Arithmetic Groups

JAMES E. HUMPHREYS

1. LATTICES IN LIE GROUPS

Arithmetic groups arise naturally as discrete subgroups of Lie groups, defined by arithmetic properties. In this lecture I want to describe some of the possibilities, especially when the Lie group is semisimple. For a comprehensive treatment, Raghunathan's book [22] would be a natural starting point (to be supplemented by more recent research papers).

(1.1) Let G be a connected Lie group. By a lattice in G is meant a discrete subgroup Γ for which G/Γ has finite measure (induced by Haar measure on G). There are two very different cases to consider: Γ is uniform (or cocompact) if G/Γ is compact, nonuniform otherwise. For example, the standard lattice $\mathbb{Z}^n$ in $\mathbb{R}^n$ is uniform, while $SL_n(\mathbb{Z})$ is a nonuniform lattice in $SL_n(\mathbb{R})$.

Both of the examples just mentioned have an obvious arithmetic flavor. To be more precise, we have to consider

a Lie group G which arises as the topological identity component $\underline{G}(\mathbb{R})^\circ$ in the $\mathbb{R}$-points $\underline{G}(\mathbb{R})$ of an algebraic group $\underline{G}$ defined over $\mathbb{Q}$ (or other number field). Many familiar Lie groups do arise in this way. If $\underline{G}$ is embedded in some general linear group GL_n, then $G \cap GL_n(\mathbb{Z})$ is often a lattice in G(e.g., when $\underline{G}$ is semisimple, by results of Borel and Harish-Chandra). Whether it is a lattice or not, $G \cap GL_n(\mathbb{Z})$ or any commensurable subgroup of $\underline{G}(\mathbb{Q})$ is called an arithmetic subgroup of G. (Recall that two groups are commensurable if their intersection has finite index in each.) We will stick to the case of groups defined over $\mathbb{Q}$; the process of "restriction of scalars" often makes this the essential case.

Several questions can be posed right away:

(1) Does a given Lie group G contain both uniform and nonuniform lattices?

(2) If G has the form $\underline{G}(\mathbb{R})^\circ$ for a $\mathbb{Q}$-group $\underline{G}$, are its arithmetic subgroups actually lattices? If so, is every lattice in G of this type?

(3) What group-theoretic properties does a lattice (or arithmetic group) Γ have? Is Γ finitely generated (f.g.)? finitely presented (f.p.)? torsion-free? What are its normal subgroups? (These questions, or others of a cohomological nature, can often be studied effectively in the context of G and its homogeneous spaces.)

Remark. "Arithmetic groups" also arise in the setting

of algebraic groups over global function fields. In another direction, one can study "S-arithmetic" subgroups, where S is a finite set of valuations including all archimedean ones.

(1.2) Lattices in solvable Lie groups have been rather thoroughly studied (cf. [22, Ch. II-IV]). To list a few of the key results, due to Mal'cev, L. Auslander, Mostow, and others, it is convenient to assume that G is simply connected (s.c.); the general case can usually be reduced to this one.

(1) Let G be a s.c. nilpotent Lie group. Then G has a lattice subgroup iff the Lie algebra of G has a basis with rational structure constants. (The idea of the proof is to obtain a lattice by exponentiating the $\mathbb{Z}$-span of such a basis.)

(2) An abstract group Γ is isomorphic to a lattice in some s.c. nilpotent Lie group iff Γ is f.g., torsion-free, nilpotent.

(3) All lattices in a s.c. nilpotent Lie group are uniform and arithmetically defined.

(4) All lattices in a s.c. solvable Lie group are uniform, but not necessarily arithmetically defined.

(5) A lattice in a s.c. solvable Lie group is polycyclic (hence f.g.). Any polycyclic group has a normal subgroup of finite index which is isomorphic to such a lattice. (Here the idea is to embed the given polycyclic

group in some $GL_n(\mathbb{Z})$ and then study its Zariski closure in $GL_n(\mathbb{C})$.)

(6) Given a lattice Γ in a s.c. solvable Lie group G, there is a faithful representation $f:G \to GL_n(\mathbb{R})$ for which $f(\Gamma) \subset GL_n(\mathbb{Z})$.

The results (2) and (5) suggest how Lie groups or algebraic groups may be profitably used to study polycyclic groups. (Cf. the recent work of F. Grunewald - P.F. Pickel - D. Segal, S. Donkin, and others.)

(1.3) The study of lattices in semi-simple Lie groups is in some respects far more complicated than in the solvable case. Lattices still turn out to be f.g. (which allows one eventually to conclude that all lattices in Lie groups are f.g. [22, 13.21]), but they may or may not be uniform. Borel showed that when G is noncompact, G has both uniform and nonuniform lattices (cf. [22, Ch. XIV]). The proof reduces quickly to the case of a simple group G isomorphic to its adjoint group. Then the idea is to find an auxiliary algebraic group $\underline{G}$ over $\mathbb{Q}$ and an epimorphism $f:\underline{G}(\mathbb{R})^\circ = G' \to G$ with compact kernel. By locating suitable arithmetic subgroups Γ' of G' with G'/Γ' compact (resp. noncompact), one gets lattices $\Gamma = f(\Gamma')$ of the desired types in G. The construction here is rather subtle. For example, to make G'/Γ' noncompact, it is essential to have a nontrivial unipotent element in Γ',

which depends on having a nonzero nilpotent element in a suitable $\mathbb{Q}$-form of the Lie algebra. Of course, in a special case like $G = SL_n(\mathbb{R})$, one might argue directly that the arithmetic subgroup $SL_n(\mathbb{Z})$ is a nonuniform lattice (cf. [8] or [10]). But even here it is difficult to exhibit straightforwardly a uniform lattice, without use of a larger auxiliary group G'.

