf{Q}[\mathbf{G}]$ of regular functions defined over $\mathbf{Q}$ on $\mathbf{G}$. As before, we fix an embedding $\mathbf{G} \hookrightarrow \mathrm{GL}_n(\mathbf{\Omega})$ and let $x_{ij} (1 \leq i, j \leq n)$ be the coordinate matrix functions on $\mathbf{G}$. Let V be the smallest finite dimensional $\mathbf{Q}$-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 $\mathbf{Q}$-regular functions over $\mathbf{G}$ which form a $\mathbf{Q}$-basis of V containing all x_{ij} (notice that all x_{ij} are $\mathbf{Q}$-linearly independent). By multiplying f_k with a suitable integer, we may assume that all f_k are $\mathbf{Z}$-polynomial functions.

For $\phi \in M$ let the action of ϕ be given by $\phi(f_i) = f_i \circ \phi = \Sigma_{1 \leq j \leq N} a_{ij}^{(\phi)} f_j$, where $a_{ij}^{(\phi)} \in \mathbf{\Omega}$ (=universal domain). Since the $\mathbf{Q}$-basis $\{f_1, ..., f_N\}$ contains all coordinate functions, it follows that the mapping $\Phi : \phi \mapsto (a_{ij}^{(\phi)})$ is a faithful $\mathbf{Q}$-representation of M into $\mathrm{GL}(V)$, where the latter is identified with $\mathrm{GL}_N(\mathbf{\Omega})$ by means of the basis $\{f_1, ..., f_N\}$. Further we will identify M with a closed $\mathbf{Q}$-subgroup of $\mathrm{GL}_N(\mathbf{\Omega})$. Thus $\phi \in M(\mathbf{Z}_p)$ if and only if $a_{ij}^{(\phi)} \in \mathbf{Z}_p$, for all i, j. Now let $\bar{f}_p : \mathbf{G} \simeq \mathbf{H}$ be the (unique) isomorphism extending the isomorphism $f_p : \mathrm{Cl}_p(G) \simeq \mathrm{Cl}_p(H)$ (so that $\bar{f}_p$ is defined over $\mathbf{Q}_p$) and let $g : \mathbf{H} \simeq \mathbf{G}$ be any $\mathbf{Q}$-isomorphism.

We now choose elements $x_1, ..., x_N$ as in Lemma 2.4. For convenience we write $a_{ij} = a_{ij}^{(\bar{f}_p)}$, where p is fixed. Then we have the following systems of equations

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

$$\vdots \qquad\qquad \vdots$$

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

Write

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

where $c, d \in \mathbf{Z} \setminus \{0\}$. Since the elements $x_i \in \mathbf{G}(\mathbf{Q})$ are finite in number, we may assume that $x_i \in \mathbf{G}(\mathbf{Z}[S_1^{-1}])$ for all i, where $\mathbf{Z}[S_1^{-1}]$ is the localization at a finite set S_1 of primes, which contains the set of primes dividing c. By Lemma 2.3, for certain finite set S_2 of primes, the isomorphism $\bar{f}_p$ (see notation above) is defined over $\mathbf{Z}_p$ for $p \notin S_2$. For a finite set S_3 of primes, we see that g is defined over $\mathbf{Z}_p$ for $p \notin S_3$. Let $S = S_1 \cup S_2 \cup S_3$. Then by solving the system A_t above with respect to $a_{t1}, ..., a_{tN}$, we have $a_{ij} = (1/r)d_{ij}$, for all i, j, where $a_{ij} \in \mathbf{Z}_p[S^{-1}]$. So for $p \notin S$ we have $g \circ f_p \in M(\mathbf{Z}_p)$ as required. ∎

Denote by $\mathcal{C}(G)$ the set

$\{(f_p) \in \prod_p M(\mathbf{Q}_p) : f_p(\mathrm{Cl}_p(G)) = \mathrm{Cl}_p(G), \forall p, f_p \in M(\mathbf{Z}_p) \text{ for almost all } p\}$.

It is clear that $\mathcal{C}(G)$ is an infinite 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 $M(\mathbf{Q})\backslash M(\mathbf{A})/\mathcal{C}(G)$ defined as follows :

If $g : \mathbf{H} \simeq \mathbf{G}$ is a $\mathbf{Q}$-isomorphism and $\bar{f}_p : \mathbf{G} \simeq \mathbf{H}$ is the isomorphism extending $f_p : \mathrm{Cl}_p(G) \simeq \mathrm{Cl}_p(H)$ for all p, then we set $a(G, H) := M(\mathbf{Q})(g \circ \bar{f}_p)\mathcal{C}(G)$. According to Proposition 2.5, $(g \circ \bar{f}_p) \in M(\mathbf{A})$ so $a(G, H)$ is an element of the set of double coset classes $M(\mathbf{Q})\backslash M(\mathbf{A})/\mathcal{C}(G)$.

