HAL open science

An introduction to arithmetic groups

Christophe Soule

To cite this version:

Christophe Soule. An introduction to arithmetic groups. 2004. hal-00001348

HAL Id: hal-00001348

https://hal.science/hal-00001348v1

Preprint submitted on 23 Mar 2004

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ccsd-00001348 (version 1) : 23 Mar 2004

An introduction to arithmetic groups

Christophe Soulé

CNRS and IHES, 35 Route de Chartres, 91440 Bures sur Yvette, France.
soule@ihes.fr

Arithmetic groups are groups of matrices with integral coefficients. They first appeared in the work of Gauss, Minkowski and others on the arithmetic theory of quadratic forms. Their *reduction theory* consists in showing that, after a linear change of variables with integral coefficients, any quadratic form can be forced to satisfy an appropriate set of inequalities.

Around 1940, Siegel developed a general theory of arithmetic subgroups of classical groups, and the corresponding reduction theory. Later on, once Chevalley, Borel, Tits and others had developed the general theory of algebraic groups, one could speak of the arithmetic subgroups of any linear algebraic group over $\mathbb{Q}$. Borel et al. extended the work of Siegel to arbitrary arithmetic groups.

These groups play a fundamental role in number theory, and especially in the study of automorphic forms, which can be viewed as complex valued functions on a symmetric domain which are invariant under the action of an arithmetic group. In the last ten years, it appeared that some arithmetic groups are the symmetry groups of several string theories. This is probably why this survey fits into these proceedings.

In a first chapter we shall describe the classical reduction theory of quadratic forms. After describing the action of $\mathrm{SL}_2(\mathbb{Z})$ on the Poincaré upper half-plane (Theorem 1) we explain how Siegel defined a fundamental domain for the action of $\mathrm{GL}_N(\mathbb{Z})$ on real quadratic forms in N variables (Theorem 2). We then proceed with the general definition of linear algebraic groups over $\mathbb{Q}$ and their arithmetic subgroups (§ 3). An important example is a construction of Chevalley which defines an arithmetic group $G(\mathbb{Z})$ when given any root system Φ together with a lattice between the root lattice and the weight lattice of Φ (3.3). In 3.4 (and in the Appendix) we explain how the group $E_7(\mathbb{Z})$ of [10] is an example of this construction. We then describe the general construction of Siegel sets and the reduction theory of arithmetic groups (Theorem 4). In particular, it follows that any arithmetic subgroup of a semi-simple algebraic group over $\mathbb{Q}$ has finite covolume in its real points.

The second chapter deals with several algebraic properties of arithmetic groups. As a consequence of reduction theory, we show that these groups are finitely generated. In fact they admit a finite presentation (Theorem 6). We give some explicit presentations of $\mathrm{SL}_N(\mathbb{Z})$, $N \geq 2$, and of the Chevalley groups $G(\mathbb{Z})$ (5.6–5.8). We then show that, up to conjugation, arithmetic groups contain only finitely many finite subgroups (Theorem 7). Furthermore, they always contain a torsion free subgroup of finite index (Theorem 8). Following Minkowski, one can compute the least common multiple of the order of the finite subgroups of $\mathrm{GL}_N(\mathbb{Z})$ (6.3). Coming back to $N = 2$, we prove that any torsion free subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is a free group (Theorem 10). We conclude this section with the open problem, raised by Nahm, of finding the minimal index of torsion free subgroups of $\mathrm{SL}_N(\mathbb{Z})$, $N \geq 3$.

One of the main properties of arithmetic groups is their "rigidity" inside the corresponding algebraic and Lie groups, at least when their rank is bigger than one. A lot of work has been accomplished on this theme. We start Chapter 3 with the congruence subgroup property, which states that any subgroup of finite index in Γ contains the group of elements congruent to the identity modulo some integer. This property holds for arithmetic subgroups of simple simply connected Chevalley groups of rank bigger than one (Theorem 13), but it is wrong for SL_2 (Corollary 18). When studying that problem, Bass, Milnor and Serre discovered that, under suitable hypotheses, any linear representation of Γ over $\mathbb{Q}$ coincides with an algebraic representation on some subgroup of finite index (Proposition 14). This important rigidity property has many consequences, including the fact that the abelianization of Γ is finite (Corollary 17).

Another approach to rigidity is Kazhdan's property (T), as explained in Theorems 19 and 20. Finally, we state the famous result of Margulis (Selberg's conjecture) that any discrete subgroup of finite covolume in a simple, non-compact, connected Lie group of rank bigger than one is "arithmetic" in a suitable sense (Theorem 21). This follows from a "superrigidity" theorem for representations of arithmetic groups (Theorem 22). Finally, we give another result of Margulis (Theorem 23), which states that arithmetic groups have rather few normal subgroups.