(1.4) As noted above, Borel's proof of the existence of both kinds of lattices in a semisimple Lie group is based on a construction of arithmetic groups. The question remains: Must all lattices be obtained in this way? To make the question precise (and to avoid uninteresting technicalities), we formulate a definition: Let G be a connected semisimple Lie group, G^* its adjoint group, $p: G \to G^*$ the canonical map. A lattice Γ in G is said to be <u>arithmetic</u> if there exists an algebraic group $\underline{G}'$ over $\mathbb{Q}$, with an arithmetic subgroup $\Gamma' \subset \underline{G}'(\mathbb{Q})$ and an epimorphism $f: \underline{G}'(\mathbb{R})^\circ \to G^*$ such that $\operatorname{Ker} f$ is compact and $f(\Gamma')$ has finite index in $p(\Gamma)$.

For certain semisimple groups of $\mathbb{R}$-rank 1, such as $SO(2,1) \cong PSL_2(\mathbb{R})$, our question actually has a negative answer: <u>There exist non-arithmetic lattices (both uniform and nonuniform)</u>. Examples involving $SO(n,1)$ $(n \leq 5)$ were first discovered by Makarov and Vinberg, while Mostow [17,18] has recently found others in the groups $SU(n,1)$

($n \leq 3$). It remains to be seen whether such examples also occur in the groups $Sp(n,1)$ and whether they are limited to low dimensions.

(1.5) For semisimple Lie groups of $\mathbb{R}$-rank ≥ 2, it was conjectured first by Selberg (in the uniform case) and later by Pyatetski-Shapiro (in the general case) that all "irreducible" lattices are arithmetic. (A lattice is irreducible if its projection to any nontrivial proper factor is non-discrete: this rules out obvious counter-examples involving products of rank 1 groups.) The first complete proofs of these conjectures were given by Margulis (cf. [12], [13], [30]), using a dazzling array of techniques. Here is a very brief indication of how he proceeds in [13].

ARITHMETICITY THEOREM. Let $\underline{G}$ be a connected semisimple algebraic group over $\mathbb{R}$, of $\mathbb{R}$-rank ≥ 2, and assume $G = \underline{G}(\mathbb{R})^\circ$ has no compact factors. Then any irreducible lattice Γ in G is arithmetic.

SUPERRIGIDITY THEOREM. Let G be as in the Arithmeticity Theorem, Γ an irreducible lattice in G. Let k be any local field of characteristic 0 ($\mathbb{R}$, $\mathbb{C}$, or a finite extension of $\mathbb{Q}_p$). Let $\underline{F}$ be a connected semisimple k-group without center, $\phi: \Gamma \to \underline{F}(k)$ a homomorphism such that $\phi(\Gamma)$ is Zariski dense in $\underline{F}$. Then: (i) If $k \neq \mathbb{R}, \mathbb{C}$, $\phi(\Gamma)$ is

relatively compact in the k-topology. (ii) If $k = \mathbb{R}$ or $\mathbb{C}$, then $\underline{F} = \underline{F}_1 \times \underline{F}_2$, a product of k-groups, where $pr_1(\phi(\Gamma))$ is relatively compact in the k-topology and $pr_2 \circ \phi : \Gamma \to \underline{F}_2$ extends to a rational homomorphism $\underline{G} \to \underline{F}_2$.

Although its formulation is technical looking, the second theorem implies the first and has other far-reaching implications (e.g., for the study of isomorphisms between simple algebraic groups over various arithmetic rings). For the proof, Margulis draws together a wide range of methods: ergodic theory, function spaces,.... Once established, it can be invoked (in several different ways) in the proof of the Arithmeticity Theorem. For example, at one stage it is known that, for the given lattice Γ, there exists a centerless semisimple matrix group $\underline{H}$ over $\mathbb{Q}$ and a monomorphism $\alpha : \Gamma \to \underline{H}(\mathbb{Q})$ with Zariski dense image. After composing with the inclusion into $\underline{H}(\mathbb{Q}_p)$, the Superrigidity Theorem forces the image of Γ to be relatively compact in the $\mathbb{Q}_p$-topology, for each prime p. This means that the powers of p in denominators of matrix entries in $\alpha(\Gamma)$ are bounded. But Γ is f.g., so the denominators in question can involve only finitely many primes. Combining these statements, $\alpha(\Gamma) \cap \underline{H}(\mathbb{Z})$ has finite index in $\alpha(\Gamma)$. This is a major step toward proving that Γ is arithmetic.

