Semi-simple Groups and Arithmetic Subgroups

Gopal Prasad

Tata Institute of Fundamental Research, Homi Bhabha Road
Colaba, Bombay 400 005, India

To my teacher
M.S. Raghunathan

In this lecture I shall report on the recent results, and open questions, related to the congruence subgroup problem, computation of the covolume of S-arithmetic subgroups, bounds for the class-number of simply connected semi-simple groups and state the finiteness theorems of [3]. We shall also briefly mention the recent work on super-rigidity of *cocompact* discrete subgroups of $\mathrm{Sp}(n, 1)$ and the $\mathbf{R}$-rank 1 form of type F_4, which implies arithmeticity of these discrete subgroups.

Notation. Throughout this report k is a global field, that is either a number field (i.e. a finite extension of the field $\mathbf{Q}$ of rational numbers) or the function field of an algebraic curve over a finite field. Let V be the set of places of k, V_∞ (resp. V_f) be the set of archimedean (resp. nonarchimedean) places. For $v \in V$, k_v will denote the completion of k at v with the natural locally compact topology and $|\ |_v$ the normalized absolute value on k_v. For $v \in V_f$, $\mathfrak{o}_v$ will denote the ring of integers of k_v, $\mathfrak{f}_v$ the residue field, p_v the characteristic of $\mathfrak{f}_v$ and q_v its cardinality. In the sequel k_v is assumed to carry the "normalized" Haar measure, see [26, 0.1]. For any finite set S of places of k containing V_∞, $\mathfrak{o}_S$ will denote the ring of S-integers of k, i.e.

$$\mathfrak{o}_S = \{x \in k \mid \ |x|_v \leqq 1 \ \text{ for all } \ v \notin S\}.$$

A will denote the ring of adèles of k. For a finite set S of places of k, let A_S be the ring of S-adèles i.e. the restricted direct product of the k_v's for $v \notin S$.

Let G be a connected semi-simple algebraic group defined over k. We fix an embedding of G in SL_n defined over k and view G as a k-subgroup of SL_n in terms of this embedding. Let S be a fixed finite set of places of k containing V_∞. Let $G_S = \prod_{v \in S} G(k_v)$ with the locally compact topology induced by the topologies on $k_v, v \in S$. We shall let Γ denote the group $G(k) \cap \mathrm{SL}_n(\mathfrak{o}_S)$. Note that Γ depends on the embedding of G in SL_n fixed above. Embedded diagonally in G_S, Γ is a discrete subgroup of finite covolume. A subgroup of G_S is said to be *S-arithmetic* if it is commensurable with Γ.

Proceedings of the International Congress
of Mathematicians, Kyoto, Japan, 1990

1. The Congruence Subgroup Problem

For any non-zero ideal $\mathfrak{a}$ of $\mathfrak{o}_S$, we have the "reduction mod $\mathfrak{a}$"

$$\pi_{\mathfrak{a}} : \mathrm{SL}_n(\mathfrak{o}_S) \to \mathrm{SL}_n(\mathfrak{o}_S/\mathfrak{a}).$$

The kernel of $\pi_{\mathfrak{a}}|_\Gamma$ will be denoted by $\Gamma_{\mathfrak{a}}$, it is by definition the *principal S-congruence subgroup of Γ of level* $\mathfrak{a}$. Since $\mathfrak{o}_S/\mathfrak{a}$ is finite, $\mathrm{SL}_n(\mathfrak{o}_S/\mathfrak{a})$ is finite and hence $\Gamma_{\mathfrak{a}}$ is of finite index in Γ. An S-arithmetic subgroup is an *S-congruence subgroup* if it contains a principal S-congruence subgroup of Γ of some level. It is not difficult to see that this notion (of S-congruence subgroups) does not depend on the choice of the k-embedding of G in SL_n.

Henceforth, G will be assumed to be absolutely almost simple and simply connected. We shall assume further that G_S is noncompact or, equivalently, for some v in S, G is isotropic at v ([24]).

The *congruence subgroup problem* in its simplest form asks whether any S-arithmetic subgroup is an S-congruence subgroup. If the answer is in the affirmative, we say that G has the congruence subgroup property (for S-arithmetic subgroups). In general the answer to the above question is in the negative. For example, as has been known since 1880, the group $\mathrm{SL}_2/\mathbf{Q}$ does not have the congruence subgroup property for $S = V_\infty$ (but the group $\mathrm{SL}_n/\mathbf{Q}$ has the congruence subgroup property for all $n > 2$ – this was proved by Bass-Lazard-Serre and Mennicke independently in 1963). If k is a totally imaginary number field, the group SL_n/k fails to have the congruence subgroup property for any n ($S = V_\infty$); see [2]. To give a precise measure of the failure, J-P. Serre introduced "the S-congruence kernel" which is a profinite group defined as follows. On $G(k)$ we introduce the following two translation invariant topologies:

(1) The *S-congruence topology*: In this the S-congruence subgroups constitute a neighborhood base at the identity. It is obvious that this is the same topology as the one induced on $G(k)$ from $G(A_S)$. By strong approximation ([23], [14], [21]), the completion of $G(k)$ with respect to the S-congruence topology is $G(A_S)$.
(2) The *S-arithmetic topology*: In this the S-arithmetic subgroups contained in $G(k)$ constitute a neighborhood base at the identity. Completion of $G(k)$ with respect to this topology will be denoted by $\widehat{G}_S$.

