Pure and Applied Mathematics Quarterly
Volume 1, Number 2
(*Special Issue: In Memory of
Armand Borel, part 1 of 3*)
241—256, 2005

Finite Presentations of Adelic Groups, the Congruence Kernel and Cohomology of Finite Simple Groups

Alexander Lubotzky

In memory of Armand Borel

Let K be a non-archimedean local field and U a compact subgroup of $GL_n(K)$. Such U is a profinite group, actually it is virtually pro-p. If $\mathrm{char}(K) = 0$, then U is finitely generated and even finitely presented as a profinite group. On the other hand if $\mathrm{char}(K) = p > 0$, then U need not be finitely generated. Moreover, even if U is finitely generated, it may be non-finitely presented (see(1.3)). On the other hand;

Theorem 1 *Let G be a connected, simply-connected, absolutely almost simple algebraic group defined over K and U an open compact subgroup of $G(K)$. Then U is a finitely presented profinite group.*

In fact, in the current paper we prove Theorem 1 under the assumption that G is K-isotropic. If G is anisotropic, then G is isomorphic to $SL_1(D)$, where D is a division algebra whose center is K. This special case turns out to be especially difficult - but it was resolved recently by Ershov [Er2].

Theorem 1 answers a question we were asked by Y. Barnea. Moreover, it settles a case left open in Raghunathan's paper [R1]: Indeed, if U is a pro - p group, then U is finitely presented if and only if $H^2(U, \mathbf{F}_p)$ is finite. The finiteness of the second cohomology of U with various coefficients was proved by

Received March 25, 2005. Partially supported by grants from BSF and NSF.

Raghunathan for char$(K) = 0$ but not for positive characteristic. Prasad and Raghunathan ([PR1], [PR2]) carried out a detailed and deep computation of the second cohomology of some local and adelic groups. In a way, the current paper and [Er2] are complementary to their work - see (6.2) for a detailed comparison and connections.

Theorem 1 has a global analogue:

Theorem 2 *Let k be a global field and G a connected, simply-connected, absolutely almost simple algebraic group defined over k. Let S be a finite set of valuations of k containing S_∞, the set of archimedean ones, and $\mathbf{A}_S$-the ring of S-adeles (i.e. $\mathbf{A}_S = \Pi^*_{v \notin S} k_v$). Let V be an open compact subgroup of $G(\mathbf{A}_S)$. Then V is a finitely presented profinite group.*

Theorem 2 implies:

Corollary 3. *Let k be a global field, $\mathcal{O}$-its ring of integers, S a finite set of valuations of k containing S_∞ and $\mathcal{O}_S$-the ring of S-integers. Assume G is a connected, simply-connected absolutely almost simple algebraic group defined over k and Γ the S-arithmetic group $G(\mathcal{O}_S)$. Then $C = \mathrm{Ker}(\widehat{G(\mathcal{O}_S)} \to G(\hat{\mathcal{O}}_S))$, the congruence kernel, is finitely generated as a normal subgroup of $G(\hat{\mathcal{O}}_S)$ unless char$(k) > 0$, G is k-isotropic and S-rank$(G) := \sum\limits_{v \in S} k_v$- rank$(G) = 1$. In the latter case, $\Gamma = G(\mathcal{O}_S)$ is infinitely generated and C is infinitely generated as a normal subgroup of $\hat{\Gamma} = \widehat{G(\mathcal{O}_S)}$.*

Note that by [Lu3], C is infinitely generated as a profinite group when the congruence subgroup property fails (see there for the precise result) . So, Corollary 3 says that even then C is finitely generated as a normal subgroup, at least when $G(\mathcal{O}_S)$ is finitely generated which is always the case unless k is of positive characteristic and S-rank $(G) = 1$.

Corollary 3 is new even for the classical modular group $\Gamma = SL_2(\mathbf{Z})$. For its importance, let us single it out and state:

Corollary 4. *Let $C = \mathrm{Ker}(\widehat{SL_2(\mathbf{Z})} \to SL_2(\hat{\mathbf{Z}}))$ be the congruence kernel of $\Gamma = SL_2(\mathbf{Z})$. Then*

(a) C is isomorphic to $\hat{F}_w$-the free profinite group on a countable number of generators. In particular, it is not finitely generated.

(b) C is finitely generated as a normal subgroup of $\hat{\Gamma} = \widehat{SL_2(\mathbf{Z})}$.

Part (a) is proved in [Me] and [Lu1]. Part (b) can be deduced from Theorem 2. Let us sketch its proof here; this will give some idea on the proof of Theorem

2: As Γ and $\hat{\Gamma}$ are finitely generated, it suffices to prove that $SL_2(\hat{\mathbf{Z}})$ is a finitely presented profinite group. Let Δ be the S-arithmetic group $SL_2(\mathbf{Z}[\frac{1}{2}])$. It is known that Δ is finitely presented and has the congruence subgroup property. Hence $\hat{\Delta}$ is a finitely presented profinite group and is isomorphic to $\prod_{p \neq 2} SL_2(\mathbf{Z}_p)$. Now,

$$SL_2(\hat{\mathbf{Z}}) = \prod_p SL_2(\mathbf{Z}_p) = SL_2(\mathbf{Z}_2) \times \hat{\Delta}.$$

As $SL_2(\mathbf{Z}_2)$ is also finitely presented (by a well known very special case of Theorem 1), $SL_2(\hat{\mathbf{Z}})$ is finitely presented and Corollary 4(b) is proved.

So, the discrete group Δ which has the congruence subgroup property helps us to analyze the congruence kernel of $\Gamma = SL_2(\mathbf{Z})$ which does not have the congruence subgroup property.

