Subgroups of algebraic groups which are clopen in the $S$-congruence topology

A. W. Mason and B. Sury
(Communicated by Andrei Jaikin-Zapirain)

Abstract. Let $K$ be a global field and $S$ be a finite set of places of $K$ which includes all those of archimedean type. Let $G$ be an algebraic group over $K$ and $G_K$ be its $K$-rational points. The authors provide a detailed proof of a lemma of Raghunathan which states that (under fairly weak restrictions) the closure in the $S$-congruence topology of a subgroup of $G_K$ normalized by an $S$-arithmetic subgroup is also open. This leads to a significant simplification in the proof of one of the principal results in a recent joint paper of the authors.

By applying the lemma to $S$-arithmetic lattices in $G$ of $K$-rank one, where $\text{char}(K) \neq 0$ and $|S| = 1$, we can provide a lower estimate for the number of subgroups of a given index in such a lattice which are not $S$-congruence. This extends previous results of the first author and Andreas Schweizer.

Introduction

Let $K$ be a global field and let $S$ be a finite non-empty set of places of $K$ containing all those of archimedean type. Let $G$ be an algebraic group over $K$. The motivation for this note is the following result [12, 4.3 Lemma].

Raghunathan’s lemma. Suppose that $G$ is connected, simply-connected and $K$-simple with strictly positive $S$-rank. Let $\Gamma$ be an $S$-arithmetic subgroup of $G_K$, the $K$-rational points of $G$. If $N$ is any non-central subgroup of $G_K$ which is normalized by $\Gamma$ then the closure of $N$ in the $S$-congruence topology is also open.

What first attracted our attention to this result is that it provides a significant simplification in the proof of one of the principal results in a recent paper [8]. A result involving a subgroup which is clopen with respect to the $S$-congruence topology is central to Weisfeiler’s celebrated work [13] on the strong approximation theorem. (Pink [9] has extended these to include, for example, global fields of all positive characteristic.) Weisfeiler’s starting point is a subgroup of $G_K$ which is both finitely generated and Zariski dense. As we shall see the hypotheses on $N$ ensure that it is Zariski dense. However Raghunathan’s lemma does not follow from [13] since in
general such an $N$ is not finitely generated. Indeed we will apply the Lemma to such subgroups. The proof [12, 4.3 Lemma] provided by Raghunathan is merely a sketch. Given the importance of this result (and the fact that the likely readership of this note will include group-theorists who are not experts in algebraic groups) it seems appropriate to provide a detailed version.

We apply this theorem to the classical case of an $S$-arithmetic lattice, $\Lambda$, in $G_{K_v}$, where $\text{char}(K) \neq 0$, $G$ has $K$-rank one and $S = \{v\}$. We prove a result on the ubiquity of finite index subgroups of $\Lambda$ which are not $S$-congruence. This extends results [7] of the first author and Andreas Schweizer for the special case where $\Lambda$ is a so-called Drinfeld modular group.

We conclude by showing that for some important special cases, in particular $G = \text{SL}_2$, the Lemma is essentially an elementary result.

1 Raghunathan’s lemma

We will make use of the notation used in [10]. Although that book is primarily concerned with fields of characteristic zero, many of the results it contains, including all those cited in this paper, hold for any characteristic. Throughout $G$ denotes an algebraic group over a field $K$. After Margulis [5, p. 60] we will assume that $G$ is a $K$-subgroup of $\text{GL}_n$, for some $n$. This provides a standard way of representing $G$ and all definitions given below will refer to this embedding. We list the following notation which will be used throughout.