We should mention a further striking consequence of Margulis' methods: With G and Γ as above, <u>each noncentral</u>

normal subgroup of Γ is of finite index. Earlier results of this type mostly depended on having a positive solution to the congruence subgroup problem.

2. FINITE GENERATION AND FINITE PRESENTATION

Given an arithmetic group Γ, it is natural to ask whether Γ is finitely generated (f.g.) and, if so, whether it is in fact finitely presented (f.p.). These questions can sometimes be answered positively by exhibiting generators and relations; but in other cases only a qualitative or indirect proof is available. And in a few situations, negative answers turn up.

(2.1) Consider a very classical example: the group $\Gamma = PSL_2(\mathbb{Z})$, or its close relative $\hat{\Gamma} = SL_2(\mathbb{Z})$, cf. [19, Ch. VIII]. Let $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $\hat{\Gamma}$, with respective images s,t,u in Γ. Note that $T = SU$. From linear algebra one knows that $\hat{\Gamma}$ is generated by S and U (or equivalently, by S and T). So Γ is generated by the elements s, t of respective finite orders 2,3. In fact, Γ is the free product of the cyclic groups they generate. To see this, it is easier to work in $\hat{\Gamma}$. It has to be shown that $A = \pm T^a S T^{e_1} S \ldots T^{e_n} S^b$ can never reduce to $\pm I$ (where $a,b \in \{0,1\}$ and $e_i \in \{1,2\}$). By rearranging, we may assume $a = b = 0$, so $A = \pm S T^{e_1} \ldots S T^{e_n}$. Now it is enough to show

that no nontrivial word in the semigroup generated by $ST = -\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $ST^2 = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$ reduces to $\pm I$. But note that for each $Z = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ in this semigroup, $(ST)Z = -\begin{pmatrix}a+c & b+d\\ c & d\end{pmatrix}$ while $(ST^2)Z = \begin{pmatrix}a & b\\ a+c & b+d\end{pmatrix}$. By induction, all entries of Z have like sign. It follows that if Z has a nonzero entry off the diagonal (which ST and ST^2 both do), the same is true for these longer words. So we can never reach $\pm I$.

(2.2) Nielsen found a finite presentation for $SL_3(\mathbb{Z})$, to which Magnus later reduced the case of $SL_n(\mathbb{Z})$ for $n \geq 3$. In a modern guise, this fits into the computation of $K_2\mathbb{Z}$ by Silvester-Milnor: $SL_n(\mathbb{Z})$ $(n \geq 3)$ is generated by the elementary matrices $E_{ij}(i \neq j)$, where E_{ij} has 1 in the (i,j) position and on the diagonal, but 0 elsewhere, subject only to the relations: $(E_{ij},E_{k\ell}) = 1$ if $j \neq k$, $i \neq \ell$; $(E_{ij},E_{jk}) = E_{ik}$ if i,j,k are distinct; $(E_{12}E_{21}^{-1}E_{12})^4 = 1$. The first two relations alone define a central extension $St_n(\mathbb{Z}) \to SL_n(\mathbb{Z})$, with kernel $K_2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$. (The covering group is called the Steinberg group.)

Other Chevalley groups $\underline{G}(\mathbb{Z})$ such as $Sp_{2n}(\mathbb{Z})$ were subsequently studied by Klingen, Wardlaw, Behr, Hurrelbrink-Rehmann, culminating in the explicit presentations of Behr [6]. He views $\underline{G}(\mathbb{Z})$ as an amalgamated product of rank 2 parabolic subgroups, via the action of $\underline{G}(\mathbb{Z})$ on a simplicial complex introduced by Soulé. Then the rank 2 cases $SL_3(\mathbb{Z})$, $Sp_4(\mathbb{Z})$, and $G_2(\mathbb{Z})$ can be plugged in.

Relatively few groups over other arithmetic rings have been treated as explicitly as these groups over $\mathbb{Z}$: mainly SL_2 over rings of integers of imaginary quadratic extensions of $\mathbb{Q}$, cf. Swan [29]. In [20] O'Meara proved that certain of the groups GL_n, SL_n over Hasse domains (rings of S-integers in global fields of arbitrary characteristic)are at least f.g.

(2.3) If one is willing to settle for less explicit information about generators and relations, far more general arithmetic (and S-arithmetic) groups can be shown to be f.p. by the reduction theory of Borel, Harish-Chandra (cf.[8], [10]). The idea is to start with a semisimple group $\underline{G}$ over $\mathbb{Q}$, with $\Gamma = \underline{G}(\mathbb{Z})$ or other arithmetic subgroup acting on a homogeneous space X of the Lie group $\underline{G}(\mathbb{R})$. There is an open "Siegel set" in X approximating a fundamental domain for the action of Γ. Then a simple lemma produces (in principle) a finite generating set in Γ:

LEMMA. Let X be a connected topological space, acted on by a group Γ(on the right). Let U be open in X, with $U.\Gamma = X$. Then the set $\Delta = \{\gamma \in \Gamma \mid U.\gamma \cap U \neq \phi\}$ generates Γ.