As every S-congruence subgroup is S-arithmetic, the S-arithmetic topology on $G(k)$ is finer than the S-congruence topology and therefore there is a continuous homomorphism $\widehat{G}_S \to G(A_S)$. It is not difficult to show that this homomorphism is surjective and its kernel, denoted $C(S,G)$, is a profinite group. $C(S,G)$ is by definition the *S-congruence kernel.* It is clear that $C(S,G)$ is trivial if, and only if, G has the congruence subgroup property (for S-arithmetic subgroups). In the more precise formulation due to Serre, the congruence subgroup problem is the problem of determining the S-congruence kernel $C(S,G)$.

We have the following topological extension

$$(*) \qquad 1 \to C(S,G) \to \widehat{G}_S \to G(A_S) \to 1$$

of $G(A_S)$ by $C(S,G)$. The natural inclusion of $G(k)$ in $\widehat{G}_S$ provides a splitting of this extension over $G(k)(\hookrightarrow G(A_S))$. It has been conjectured that, under a fairly general hypothesis, (*) is a central extension i.e., $C(S,G)$ is central in $\widehat{G}_S$, see Section 4 below. We shall devote the next two sections to topological central extensions.

2. Topological Fundamental Group

A topological extension

$$(+) \qquad 1 \to \mathscr{C} \to \mathscr{E} \to \mathscr{G} \to 1 \ ,$$

of a locally compact and second countable topological group $\mathscr{G}$ by $\mathscr{C}$, with $\mathscr{E}$ locally compact and second countable, is a universal topological central extension (u.t.c.e.) of $\mathscr{G}$ if it is a central extension i.e., $\mathscr{C}$ is a closed central subgroup of $\mathscr{E}$, and given any topological central extension

$$1 \to C \to E \to \mathscr{G} \to 1 \ ,$$

with E locally compact and second countable, there is a *unique* continuous homomorphism $\varphi : \mathscr{E} \to E$ making the following diagram commutative

$$\begin{array}{ccccccccc} 1 & \to & \mathscr{C} & \to & \mathscr{E} & \to & \mathscr{G} & \to & 1 \\ & & \downarrow & & \downarrow \varphi & & \| & & \\ 1 & \to & C & \to & E & \to & \mathscr{G} & \to & 1 \ . \end{array}$$

It is clear that if $\mathscr{G}$ admits a u.t.c.e., the latter is unique upto natural equivalence. In case (+) is a u.t.c.e. of $\mathscr{G}$, $\mathscr{C}$ is by definition the *topological fundamental group* of $\mathscr{G}$ and it is denoted by $\pi_1(\mathscr{G})$. If $\mathscr{G}$ is a connected real semi-simple Lie group, then $\pi_1(\mathscr{G})$ coincides with the usual (algebraic topological) fundamental group of $\mathscr{G}$. It follows from certain results of Moore [20], that if $\mathscr{G}$ is *perfect* i.e. if it is its own commutator, and the cohomology group $H^2_m(\mathscr{G},\mathbf{R}/\mathbf{Z})$, based on measurable cochains, is finite, then $\mathscr{G}$ admits a u.t.c.e. and $\pi_1(\mathscr{G})$ is isomorphic to the dual of $H^2_m(\mathscr{G},\mathbf{R}/\mathbf{Z})$. It is also known that if $\mathscr{G}$ is totally disconnected, then the cohomology theory of $\mathscr{G}$ based on measurable cochains is identical with the theory based on continuous cochains [37].

If v is a nonarchimedean place where G is isotropic, then $G(k_v)$ is perfect (in fact any proper normal subgroup is central) and the cohomology group $H^2(G(k_v),\mathbf{R}/\mathbf{Z})$, defined in terms of continuous cochains, is essentially known:

Theorem 1. *Let v be a nonarchimedean place of k such that G is isotropic at v (or, equivalently, $G(k_v)$ is noncompact), then $H^2(G(k_v),\mathbf{R}/\mathbf{Z})$ is isomorphic to a subgroup, of index at most two, of the dual $\hat{\mu}(k_v)$ of the finite group $\mu(k_v)$ of roots of unity in k_v. Moreover, if at least one of the following three conditions holds, then it is isomorphic to $\hat{\mu}(k_v)$.*

(i) G is quasi-split over an odd degree extension of k_v;

(ii) k_v is not an extension of $\mathbf{Q}_2$;

(iii) k_v contains a primitive fourth root of unity.

As a consequence, if G is isotropic at v, then $G(k_v)$ admits a u.t.c.e. and $\pi_1(G(k_v))$ is isomorphic to the dual of $H^2(G(k_v), \mathbf{R}/\mathbf{Z})$.

It is expected that for any nonarchimedean place v where G is isotropic, $H^2(G(k_v), \mathbf{R}/\mathbf{Z})$ is isomorphic to $\hat{\mu}(k_v)$. For the spin group of a quadratic form over k which is of Witt index at least 2 at v, this is proved in [27, 1.9] and the same proof would take care of some other classical groups.