$K$ a global field;
$S$ a finite non-empty set of places of $K$ including all archimedean places;
$\mathcal{O}(S)$ the ring of all $S$-integers in $K$;
$K_v$ the completion of $K$ with respect to a non-archimedean place $v$;
$\mathcal{O}_v$ the valuation ring of $K_v$;
$p_v$ the maximal ideal of $\mathcal{O}_v$;
$F_v$ the residue field of $\mathcal{O}_v$;
$G_F$ the group of $F$-rational points of $G$, where $F$ is a field containing $K$;
$G_R$ the group of $R$-integral points of $G$, where $R$ is a ring contained in $K_v$;
$G_R(q)$ the principal congruence subgroup of $G_R$, where $q$ is an $R$-ideal.

We recall that $K_v$ is a local field and that $\mathcal{O}_v$ is a local ring whose residue field $F_v$ is finite. By definition

$$\mathcal{O}(S) = \bigcap_{v \notin S} (K \cap \mathcal{O}_v).$$

The subgroups $G_{\mathcal{O}(S)}(a)$, where $a \neq \{0\}$, form the basis of a topology on $G_K$ called the $S$-congruence topology. The topology on $K_v$ induces another topology on $G_{K_v}$ for which the $G_{\mathcal{O}_v}(p_v^t)$, where $t \geq 1$, provide a base of the neighbourhoods of the identity; see [10, p. 134]. Let $X$ be the restricted topological product [10, p. 161] of $G_{K_v}$ with respect to the distinguished (open, compact) subsets, $G_{\mathcal{O}_v}$, where $v \notin S$.

We recall that the topology induced on the embedding of $G_K$ in $X$ (via the usual “diagonal map”) coincides with the $S$-congruence topology on $G_K$. Let $H$ be any
subgroup of $G_K$. Then we can identify the closure of $H$ in $X$ with the (profinite) completion of $H$ with respect to its $S$-congruence topology. We begin by providing a detailed version of the proof of [12, 4.3. Lemma].

**Notation.** Let $H$ be a subgroup of $G_K$. We denote the $S$-closure of $H$ in $G_K$ (or $X$) by $\bar{H}$ and the Zariski closure of $H$ in $G$ by $\bar{H}$.

**Theorem 1.1** (Raghunathan). Suppose that $G$ is connected, simply-connected and $K$-simple with strictly positive $S$-rank. Let $\Gamma$ and $N$ be subgroups of $G_K$ for which:

(i) $\Gamma$ is $S$-arithmetic, i.e. commensurable with $G_{\ell(S)}$;
(ii) $N$ is non-central and normalized by $\Gamma$.

Then $\bar{N}$ is also open in the $S$-congruence topology on $G_K$.

**Proof.** It suffices to prove that $\bar{N}$ is open in $X$. We begin by showing that $N$ is Zariski dense in $G$. Now $\hat{\Gamma}$ normalizes $\hat{N}$. But $\hat{\Gamma} = G$ by [5, 3.2.10, p. 64] and $\hat{N}$ is defined over $k$ by [5, 2.5.3, p. 56]. Hence $\bar{N} = G$.

The closure of $\Gamma$ in $G_K$ in the $S$-congruence topology is open and so $\bar{\Gamma}$ (in $X$) contains a subgroup of the type

$$\prod_{v \notin S} \Gamma_v,$$

where

(i) each $\Gamma_v$ is open in $G_K$,
(ii) $\Gamma_v = G_{\ell_v}$, for all but finitely many $v$.

Then, since $\bar{N}$ is normalized by $\bar{\Gamma}$, $\bar{N}$ contains

$$\prod_{v \notin S} [\bar{N}_v, \Gamma_v],$$

where $\bar{N}_v$ is the projection of $\bar{N}$ into $G_v$. It suffices therefore to prove that, for all $v \notin S$,

(a) $[\bar{N}_v, \Gamma_v]$ is open in $G_K$,
(b) $[\bar{N}_v, \Gamma_v] \supseteq G_{\ell_v}$, for all but finitely many $v$.