(The proof is easy: Let Γ' be the subgroup generated by Δ, so $U.\Gamma'$ is open. If $U.\gamma \cap U.\gamma' \neq \phi$ for $\gamma \in \Gamma$, $\gamma' \in \Gamma'$, we get $\gamma \in \Delta\gamma' \subset \Gamma'$. Since X is connected, this forces $U.\Gamma' = X$, whence $\Gamma' = \Gamma$.)

That Δ is <u>finite</u> in the case of our arithmetic group

is the hard thing to prove, and the proof gives little insight into the nature of Δ even for familiar groups Γ. (It is somewhat like proving that class numbers are finite without actually calculating them.)

Behr [4] went on to show that the group Γ above is in fact f.p., where the relations involving elements of Δ are the "obvious" ones (cf. [10,13.4]). By using the Bruhat-Tits theory of reductive groups over local fields, Kneser and Behr were also able to treat S-arithmetic groups in a similar spirit.

(2.4) For arithmetic subgroups of algebraic groups over number fields, the methods of Borel, Harish-Chandra, Behr lead to positive results about finite presentability. But for groups over function fields, there are some negative results, and in general the terrain has been less well explored.

Here is a brief survey of the best studied situation: $\underline{G}$ is a Chevalley group (scheme), usually assumed to be simply connected, e.g., SL_n or Sp_{2n}. K is a function field in one variable over $\mathbb{F}_q$, such as $\mathbb{F}_q(t)$ with t transcendental. S is a finite nonempty set of primes of K, and O_S is the ring of S-integers in K(e.g., $\mathbb{F}_q[t]$ or $\mathbb{F}_q[t,t^{-1}]$ in case $|S| = 1$ or 2, $K = \mathbb{F}_q(t)$). Finally, $\Gamma = \underline{G}(O_S)$ is the S-arithmetic group in question. The known results depend crucially on two numerical invariants:

r = rank $\underline{G}$ (e.g., $n-1$ for SL_n and n for Sp_{2n}), $s = |S|$. For example, Behr [5] shows (in a much more general setting) that Γ is f.g. unless $r = s = 1$. Whether Γ is f.p. in this case remains unsettled except in a few cases indicated in the table below.

	$s = 1$	$s = 2$	$s \geq 3$
$r = 1$	$SL_2(\mathbb{F}_q[t])$ is not f.g. (Nagao)	$SL_2(O_S)$ is not f.p. (Stuhler [27])	$SL_2(O_S)$ is f.p. (Stuhler [27])
$r = 2$	$SL_3(\mathbb{F}_q[t])$ is not f.p. (Behr, Soulé [7])	$\underline{G}(\mathbb{F}_q[t,t^{-1}])$ is f.p. (except possibly G_2) (Hurrelbrink [11])	?
$r \geq 3$	$\underline{G}(\mathbb{F}_q[t])$ is f.p. (Rehmann, Soulé [24])	$\underline{G}(\mathbb{F}_q[t,t^{-1}])$ is f.p. (Hurrelbrink [11])	?

Rehmann has formulated a general conjecture for a semi-simple group (scheme) $\underline{G}$ and corresponding S-arithmetic subgroups. Here the rank r_v of $\underline{G}$ over the different completions K_v of K ($v \in S$) may vary, so the crucial number is $r_\infty = \sum_{v \in S} r_v$ (= rs for a Chevalley group). The conjecture is that Γ is not f.g. when $r_\infty = 1$, that Γ is f.g. but not f.p. when $r_\infty = 2$, and that Γ is f.p. when $r_\infty \geq 3$.

(2.5) It is not difficult to visualize how one might go

about proving that some f.g. group is f.p. But how can it be shown that such a group is not f.p.? In [7] Behr uses a method somewhat like that of Stuhler [27] to deal with $\Gamma = SL_3(\mathbb{F}_q[t])$ (or other rank 2 group when $-1 \notin \mathbb{F}_q^2$). Here is a very rough sketch of the method.

Γ is a discrete subgroup of the locally compact group $G = SL_3(k)$, where k is the completion of $\mathbb{F}_q(t)$ relative to a valuation for which $1/t$ is a prime element. The Bruhat-Tits theory yields an associated "building" I, a simplicial complex made up of "apartments", each in turn subdivided into "quarters". G and hence Γ acts on I. Fix a quarter Q in an apartment A. Then a geometric argument due to Soulé shows that every simplex in I is sent by Γ to a unique simplex in Q. But Q is in a natural way an increasing union of bounded subsets $Q(n)$, whence $I = \bigcup_n I(n)$ if $I(n) = \Gamma.Q(n)$.

Now the "Weyl group" W of the Tits system in G is just an affine Weyl group (the symmetric group S_3 extended by translations), and A is covered by W-translates of a simplex $C_0 \subset Q$ whose vertices may be identified with certain large subgroups P_0, P_1, P_2 of G. It can be shown that Γ is generated by Γ_0 and $\Gamma_1 \cap \Gamma_2$ (where $\Gamma_i = \Gamma \cap P_i$), with Γ_i stabilizing the vertex P_i. So words in these generators yield edge-paths in I, and relations correspond to closed paths at the vertex P_0. Suppose Γ to be f.p.

for this set of generators. Since I is contractible, the paths belonging to relations can be contracted to P_0, each contraction involving only finitely many simplices (hence all taking place in some I(n)). To reach a contradiction, Behr then exhibits for each n some relation whose path is not contractible in I(n).