Proposition 2.6. *The correspondence defined above is a well-defined map.*

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 $\mathbf{Q}$-isomorphism, and for all p, let $f'_p : \mathrm{Cl}_p(G) \simeq \mathrm{Cl}_p(H)$ be an isomorphism with the extension $\bar{f}'_p : \mathbf{G} \to \mathbf{H}$. Then we have

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

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

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

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

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

∎

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

Proposition 2.7. *If (G, H) and (G, K) have the same double coset class, then $H = K$.*

Proof. With notation of the proof of Proposition 2.6, by the assumption we have for all primes p

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

where $g_{\mathbf{Q}} \in M(\mathbf{Q})$ and $(h_p) \in \mathcal{C}(G)$. Write $f' = g_{\mathbf{Q}}^{-1} \circ f$, $\bar{g}'_p = \bar{g}_p \circ h_p$. Then for all p we have $f' \circ \bar{f}_p = g \circ \bar{g}'_p$, or $g^{-1} \circ f' = \bar{g}'_p \circ \bar{f}_p^{-1}$, i.e., $g^{-1} \circ f'$ is a $\mathbf{Q}$-isomorphism $\mathbf{H} \simeq \mathbf{K}$, mapping $\mathrm{Cl}_p(H)$ onto $\mathrm{Cl}_p(K)$ 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 $(g^{-1} \circ f')(h) \in \mathrm{Cl}_p(K)$ for all p. Thus

$$(g^{-1} \circ f')(h) \in \mathbf{K}(\mathbf{Q}) \cap (\bigcap_p \mathrm{Cl}_p(K)) = K$$

by the assumption that the groups G_i are big. 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 $H \simeq K$; thus $H = K$ since all groups G_i are mutually non-isomorphic. Proposition 2.7 is proved. ■

The preceding observations show that the cardinality of $\mathcal{B}(G)$ is not greater than the cardinality of $M(\mathbf{Q}) \backslash M(\mathbf{A}) / \mathcal{C}(G)$. 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 adeles of $\mathbf{A}$. In particular we have

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

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

Proposition 2.8. *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

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

Passing to a open standard subgroup G' (of finite index) of $\mathbf{G}(\mathbf{Z}_p)$ we need only show that G'^m is of finite index in G'. It is known ([DDMS], Theorem. 8.31), that G' is a uniform pro-p-group of finite rank, say, d, and G' is topologically generated by its d elements $g_1, ..., g_d$ (loc. cit., Theorem 3.17). Also, by (loc. cit., Theorem 4.9) there exists a homeomorphism $\psi : \mathbf{Z}_p^d \simeq G'$, such that $\psi(x_1, ..., x_d) = g_1^{x_1} \cdots x_d^{g_d}$. Therefore $\psi((m\mathbf{Z}_p)^d)$ is an open subset of G', since $m\mathbf{Z}_p$ is open in

$\mathbf{Z}_p$. It is clear that $\psi((m\mathbf{Z}_p)^d) \subset G'^m$, hence G'^m is open in G' and also of finite index.

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. ∎

Remark 2.9. We can use similar arguments as in the proof of Proposition 2.8 to prove (compare also with [Seg]) that for a given compact p-adic analytic group, the number of its subgroups of given index m is finite. By using this, in combination with Bruhat - Tits result about maximal compact subgroups of reductive p-adic groups [BrT], one can show that there is only a finite number of subgroups of $\mathbf{G}(\mathbf{Q}_p)$ containing $\mathbf{G}(\mathbf{Z}_p)$ with given index m, up to $\mathbf{G}(\mathbf{Q}_p)$-conjugacy.

Now we denote by

$$M(\mathbf{Z}_p, \mathrm{Cl}_p(G)) := \{f \in M(\mathbf{Z}_p) : f(\mathrm{Cl}_p(G)) = \ Cl_p(G)\}.$$

From [MVW], Theorem 7.3, or [N], Theorem 5.4, we know that $\mathrm{Cl}_p(G) = \mathbf{G}(\mathbf{Z}_p)$ 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 Proposition 2.5), 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 $M(\mathbf{Z}_p, \mathrm{Cl}_p(G)) = M(\mathbf{Z}_p)$. We also need the following

Proposition 2.10. *$M(\mathbf{Z}_p, \mathrm{Cl}_p(G))$ is of finite index in $M(\mathbf{Z}_p)$.*