For the group SL_2 the above theorem is due to Moore [19]. For other Chevalley groups (i.e. groups which split over k) he proved that $H^2(G(k_v), \mathbf{R}/\mathbf{Z})$ is isomorphic to a subgroup of $\hat{\mu}(k_v)$, and about ten years later Deodhar [7] showed that this holds also when G is quasi-split over k_v (i.e. contains a Borel subgroup defined over k_v). Soon after Moore proved his result, Matsumoto showed, by constructing a suitable topological central extension of $G(k_v)$, that if G is a Chevalley group, the above cohomology group is actually isomorphic to $\hat{\mu}(k_v)$, and an observation of Deligne implies that this is also the case if G is quasi-split over k_v, see [28, §5]. Bak and Rehmann [1] have proved the above theorem, as well as Theorem 3 stated below, for groups of inner type A of relative rank $\geqq 2$ using K-theoretic methods.

In the generality stated above, the theorem is proved in [28] using the results of Moore, Matsumoto, Deodhar and Deligne and the Bruhat-Tits theory of reductive groups over nonarchimedean local fields. The complete proof of the above theorem is quite long and difficult and involves some case considerations. It is desirable to have a shorter and simpler proof.

The known results on $H^2(G(k_v), \mathbf{R}/\mathbf{Z})$ in case $G(k_v)$ is compact (or, equivalently, G is anisotropic at v) are summarised below.

Theorem 2. *Let v be a nonarchimedean place such that $G(k_v)$ is compact (then, as is well known, there is a central division algebra D_v over k_v such that $G(k_v)$ is isomorphic to the group $\mathrm{SL}_1(D_v)$ of elements of reduced norm 1 in D_v, and) the cohomology group $H^2(G(k_v), \mathbf{R}/\mathbf{Z})$, based on continuous cochains, is a finite group of order a power of p_v, where p_v is the characteristic of the residue field of k_v. It is cyclic if D_v is not the quaternion central division algebra over $\mathbf{Q}_2$ and is trivial if k_v does not contain a primitive p_v-th root of unity and D_v is not the quaternion central division algebra over $\mathbf{Q}_3$.*

This theorem is proved in [30]. The precise computation of $H^2(\mathrm{SL}_1(D_v), \mathbf{R}/\mathbf{Z})$ has not yet been done. We conjecture that it is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ if D_v is the quaternion central division algebra over $\mathbf{Q}_2$, it is isomorphic to $\mathbf{Z}/3\mathbf{Z}$ if D_v is the quaternion central division algebra over $\mathbf{Q}_3$, and is isomorphic to the p_v-primary component of the dual $\hat{\mu}(k_v)$ of the group of roots of unity in k_v in all other cases.

Remark. Theorems 1 and 2 imply that, for any finite set S of places of k, $H^2(G(A_S), \mathbf{R}/\mathbf{Z})$ is the direct product of the $H^2(G(k_v), \mathbf{R}/\mathbf{Z}), v \notin S$. If moreover $G(A_S)$ is perfect, then it admits a u.t.c.e. and its topological fundamental group is the direct sum (with discrete topology) of the $\pi_1(G(k_v)), v \notin S$; see [27, Theorem 2.4]. This implies that if $C(S, G)$ is central in $\widehat{G}_S$, then it is actually finite [27, §2].

3. The S-Metaplectic Kernel

Let $\mathscr{H}$ be a subgroup of a locally compact second countable topological group $\mathscr{G}$. Assume that $\mathscr{H}$ is perfect and $\mathscr{G}$ admits a u.t.c.e. Then there is a topological central extension

$$1 \to C \to E \to \mathscr{G} \to 1,$$

with E locally compact and second countable, which splits over $\mathscr{H}$ and which is universal with respect to this property. The *relative topological fundamental group* $\pi_1(\mathscr{G}, \mathscr{H})$ is then by definition the group C.

The *S-metaplectic kernel* is the group

$$M(S, G) = \operatorname{Ker}\left(H^2(G(A_S), \mathbf{R}/\mathbf{Z}) \xrightarrow{\text{rest}} H^2(G(k), \mathbf{R}/\mathbf{Z})\right);$$

where $H^2(G(k), \mathbf{R}/\mathbf{Z})$ denotes the second cohomology of the abstract group $G(k)$ with coefficients $\mathbf{R}/\mathbf{Z}$. The topological central extensions of $G(A_S)$ by $\mathbf{R}/\mathbf{Z}$, which split over the subgroup $G(k)$, are classified by the S-metaplectic kernel. It is obvious that if $G(k)$ is perfect, then $M(S, G)$ is isomorphic to the Pontrjagin dual of the relative fundamental group $\pi_1(G(A_S), G(k))$.