There are many results on arithmetic groups which are not covered by these notes. These include the different methods to compactify the quotient of a symmetric domain by the action of an arithmetic group (Baily-Borel-Satake, Borel-Serre...), the cohomology of arithmetic groups (Borel, Serre, Franke,...), and the ergodicity of their action on Lie groups (Margulis, Ratner,...).

I thank P. Cartier, B. Julia, W. Nahm, N. Nekrasov and J-P. Serre for helpful discussions.

I. Reduction theory

1 The reduction theory of quadratic forms

1.1

Groups of matrices with integral coefficients first appeared, in the work of Gauss, Hermite, Minkowski and others, as the symmetry groups for a specific diophantine problem: which integers can be represented by a given quadratic form?

Recall that any positive integer is the sum of four squares. More generally, consider a quadratic form in N variables

$$\varphi(x) = \sum_{1 \le i,j \le N} a_{ij}\, x_i\, x_j \tag{1}$$

where $a_{ij} = a_{ji}$. We assume that φ is positive definite: for any vector $x = (x_i) \in \mathbb{R}^N$, $\varphi(x) \ge 0$ and $\varphi(x) = 0$ iff $x = 0$. When all coefficients a_{ij} are integers, we say that a given integer $k \in \mathbb{N}$ is *represented by* φ if there exists $x \in \mathbb{Z}^N$ such that $\varphi(x) = k$.

Let now $\gamma \in \mathrm{GL}_N(\mathbb{Z})$ be an N by N square matrix with integral coefficients, the inverse of which has integral coefficients as well, i.e. such that $\det(\gamma) = \pm 1$. Let ${}^t\gamma$ be the transpose of the matrix γ. When we change the coordinates of x by ${}^t\gamma$, we get a new quadratic form $\gamma \cdot \varphi$:

$$(\gamma \cdot \varphi)(x) = \varphi\left({}^t\gamma(x)\right), \tag{2}$$

for all $x \in \mathbb{R}^N$. Since $\gamma_1(\gamma_2(\varphi)) = (\gamma_1\, \gamma_2)(\varphi)$, formula (2) defines an action of $\mathrm{GL}_N(\mathbb{Z})$ on positive definite quadratic forms. It follows from (2) that k is represented by φ iff k is represented by $\gamma \cdot \varphi$ for all $\gamma \in \mathrm{GL}_N(\mathbb{Z})$. Therefore, when studying the integral values of φ we may replace φ by any form equivalent to it.

The *reduction theory of quadratic forms* consists in studying the orbits of $\mathrm{GL}_N(\mathbb{Z})$ on quadratic forms, and finding a good set of representatives for this action. Let X be the set of positive definite quadratic forms

$$\varphi(x) = \sum_{1 \le i,j \le N} a_{ij}\, x_i\, x_j\,,$$

where $a_{ij} = a_{ji}$ are real numbers. We look for a "small" subset $D \subset X$ such that any point of X is the translate of a point in D by an element of Γ; in other words:

$$\Gamma \cdot D = X\,.$$

1.2

Consider first the case $N = 2$. Any positive definite binary form φ can be written uniquely

$$\varphi(x, y) = a(zx + y)(\bar{z}x + y) \tag{3}$$

where $a > 0$ and z is a complex number with positive imaginary part. The action of positive scalars on X commutes with $\mathrm{GL}_N(\mathbb{Z})$ (for any $N \geq 2$) and (3) tells us that, when $N = 2$, the quotient $X/\mathbb{R}_+^*$ is isomorphic to the Poincaré upper half plane

$$\mathcal{H} = \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}\,.$$

The action of $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ is given by

$$\gamma(z) = \frac{az + b}{cz + d}\,. \tag{4}$$

Theorem 1. *Let D be the set of $z \in \mathcal{H}$ such that $|z| \geq 1$ and $|\operatorname{Re}(z)| \leq 1/2$ (Figure 1). Then*

$$\mathcal{H} = \Gamma \cdot D\,.$$

Remark. If z lies in the interior of D and $\gamma(z) = z$, then $\gamma = \pm\,\mathrm{Id}$. Furthermore, if $|z| > 1$ and $\gamma(z) = z$, then $\operatorname{Re}(z) = \pm 1/2$ and $\gamma(z) = z + 1$ or $z - 1$.