3. NORMAL SUBGROUPS

Another natural question to ask about an arithmetic (or S-arithmetic) group is this: What are its normal subgroups? Paradoxically, the answer is more complicated for "small" groups like $SL_2(\mathbb{Z})$ than for "big" groups like $SL_{200}(\mathbb{Z})$.

(3.1) Consider again the modular group $\Gamma = PSL_2(\mathbb{Z})$, cf. [19, Ch. VIII]. It was seen in (2.1) that Γ is a free product of cyclic groups generated by elements s of order 2 and t of order 3. Note that $u = st$ has infinite order (as the image of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$). Much is known about normal subgroups of small index in Γ. The subgroup Γ^2(resp.Γ^3) generated by all squares (resp. cubes) is just the normal closure of t (resp. s), and has index 2 (resp. 3). These are the only normal subgroups having index 2 or 3. The

derived group (Γ,Γ) is their intersection, having index 6, and $\Gamma^{ab} = \Gamma/(\Gamma,\Gamma)$ is generated by the image of u. It can be shown that every proper normal subgroup of finite index d other than Γ^2,Γ^3 is free, of rank $1+(d/6)$. For example, (Γ,Γ) is free of rank 2, with generators $stst^2$ and st^2st. (Thus the derived group of (Γ,Γ) is free of infinite rank and has infinite index in Γ.)

There are other obvious normal subgroups of finite index: $\Gamma(n)$ = kernel of natural map $\Gamma \to PSL_2(\mathbb{Z}/n\mathbb{Z})$ $(n\geq 1)$ = principal congruence subgroup of level n. Any subgroup including one of these is called a congruence subgroup. The notion of level can be extended to any normal subgroup Δ (say of index d): the level of Δ is the least positive n for which $u^n \in \Delta$ (so $n|d$). For example, (Γ,Γ) has level 6 and includes the subgroup $\Gamma(6)$, whose index in Γ is 72. Wohlfahrt gave a nice criterion: Let $\Delta \lhd \Gamma$ have level n. Then Δ is a congruence subgroup iff $\Delta \supset \Gamma(n)$. In fact, relatively few subgroups of finite index are congruence subgroups. For example, Γ has infinitely many normal subgroups of level 6, but only 4 of them include $\Gamma(6)$.

(3.2) Congruence subgroups can be defined in a rather general setting. Let K be any global field (a number field or a function field in one variable over a finite field). Take S to be any finite nonempty set of valuations of K, including at least the archimedean ones. Then let A be the

ring of S-integers in K, the elements at which all $v \notin S$ take nonnegative values. (When S consists of the archimedean valuations of a number field, A is just the usual ring of algebraic integers.) For a linear algebraic group $\underline{G}$ over K, the S-arithmetic subgroup $\Gamma_A = \underline{G}(A)$ has a principal congruence subgroup Γ_q for each nonzero ideal q of A, defined to be the kernel of the canonical map $\underline{G}(A) \to \underline{G}(A/q)$. As before, a subgroup of Γ_A containing one of these is called a congruence subgroup. Then it may be asked: Is every subgroup of finite index a congruence subgroup?

(It may also be asked whether Γ_A has any "non-obvious" normal subgroups of infinite index. Though apparently unrelated to the first question, this question can often be studied effectively in tandem with the congruence subgroup problem.)

Serre formulated the problem in an elegant way, by considering simultaneously the group $G = \underline{G}(K)$ and its S-arithmetic (resp. congruence) subgroups, cf. [3], [10], [14], [25]. This leads to a short exact sequence $1 \to C(G) \to \hat{G} \to \overline{G} \to 1$, involving the respective completions $\hat{G}$, $\overline{G}$ of G in the topology whose fundamental system of neighborhoods of 1 consists of the S-arithmetic (resp. congruence) subgroups. Restrictions to the closures $\hat{\Gamma}_A$, $\overline{\Gamma}_A$ of Γ_A yields the related sequence: $1 \to C(G) \to \hat{\Gamma}_A \to \overline{\Gamma}_A \to 1$.

The question then becomes: Is C(G) trivial (and, if not, how big is it)? In case G is simple and simply connected, $\overline{G}$ and $\overline{\Gamma}_A$ have straightforward descriptions, due to strong approximation; e.g., $\overline{\Gamma}_A$ is just the product of the groups $\underline{G}(A_v)$ taken over the integers A_v of all completions $K_v (v \not\in S)$.

(3.3) The case $\underline{G} = SL_2$ can serve as a microcosm of the congruence subgroup problem for simple algebraic groups. In this and the following lecture I want to sketch some of the key points in Serre [25]. Consider first the "negative" results: When $|S| = 1$, C(G) is infinite. This involves three separate cases:

(1) The "rational" case $A = \mathbb{Z}$ (cf. (3.1) above).