Proof. By assumption $G \subset \mathbf{G}(\mathbf{Z})$; so it follows that for all p we have $\mathrm{Cl}_p(G) \subset \mathbf{G}(\mathbf{Z}_p)$ and $\mathrm{Cl}_p(G)$ is a subgroup of finite index in $\mathbf{G}(\mathbf{Z}_p)$ since it is an open subgroup of the compact group $\mathbf{G}(\mathbf{Z}_p)$. Let

$$t = [\mathbf{G}(\mathbf{Z}_p) : \mathrm{Cl}_p(G)] < \infty,$$

and $\mathrm{Cl}_p(G) = A_1, \ldots, A_k$ be all subgroups of $\mathbf{G}(\mathbf{Z}_p)$ of index t (see Prop. 2.8). Then for any $f \in M(\mathbf{Z}_p)$ we have $[\mathbf{G}(\mathbf{Z}_p) : f(A_j)] = [f(\mathbf{G}(\mathbf{Z}_p)) : f(A_j)] = [\mathbf{G}(\mathbf{Z}_p) : A_j] = t$. So f acts transitively on the set $\{A_1, \ldots, A_k\}$. Thus 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 $[M(\mathbf{Z}_p) : \mathrm{Ker}\,\psi] < \infty$. It is obvious that $\mathrm{Ker}\,\psi \subset M(\mathbf{Z}_p, \mathrm{Cl}_p(G))$ and the proposition follows. ∎

Now we are able to show

Proposition 2.11. *With above notation we have*

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

Proof. We have $\mathrm{Card}(M(\mathbf{Q})\backslash M(\mathbf{A})/\mathcal{D}) =$
$\mathrm{Card}(M(\mathbf{Q})\backslash M(\mathbf{A})/(\prod_{p\notin W} M(\mathbf{Z}_p) \times \prod_{p\in W} M(\mathbf{Z}_p, \mathrm{Cl}_p(G)))) \leq$
$\mathrm{Card}(M(\mathbf{Q})\backslash M(\mathbf{A})/M(\mathbf{A}(\infty))) \times \prod_{p\in W}[M(\mathbf{Z}_p) : M(\mathbf{Z}_p, \mathrm{Cl}_p(G))] < \infty$
by the main theorem of Borel ([Bor]) and by Proposition 2.10. ∎

The proof of Theorem 2.1 now follows from the results above.

Acknowledgement. I would like to thank Professor B. Mazur for his interest and valuabale suggestions regarding this paper, Professor R. Pink for sending his papers which help a great deal the work over this paper, and Professor Hofmann for valuable suggestions toward improving the readability of the text. This work has been done thanks to the support of the Fund. Research Program of Vietnam, the Abdus Salam I.C.T.P (Italy), and the Swedish International Developement Agency (S.I.D.A).

References

[Bor] Borel, A., *Some finiteness properties of adele groups over number fields*, Pub. Math. I. H. E. S. **16** (1963), 101–126.

[BS] Borel, A., et J.-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comm. Math. Helv. **39** (1964), 111–164.

[BrT] Bruhat, F., et J. Tits, *Groupes réductifs sur un corps local*, Pub. Math. I. H. E. S. **41** (1972), 1–240.

[DDMS] Dixon, J. D., M. P. F. du Sautoy, A., and D. Segal, "Analytic pro-p-groups," London Math. Soc. Lec. Note Ser. **157**, Cambridge, 2-nd revised and enlarged ed., 1999.

[HM] Hochschild, G., and G. Mostow, *Automorphisms of algebraic groups*, J. Algebra **23** (1969), 435–443.

[MVW] Matthews, C. R., L. N. Vasserstein, and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups I*, Proc. London. Math. Soc. **48** (1984), 514–532.

[Ma] Mazur, B., *On the passage from local to global in number theory*, Bull. Amer. Math. Soc. **29** (1993), 14–50.

[No] Nori, M., *On subgroups of* $GL_n(\mathbf{F_p})$, Inv. Math. **88** (1987), 257–275.

[Pin] Pink, R., *Compact subgroups of linear algebraic groups*, J. Algebra, **206** (1998), 438–504.

[Se] Serre, J.-P., "Lie algebras and Lie groups," Harvard Lecture Notes, 1964; (2nd printing : Lecture Notes in Math. **1500**, Springer-Verlag, Berlin-Heidelberg-New York, 1992.).

[Seg] Segal, D., *Some remarks on p-adic analytic groups*, Bull. London Math. Soc. **31** (1999), 149–153..

Nguyêñ Q. Thắńg
Institute of Mathematics
P. O. Box 631, Bo Ho
Hanoi-Vietnam
nqthang@thevinh.ncst.ac.vn

Received February 13, 2001
and in final form May 31, 2002