**Proof of (a).** Here the approach is similar to other applications of Lie theory. (See, for example, [2, Section 9].) We provide an outline. Let $L = L(G)$ be the Lie algebra of $G$ and let

$$L_0 = \sum_{n \in \bar{N}_v} (\text{Ad}(n) - 1)L.$$
Now $L_0$ is invariant under $\text{Ad}(\overline{N}_v)$. From the above $\overline{N}_v$ is Zariski dense in $G$ (since it contains $N$) and so

(i) $L_0$ is invariant under $\text{Ad}(G)$,

(ii) $(\text{Ad}(g) - 1)x \in L_0$, for all $g \in G$, $x \in L$.

We now make use of the hypothesis that $G$ is simply-connected to conclude that $L_0 = L$. (See [2, 3.6].) Since $L$ is a finite dimensional vector space of dimension $d = \text{dim } G$ over the algebraic closure $K^c$ of $K$, there exist $n_1, \ldots, n_d \in \overline{N}_v$ such that

$$\sum_{i=1}^{d} (\text{Ad}(n_i) - 1)L = L.$$ 

Now consider the morphism of $K_v$-manifolds

$$\phi : G_K^{(d)} = G_{K_v} \times \cdots \times G_{K_v} \to G_{K_v},$$

defined by

$$\phi((g_1, \ldots, g_d)) = \prod_{i=1}^{d} [n_i, g_i].$$

Then, as in the proof of [10, Theorem 3.3, p. 114], which is based on the Inverse Function Theorem [10, Theorem 3.2, p. 110] (and using [10, Lemma 3.1, p. 113]), it can be shown that $\text{Im } \phi$ contains an (open) neighbourhood of the identity in $G_{K_v}$. Using the fact that $\overline{F}_v^{(d)}$ is open in $G_{K_v}^{(d)}$ it follows that $\phi(\overline{F}_v^{(d)})$ contains an neighbourhood of the identity.

**Proof of** (b). We may assume without loss of generality that $N$ is generated by the $\Gamma$-conjugates of finitely many of its elements. It follows that there exists a finite set $S'$, containing $S$, such that, for all $v \notin S'$,

(i) $\Gamma \leq G_{\ell_v}$,

(ii) $\overline{F}_v = G_{\ell_v}$,

(iii) $N \leq G_{\ell_v}$.

Let $\tilde{N}_v = [\overline{N}_v, \overline{F}_v]$. Then from the above, for all $v \notin S'$,

(i) $\tilde{N}_v \cap G_{\ell_v} \leq G_{\ell_v}$,

(ii) $[\Gamma, N] \leq \tilde{N}_v \cap G_{\ell_v}$.

Recall that $F_v$ is the (finite) residue field of $\mathcal{O}_v$ (i.e. $\mathcal{O}_v/p_v$). For each $s \geq 0$, let

$$G_{\ell_v}(p_v^s) = \{ Y \in G_{\ell_v} : Y - I_n \in M_n(p_v^s) \}.$$
It is known [10, Proposition 3.20, p. 146] that
\[ \overline{G_{\mathcal{O}}(p)} = G_{\mathcal{O}}(p) \overline{G_{\mathcal{O}}(p)} \].

It is also known [10, Proposition 7.5, p. 406] that, if \(|F_v| \geq 4\), then \(G_{F_v}\) has no non-trivial, non-central normal subgroups. We wish to prove that, for all but finitely many \(v \not\in S'\), the normal subgroup \(N_v \cap G_{\mathcal{O}_v}\) does not map into the centre of \(G_{F_v}\). Suppose to the contrary that \(N_v \cap G_{\mathcal{O}_v}\) is central \((\text{mod } G_{\mathcal{O}_v}(p_v))\), for infinitely many \(v\). Then, for all these \(v\), \([[N, \Gamma], \Gamma]\) is contained in \(G_{\mathcal{O}_v}(p_v)\). It follows that
\[ [[N, \Gamma], \Gamma] = 1. \]

Now \(N\) and \(\Gamma\) are Zariski dense and so by [1, Proposition, p. 59]
\[ [[G, G], G] = 1. \]

This contradicts the fact that \([G, G] = G\) [1, Proposition, p. 181]. We deduce that there exists a finite set \(S''\), containing \(S'\), for which

(i) \( (N_v \cap G_{\mathcal{O}_v}) G_{\mathcal{O}_v}(p_v) = G_{\mathcal{O}_v} \),

(ii) \( G_{\mathcal{O}_v}\) is perfect.