(2) The "imaginary quadratic" case, e.g., $A = \mathbb{Z}[i]$.

(3) The "characteristic p" case, e.g., $A = \mathbb{F}_q[t]$ (q = power of p).

In the first two cases, C(G) actually has the cardinality c of the continuum, while in the third case $|C(G)| = 2^c$. (According to Mel'nikov [15], the structure of C(G) in case (1) is that of a "free profinite group of countable rank".)

(3.4) To show that C(G) is infinite in each case, Serre first replaces Γ_A by a suitable torsion-free subgroup Γ of finite index (without loss of generality). For example, Γ can be the derived group of Γ_A in case (1), or can be

a principal congruence subgroup in case (3). Then a key step is to prove that $\Gamma^{ab} = \Gamma/(\Gamma,\Gamma)$ is <u>infinite</u> in each case:

(1)(2) Γ^{ab} is a f.g. infinite abelian group.

(3) Γ^{ab} is the direct sum of a f.g. group and a vector space over $\mathbb{F}_p$ of countably infinite dimension. (In particular, Γ itself cannot be f.g., cf. (2.4).)

Case (1) is classical, since torsion-free here implies free, cf. (2.1). In the other cases, Serre defines an auxiliary group $U(\Gamma)$, the direct sum of intersections of Γ with various maximal unipotent subgroups of G, and a natural map $\alpha: U(\Gamma) \to \Gamma^{ab}$. In case (2), Γ and hence Γ^{ab} is already known to be f.g. [20]. If h is the class number of K, $U(\Gamma)$ turns out to be free abelian of rank 2h, while $\operatorname{Ker}\alpha$ has rank h, forcing Γ^{ab} to be infinite. The proof depends on an identification of α with a map of homology groups: $H_1(\partial X_\Gamma) \to H_1(X_\Gamma)$, where $X = SL_2(\mathbb{C})/SU_2(\mathbb{C})$ and the orbit space X/Γ has a compactification X_Γ.

(3.5) It still has to be deduced that C(G) is infinite. Cases (1) and (2) can be argued together: Let C_Γ be the intersection of C(G) with the closure of Γ in $\hat{G}$. If C(G) were finite, C_Γ would be also. Then the arguments of Bass-Milnor-Serre [3,§16], which depend just on the finiteness of the congruence kernel, would imply the finiteness of $H^1(\Gamma,\mathbb{Z}) = \operatorname{Hom}(\Gamma^{ab},\mathbb{Z})$, contrary to (3.4).

In [3] it is essential that the characteristic be 0, e.g., to get the splitting of short exact sequences of finite dimensional $K\Gamma$-modules, or to apply results of Lazard on p-adic groups.

For case(3), one can argue that $|\overline{\Gamma}| = c$, since the congruence topology has a countable basis of neighborhoods of 1. On the other hand, the result of (3.4) on Γ^{ab} implies that $\hat{\Gamma}$ maps onto the second dual $\hat{V}$ of an infinite dimensional vector space V over $\mathbb{F}_p$; here $|\hat{V}| = 2^c$, forcing $|C(G)| \geq 2^c$. (Alternatively, Serre [26,II,2.7] uses the action on the Bruhat-Tits tree to show more directly that the set of S-arithmetic subgroups of Γ has cardinality c.)

4. NORMAL SUBGROUPS (CONTINUED)

(4.1) Retain the notation of (3.2): $\underline{G}$, K, S, A, Γ_A, G. etc. When $\underline{G} = SL_2$ and $|S| = 1$, the congruence kernel C(G) is infinite and the congruence subgroup problem has therefore a strongly negative solution. Serre's proof involves a close study of the group structure of Γ_A, G, and of the way Γ_A (or its subgroup Γ) acts on a related topological space, but requires no delicate arithmetic information. When $|S| \geq 2$, deeper arithmetic considerations enter into the solution, which is positive or "almost" positive:

THEOREM (Serre). Let $\underline{G} = SL_2$, $|S| \geq 2$. Then $C(G) \cong \mu$ (the finite group of roots of unity in K) if K is a totally imaginary number field and S the set of all archimedean valuations. Otherwise $C(G) = 1$.

The simplest case occurs when $K = Q$, $S = \{p,\infty\}$. (This had been studied earlier by Ihara and Mennicke.)

The assumption $|S| \geq 2$ crucially affects the structure of the group U of units of A, which has the form $\mu \times \mathbb{Z}^{|S|-1}$. In particular, U now has elements of infinite order.

(4.2) The proof of Serre's theorem involves showing that C(G) lies in the <u>center</u> of G. Here an essential role is played by an auxiliary family of normal subgroups of Γ_A: for a nonzero ideal q of A, E_q is the normal subgroup generated by "q-elementary" matrices in Γ_q. (It is unclear at first whether E_q has finite index or not.) Now the proof goes in steps.

(1) Any subgroup N of finite index in Γ_A includes some E_q. (We may assume N is normal, of index n, so $q = nA$ will do if char K = 0. In characteristic p, the choice of q is a bit more complicated and uses the fact that the set of $u \in U$ with $\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \in N$ has finite index in N.)