The proof illustrates the main ingredient of the proof of Theorem 2: The group V there is virtually a product of groups like U from Theorem 1, but this is an infinite product. So we cannot use "local to global" methods to deduce Theorem 2 from Theorem 1.

To prove 2, we show that a finite index subgroup V_1 of V can be presented as a product $V_1 = V_2 \times V_3$ where V_3 is a product of finitely many groups of type U of Theorem 1 and V_2 is the profinite completion of a suitable finitely presented S-arithmetic group Δ which has the congruence subgroup property. Some care should be taken here as, in positive characteristic, S-arithmetic subgroups are not necessarily finitely presented. Anyway, as in the argument before, V_2 is therefore a finitely presented profinite group. So will be V_1 (and V) provided we ensure that V_3 is. This is indeed the case by Theorem 1.

In spite of the fact that Theorem 1 is a local theorem, "half" of its proof is based on global consideration. In fact, Theorem 1 is separated to two cases with completely different proofs:

I. G is isotropic; in this case we prove Theorem 1 by presenting U as a suitable quotient of a global group V- as in Theorem 2 - being careful that it would be a quotient of a group like V_2 above, by finitely many relations. So, the local case is deduced from a global result!

II. G is anisotropic. In this case G must be the norm one elements of a division algebra over K (see [PR, Theorem 6.5]) and a detailed structure of G is given in [Ri] and [PR2]. The method we apply for the isotropic case does not work here since the congruence subgroup property is still open for anisotropic groups of type A_n.

This case was left unsettled in an early draft of the current paper and it has been solved recently by M.Ershov [Er2] who introduced a new method to show that a pro-p group U is finitely presented, based on cohomology computation of some associated Lie algebras. By a somewhat similar method he also showed that the Nottingham group is finitely presented [Er1] and it seems to have the potential to be applied to other pro-p groups.

The above mentioned results (1, 2 and 3) are proved in sections 2, 3 and 4, respectively. In Section 5, we show how Theorem 2 can be used to prove a partial result toward a conjecture of Holt [H] bounding the dimensions of the second cohomology groups of finite simple groups. So, somewhat surprisingly, the congruence subgroup property of arithmetic groups finds its way to imply results on the cohomology of finite simple groups. We end in §6 with remarks and suggestions for further research.

Acknowledgement: The author is grateful to A. Rapinchuk for various suggestions including the proof of Lemma 3.1. We also benefitted from conversations and remarks of M. Ershov, G. Prasad and E. Zelmanov.

1. Preliminaries and first observations

(1.1) Let H be a profinite group. H is finitely generated if H has a finite subset X generating a dense subgroup of H. We denote by $d(H)$ the minimal number of (topological) generators of H. H is finitely presented if for some $n \in \mathbf{N}$ there exists an epimorphism from the free profinite group $\hat{F}_n$ onto H with kernel N and there is a finite subset R of N such that N is the minimal closed normal subgroup of $\hat{F}_n$ containing R.

The usual properties of finitely presented discrete groups hold also in the category of profinite groups. We mention a few properties which will be used frequently:

(a) If H_1 is of finite index in H_2, then H_1 is finitely presented iff H_2 is.

(b) Let H_1 be a finitely generated profinite group, $N \lhd H_1$ and $H_2 = H_1/N$. If H_2 is finitely presented, then N is the (closed) normal closure in H_1 of finitely many elements. If H_1 is finitely presented, then the converse is also true, i.e. H_2 is finitely presented if and only if N is finitely generated as a normal subgroup of H_1 .

(c) The profinite completion of a discrete finitely presented group is a finitely presented profinite group.

The proofs of these properties are essentially the same as their analogues for discrete groups. But one should be slightly careful as we are not allowed to work with ordinary words. For example, to see (b): Let $\pi : \hat{F}_d \to H_1$ be an epimorphism from the free profinite group $\hat{F}_d$ onto H_1 with kernel K and ψ the given epimorphism from H_1 to H_2 with kernel N. Denote $\tilde{N} = \mathrm{Ker}(\psi \circ \pi)$. If H_2 is finitely presented, then $\tilde{N}$ is generated as a normal subgroup of $\hat{F}_d$ by finitely many elements (this fact is independent of the specific presentation of H_2; if it is true with one presentation it is true with all - see [Lu5]) and hence the same is true for N as a normal subgroup of H_1.

Conversely, if H_1 is finitely presented, then K is finitely generated as a normal subgroup of $\hat{F}_d$ and if N is also finitely generated as a normal subgroup of H_1, then $\tilde{N}$ is finitely generated (as a normal subgroup) over K and hence altogether $\tilde{N}$ is finitely generated as a normal subgroup of $\hat{F}_d$ and H_2 is finitely presented.

(1.2.) In a similar way, one defines a pro-p group H to be finitely presented in the category of pro-p groups. In [Lu5], it was shown that finitely generated free pro-p groups are finitely presented in the category of all profinite groups. From this and (b) it follows that a pro-p group is finitely presented in the category of pro-p groups iff it is finitely presented in the category of all profinite groups.

The following criterion is well known.

Proposition A finitely generated pro-p group H is finitely presented iff $H^2(H, \mathbf{F}_p)$ is finite.

There is also a cohomological criterion for a finitely generated profinite group to be finitely presented ([Lu5, Theorem 0.3]); see §5 below.

(1.3.) If K is a non-archimedean local field and U a compact subgroup of $GL_n(K)$ then U is virtually pro-p. If $\mathrm{char}(K) = 0$, then U is virtually "uniform powerful" and hence finitely presented (see [DDMS, Prop. 4.32]). On the other hand, if $\mathrm{char}(K) = p > 0$, U need not be finitely generated, e.g. $U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbf{F}_p[[t]] \right\}$ or $U = PGL_p(\mathbf{F}_p[[t]])$ which is mapped onto $\mathbf{F}_p[[t]]^*/(\mathbf{F}_p[[t]]^*)^p$. The latter is an infinitely generated elementary abelian p-group. Incidently, the last example shows that Theorem 1 does not hold without the assumption that G is simply connected.