For (ii) see [11, Section 2.3].\(^1\) For each, \(v \not\in S''\), it follows that
\[ G_{\mathcal{O}_v}/N_v \cap G_{\mathcal{O}_v} \cong G_{\mathcal{O}_v}(p_v)/N_v \cap G_{\mathcal{O}_v}(p_v). \]

Now \([G_{\mathcal{O}_v}(p_v), G_{\mathcal{O}_v}(p_v')] \leq G_{\mathcal{O}_v}(p_v^{s+t})\) and so, by part (a), \(G_{\mathcal{O}_v}/N_v \cap G_{\mathcal{O}_v}\) is solvable. By (ii) then \(N_v \cap G_{\mathcal{O}_v} = G_{\mathcal{O}_v}\). This completes the proof. \(\square\)

The following consequence is immediate.

**Corollary 1.2.** With the notation of the Theorem 1.1, there exists \(q_0 \neq \{0\}\) such that
\[ \overline{N} = \bigcap_{q \neq \{0\}} N \cdot G_{E(S)}(q) = N \cdot G_{E(S)}(q_0). \]

The ideal \(q_0\) is, of course, not unique. It is clear that if Corollary 1.2 holds for \(q_0\) then it also holds for any non-zero ideal \(q_0'\) contained in \(q_0\). In practise it is convenient to choose \(q_0\) so that the index \(|G_{E(S)} : G_{E(S)}(q_0)|\) is minimal. In the final section we will show in detail for some special cases how \(N\) and \(q_0\) are related.

Theorem 1.1, of course, holds trivially for the case where \(N\) is commensurable with \(\Gamma\). For a non-trivial example of \(N\) to which it applies consider the case of the

\(^1\) The authors are indebted to Professor Rapinchuk for providing this reference.
classical modular group, i.e. $G = \text{SL}_2$, $K = \mathbb{Q}$, $S = \{\infty\}$ and $\Gamma = \text{SL}_2(\mathbb{Z})$. Let $M$ be a normal subgroup of finite index in $\Gamma$. Then with finitely many exceptions $M$ is a free non-abelian group of finite rank. For such an $M$ take $N = [M, M]$. Then $N$ is free of infinite rank and hence is not $S$-arithmetic.

2 Arithmetic lattices in rank one groups

Throughout this section we assume that $\text{char}(K) \neq 0$. We fix a (non-archimedean) place $v$ of $K$ and let $S = \{v\}$. (The simplest example of such an $\mathcal{O}(S)$ is the polynomial ring $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the finite field of order $q$.) In addition to the hypotheses in the statement of Theorem 1.1, we assume that $G$ is absolutely almost simple and that the $Kv$-rank of $G$ is 1.

Let $\Lambda$ be a non-uniform, $S$-arithmetic lattice in (the locally compact group) $G_{Kv}$. By definition

(i) $\Lambda$ is a discrete subgroup of $G_{Kv}$;
(ii) $\mu(G_{Kv}/\Lambda)$ is finite, where $\mu$ is a Haar measure on $G_{Kv}$;
(iii) $G_{Kv}/\Lambda$ is not compact;
(iv) $\Lambda$ is commensurable with $G_{\mathcal{O}(S)}$.

For our purposes it suffices to assume that $\Lambda$ is a (finite index) subgroup of $G_{\mathcal{O}(S)}$.