Proof (see [24], VII, 1.2). Fix $z \in \mathcal{H}$. We have

$$\operatorname{Im}(\gamma(z)) = \frac{\operatorname{Im}(z)}{|cz + d|^2}\,,$$

and, given $A > 0$, there exist only finitely many $(c, d) \in \mathbb{Z}^2$ such that $|cz+d|^2 \leq A$. Therefore we can choose γ such that $\operatorname{Im}(\gamma(z))$ is maximal. Let $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Since $T(z) = z + 1$ we can choose $n \in \mathbb{Z}$ such that

$$|\operatorname{Re}(T^n\,\gamma(z))| \leq 1/2\,.$$

We claim that $z' = T^n\,\gamma(z)$ lies in D, i.e. $|z'| \geq 1$. Indeed, if $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we get $S(z') = -1/z'$, hence

$$\operatorname{Im}(S(z')) = \frac{\operatorname{Im}(z')}{|z'|^2}\,.$$

Since the imaginary part of z' is maximal, this implies $|z'| \geq 1$.

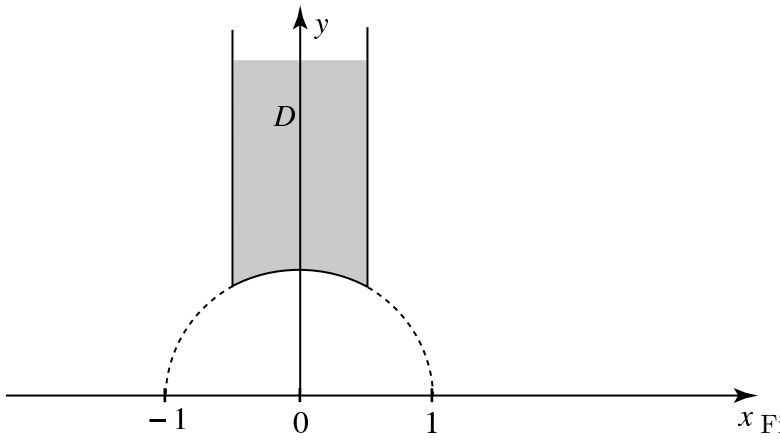

Figure 1

2 Siegel sets

More generally, when $N \geq 2$, any positive definite real quadratic form φ in N variables can be written uniquely in the following way:

$$\begin{aligned}\varphi(x) = {} & t_1(x_1 + u_{12}\,x_2 + u_{13}\,x_3 + \cdots + u_{1N}\,x_N)^2 \\ & + t_2(x_2 + u_{23}\,x_3 + \cdots + u_{2N}\,x_N)^2 \\ & + \cdots \\ & + t_N\,x_N^2\,,\end{aligned} \tag{5}$$

where $t_1, \ldots, t_N$ are positive real numbers and $u_{ij} \in \mathbb{R}$.

Theorem 2 ([3], Th. 1.4). *After replacing φ by $\gamma \cdot \varphi$ for some $\gamma \in \mathrm{GL}_N(\mathbb{Z})$, we can assume that*

$$|u_{ij}| \leq 1/2 \quad \textit{when} \quad 1 \leq i < j < N$$

and

$$t_i \leq \frac{4}{3}\,t_{i+1} \quad \textit{when} \quad 1 \leq i \leq N-1\,.$$

The subset $\mathfrak{S}$ of X defined by the inequalities of Theorem 2 is called a *Siegel set* (see (9) below for a general definition). When $N = 2$, $\mathfrak{S}$ is the shaded region in Figure 2 below, and Theorem 2 follows from Theorem 1.

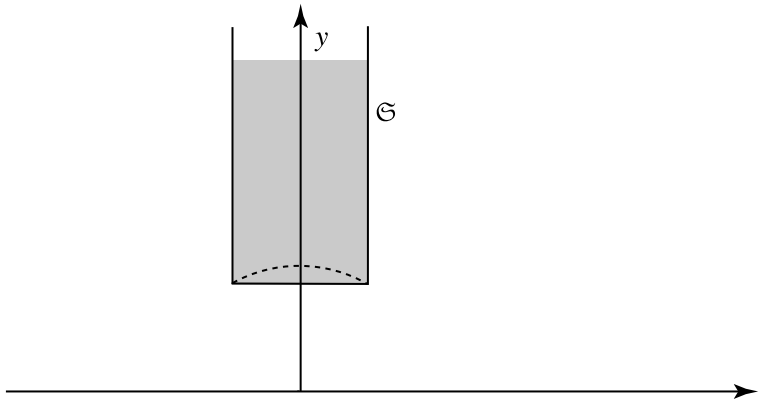

Figure 2

3 Arithmetic groups

3.1

Let $N \geq 1$ be an integer and G a subgroup of $\mathrm{GL}_N(\mathbb{C})$. The group G is called *linear algebraic over* $\mathbb{Q}$ if there exist polynomials $P_1, \ldots, P_k$ with coefficients in $\mathbb{Q}$ in the variables x_{ij}, $1 \leq i, j \leq N$ and u such that G is the set of elements $g = (g_{ij}) \in \mathrm{GL}_N(\mathbb{C})$ such that