We now come back to the congruence subgroup problem. Assume that $G(k)$ is perfect and $C(S, G)$ is central in $\widehat{G}_S$ (see Section 4 below). Then adapting an argument of [2, §15] and using Theorem 1, it can be proved that (*) is the universal extension in the category of topological central extensions of $G(A_S)$ splitting over $G(k)$, see [27, §2]. In particular, $C(S, G)$ is isomorphic to the relative fundamental group $\pi_1(G(A_S), G(k))$ and so it is isomorphic to the Pontrjagin dual of the S-metaplectic kernel $M(S, G)$. Thus to determine the S-congruence kernel, it is enough to compute $M(S, G)$. Also, in the theory of automorphic forms (of fractional weights) it is of critical importance to know the topological central extensions of $G(A)$ which split over $G(k)$; these are determined by $M(\phi, G)$. Now we state the following theorem which "determines" $M(S, G)$ for all k-isotropic G.

Theorem 3. *Assume that G is isotropic over k. Let S be an arbitrary finite set of places of k. Then $M(S, G)$ is trivial if S contains either a nonarchimedean place, or a real place v such that the group $G(k_v)$ is not topologically simply connected. In general $M(S, G)$ is isomorphic to a subgroup of the dual $\hat{\mu}(k)$ of the group of roots of unity in k.*

For Chevalley groups this theorem was proved by Moore [19] and for groups which are quasi-split over k, it was proved by Deodhar [7]. For the group $G = \mathrm{SL}_2$, Moore in fact proved that $M(S, G)$ is trivial if S contains a noncomplex place and it is isomorphic to $\hat{\mu}(k)$ otherwise [1]. Soon after this, Matsumoto proved that for all Chevalley groups G, $M(S, G)$ is isomorphic to $\hat{\mu}(k)$ if S does not contain any noncomplex place. The same holds for any group which is quasi-split over k as was observed by Deligne. If either $S \supset V_\infty$ or k is a totally imaginary number field, the precise computation of $M(S, G)$ for the groups $\mathrm{SL}_n (n \geqq 3)$ and

[1] This result is equivalent to his theorem on the "uniqueness of the reciprocity law of global class field theory" – see [4] for an elegant proof of the latter.

$Sp_{2n}(n \geqq 2)$ is already in [2], and following the ideas of this paper, Vaserstein [35] computed the metaplectic kernel for many other classical groups. In 1981, Bak, in a Comptes Rendus note, outlined a proof of this theorem for all groups of classical type of relative rank at least two which uses the results of [1].

For arbitrary simply connected k-isotropic groups, the above theorem was proved by Prasad and Raghunathan in 1980 [27], and besides the results of Moore and Deodhar for split and quasi-split groups, the proof uses the results of [28] on topological central extensions of $G(k_v)$. Note that for a real place v, the condition that $G(k_v)$ is not topologically simply connected is equivalent to the condition imposed in [27, 3.4(ii)].

It is likely that if G is k-isotropic, $S \subset V_\infty$, and for every v in S, $G(k_v)$ is topologically simply connected, then $M(S, G)$ is isomorphic to $\hat{\mu}(k)$. This has been verified for many of the classical groups and some groups of exceptional types.

A variant of Moore's theorem on the "uniqueness of the reciprocity law", announced in [25], together with the results of [28, 30], can be used to compute $M(S, G)$, modulo 2-torsion, for all k-anisotropic G. For some results in this direction see [32].

4. Projective-Simplicity of $G(k)$ and Centrality of $C(S, G)$

It has been conjectured by Kneser, Platonov and Margulis that *if G is isotropic at each nonarchimedean place, then $G(k)$ is projectively-simple* i.e. it does not contain any proper noncentral normal subgroup, *and if it is anisotropic at some nonarchimedean place, then (as is well known, G is of type* A *and) any noncentral normal subgroup of $G(k)$ is the intersection of $G(k)$ with a normal subgroup of $\prod_{v \in \mathcal{S}} G(k_v)$, where $\mathcal{S}$ is the (finite) set of nonarchimedean places of k where G is anisotropic.* This conjecture is known to hold for all k-isotropic groups except possibly for certain *outer* forms of type E_6 of k-rank 1 which require division algebras of degree 3 for their construction. For anisotropic groups, the results are much less complete. In 1980, inspired by [22], Margulis [16] proved the above conjecture for groups of type A_1. This implies the projective-simplicity of the spin group of any quadratic form in 3 or 4 variables which is isotropic at all nonarchimedean places of k. Projective-simplicity of the spin group of any quadratic form in at least five variables was proved already in 1956 by Kneser [9] by an ingenious method. Borovoi and Chernousov have recently proved the projective-simplicity of $G(k)$ whenever G is of absolute rank at least two and it splits over a quadratic extension of k (this class includes all groups of type B, C, E_7, E_8, F_4 and G_2); and now Sury and Tomanov have independently established this for G of type A_3, which is isotropic at all nonarchimedean places – this implies the projective-simplicity of $G(k)$ for all groups G of type D (except the triality forms). But the anisotropic groups of (inner and outer type) A_n (n arbitrary) pose a serious challenge.

It may be of interest to note here that it follows from the well known result of Margulis [15] on normal subgroups of lattices [2] in semi-simple groups, and

[2] A *lattice* in a locally compact unimodular group is a discrete subgroup of finite covolume (with respect to any Haar measure).

the strong approximation property, that any noncentral normal subgroup of $G(k)$ is of finite index in $G(k)$ (see, for example, [23]). Moreover, it is easy to show that if G is isotropic at all the nonarchimedean places of k and has the congruence subgroup property for some S, then $G(k)$ is projectively-simple.