Even if U is finitely generated it needs not be finitely presented as the following example shows:

Example. Let $U = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; b \in \mathbf{F}_p[[t]], a \in T \right\}$ where T is the closure of the cyclic subgroup of $\mathbf{F}_p[[t]]^*$ generated by $1 + t$. One can see that U is isomorphic to the completed wreath product $\mathbf{Z}_p wr \mathbf{F}_p$ i.e., $\mathbf{Z}_p \ltimes \mathbf{F}_p^{\infty}$, which is clearly a finitely generated group. But it is not finitely presented, see [W,p.270]. In fact, we have the following general result:

Proposition (Wilson [W, Cor. 12.5.10]) Let U be a finitely presented solvable pro-p group and let N be a closed normal subgroup such that $G/N \simeq \mathbf{Z}_p$. Then N is finitely generated.

(1.4.) Let us now use the notations of Corollary 3. So Γ is an S-arithmetic group $\Gamma = G(k) \cap GL_n(\mathcal{O}_S)$ (w.r.t. to some fixed embedding of G into GL_n). If $\mathrm{char}(k) = 0$, then Γ is always finitely presented. The same holds if $\mathrm{char}(k) > 0$ and G is anisotropic. On the other hand, if $\mathrm{char}(k) = p > 0$ and G is isotropic, i.e., k-rank $(G) \geq 1$, a well known theorem of Behr [Be] says that everything depends on $s = S\text{-rank}(G) := \sum_{\nu \in S} k_\nu\text{-rank}(G)$. If $s = 1$, Γ is not finitely generated, if $s = 2$, Γ is finitely generated, but not finitely presented, while if $s \geq 3$, Γ is finitely presented.

It is interesting to note that our Theorems 1 and 2 do not distinguish between the different ranks - so while $SL_2(\mathbf{F}_p[t])$ (resp. $SL_3(\mathbf{F}_p[t])$) is not finitely generated (resp. finitely presented), $SL_2(\mathbf{F}_p[[t]])$ (resp. $SL_3(\mathbf{F}_p[[t]])$) is.

2. Proof of Theorem 1: the isotropic case

In this section, we prove Theorem 1 under the additional hypothesis that G is isotropic over K. As mentioned before, the anisotropic case is dealt with by an entirely different method in [Er2].

Let $\mathcal{G}$ be a connected, simply-connected absolutely almost simple group which is defined and isotropic over a global field k such that $K = k_{v_0}$ for some valuation v_0 and such that $\mathcal{G}(k_{v_0})$ is isomorphic to $G(K)$. Let S be a finite set of valuations of k containing S_∞ - the set of the archimedean valuations and such that: (i) $v_0 \notin S$ (ii) The S-arithmetic group $\Gamma = \mathcal{G}(\mathcal{O}_S)$ is finitely presented and (iii) $\Gamma = \mathcal{G}(\mathcal{O}_S)$ has the congruence subgroup property, i.e., $\mathrm{Ker}(\widehat{\mathcal{G}(\mathcal{O}_S)} \to \mathcal{G}(\hat{\mathcal{O}}_S))$ is finite.

Such an S does exist: Recall that for almost every valuation v of $k, \mathcal{G}$ is quasi-split over k_v ([PR, p.281]) and in particular, also of k_v-rank ≥ 1. So by enlarging S if needed, we ensure that $\sum_{v \in S} k_v\text{-rank}(\mathcal{G}) \geq 3$ which implies by Behr's Theorem (see (1.4)) that Γ is finitely presented. Moreover, by Raghunathan [R2, p.74] Γ has the congruence subgroup property.

Now (ii) implies that the profinite completion $\hat{\Gamma}$ is finitely presented and (iii) implies that this holds also for $\mathcal{G}(\hat{\mathcal{O}}_S) = \prod\limits_{v \notin S} \mathcal{G}(\mathcal{O}_S)$.

Furthermore, if $S_1 = S \cup \{v_0\}$, then

$$\mathcal{G}(\hat{\mathcal{O}}_{S_1}) = \prod_{v \notin S_1} \mathcal{G}(\mathcal{O}_v)$$

so $\mathcal{G}(\hat{\mathcal{O}}_S) = \mathcal{G}(\mathcal{O}_{S_1}) \times \mathcal{G}(\mathcal{O}_{v_0})$. Thus $\mathcal{G}(\hat{\mathcal{O}}_{S_1})$ is a quotient of $\mathcal{G}(\hat{\mathcal{O}}_S)$ and hence it is finitely generated. At the same time $\hat{\mathcal{G}}(\mathcal{O}_{S_1})$ can be regarded as a normal subgroup of $\hat{\mathcal{G}}(\mathcal{O}_S)$. This implies that the quotient $\mathcal{G}(\hat{\mathcal{O}}_S)/\mathcal{G}(\hat{\mathcal{O}}_{S_1}) = \mathcal{G}(\mathcal{O}_{v_0})$ is a finitely presented group. The latter is commensurable to U. So U is also finitely presented as claimed.

3. Proof of Theorem 2

For the proof, we need the following lemma:

Lemma 3.1. Let k and G be as in Theorem 2. Then there exists a connected, simply-connected absolutely almost simple, *quasi-split* group $\mathcal{G}$ defined over k, such that for almost every valuation v of k, $\mathcal{G}(k_v)$ is isomorphic to $G(k_v)$.