$$P_1(g_{ij}, \det(g)^{-1}) = P_2(g_{ij}, \det(g)^{-1}) = \cdots = P_k(g_{ij}, \det(g)^{-1}) = 0\,.$$

The group $G(\mathbb{Q}) = G \cap \mathrm{GL}_N(\mathbb{Q})$ is called the group of *rational points* of G.

Given Γ_1 and Γ_2 two subgroups of G, we say that Γ_1 and Γ_2 are *commensurable* when their intersection $\Gamma_1 \cap \Gamma_2$ has finite index in both Γ_1 and Γ_2.

Definition. *Given $N \geq 1$ and $G \subset \mathrm{GL}_N(\mathbb{C})$ a linear algebraic group over $\mathbb{Q}$, an* arithmetic subgroup *of G is a subgroup Γ of $G(\mathbb{Q})$ which is commensurable with $G \cap \mathrm{GL}_N(\mathbb{Z})$.*

3.2

A morphism $f : G \to G'$ of linear algebraic groups over $\mathbb{Q}$ is a group morphism defined by polynomials with coefficients in $\mathbb{Q}$ (note that f needs *not* extend to a morphism between the ambient linear groups).

Proposition 3 ([3] Cor. 7.13, (3)). *If $\Gamma \subset G(\mathbb{Q})$ is an arithmetic subgroup of G and $f : G \to G'$ a morphism of linear algebraic groups over $\mathbb{Q}$, the image $f(\Gamma)$ is contained in some arithmetic group $\Gamma' \subset G'(\mathbb{Q})$.*

Remarks. 1) If $G \subset \mathrm{GL}_N(\mathbb{C})$ is a linear algebraic group over $\mathbb{Q}$, we may consider its ring of rational functions

$$A = \mathbb{Q}\,[x_{ij}, u]/\langle P_1, \ldots, P_k\rangle\,.$$

This $\mathbb{Q}$-algebra is finitely generated over $\mathbb{Q}$ and carries a Hopf structure coming from the group structure of G. Therefore $G_{\mathbb{Q}} = \mathrm{Spec}(A)$ is an *affine group scheme* over $\mathbb{Q}$ [W]. The group G is the set of complex points $G = \mathrm{Hom}(\mathrm{Spec}(\mathbb{C}), G_{\mathbb{Q}})$ and $G(\mathbb{Q})$ is the set of rational points of $G_{\mathbb{Q}}$. Note that the definition of $G_{\mathbb{Q}}$ does not refer anymore (up to isomorphism) to a particular linear embedding.

2) When $f : G \to G'$ is an isomorphism, it follows from Proposition 3 that $f(\Gamma)$ is arithmetic. This proves that the class of arithmetic subgroups of G is intrinsic, i.e. it depends only on $G_{\mathbb{Q}}$ and not on the choice of the embedding $G \subset \mathrm{GL}_N(\mathbb{C})$.

3) Another consequence of Proposition 3 is that, for any lattice $\Lambda \subset \mathbb{Q}^N$ (i.e. a free $\mathbb{Z}$-module of rank N), the group Γ of elements $\gamma \in G(\mathbb{Q})$ such that $\gamma(\Lambda) = \Lambda$ is arithmetic.

3.3

The following general construction of arithmetic groups is due to Chevalley.

3.3.1

Let E be a finite dimensional real euclidean vector space, and $\Phi \subset E$ a *root system* ([11], 9.2). Let $L_0 \subset E$ be the lattice spanned by Φ (the *lattice of roots*) and L_1 the *lattice of weights*, i.e. those $\lambda \in E$ such that $\langle \lambda, \alpha\rangle \in \mathbb{Z}$ for all $\alpha \in \Phi$. The lattice L_0 is contained in L_1. Choose a lattice L such that