(2) A non-central subgroup H of G normalized by an S-arithmetic subgroup N includes E_q for some q. (H must

contain some matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ac \neq 0$, otherwise its Zariski closure in SL_2 would be a proper, normal, but non-central subgroup. Now (1) yields an $E_{q'} \subset N$, and some delicate manipulation of matrix entries using elements of infinite order in U yields the required $E_q \subset H$.)

(3) Set $C_q = \Gamma_q/E_q \triangleleft \Gamma_A/E_q$. If $u \in U$, $m = |u|$, then the image of $\begin{pmatrix} u^m & 0 \\ 0 & u^{-m} \end{pmatrix}$ in Γ_A/E_q centralizes C_q. (The proof is not easy: it requires Čebotarev density, Artin reciprocity, etc.)

(4) Let $C = \varprojlim C_q$. Γ_A acts (via inner automorphisms) on C_q, hence on C, and this action extends (via (2)) to an action of G on C. This action is trivial, whence C_q is abelian (and f.g. since Γ_q is). (The kernel of the action contains $\begin{pmatrix} u^m & 0 \\ 0 & u^{-m} \end{pmatrix}$ by (3), hence is infinite. But G is almost simple.)

(5) $C(G) \cong \varprojlim \hat{C}_q$ (profinite completions), and thus C(G) is central in $\hat{G}$. (This follows from (4).)

(4.3) Now the proof shifts gears, applying the theory of Moore [16] to the central extension $1 \to C(G) \to \hat{G} \to \overline{G} \to 1$. This theory implies that G is isomorphic to the "universal covering" of $\overline{G}$ (relative to G), with C(G) isomorphic to the relative fundamental group $\pi_1(\overline{G},G)$. As a result of

Moore's calculation of fundamental groups, $C(G)$ is of the form asserted in (4.1). Moreover, C_q turns out to be finite and cyclic, of order dividing m in the totally imaginary case but trivial otherwise; so the index of E_q in Γ_A is finite after all, and $C \cong C(G)$. As a further byproduct of step (2) above, we see that for any subgroup N of finite index in Γ_A, the normal subgroups of N all have finite index or lie in $\{\pm 1\}$. For example, N^{ab} is finite (in contrast to what can happen if $|S| = 1$).

It should be emphasized that Moore's determination of relative fundamental groups involves the whole arsenal of class field theory. So by the time Serre concludes his argument he has invoked a considerable amount of arithmetic in order to answer what might seem to be a straightforward group-theoretic question.

(4.4) When $\underline{G}$ is a Chevalley group (simple, simply connected, split over K) of rank ≥ 2, the solution of the congruence subgroup problem is "almost" positive in the same sense as above. For example, take S to be the set of archimedean valuations of a number field K. Then $C(G) \cong \mu$ if K is totally imaginary; otherwise $C(G) = 1$. This situation was studied independently by Mennicke and by Bass-Lazard-Serre when $\underline{G} = SL_n$ $(n \geq 3)$ over $\mathbb{Q}$, then for $\underline{G} = SL_n$ or Sp_{2n} by Bass-Milnor-Serre [3]. Matsumoto [14] completed the treatment of Chevalley groups by making

heavy use of the results of Moore [16]. (For a partial exposition, see [10].)

(4.5) The congruence subgroup problem for other simple algebraic groups over K has not yet been fully solved, but there has been substantial recent progress. The most likely conjecture goes as follows (for $\underline{G}$ absolutely simple, simply connected): Let r_v be the rank of $\underline{G}$ over the completion K_v of K for each $v \in S$, and set $r = \Sigma\, r_v$ (sum over S). In case S contains non-archimedean valuations, require $\underline{G}$ to have positive K_v-rank for each such v. (This is a kind of non-compactness.). Then C(G) ought to be finite when $r \geq 2$, as for Chevalley groups of rank ≥ 2. Moreover, C(G) ought to be trivial unless K is a totally imaginary number field and S its set of archimedean valuations; in this case C(G) ought to be μ (or conceivably a quotient of μ).

Here is a quick summary of some recent work in this direction.

In [23] Raghunathan showed that C(G) is finite if K is a number field and $\underline{G}$ has K-rank at least 2 (while C(G) has a p-subgroup of finite index in the function field case). He also showed that each normal subgroup of an S-arithmetic group (when $\underline{G}$ has K-rank ≥ 2) is either finite and central, or else includes an S-elementary subgroup (whose index is finite in the given arithmetic group). As

in the earlier work, it is essential to show that certain extensions are central. Building on this work, Deodhar [9], has gotten more precise results in the case of quasi-split groups (including D_4).

Bak-Rehmann [2] have made a detailed study of non-split groups of type A. In particular, they solve the congruence subgroup problem for many groups $SL_2(D)$ and "most" groups $SL_n(D)$, $n \geq 3$, where D is a finite dimensional central division algebra over a global field.

More recently Bak [1] has announced a more comprehensive solution of the problem for classical groups (other than D_4) of rank at least 2. This involves a reduction to the cases treated in [2], and uses heavily some techniques of algebraic K-theory. (Cf. his monograph, K-theory of forms, Ann. of Math. Studies 98 (1981).)