Based on the results of [2, 33] on SL_n and Sp_{2n}, and [18], where the centrality of the S-congruence kernel was proved for all Chevalley groups of rank $\geqq 2$, it has been conjectured that for arbitrary (simply connected) G, $C(S,G)$ *is central in* $\widehat{G}_S$ *if* $\sum_{v\in S} k_v\text{-rank}(G) \geqq 2$ *and* G *is isotropic at all nonarchimedean* $v \in S$. Using some of the ideas of [2, 33], Vaserstein [35] showed that this conjecture holds for all classical groups of k-rank at least two. Raghunathan has proved the above conjecture for all k-isotropic groups [31]; his proof does not require any case-by-case analysis.

For the spin group of an arbitrary (not necessarily isotropic) quadratic form in at least five variables the above conjecture on the centrality of $C(S,G)$ was proved by Kneser [10]. Refining and using his ideas, Rapinchuk and Tomanov have recently proved the conjecture for all anisotropic groups of type $\mathsf{B}_r (r \geqq 2)$, $\mathsf{C}_r (r \geqq 2)$, $\mathsf{D}_r (r \geqq 5)$, E_7, E_8, F_4, G_2, and the groups of type ${}^2\mathsf{A}_r (r \geqq 3)$ which split over a quadratic extension of k. The question of centrality of the S-congruence kernel for anisotropic groups of type A is a very interesting open problem–its solution may require new insight into the structure and geometry of central division algebras over global fields.

5. The Hasse Principle and Tamagawa Number

If k is a global function field, then the Galois cohomology $H^1(k,G)$ is trivial (this was proved by Harder). On the other hand, if k is a number field, it has been known for quite some time that the "Hasse principle" i.e., the assertion that the natural morphism

$$H^1(k,G) \to \prod_{v \in V_\infty} H^1(k_v, G)$$

is injective, holds for all (simply connected) G of type other than E_8. The Hasse principle has now been verified for groups of type E_8 by Chernousov [5].

If k is number field, let D_k be the absolute value of the discriminant of $k/\mathbf{Q}$ and if k is a global function field, let q_k be the cardinality of its field of constants, g_k the genus of k and $D_k = q_k^{2g_k-2}$.

Let ω be an invariant exterior form on G, of maximal degree, defined over k. Then for each place v, the form ω , and the normalized Haar measure on k_v, determine a Haar measure on $G(k_v)$ which we denote by ω_v.

Let $P = (P_v)_{v \in V_f}$ be a fixed *coherent* collection of parahoric subgroups: for each $v \in V_f, P_v$ is a parahoric subgroup of $G(k_v)$ such that the product $\prod_{v\in V_\infty} G(k_v) \cdot \prod_{v \in V_f} P_v$ is an open subgroup of $G(A)$. (Recall that a subgroup of $G(k_v)$ is said to be an *Iwahori subgroup* if it is the normalizer of a maximal pro-p_v subgroup of $G(k_v)$ or, equivalently, it is the stabilizer of a chamber (i.e. a simplex of maximal dimension) in the Bruhat-Tits building of $G(k_v)$. Any subgroup containing an Iwahori subgroup is called a *parahoric subgroup.*) It is known that, as G is semi-simple, the product $\prod \omega_v(P_v)$ is absolutely convergent and so there is a Haar measure μ on $G(A)$ which on the open subgroup $\prod_{v\in V_\infty} G(k_v)\cdot\prod_{v\in V_f} P_v$ coincides with the measure $D_k^{-\frac{1}{2}\dim G}\prod_{v\in V_\infty}\omega_v\cdot\prod_{v\in V_f}\omega_v|_{P_v}$. It is obvious from the product formula (i.e. $\prod_v |x|_v = 1$ for $x\in k^\times$) that the measure μ is independent of the k-form ω and it is called the *Tamagawa measure.* The *Tamagawa number* of G/k, to be denoted $\tau_k(G)$, is the positive real number $\mu(G(A)/G(k))$. It was conjectured by Weil that for all (simply connected absolutely almost simple) $G, \tau_k(G) = 1$. This conjecture has recently been proved by Kottwitz, over number fields, without any case-by-case considerations (see [11], and also [26, 3.3]). Using Arthur's trace formula and the Hasse principle, he has in fact shown that if k is a number field and $\mathscr{G}$ is the unique quasi-split *inner* k-form of G, $\tau_k(G) = \tau_k(\mathscr{G})$; this result was conjectured by Langlands. Now since the Tamagawa number of any simply connected quasi-split group is 1 [12, 13], Weil's conjecture follows.

Weil's conjecture remains unproven for groups defined over global function fields. It is still unknown, for example, if over such a k, the Tamagawa number of every outer k-form of type A is 1.