$$L_0 \subset L \subset L_1\,.$$

Given Φ and L, Chevalley defines as follows a linear algebraic group G over $\mathbb{Q}$ ([7], [26], [11] Chapter VII). Let $\mathcal{L}$ be a complex Lie algebra and $\mathcal{H} \subset \mathcal{L}$ a Cartan subalgebra such that Φ is the set of roots of $\mathcal{L}$ with respect to $\mathcal{H}$. If $\ell = \dim_{\mathbb{C}} \mathcal{H}$ and if $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ is a basis of Φ, we can choose a *Chevalley basis* of $\mathcal{L}$, i.e. a basis $\{X_\alpha, \alpha \in \Phi\,;\ H_i, 1 \le i \le \ell\}$ such that $H_i \in \mathcal{H}$ and

$$[H_i, H_j] = 0$$

$$[H_i, X_\alpha] = \langle \alpha, \alpha_i\rangle\, X_\alpha$$

$$[X_\alpha, X_{-\alpha}] \in \bigoplus_{i=1}^{\ell} \mathbb{Z}\, H_i$$

$$[X_\alpha, X_\beta] = \begin{cases} N_{\alpha\beta}\, X_{\alpha+\beta} & \text{when } \alpha+\beta \in \Phi \\ 0 & \text{otherwise, } \alpha+\beta \neq 0\,. \end{cases}$$

Here $N_{\alpha\beta} \in \mathbb{Z}$ and $N_{-\alpha,-\beta} = -N_{\alpha\beta}$. Consider a faithful (i.e. injective) representation

$$\rho : \mathcal{L} \to \mathrm{End}(V)$$

of $\mathcal{L}$ on a finite dimensional complex vector space V such that L is the set of weights of ρ ([11], Ex. 21.5). For any root $\alpha \in \Phi$, the endomorphism $\rho(X_\alpha)^n = 0$ when n is big enough so it makes sense to define G as the group of endomorphisms of V generated by the exponentials

$$\exp(t\,\rho(X_\alpha)) = \sum_{n\geq 0} t^n \,\frac{\rho(X_\alpha)^n}{n!}$$

for all $t \in \mathbb{C}$ and $\alpha \in \Phi$.

One can choose a basis of V such that its $\mathbb{Z}$-span M is stable by the action of every endomorphism $\frac{\rho(X_\alpha)^n}{n!}$, $n \geq 1$, $\alpha \in \Phi$ (such a lattice is called *admissible*). If the embedding $G \subset \mathrm{GL}_r(\mathbb{C})$ is defined by such a basis ($r = \dim_{\mathbb{C}} V$), G is the set of zeroes of polynomials with $\mathbb{Q}$-coefficients ([26], § 5, Th. 6). It can be shown [7] [26] that, up to canonical isomorphism, the linear algebraic group G over $\mathbb{Q}$ depends only on Φ and L.

When $L = L_0$, the group G is called *adjoint*, and when $L = L_1$ it is called *simply connected* (or "universal").

3.3.2

Let Φ, L, ρ and M be as above. The group $G(\mathbb{Z}) = \{g \in G$ such that $g(M) = M\}$ is an arithmetic subgroup of G. Up to canonical isomorphism (defined by means of polynomials with integral coefficients, respecting the inclusion $G(\mathbb{Z}) \subset G(\mathbb{Q})$) it depends only on Φ and L. In fact, Chevalley proves in [7] that (Φ, L) defines an affine group scheme $G_{\mathbb{Z}}$ over $\mathbb{Z}$, and

$$G(\mathbb{Z}) = \mathrm{Hom}(\mathrm{Spec}(\mathbb{Z}), G_{\mathbb{Z}})$$

is its set of integral points.

3.4

The group of integral points of the simply connected Chevalley group scheme of type A_n (resp. B_n) is the group $\mathrm{SL}_n(\mathbb{Z})$ of integral matrices with determinant one (resp. the group $\mathrm{Sp}_{2n}(\mathbb{Z})$ of symplectic matrices in $\mathrm{SL}_{2n}(\mathbb{Z})$).

Another example is the simply connected Chevalley group scheme G of type E_7 over $\mathbb{Z}$ and its set $G(\mathbb{Z})$ of integral points. Consider the split Lie group $E_{7(+7)}$ of type E_7 and its fundamental representation $E_{7(+7)} \subset \mathrm{Sp}_{56}(\mathbb{R})$ of dimension 56, as described in [8], Appendix B. Let $E_7(\mathbb{Z}) = E_{7(+7)} \cap \mathrm{Sp}_{56}(\mathbb{Z})$ as in [10]. We shall prove in the Appendix that

$$E_7(\mathbb{Z}) = G(\mathbb{Z})\,. \tag{6}$$

3.5

Assume F is a number field (a finite extension of $\mathbb{Q}$). We can define linear algebraic groups G over F in the same way as when $F = \mathbb{Q}$, by choosing a complex embedding of F or more intrinsically as in 3.2 Remark 1). Matrices in G with coefficients in the integers of F are arithmetic groups.