Independently, Prasad and Raghunathan [21] have made considerable progress on the congruence subgroup problem and the related "metaplectic" conjecture.

One final remark: It is known that a non-split simple, simply connected group $\underline{G}$ of positive K-rank contains a simply connected split group of the same rank (constructed by Borel-Tits). It is worth asking whether the respective congruence kernels can be related directly, since the latter is known explicitly. Such comparisons with split or quasi-split subgroups already play a role in the work of Deodhar and Prasad-Ragunathan.

REFERENCES

1. A. Bak, Le problème des sous-groupes de congruence et le problème métaplectique pour les groupes classiques de rang > 1, C.R. Acad. Sci. Paris 292 (1981), 307-310.

2. A. Bak, U. Rehmann, The congruence subgroup and metaplectic problems for $SL_{n\geq 2}$ of division algebras (preprint)

3. H. Bass, J. Milnor, J.-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), Inst. Hautes Études Sci. Publ. Math. 33 (1967), 59-137.

4. H. Behr, Über die endliche Definierbarkeit verallgemeinerter Einheitengruppen, II, Invent. Math. 4 (1967), 265-274.

5. H. Behr, Endliche Erzeugbarkeit arithmetischer Gruppen über Funktionenkörpern, Invent. Math. 7 (1969), 1-32.

6. H. Behr, Explizite Präsentation von Chevalleygruppen über $\mathbb{Z}$, Math. Z. 141 (1975), 235-241.

7. H. Behr, $SL_3(\mathbb{F}_q[t])$ is not finitely presentable, pp. 213-224 in: Homological Group Theory, L.M.S. Lect. Note Ser. 36, Cambridge U. Press, 1979.

8. A. Borel, Introduction aux groupes arithmétiques, Hermann, Paris, 1969.

9. V.V. Deodhar, On central extensions of rational points of algebraic groups, Amer. J. Math. 100 (1978), 303-386.

10. J.E. Humphreys, Arithmetic Groups, Lect. Notes in Math. 789, Springer, Berlin, 1980.

11. J. Hurrelbrink, Endlich präsentierte arithmetische Gruppen und K_2 über Laurent-Polynomringen, Math. Ann. 225 (1977), 123-129.

12. G.A. Margulis, Discrete groups of motions of manifolds of nonpositive curvature, Amer. Math. Soc. Transl. (Ser. 2) 109 (1977), 33-45 [Russian original appears in proceedings of 1974 Intl. Congr. Math., Vancouver]

13. G.A. Margulis, Arithmeticity of irreducible lattices in semi-simple groups of rank greater than 1 [Russian], appendix to Russian translation of [22], Mir, Moscow, 1977.

14. H. Matsumoto, Sur les sous-groupes arithmétiques des groupes semi-simples déployés, Ann. Sci. École Norm. Sup. 2 (1969), 1-62.

15. O.V. Mel'nikov, Congruence kernel of the group $SL_2(\mathbb{Z})$, Soviet Math. Dokl. 17 (1976), 867-870.

16. C.C. Moore, Group extensions of p-adic and adelic linear groups, Inst. Hautes Études Sci. Publ. Math. 35 (1969), 5-70.

17. G.D. Mostow, On a remarkable class of polyhedra in complex hyperbolic space, Pacific J. Math. 86 (1980), 171-276.

18. G.D. Mostow, Existence of nonarithmetic monodromy groups, Proc. Natl. Acad. Sci. USA 78 (1981), 5948-5950.

19. M. Newman, Integral Matrices, Academic Press, New York, 1972.

20. O.T. O'Meara, On the finite generation of linear groups over Hasse domains, J. Reine Angew. Math. 217 (1965), 79-108.

21. G. Prasad, M.S. Raghunathan (to appear).

22. M.S. Raghunathan, Discrete Subgroups of Lie Groups, Springer, Berlin, 1972.

23. M.S. Raghunathan, On the congruence subgroup problem, Inst. Hautes Études Sci. Publ. Math. 46 (1976), 107-161.

24. U. Rehmann, S. Soule, Finitely presented groups of matrices, pp. 164-169 in: Algebraic K-Theory (Evanston 1976), Lect. Notes in Math. 551, Springer, Berlin, 1976.

25. J.-P. Serre, Le problème des groupes de congruence pour SL_2, Ann. of Math. 92 (1970), 489-527.

26. J.-P. Serre, Arbres, amalgames, SL_2, Astérisque 46 (1977)

27. U. Stuhler, Zur Frage der endlichen Präsentierbarkeit gewisser arithmetischer Gruppen im Funktionenkörperfall, Math. Ann. 224 (1976), 217-232.

28. U. Stuhler, Homological properties of certain arithmetic groups in the function field case, Invent. Math. 57 (1980), 263-281.

29. R.G. Swan, Generators and relations for certain special linear groups, Adv. in Math. 6 (1971), 1-77.

30. J. Tits, Travaux de Margulis sur les sous-groupes discrets de groupes de Lie, Sém. Bourbaki 1975/76, Exp. 482, Lect. Notes in Math. 567, Springer, Berlin, 1977.