Proof. Let G_0 be the split form of the group G. The k-forms of G_0 are classified by the elements of $H^1(k, \mathrm{Aut}(G_0))$ (see [PR ,§6]). Now, $\mathrm{Aut}(G_0)$ is a semi-direct product of $\mathrm{Aut}(D)$ (= the automorphisms of the Dynkin diagram associated to G_0) and $\mathrm{Int}(G_0)$ (= the inner automorphisms of G_0). There is a natural map $f : H^1(k, \mathrm{Aut}(G_0)) \to H^1(k, \mathrm{Aut}(D))$. Let $c \in H^1(k, \mathrm{Aut}(G_0))$ denote the cocycle that corresponds to G.

As $\mathrm{Aut}(G_0) = \mathrm{Int}(G_0) \rtimes \mathrm{Aut}(D)$, we can consider $f(c)$ also as an element of $H^1(k, \mathrm{Aut}(G_0))$. Twisting the split form G_0 by $f(c)$ will give a quasi-split form $\mathcal{G}$ (since the Borel subgroup is preserved by $\mathrm{Aut}(D)$ and hence still defined over k). By [P, Lemma 2.0] $\mathcal{G}$ is the unique quasi-split form in the same inner class as G.

Look now over k_v, still $\mathcal{G}$ and G are at the same inner class, $\mathcal{G}$ is of course quasi-split for all v and G is quasi-split for almost all v. Again, as before, there is a unique quasi-split form in every k_v-inner class, so for almost every v, $G(k_v) \simeq \mathcal{G}(k_v)$.

Lemma 3.1 is now proved. To prove Theorem 2, we can replace V by a finite index subgroup and assume that V has the form $\prod\limits_{v \notin S} M_v$, where each M_v is compact open in $G(k_v)$ and for almost every $v, M_v = G(\mathcal{O}_v)$. From Theorem 1, we know that each M_v is finitely presented, but in general, an infinite product of finitely presented groups is not finitely presented (see (6.1)).

Let $\mathcal{G}$ be as in Lemma 3.1, and $S_1 = \{v \mid \mathcal{G}(k_v) \not\simeq G(k_v)\}$. So S_1 and $S' = S_1 \cup S$ are finite. Write $V = V_1 \times V_2$ where $V_1 = \prod\limits_{\nu \notin S'} M_v$ and $V_2 = \prod\limits_{\nu \in S' \setminus S} M_\nu$.

As V_2 is a finite product of local (finitely presented) groups, it is finitely presented. We are left to prove that V_1 is finitely presented. Now, we argue in a similar way to the proof in §2: V_1 is an open subgroup of $\mathcal{G}(\hat{\mathcal{O}}_{S'})$. Let S'' be a finite set of valuations containing S' such that $S''\text{-rank}(\mathcal{G}) := \sum\limits_{v \in S''} k_\nu\text{-rank}(\mathcal{G}) \geq 3$. (Such S'' clearly exists, as $\mathcal{G}$ is quasi split over every k_ν). Thus the S-arithmetic group $\Gamma = \mathcal{G}(\mathcal{O}_{S''})$ is finitely presented by Behr's Theorem (see (1.4)) and has the congruence subgroup property by Raghunathan's Theorem ([R2]). The group $\mathcal{G}(\hat{\mathcal{O}}_{S''})$ is, therefore, a finitely presented profinite group. Now, V_2 is commensurable to $V_3 \times \mathcal{G}(\hat{\mathcal{O}}_{S''})$ where $V_3 = \prod\limits_{\nu \in S'' \setminus S'} M_\nu$. As $S'' \setminus S'$ is finite, V_3 is also finitely presented. This proves that V_2 is finitely presented and so is V.

Theorem 2 is now proven.

§4. Proof of Corollary 3

Assume first that we are not in the excluded case (char$(k) > 0$ and S-rank$(G) = 1$). Then by the result of Behr mentioned in (1.4), $\Gamma = G(\mathcal{O}_S)$ is finitely generated, hence $\hat{\Gamma} = \widehat{G(\mathcal{O}_S)}$ is a finitely generated profinite group. By Theorem 2, $G(\hat{\mathcal{O}}_S)$ is a finitely presented profinite groups. So, an elementary group theoretical argument implies (see (1.1)(b)) that $C = \text{Ker}(\widehat{G(\mathcal{O}_S)} \to G(\hat{\mathcal{O}}_S))$ is finitely generated as a normal subgroup of $\widehat{G(\mathcal{O}_S)}$.

Assume now that char$(k) > 0$, G is k-isotropic and S-rank $(G) = 1$. In this case, Behr's result says that $\Gamma = G(\mathcal{O}_S)$ is not finitely generated. In fact, in this case $|S| = 1$, so $S = \{v\}$, and Γ is a non-uniform lattice in the rank one k_v-group $G(k_v)$, so it is a "non-uniform tree lattice" (see [Lu2] and [BL]) and hence not finitely generated. Furthermore, we have proven in [Lu2] that Γ has a finite index congruence subgroup Δ which is a free product of a finitely generated free group and finitely many "cusp subgroups". In particular, it is shown there that Δ is mapped onto the infinite elementary abelian group $\bigoplus\limits_{i=1}^{\infty} C_p$, where C_p is the cyclic group of order p.