However, these definitions do *not* enlarge the class of arithmetic groups. Indeed $G(F)$ can be viewed as the group of rational points $H(\mathbb{Q}) = G(F)$, where $H = \mathrm{Res}_{F/\mathbb{Q}}\, G$ is the *restriction of scalars* of G from F to $\mathbb{Q}$ ([3] 7.16, [21] Chapter 3, § 6.1).

For example, let $d > 0$ be a positive integer which is not a square. Consider the subgroup H of $\mathrm{GL}_2(\mathbb{C})$ made of matrices $g = (g_{ij})$ such that $g_{11} = g_{22}$, $g_{21} = dg_{12}$ and $\det(g) = 1$. In other words each $g \in H$ can be written

$$g = x \cdot 1 + y \cdot \sigma$$

where $\sigma = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}$. Note that $\sigma^2 = d \cdot 1$. The group H is the restriction of scalars $\mathrm{Res}_{F/\mathbb{Q}}\, \mathrm{GL}_1$ where $F = \mathbb{Q}\,(\sqrt{d})$. Note that $H(\mathbb{R})$ is isomorphic to $\mathbb{R}^*$ (map $x \cdot 1 + y \cdot \sigma$ to $x + y\sqrt{d}$) but H is not isomorphic to GL_1 over $\mathbb{Q}$. We have $H(\mathbb{Q}) = F^*$, and the group of units $\mathcal{O}_F^*$ is an arithmetic subgroup of H.

4 The reduction theory of arithmetic groups

4.1

Theorem 1 can be extended to all arithmetic subgroups of reductive groups. We first need some definitions. A linear algebraic group U is called *unipotent* (resp. *solvable*) when there exists a finite filtration $\cdots \subset U_i \subset U_{i+1} \subset \cdots \subset U$ of U by (Zariski) closed normal subgroups such that each quotient U_{i+1}/U_i is isomorphic (over $\mathbb{Q}$) to the additive group (resp. is abelian). If G is any linear algebraic group over $\mathbb{Q}$, the *unipotent radical* $R_u(G)$ (resp. the *radical* $R(G)$) is the maximal closed connected unipotent (resp. solvable) normal subgroup of G. Of course $R_u(G)$ is contained in $R(G)$. The group G is called *reductive* (resp. *semi-simple*) when $R_u(G) = \{1\}$ (resp. $R(G) = \{1\}$).

Let G be a reductive linear algebraic group over $\mathbb{Q}$, let G^0 be the connected component of the unit element $1 \in G$, and let P be a minimal *parabolic subgroup* of G^0 over $\mathbb{Q}$, i.e. a minimal closed connected subgroup $P \subset G^0$ such that the variety G/P^0 is projective. According to [3], Th. 11.4, i), one can write P as a product of subgroups

$$P = M \cdot S \cdot U\,, \tag{7}$$

where $U = R_u(P)$ and S is a maximal split $\mathbb{Q}$-torus of P (i.e. S is isomorphic over $\mathbb{Q}$ to a power of the multiplicative group). Let $X(Z(S))$ be the set of

characters $\chi : Z(S) \to \mathrm{GL}_1$ over $\mathbb{Q}$ of the centralizer $Z(S)$ of S in G^0. Then M is defined as the connected component of 1 in the intersection $\cap \ker(\chi)$ of the kernels of all the characters $\chi \in X(Z(S))$.

Furthermore, if $G(\mathbb{R}) = G \cap \mathrm{GL}_N(\mathbb{R})$ is the group of real points of G and K a maximal compact subgroup of this Lie group $G(\mathbb{R})$, we may write, according to [3] 11.19,

$$G(\mathbb{R}) = P(\mathbb{R}) \cdot K = M^0 \cdot N \cdot A \cdot K \tag{8}$$

where M^0 (resp. A) is the (usual) connected component of 1 in $M(\mathbb{R})$ (resp. $S(\mathbb{R})$), and $N = U(\mathbb{R})$. The decomposition (8) generalizes the Iwasawa decomposition.

4.2

For example, when $G = \mathrm{GL}_N(\mathbb{C})$, we can choose for K the group $O_N(\mathbb{R})$ of orthogonal matrices, for P lower triangular matrices, for S diagonal ones, for N lower unipotent matrices and $M = \{1\}$. Define a map from $\mathrm{GL}_N(\mathbb{R})$ to the space X of real positive definite quadratic forms by the formula

$$\varphi(x) = \|{}^t g(x)\|^2 .$$

Using this map, we see that (8) follows from (7) in this case.