6. Covolumes of S-Arithmetic Subgroups, Bound for Class Numbers and the Finiteness Theorems

We shall now describe a formula for the covolume of S-arithmetic subgroups with respect to a natural Haar measure on G_S. We begin by describing a natural Haar measure μ_v on $G(k_v)$ for any place v of k. For a nonarchimedean place v of k, let μ_v be the Tits measure on $G(k_v)$ i.e. the Haar measure with respect to which the volume of any Iwahori subgroup of $G(k_v)$ is 1. If v is archimedean, then k_v is either $\mathbf{R}$ or $\mathbf{C}$ and μ_v is the Haar measure on $G(k_v)$ such that, in the induced measure, any maximal compact subgroup of $R_{k_v/\mathbf{R}}(G)(\mathbf{C})$ has volume 1. Now on $G_S = \prod_{v\in S} G(k_v)$ we take the product measure $\mu_S := \prod_{v\in S}\mu_v$.

Let $\mathscr{G}$ be the unique quasi-split *inner* k-form of G. For each nonarchimedean place v, we fix a parahoric subgroup $\mathscr{P}_v$ of $\mathscr{G}(k_v)$ of maximal volume such that $\prod_{v\in V_\infty}\mathscr{G}(k_v)\cdot\prod_{v\in V_f}\mathscr{P}_v$ is an open subgroup of $\mathscr{G}(A)$.

As in Section 5, let $P = (P_v)_{v\in V_f}$ be a fixed coherent collection of parahoric subgroups. Let S be a finite set of places containing V_∞ and let $\Lambda = G(k)\cap\prod_{v\notin S} P_v$. In its natural embedding in G_S, Λ is an S-arithmetic subgroup. Let G_v denote the smooth affine $\mathfrak{o}_v$-group scheme associated with the parahoric subgroup P_v by the Bruhat-Tits theory ([34, 3.4]). Let $\overline{G}_v := G_v\otimes_{\mathfrak{o}_v}\mathfrak{f}_v$ be the reduction mod $\mathfrak{p}_v$ of G_v. Let $\overline{T}_v$ be a maximal $\mathfrak{f}_v$-torus of $\overline{G}_v$ containing a maximal $\mathfrak{f}_v$-split torus and $\overline{M}_v$ be the maximal reductive $\mathfrak{f}_v$-subgroup containing $\overline{T}_v$. Note that $\overline{M}_v$ depends on the choice of P_v. Let $\overline{\mathscr{G}}_v, \overline{\mathscr{T}}_v$ and $\overline{\mathscr{M}}_v$ be similarly defined $\mathfrak{f}_v$-groups associated with $\mathscr{G}$ and the parahoric subgroup $\mathscr{P}_v$.

If $\mathscr{G}/k$ is not a triality form of type ${}^6\mathsf{D}_4$, let ℓ be the smallest extension of k over which $\mathscr{G}$ splits. If $\mathscr{G}/k$ is of type ${}^6\mathsf{D}_4$, let ℓ be a fixed extension of k of degree 3 contained in the Galois extension of degree 6 over which $\mathscr{G}$ splits. Let D_ℓ be the absolute value of the discriminant of $\ell/\mathbf{Q}$ if k is a number field and

$D_\ell = q_\ell^{2g_\ell - 2}$ if k is a global function field, where q_ℓ is the cardinality of the finite field of constants in ℓ and g_ℓ is the genus of ℓ.

The integer $\mathfrak{s}(\mathcal{G})$: If $\mathcal{G}$ splits over k, let $\mathfrak{s}(\mathcal{G}) = 0$. If $\mathcal{G}$ is a k-form of type ${}^2\mathsf{A}_r$, with r even, let $\mathfrak{s}(\mathcal{G}) = \frac{1}{2}r(r+3)$; if $\mathcal{G}$ is a k-form of type ${}^2\mathsf{A}_r$ (r odd), ${}^2\mathsf{D}_r$ (r arbitrary) or ${}^2\mathsf{E}_6$, let $\mathfrak{s}(\mathcal{G}) = \frac{1}{2}(r-1)(r+2), 2r-1$ or 26 respectively. If $\mathcal{G}$ is a triality form of type ${}^3\mathsf{D}_4$ or ${}^6\mathsf{D}_4$, then let $\mathfrak{s}(\mathcal{G}) = 7$.

The following theorem provides a "computable" formula for the volume of S-arithmetic quotients of G_S. It is proved in [26] .

Theorem 4. *Let $m_1 \leqq \cdots \leqq m_r$ be the exponents of the Weyl group of the absolute root system of G. Then*

$$\mu_S(G_S/\Lambda) = D_k^{\frac{1}{2}\dim G}(D_\ell/D_k^{[\ell:k]})^{\frac{1}{2}\mathfrak{s}(\mathcal{G})}\left(\prod_{v\in V_\infty}\left|\prod_{i=1}^{r}\frac{m_i!}{(2\pi)^{m_i+1}}\right|_v\right)\tau_k(G)\mathcal{E}(P)\ ;$$

where

$$\mathcal{E}(P) = \prod_{v\in S_f}\frac{q_v^{(r_v+\dim\overline{\mathcal{M}}_v)/2}}{\#\overline{T}_v(\mathfrak{f}_v)}\cdot\prod_{v\notin S}\frac{q_v^{(\dim\overline{M}_v+\dim\overline{\mathcal{M}}_v)/2}}{\#\overline{M}_v(\mathfrak{f}_v)}\ ,$$

$S_f = S\cap V_f$, and for $v\in V_f$, $r_v(=\dim\overline{T}_v)$ is the rank of G over the maximal unramified extension of k_v.