Let now $\hat{\Delta}$ be the profinite completion of Δ and $\bar{\Delta}$ its closure in $G(\hat{\mathcal{O}}_S)$. Then $C = \operatorname{Ker}(\hat{\Delta} \to \bar{\Delta})$ and C is finitely generated as normal subgroup of $\hat{\Gamma}$ if and only if it is so in $\hat{\Delta}$. But taking abelianizations, we see that $\hat{\Delta}/[\hat{\Delta}, \hat{\Delta}]$ is mapped onto the infinitely generated group $\prod_{i=1}^{\infty} C_p$ while $\bar{\Delta}$ being a finite index open subgroup in the semisimple adelic group $G(\hat{\mathcal{O}}_S)$ has finite abelianization. This implies that $(\operatorname{Ker}(\hat{\Delta}/[\hat{\Delta}, \hat{\Delta}] \to \bar{\Delta}/[\bar{\Delta}, \bar{\Delta}])$ is infinitely generated, hence C cannot be finitely generated as a normal subgroup of $\hat{\Delta}$ or $\hat{\Gamma}$.

§5. Cohomology of finite simple groups

In this section we will present an unexpected contribution of the congruence subgroup property to the cohomology of finite simple groups. This will be in the form of a partial result toward a conjecture of Holt [H].

For a finite group G denote

$$h(G) = \sup_p \sup_M \{ \frac{\dim H^2(G, M)}{\dim M} \Bigm| M \text{ is a simple } \mathbf{F}_p[G] - \text{module}\}$$

The main result of [H] says that for finite simple groups G, $h(G) = O(\log |G|)$. Holt conjectures furthermore that $h(G) = O(1)$, i.e., bounded by a constant when G runs over all finite simple groups.

We can use the results of the current paper to give some partial results in this direction.

Proposition 5.1. Let $\mathbf{G}$ be a simple Chevalley scheme (e.g. $\mathbf{G} = SL_n$). Then

(1) $h(\mathbf{G}(\mathbf{F}_p)) = O(1)$ when p runs over all primes and similarly
$h(\mathbf{G}(\mathbf{F}_p)/Z(\mathbf{G}(\mathbf{F}_p)) = O(1)$.

(2) For a fixed prime p, $h(\mathbf{G}(\mathbf{F}_{p^r})) = O(1)$ where $r \in \mathbf{N}$, and similarly
$h(\mathbf{G}(\mathbf{F}_{p^r})/Z(\mathbf{G}(\mathbf{F}_{p^r})) = O(1)$.

To prove Proposition 5.1, let us start with recalling a few results from [Lu5] on profinite presentations.

Let G be a finitely generated profinite group with $d(G) = d$. Let $r(G)$ be the minimal number of relations in any presentation of G as a quotient of a free profinite group. It is shown there that $r(G)$ is realized by a presentation with d

generators, $1 \to R \to \hat{F}_d \to G \to 1$ and

$$r(G) = \begin{cases} 1 & \text{if } G \text{ is } d\text{-abelian-indexed and not } \hat{F}_d \\ d_G(\bar{R}) & \text{otherwise} \end{cases}$$

where $d_G(\bar{R})$ is the number of (topological) generators of the G-module $\bar{R} = R/[R,R]$.

See there for the definition of d-abelian-indexed. Anyway, if G is finite, then always $r(G) = d_G(\bar{R})$, $\bar{R}$ is the G-relation module, i.e., $R/[R,R]$ as a G-module. It is also shown there (Theorem 5.1) that

$$d_G(\bar{R}) = \sup_p \sup_M \left\{ [[\frac{\dim H^2(G,M) - \dim H^1(G,M)}{\dim M}]] + d - \xi_M \right\}$$

when M runs over all the $\mathbf{F}_p[[G]]$-simple modules, $\xi_M = 0$ if M is trivial and 1 if not, and for a real number q, $[[q]]$ denotes the smallest integer which is at least q.

Now, every one-cocycle is determined on the generators, hence $\frac{\dim H^1(G,M)}{\dim M} \leq d(G)$ (see [AG] for stronger results for finite simple groups). We can therefore deduce:

Corollary 5.2. *$h(G) - 1 \leq r(G) \leq h(G) + d(G) + 1$.*

Now, as all finite simple groups are generated by two elements, Holt's conjecture is equivalent to:

Conjecture 5.3. There exists a constant c such that every finite simple group has a profinite presentation with at most c relations.

In fact, in [Lu4], the results of Holt [H] were used to show that every finite simple group has a profinite presentation with $O(\log|G|)$ relations. (For ordinary presentations this is still an open problem - see [Ma]). This was enough in order to deduce the Mann-Pyber conjecture on the normal subgroup growth of free groups.

We are now ready for:

Proof of Proposition 5.1. (1) By Theorem 2, the profinite group $\mathbf{G}(\hat{\mathbf{Z}})$ is finitely presented. It suffices therefore to show that $\mathbf{G}(\mathbf{F}_p)$ is obtained as a quotient of $\mathbf{G}(\hat{\mathbf{Z}})$ by a number of relations which is independent of p. Indeed, $\mathbf{G}(\hat{\mathbf{Z}}) = \prod_{q \text{ prime}} \mathbf{G}(\mathbf{Z}_q)$, so $\mathbf{G}(\mathbf{Z}_p)$ is obtained from $\mathbf{G}(\hat{\mathbf{Z}})$ by dividing by $\prod_{q \neq p} \mathbf{G}(\mathbf{Z}_q)$. The latter is also a quotient of $\mathbf{G}(\hat{\mathbf{Z}})$, so its number of generators is bounded by $d(\mathbf{G}(\hat{\mathbf{Z}}))$ and so independent of p. Now, $\mathbf{G}(\mathbf{F}_p)$ is obtained from $\mathbf{G}(\mathbf{Z}_p)$ by dividing by the first congruence subgroup - whose number of generators is $\dim(G)$

[DDMS] - so again independent of p. Finally, the center of $\mathbf{G}(\mathbf{F}_p)$ is cyclic or two-generated so one or two more relations will give $\mathbf{G}(\mathbf{F}_p)/Z(\mathbf{G}(\mathbf{F}_p))$ and (1) is proved.