4.3

We come back to the notations of § 4.1. Let $X(S) = \mathrm{Hom}_S(S, \mathrm{GL}_1)$ be the set of characters of S over $\mathbb{Q}$, and let $\Phi \subset X(S)$ be the set of roots of G. The group U defines an ordering of Φ ([3], 11.6 (3)) and we let $\Delta \subset \Phi$ be the set of positive simple roots. For any real number $t > 0$ let

$$A_t = \{a \in A |\, \alpha(a) \leq t \text{ for all } \alpha \in \Delta\} .$$

If ω is any compact neighbourhood of 1 in $M^0 \cdot N$ we define

$$\mathfrak{S}_{t,\omega} = \omega \cdot A_t \cdot K , \tag{9}$$

a subset of $G(\mathbb{R})$ by (8). This set $\mathfrak{S}_{t,\omega}$ is called a *Siegel set*.

Theorem 4. *Let G be a reductive linear algebraic group over $\mathbb{Q}$ and Γ an arithmetic subgroup of G.*

i) ([3], Th. 1.3.1) *One can choose $t > 0$ and ω as above, and a finite subset C in $G(\mathbb{Q})$ such that*
$$G(\mathbb{R}) = \Gamma \cdot C \cdot \mathfrak{S}_{t,\omega} .$$

ii) ([3], Th. 15.4) *For any choice of t and ω, and any $g \in G(\mathbb{Q})$, the set of elements $\gamma \in \Gamma$ such that $g \cdot \mathfrak{S}_{t,\omega}$ meets $\gamma \cdot \mathfrak{S}t, \omega$ is* finite.

iii) ([3], Lemma 12.5) *The Haar measure of any Siegel set is finite iff the set of rational characters* $X(G^0)$ *is trivial.*

Corollary 5. *With the same hypotheses:*

i) *The quotient* $\Gamma\backslash G(\mathbb{R})$ *is compact iff* G *is* anisotropic *over* $\mathbb{Q}$ (i.e. $S = U = \{1\}$).
ii) *The (invariant) volume of* $\Gamma\backslash G(\mathbb{R})$ *is finite iff* G^0 *has no nontrivial character over* $\mathbb{Q}$ *(e.g. if* G *is semi-simple).*

II. Some algebraic properties of arithmetic groups

5 Presentations

5.1

Let S be a set. The *free group* $F(S)$ over S is defined by the following universal property: S is contained in $F(S)$ and, given any group G and any map of sets $\varphi : S \to G$, there exists a unique group morphism $\tilde{\varphi} : F(S) \to G$ which coincides with φ on S, i.e. such that the diagram

$$\begin{tikzcd} F(S) \arrow[rr, "\tilde{\varphi}"] & & G \\ & S \arrow[ul] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

commutes.

Clearly $F(S)$ is unique up to unique isomorphism. A construction of $F(S)$ is given in [14] I, § 8, Prop. 7.

5.2

Given a group G, a *presentation* of G is a pair (S, R) where $S \subset G$ is a subset of G and $R \subset F(S)$ is a subset of the free group over S such that

i) S spans G, i.e. the canonical map $F(S) \to G$ is surjective;
ii) the kernel of the map $F(S) \to G$ is the smallest normal subgroup $\langle R \rangle$ of $F(S)$ containing R.

It follows from i) and ii) that G is isomorphic to $F(S)/\langle R \rangle$. We say that G is generated by S, with relations $r = 1$ for all $r \in R$.

When S and R are finite, (S, R) is a *finite presentation* of G.

5.3

For example, when $S = \{x, y\}$ consists of two elements and $R = \{x^2, y^2, (xy)^3\}$ the group $G = F(S)/\langle R \rangle$ is the group S_3 of permutations of three elements. This can be seen by mapping x (resp. y) to the permutation $(123) \to (213)$ (resp. $(123) \to (132)$).

5.4

Here are two finite presentations of $\mathrm{SL}_2(\mathbb{Z})$:

a) $\mathrm{SL}_2(\mathbb{Z})$ is generated by $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ with relations

$$(x^{-1}\, y\, x^{-1})^4 = 1 \qquad \text{and} \qquad x\, y^{-1}\, x = y^{-1}\, x\, y^{-1}\,.$$

b) $\mathrm{SL}_2(\mathbb{Z})$ is generated by $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ with relations $W^2 = A^3$ and $W^4 = 1$.