The results involved in the proof of this theorem provide the following lower bound for the class number of simply connected anisotropic groups (see [26, Theorem 4.3]).

Theorem 5. *Assume that G is anisotropic over k and moreover $G_\infty := \prod_{v\in V_\infty}G(k_v)$ is compact. Then the class number $\#\left(G_\infty\prod_{v\in V_f}P_v\backslash G(A)/G(k)\right)$ of G/k with respect to P is at least*

$$D_k^{\frac{1}{2}\dim G}(D_\ell/D_k^{[\ell:k]})^{\frac{1}{2}\mathfrak{s}(\mathcal{G})}\left(\prod_{v\in V_\infty}\left|\prod_{i=1}^{r}\frac{m_i!}{(2\pi)^{m_i+1}}\right|_v\right)\tau_k(G)\zeta(P)\ ;$$

where

$$\zeta(P) = \prod_{v\in V_f}\frac{q_v^{(\dim\overline{M}_v+\dim\overline{\mathcal{M}}_v)/2}}{\#\overline{M}_v(\mathfrak{f}_v)}\ .$$

In [3, §7] this theorem is used to prove the following finiteness theorem.

Theorem 6. *Given a positive integer c, let $\mathcal{C}_c$ be the set of pairs (k, G) consisting of a number field k and a connected, simply connected absolutely almost simple group G such that G is anisotropic over k, $G_\infty := \prod_{v\in V_\infty}G(k_v)$ is compact, and the class number $\#\left(G_\infty\prod_{v\in V_f}P_v\backslash G(A)/G(k)\right)$ of G/k with respect to some coherent collection of parahoric subgroups $(P_v)_{v\in V_f}$ is less than c. Then (up to natural equivalence) $\mathcal{C}_c$ is finite.*

The formula for the volume of S-arithmetic quotients given above and certain number theoretic estimates have been used in [3] to prove that in characteristic zero, there are only finitely many distinct S-arithmetic subgroups Γ of covolume $\leqq c$, where c is a given positive number. Also, there are only finitely many S-arithmetic Γ with $0 \neq |\chi(\Gamma)| < c$, where $\chi(\Gamma)$ is the Euler-Poincaré characteristic of Γ in the sense of C. T. C. Wall. For precise results, see [3].

7. Super-Rigidity and Arithmeticity of Lattices

According to a celebrated theorem of Margulis (annonced at the ICM held in 1974), *irreducible* lattices [3] in real semi-simple groups of **R**-rank > 1 are super-rigid[4]. It follows rather easily from this that such lattices are arithmetic. On the other hand, it has been known for almost thirty years that the groups $\mathrm{SO}(n,1)$ contain non-arithmetic lattices for $n \leqq 5$. In 1986, Gromov and Piatetski-Shapiro, employing a nice geometric construction, showed that for each n, $\mathrm{SO}(n,1)$ contains plenty of non-arithmetic lattices([8]). Mostow has constructed non-arithmetic lattices in $\mathrm{SU}(2,1)$ and $\mathrm{SU}(3,1)$; however, whether lattices in $\mathrm{SU}(n,1)$ are all arithmetic if n is sufficiently large is still an open question.

Corlette [6] has now established the super-rigidity of real representations of *cocompact* discrete subgroups in the remaining semi-simple groups of **R**-rank 1, namely the groups $\mathrm{Sp}(n,1)$ and the **R**-rank 1 form of type F_4, using his basic theorem on the existence of a harmonic map in any given homotopy class of maps from a compact riemannian manifold into a locally symmetric space; and just a few weeks ago I have learnt that Gromov and Schoen have proved that any representation of such a discrete cocompact subgroup over a p-adic field is bounded by developing an analogue of the theory of harmonic maps for maps from a riemannian manifold into a Bruhat-Tits building. Now, as in the case of groups of **R**-rank > 1, arithmeticity of cocompact discrete subgroups of the groups $\mathrm{Sp}(n,1)$ and the **R**-rank 1 form of type F_4 follows.

Acknowledgements. I thank the University of Michigan for inviting me to deliver the Fall 1989 Keeler lectures, and Mr. M.S. Keeler for instituting this lectureship. This address is in part based on my Keeler lectures. I also thank the Japan Association for Mathematical Sciences for financial support to attend the ICM.

References

1. Bak, A., Rehmann, U.: The congruence subgroup and metaplectic problems for $\mathrm{SL}_{n\geqq 2}$ of division algebras. J. Alg. **78** (1982) 475–547
2. Bass, H., Milnor, J., Serre, J–P.: Solution of the congruence subgroup problem for SL_n and Sp_{2n}. Publ. Math. IHES **33** (1967) 59-137

[3] A lattice in a semi-simple linear analytic group is said to be *irreducible* if no subgroup of it of finite index is a direct product of two infinite normal subgroups.