Part (2) is proved in a similar way using $\mathbf{G}(\widehat{\mathbf{F}_p[t]})$ instead of $\mathbf{G}(\hat{\mathbf{Z}})$.

We remark that a more careful argument shows that $\prod\limits_{q\neq p} \mathbf{G}(\mathbf{Z}_p)$ is generated by one element as a normal subgroup and similarly the congruence subgroup of $\mathbf{G}(\mathbf{Z}_p)$. However, to prove Holt's conjecture in full, we need a uniform bound on profinite presentations of $\mathbf{G}(\hat{\mathbf{Z}})$ in Theorem 2.

For more discussion, see (6.6) below.

§6. Some concluding remarks

(6.1) Recall that among discrete groups, there are uncountably many isomorphism classes of finitely generated groups but clearly only countably many of them are finitely presented. On the other hand:

Proposition 6.1. There are uncountably many finitely presented profinite groups.

Proof. Let $d \in \mathbf{N}$ be a fixed integer ≥ 2 and let $\mathcal{P}$ be an arbitrary set of primes. The group $H_{\mathcal{P}} = \prod\limits_{p\in\mathcal{P}} SL_d(\mathbf{Z}_p)$ is finitely presented. Indeed, it is a quotient of $SL_d(\hat{\mathbf{Z}}) = \prod\limits_{\text{all } p} SL_d(\mathbf{Z}_p)$ by the finitely generated normal subgroup $\prod\limits_{p\notin\mathcal{P}} SL_d(\mathbf{Z}_p)$. Clearly, for two different sets of primes $\mathcal{P}_1$ and $\mathcal{P}_2$, $H_{\mathcal{P}_1}$ and $H_{\mathcal{P}_2}$ are not isomorphic.

Note however, that in general a direct product of infinitely many finitely presented groups is not finitely presented. For example, each $PSL_d(\mathbf{Z}_p)$ is finitely presented but $\prod\limits_p PSL_d(\mathbf{Z}_p) = PSL_2(\hat{\mathbf{Z}})$ is not finitely presented since it is a quotient of the finitely presented group $SL_d(\hat{\mathbf{Z}})$ by its infinitely generated center $Z = \prod\limits_p Z(SL_d(\mathbf{Z}_p))$ (see (1.1)(b)).

(6.2.) Our results are related to those of Prasad and Raghunathan in [PR1] and [PR2].

If k, G and S are as in Theorem 2, the congruence subgroup problem asks for the kernel $C(G,S) = \operatorname{Ker}(\widehat{G(k)} \to \overline{(G(k)})$ when $\widehat{G(k)}$ (resp. $\overline{G(k)}$) is the completion of $G(k)$ with respect to the S-arithmetic (resp. S-congruence) topology, i.e., the topology for which the S-arithmetic (resp. S-congruence) subgroups serve as a basis for the neighborhoods of the identity. Following a long line of research and authors (see [Rap] for a detailed history) Raghunathan proved that if $k-\text{rank}(G) \geq 1$ and $S-\text{rank}(G) \geq 2$ then $C(G,S)$ is central in $\widehat{G(k)}^+$, $\widehat{G(k)}^+$ is a subgroup of $\widehat{G(k)}$ which in almost all cases is known to be equal to $\widehat{G(k)}$ and in any case is of finite index there. This led attention to calculating central extensions of $\overline{G(k)}$. The latter is the group of S-adeles: i.e., $\overline{G(k)} = G(\mathbf{A}_S) = \prod\limits_{\nu \notin S} G(k_v)$. Central extensions of adelic groups of these kind are of importance also for other reasons ("the metaplectic conjecture") and a good amount of work has been dedicated to their computation with the ultimative answer given by Prasad and Rapinchuk [PrR1], [PrR2].

Now, computing central extension lead to $H^2(G(\mathbf{A}_S), \mathbf{R}/\mathbf{Z})$. The latter is related to a product of $H^2(G(k_v), \mathbf{R}/\mathbf{Z})$ for $v \notin S$. So, computing $H^2(G(K), \mathbf{R}/\mathbf{Z})$ for a local field K was a problem of special importance. This problem was solved to a large extent by Prasad and Raghunathan [PR1], [PR2] (see also ([PrR1]), who showed, in particular, that this is always a finite group (and computed it precisely when G is K-isotropic). From their result it follows immediately that $H^2(G(K), \mathbf{F}_p)$ is finite (look at the exact sequence $1 \to A \to \mathbf{R}/\mathbf{Z} \xrightarrow{\pi} \mathbf{R}/\mathbf{Z} \to 1$, where $\pi(x) = px$. Then $A \simeq \mathbf{F}_p$. The finiteness of $H^1(G(K), \mathbf{R}/\mathbf{Z})$ and $H^2(G(K), \mathbf{R}/\mathbf{Z})$ implies the finiteness of $H^2(G(K), \mathbf{F}_p)$).

Let now U be an open pro-p subgroup of $G(K)$. So our Theorem 1 basically claims that $H^2(U, \mathbf{F}_p)$ is finite.

We do not see a way to deduce our result from those of Prasad and Raghunathan. This is especially frustrating in the anisotropic case: Here $G(K)$ is compact, by [PR2], $H^2(G(K), \mathbf{F}_p)$ is finite, but it does not seem that their result works for the finite index subgroups. Recall that in this case $G(K)$ has a normal open pro-p subgroup N of index prime to p. Proving Theorem 1 for this N would imply it to any other open subgroup. This is what has been done by Ershov [Er2] by a fairly complicated and long proof.