Notation. For each non-zero $\mathcal{O}(S)$-ideal $q$ let

$$U_\Lambda(q) = \langle u \in \Lambda \cap G_{\mathcal{O}(S)}(q) : u \text{ is unipotent} \rangle.$$

An immediate consequence of Theorem 1.1 is the following.

Lemma 2.1. The closure of $U_\Lambda(q)$ in $G_K$ in the $S$-congruence topology is also open.

N.B. It is well-known that in this case $\text{SL}_2(\mathcal{O}(S))$ and hence $U_\Lambda(q)$ are not finitely generated. (This extends a classical result for $\text{SL}_2(\mathbb{F}_q[t])$ due to Nagao.)

One important consequence of Lemma 2.1 is that Lemma 5.7 in [8] is true for all $q$ so that, in the terminology of [8], the principal result always holds. This leads to a significant simplification in the proofs of [8]. Specifically Zel’manov’s solution [14] of the restricted Burnside problem for topological groups is no longer required.

Associated with $G_{Kv}$ is its Bruhat-Tits building which in this case is a tree $\mathcal{F}$ (since the $K_v$-rank of $G$ is 1). Bass-Serre theory shows how a presentation for $\Lambda$ can be inferred from its action on $\mathcal{F}$, via the structure of the quotient graph $\Lambda \backslash \mathcal{F}$. In confirming a conjecture of Serre, Lubotzky has shown [4, Theorem 7.5] that $\Lambda$ contains infinitely many finite subgroups which are not $S$-congruence, i.e. so-called $S$-non-congruence subgroups. Our results can be used to provide information on the ubiquity of the $S$-non-congruence subgroups of $\Lambda$.

It is known [4, Theorem 6.1] that the first Betti number of $\Lambda \backslash \mathcal{F}$, $b_1(\Lambda \backslash \mathcal{F})$, is finite.
Theorem 2.2. Let $F_r$ be the free group on $r$ generators, where $r = b_1(\Lambda \setminus \mathcal{T})$ and let $f(r,n)$ denote the number of index $n$ subgroups of $F_r$. Let $nc(\Lambda, n)$ be the number of $S$-non-congruence subgroups of index $n$ in $\Lambda$. Then there exists a constant $n_0 = n_0(\Lambda)$ such that, if $n > n_0$, then

$$nc(\Lambda, n) \geq f(r,n).$$

Moreover, if $r \geq 1$, then for all $n > n_0$, there exists at least one normal, $S$-non-congruence subgroup of index $n$ in $\Lambda$.

Proof. Let $\Lambda(q) = \Lambda \cap G_{\mathcal{O}(S)}(q)$. Then by Corollary 1.2 and Lemma 2.1

$$\Lambda(q_0) \leq \bigcap_{q \neq \{0\}} U_\Lambda(\mathcal{O}(S)).\Lambda(q),$$

for some non-zero $q_0$. We choose $q_0$ so that $n_0 = |\Lambda : \Lambda(q_0)|$ is minimal.

Now let $\Lambda_V$ be the subgroup of $\Lambda$ generated by all the stabilizers in $\Lambda$ of the vertices of $\mathcal{T}$. By standard Bass-Serre theory we have

$$\Lambda/\Lambda_V \cong F_r.$$

In addition, since $U_\Lambda(\mathcal{O}(S))$ is generated by elements of finite order,

$$U_\Lambda(\mathcal{O}(S)) \leq \Lambda_V.$$

Suppose $\Lambda_c$ is a congruence subgroup of $\Lambda$ containing $\Lambda_V$. Then by the above

$$\Lambda(q_0) \leq \Lambda_c,$$

which implies that $|\Lambda : \Lambda_c| \leq n_0$. The first part follows.

For the second part note that when $r \geq 1$ there exists an epimorphism

$$\theta : \Lambda/\Lambda_V \to \mathbb{Z}. \quad \square$$

Notes.

(i) In many cases $b_1(\Lambda \setminus \mathcal{T})$ is non-zero. More precisely it is known [8, Lemma 3.7] that in this situation every $S$-arithmetic lattice contains lattices of the same type with arbitrarily large first Betti numbers.