[4] For a detailed proof see [17]. Super-rigidity and arithmeticity in arbitrary characteristic has been proved in [36].

3. Borel, A., Prasad, G.: Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups. Publ. Math. IHES **69** (1989) 119–171; Addendum: *ibid* **71** (1990)
4. Chase, S., Waterhouse, W.: Moore's theorem on uniqueness of reciprocity laws. Invent. math. **16** (1972) 267–270
5. Chernousov, V.: On the Hasse principle for groups of type E_8. Soviet Math. Dokl.**39** (1989)
6. Corlette, K.: Archimedean super-rigidity and hyperbolic geometry (preprint)
7. Deodhar, V.: On central extensions of rational points of algrebaic groups. Amer. J. Math. **100** (1978) 303–386
8. Gromov, M., Piatetski-Shapiro, I.: Non-arithmetic groups in Lobachevsky spaces. Publ. Math. IHES **66** (1988) 93–103
9. Kneser, M.: Orthogonale Gruppen über algebraischen Zahlkörpern. J. Reine Angew. Math. **196** (1956) 213–220
10. Kneser, M.: Normalteiler ganzzahliger Spingruppen. J. Reine Angew. Math. **311/312** (1979) 191–214
11. Kottwitz, R.: Tamagawa numbers. Ann. Math. **127** (1988) 629–646
12. Langlands, R.: The volume of the fundamental domain. Proc. AMS Symp. Pure Math. **9** (1966) 143–148
13. Lai, K.: Tamagawa number of reductive algebraic groups. Compos. Math. **41** (1980) 153–188
14. Margulis, G.: Cobounded subgroups of algebraic groups over local fields. Funct. Anal. Appl. **11** (1977) 119–128
15. Margulis, G.: Finiteness of quotient groups of discrete subgroups. Funct. Anal. Appl. **13** (1979) 178–187
16. Margulis, G.: On the multiplicative group of a quaternion algebra over a global field. Soviet Math. Dokl. **21** (1980) 780–784
17. Margulis, G.: Arithmeticity of the irreducible lattices in the semi-simple groups of rank greater than 1. Invent. math. **76** (1984) 93–120
18. Matsumoto, H.: Sur les sous-groupes arithmétiques des groupes semi-simples déployés. Ann. Sci. École Norm. Sup., 4^e^ sér. **2** (1969) 1–62
19. Moore, C.: Group extensions of p-adic and adelic linear groups. Publ. Math. IHES **35** (1968) 157–222
20. Moore, C.: Group extensions and cohomology for locally compact groups, III and IV. Transactions AMS **221** (1976) 1–58
21. Platonov, V.: The problem of strong approximation and the Kneser-Tits conjecture. Math. USSR Izv. **3** (1969) 1139–1147; Addendum: *ibid* **4** (1970) 784–786
22. Platonov, V., Rapinchuk, A.: On the group of rational points of three-dimensional groups. Soviet Math. Dokl. **20** (1979) 693–697
23. Prasad, G.: Strong approximation. Ann. Math. **105** (1977) 553–572
24. Prasad, G.: Elementary proof of a theorem of Bruhat-Tits and Rousseau. Bull. Soc. Math. France **110** (1982) 197–202
25. Prasad, G.: A variant of a theorem of Calvin Moore. C. R. Acad. Sci. (Paris) Sér. I **302** (1982) 405–408
26. Prasad, G.: Volumes of S-arithmetic quotients of semi-simple groups. Publ. Math. IHES **69** (1989) 91–117
27. Prasad, G., Raghunathan, M.S.: On the congruence subgroup problem: Determination of the "metaplectic kernel". Invent. math. **71** (1983) 21–42
28. Prasad, G., Raghunathan, M.S.: Topological central extensions of semi-simple groups over local fields. Ann. Math. **119** (1984) 143–268
29. Prasad, G., Raghunathan, M.S.: On the Kneser-Tits problem. Comment. Math. Helv. **60** (1985) 107–121

30. Prasad, G., Raghunathan, M.S.: Topological central extensions of $SL_1(D)$. Invent. math. **92** (1988) 645–689
31. Raghunathan, M.S.: On the congruence subgroup problem. Publ. Math. IHES **46** (1976) 107–161; second part: Invent. math. **85** (1986) 73–117
32. Rapinchuk, A.: Multiplicative arithmetic of division algebras over number fields and the metaplectic problem. Math. USSR Izv. **31** (1988) 349–379
33. Serre. J–P.: Le problème des groupes de congruence pour SL_2. Ann. Math. **92** (1970) 489-527
34. Tits, J.: Reductive groups over local fields. Proc. AMS Symp. Pure Math. **33** (1979), part 1, 29–69
35. Vaserstein, L.: The structure of classical arithmetic groups of rank greater than one. Math. USSR Sb. **20** (1973) 465–492
36. Venkataramana, T.: On super-rigidity and arithmeticity of lattices in semi-simple groups over local fields of arbitrary characteristic. Invent. math. **92** (1988) 255–306
37. Wigner, D.: Algebraic cohomology of topological groups. Transactions AMS **178** (1973) 83–93