In the other direction: The finiteness of $H^1(U, \mathbf{F}_p)$ (which is well known) and that of $H^2(U, \mathbf{F}_p)$ (proven here and in [Er2]) imply the finiteness of $H^2(G(K), \mathbf{F}_p)$ (using the spectral sequence given in Section 3 of [PR1] - see also §6 there)). But it does not seem to imply the stronger result of Prasad and Raghunathan claiming that $H^2(G(K), \mathbf{R}/\mathbf{Z})$ is finite. We do not know if $H^2(U, \mathbf{R}/\mathbf{Z})$ is finite (when $\text{char}(K) > 0$). If this would be the case the finiteness of $H^2(G(K), \mathbf{R}/\mathbf{Z})$ could be deduced from it.

(6.3.) Look again at $C = \text{Ker}(\widehat{SL_2(\mathbf{Z})} \to SL_2(\hat{\mathbf{Z}}))$. It is also equal to $\text{Ker}(\widetilde{SL_2(\mathbf{Q})} \to SL_2(\mathbf{A}_f))$ where $\widetilde{SL_2(\mathbf{Q})}$ is the completion, as in (6.2), of $SL_2(\mathbf{Q})$ with respect to the arithmetic topology of $SL_2(\mathbf{Q})$. By Corollary 4, C is finitely generated as a normal subgroup of $\widehat{SL_2(\mathbf{Z})}$ and hence also as a normal subgroup of $\widetilde{SL_2(\mathbf{Q})}$. We have learned recently that Prasad and Rapinchuk ([PrR2]) proved that as a normal subgroup of $\widetilde{SL_2(\mathbf{Q})}$, C can be generated by a single element. Our method cannot prove this while their method cannot prove that C is finitely generated in $\widehat{SL_2(\mathbf{Z})}$; they need the full $\widetilde{SL_2(\mathbf{Q})}$.

Looking now at abelianization: we mention in Corollary 4(a) that $C \simeq \hat{F}_w$ and so $W = C/[C, C]$ is a free abelian profinite group on countable number of generators. By Corollary 4(b), W is a finitely generated $SL_2(\hat{\mathbf{Z}})$ and $SL_2(\mathbf{A}_f)$ module. It will be interesting to analyze further this $SL_2(\mathbf{A}_f)$-module. We mention in passing that just like $SL_2(\mathbf{Q})$ is a discrete subgroup, in fact a lattice, in $H = SL_2(\mathbf{A}) = SL_2(\mathbf{R}) \times SL_2(\mathbf{A}_f)$, $SL_2(\mathbf{Q})$ sits as a lattice in $\tilde{H} = SL_2(\mathbf{R}) \times \widetilde{SL_2(\mathbf{Q})}$. Now $H/SL_2(\mathbf{Q}) = SL_2(\mathbf{A})/SL_2(\mathbf{Q})$ is equal to the inverse limit $\varprojlim SL_2(\mathbf{R})/\Gamma$ when Γ runs over the congruence subgroups of $SL_2(\mathbf{Z})$. In a similar way, $\tilde{H}/SL_2(\mathbf{Q})$ is the inverse limit $\varprojlim SL_2(\mathbf{R})/\Gamma$ when this time Γ runs over *all* finite index subgroups of $SL_2(\mathbf{Z})$. It is well known that $L^2(H/SL_2(\mathbf{Q})) = L^2(SL_2(\mathbf{A})/SL_2(k))$ captures the modular forms of $SL_2(\mathbf{R})$ w.r.t. to congruence subgroups and a similar argument shows that $L^2(\tilde{H}/SL_2(\mathbf{Q}))$ plays a similar role with respect to all finite index subgroups. The study of W as $SL_2(\mathbf{A}_f)$ module may be of some relevance for these topics.

(6.4.) In comparison with (6.3), let's look at

$$C = \text{Ker}(\widehat{SL_2(\mathbf{F}_q(t))} \to SL_2(\widehat{\mathbf{F}_q(t)})) = \text{Ker}(\widetilde{SL_2(\mathbf{F}_q(t))} \to SL_2(\mathbf{A}_f))$$

where here $\mathbf{A}_f$ is the adelic completion of $\mathbf{F}_q(t)$ at all primes. While we proved in Corollary 3 that C is not finitely generated as a normal subgroup of $\widehat{SL_2(\mathbf{F}_q(t))}$, it may still be a finitely generated as a normal subgroup of $\widetilde{SL_2(\mathbf{F}_q(t))}$. We tend to believe that this is indeed the case.

(6.5.) As pointed out in (1.3), Theorem 1 is not true if G is not simply-connected. Let us make here the observation that it is still true then if U is finitely generated. Indeed, let $\pi : \tilde{G} \to G$ be the simply connected cover of G. Then over K, $\pi(\tilde{G}(K))$ is closed and normal in $G(K)$ and the quotient $D = G(K)/\pi(\tilde{G}(K))$ is abelian compact of finite exponent (see [BT, 3.19(ii)]). Hence if U is finitely generated open subgroup of $G(K)$ its image in D is finite and open in D so D is finite, so $U_1 = \pi(\tilde{G}(K)) \cap U$ is of finite index in U. We can pull this group back to $\tilde{G}(K)$ (recall that Ker π is finite) to deduce from Theorem 1 that U_1 and hence U is finitely presented.

Theorem 2 is not true without the assumption that G is simply connected, even if V is finitely generated. Take for example, $PSL_2(\hat{\mathbf{Z}})$ which is a quotient of $SL_2(\hat{\mathbf{Z}})$ by the infinitely generated center. By Theorem 2, $SL_2(\hat{\mathbf{Z}})$ is finitely presented but by (1.1)(b), $PSL_2(\hat{\mathbf{Z}})$ is not, as we also mentioned in (6.1).