(ii) The Drinfeld modular group. For the case where $G = SL_2$ (with as above $S = \{v\}$) the group $SL_2(\mathcal{O}(S))$ is a non-uniform $S$-arithmetic lattice in $G_K$. It (or, more generally, $GL_2(\mathcal{O}(S))$) plays a fundamental role [3] in the theory of Drinfeld modular curves, analogous to that of the modular group $SL_2(\mathbb{Z})$ in the classical theory of modular forms. It is known [7, Theorem 2.10] precisely when $b_1(SL_2(\mathcal{O}(S)) \setminus \mathcal{T})$ is zero. (This happens in only four cases.) In addition when
\( \Lambda = SL_2(\mathcal{O}(S)) \) it is known [7, Theorem 1.2] that Theorem 2.1 holds for all \( n \geq 1 \), i.e. \( n_0 = 1 \), equivalently, \( q_0 = \mathcal{O}(S) \).

3 The case \( G = SL_2 \)

In the final section we show that in some important special cases it is possible to prove an explicit version of Raghunathan’s lemma in an elementary way which does not involve any Lie theory. We revert here to \( K \) of any characteristic and any \( S \).

**Definition.** Let \( H \) be a subgroup of \( SL_2(\mathcal{O}(S)) \). The order of \( H \), \( o(H) \), is the \( \mathcal{O}(S) \)-ideal generated by all \( h_{12}, h_{21}, h_{11} - h_{22} \), where \( (h_{ij}) \in H \).

**Definition.** For each \( \mathcal{O}(S) \)-ideal \( q \), let

\[
\psi(q) = \begin{cases} 
12q, & \text{char}(K) = 0, \\
q^4, & \text{char}(K) \neq 0.
\end{cases}
\]

**Notation.** For each \( \mathcal{O}(S) \)-ideal \( q \) let

\[
SL_2(q) = \{ X \in SL_2(\mathcal{O}(S)) : X \equiv I_2 \pmod{q} \}.
\]

**Lemma 3.1.** Let \( N \) be a non-central normal subgroup of \( SL_2(\mathcal{O}(S)) \), with \( o(N) = n \neq \{0\} \). Let \( q \) be any non-zero \( \mathcal{O}(S) \)-ideal. If \( n' = n + q \), then

\[
SL_2(\psi(n')) \subseteq N.SL_2(q).
\]

**Proof.** The proof follows from [6, Theorems 3.6, 3.10, 3.14] since \( M = N.SL_2(q) \) is an \( S \)-congruence subgroup whose level

\[
o(M) = n + q.
\]

**Theorem 3.2.** Let \( N \) be a non-central normal subgroup of \( SL_2(\mathcal{O}(S)) \). Then

\[
\bar{N} = \bigcap_{q \neq \{0\}} N.SL_2(q) = N.SL_2(\psi(n)),
\]

where \( n = o(N) \).

Under further restrictions Theorem 3.2 can be improved. For example, from the results of [6] it follows that, if \( o(N) \) is prime to 6, then

\[
\bar{N} = \bigcap_{q \neq \{0\}} N.SL_2(q) = N.SL_2(n).
\]

In particular, if \( o(N) = \mathcal{O}(S) \), then \( \bar{N} = SL_2(\mathcal{O}(S)) \).
Acknowledgements. The authors are indebted to Professors Prasad and Raghunathan for their assistance with the proof of Theorem 1.1. The authors are also grateful to the referee whose comments have led to an improved version of this paper.

References


Received 31 July, 2010; revised 20 January, 2011

A. W. Mason, Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland, United Kingdom
E-mail: awm@maths.gla.ac.uk

B. Sury, Statistics-Mathematics Unit, Indian Statistical Institute, Bangalore 560 059, India
E-mail: sury@isibang.ac.in