(6.6.) One can prove Proposition 5.1 (and even a somewhat stronger result) directly from the congruence subgroup property of $\mathbf{G}(\mathbf{Z})$ (and $\mathbf{G}(\mathbf{F}_p[t])$) without passing through Theorem 2. For example, take $\mathbf{G} = SL_n, (n \geq 3)$, then one can deduce from the congruence subgroup property that if one takes a finite presentation for $SL_n(\mathbf{Z})$ and adds one relation $E_{12}^p = 1$, where E_{12} is the elementary $(1,2)$-matrix (i.e., one on the diagonal and at the $(1,2)$-entry and zero elsewhere) then we get a presentation for $SL_n(\mathbf{F}_p)$, whose size is independent of p. Similar argument works for all the Chevalley groups. This argument proves that the family $\mathbf{G}(\mathbf{F}_p)$ has even ordinary presentation of bounded size. So, it is stronger than Proposition 5.1 which provides only such profinite presentation. This result for $\mathbf{G}(\mathbf{F}_p)$ can be also deduced from the Curtis-Steinberg-Tits presentation (see [BGKLP, (4.2)]) - but it seems that not the result for $\mathbf{G}(\mathbf{F}_{p^e})$. We mention in passing that the argument here also shows that these groups have "short presentations" in the sense of [BGKLP] where presentations are measured by their length in bits, rather than by the cardinality of the set of relations.

Finally, we should mention that we actually do not know if the argument given here really proves something stronger than the one given in §5. As of now, it seems that no finite group is known whose ordinary presentation needs strictly more relations than its profinite presentation. But, it is expected that such a group exists. It may even be that all finite simple groups can be presented with a bounded number of relations. This is not likely to be true, but if it is true, it will be a much stronger statement than Holt's conjecture.

References

[AG] M. Aschbacher, R.M. Guralnick, Some applications of the first cohomology group, J. Algebra 90 (1984) 446-460.

[BGKLP] L. Babai, A.J. Goodman, W.M. Kantor, E.M. Luks, P.P. Palfy, Short presentations for finite groups, J. Algebra 194 (1997) 79-112.

[BL] H. Bass, A. Lubotzky, Tree Lattices, Progress in Mathematics 176, Birkhäuser, 2001.

[Be] H. Behr, Arithmetic groups over function fields I. A complete characterization of finitely generated and finitely presented arithmetic subgroups of reductive algebraic groups, J. Reine. Angew Math. 495 (1997) 79-118.

[BT] A. Borel, J. Tits, Homomorphismes "abstraits" de groupes algébriques simples, Ann. of Math. (2) 97 (1973), 499-571.

[DDMS] J.D. Dixon, M.P.F. Du Sautoy, A. Mann and D. Segal, Analytic Pro-p Groups. (2nd edition), Cambridge Studies in Advanced Mathematics 61, Cambridge University Press 1999.

[Er1] M. Ershov, The Nottingham group is finitely presented, J. London Math. Soc., to appear.

[Er2] M. Ershov, Finite presentations of $SL_1(D)$, preprint.

[H] D.F. Holt, On the second cohomology group of a finite group, Proc. LMS 55 (1987) 22-36.

[Lu1] A. Lubotzky, Free quotients and the congruence kernel of SL_2, J. Algebra 77 (1982) 411-418.

[Lu2] A. Lubotzky, Lattices in rank one Lie groups over local fields, Geom. Funct. Anal. 1 (1991), no. 4, 406-431.

[Lu3] A. Lubotzky, Subgroup growth and congruence subgroups, Invent. Math. 119 (1995) 267-295.

[Lu4] A. Lubotzky, Enumerating boundedly generated finite groups, J. Algebra 238 (2001) 194-199.

[Lu5] A. Lubotzky, Profinite presentations, J. Algebra 242 (2001) 672-690.

[Ma] A. Mann, Enumerating finite groups and their defining relations, J. Group Theory 1 (1998) 59-64.

[Me] O.V. Melnikov, Congruence kernel of the group $SL_2(\mathbf{Z})$, Dokl. Akad. Nauk SSSR 228 (1976) 1034-1036.

[PR] V. Platonov, A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, Boston 1994.

[P] G. Prasad, Volumes of S-arithmetic quotients of semi-simple groups, Publ. Math. IHES 69 (1989) 91-117.

[PR1] G. Prasad, M.S. Raghunathan, Topological central extensions of semisimple groups over local fields, Ann. of Math. 119 (1984) 143-268.

[PR2] G. Prasad, M.S. Raghunathan, Topological central extensions of $SL_1(D)$, Invent. Math. 92 (1988) 645-689.

[PrR1] G. Prasad, A. Rapinchuk, Computation of the metaplectic kernel, Publ. Math. IHES 84 (1996) 91-187.

[PrR2] G. Prasad, A. Rapinchuk, On centrality of the congruence kernel, in preparation.

[R1] M.S. Raghunathan, On the congruence subgroup problem, Publ. Math. IHES 46 (1976) 107-161.

[R2] M.S. Raghunathan, On the congruence subgroup problem, Invent. Math. 85 (1986) 73-117.

[Rap] A. Rapinchuk, Congruence subgroup problem for algebraic groups: old and new, Journees Arithmetiques, 1991 (Geneva). Asterisque 209 (1992) 11, 73-84.

[Ri] C. Riehm, The norm 1 group of p-adic division algebras, Amer. J. Math. 92 (1970) 499-523.

[W] J. Wilson, Profinite Groups, London Mathematical Society Monographs, New Series, 19. The Clarendon Press, Oxford University Press, New York, 1998.

Alexander Lubotzky
Institute of Mathematics
Hebrew University
Jerusalem 91904
ISRAEL
and
Department of Mathematics
Yale University
P.O.Box 208283
New Haven, CT 06520-8283
USA
alexlub@math.huji.ac.il