5.5

In general we have the following

Theorem 6 ([4], [23]). *Let Γ be an arithmetic subgroup of a linear algebraic group G over $\mathbb{Q}$. Then Γ is finitely presented.*

In other words, Γ admits a finite presentation. Let us indicate why Γ is finitely generated. Let K be a maximal compact subgroup of $G(\mathbb{R})$ and $X = G(\mathbb{R})/K$. We claim that we can find a closed subset $D \subset X$ such that

a) $\Gamma \cdot D = X$;
b) the subset $S \subset \Gamma$ of those γ such that $\gamma \cdot D \cap D \neq \emptyset$ is finite.

Indeed, when G is reductive we can take for D the union $\bigcup_{g \in C} g \cdot \mathfrak{S}_{t,\omega}$ of finitely many translates of a (well chosen) Siegel set; see Theorem 4, i) and ii). When G is arbitrary, it is a semi-direct product

$$G = R_u(G) \cdot H, \tag{10}$$

where H is reductive over $\mathbb{Q}$ ([3] 7.15) and $R_u(G)$ is the unipotent radical of G. The quotient $(R_u(G) \cap \Gamma)\backslash R_u(G)$ is compact so we can choose a compact subset $\Omega \subset R_u(G)$ such that $R_u(G) = (R_u(G) \cap \Gamma) \cdot \Omega$. Let $D' \subset H(\mathbb{R})/K$ be such that a) and b) are true for D' and $\Gamma \cap H$ (note that $K \cap R_u(G)$ is trivial). Then one can check that $D = \Omega \cdot D'$ and Γ satisfy a) and b).

From this we derive that S spans Γ. Indeed, it follows from (8) and (10) that X is homeomorphic to a euclidean space and, in particular, it is path connected. Given $\gamma \in \Gamma$, choose a continuous path $c : [0,1] \to X$ such that $x = c(0)$ lies in D and $c(1) = \gamma \cdot x$. Since $c([0,1])$ is compact, there exists a finite sequence $\gamma_1, \ldots, \gamma_k$ in Γ such that $\gamma_1 = 1$, $\gamma_i \cdot D \cap \gamma_{i+1} \cdot D \neq \emptyset$ when $i < k$, and $\gamma_k = \gamma$. Define $s_i = \gamma_i^{-1}\, \gamma_{i+1}$, $i < k$. Since $s_i \cdot D \cap D \neq \emptyset$, these elements lie in S. On the other hand,

$$\gamma = s_1 \ldots s_{k-1}\,,$$

therefore S spans Γ.

5.6

Theorem 6 gives us general information, but it is still of interest to have explicit presentations of arithmetic groups. For instance, consider the case of $\mathrm{SL}_N(\mathbb{Z})$, $N \geq 3$. For any pair of indices (i,j), $1 \leq i \neq j \leq N$, denote by $x_{ij} \in \mathrm{SL}_N(\mathbb{Z})$ the matrix which is equal to one on the diagonal and at the entry (i,j), and zero otherwise:

$$x_{ij} = \begin{pmatrix} 1 & 0 & & j & \\ & 1 & 0 & | & \\ & & 1 & 1 & -i \\ 0 & & \ddots & 0 & \\ & 0 & & 1 & \\ & & 0 & 1 & \\ & & & & 1 \end{pmatrix}.$$

These matrices x_{ij}, $1 \leq i \neq j \leq N$, generate $\mathrm{SL}_N(\mathbb{Z})$, and the following relations give a presentation:

$$[x_{ij}, x_{k\ell}] = 1 \qquad \text{if } j \neq k \text{ and } i \neq \ell\,;$$

$$[x_{ij}, x_{jk}] = x_{ik} \qquad \text{if } i,j,k \text{ are distinct}\,;$$

$$(x_{12}\, x_{21}^{-1}\, x_{12})^4 = 1\,.$$

As usual, $[g,h]$ is the commutator $ghg^{-1}h^{-1}$. This fact is due to Magnus and Nielsen (see [20] Cor. 10.3).

Remark. There are known bounds for the number of elementary matrices $x_{ij}^a, a \in \mathbb{Z}$, needed to write any element of $\mathrm{SL}_N(\mathbb{Z})$ [6]. For instance, any element of $\mathrm{SL}_3(\mathbb{Z})$ is the product of at most 60 elementary matrices.

5.7

The group $\mathrm{SL}_N(\mathbb{Z})$ can be generated by two elements only, for instance x_{21} and the matrix (g_{ij}) where

$$g_{ij} = \begin{cases} 1 & \text{if } 1 \leq i \leq N-1 \text{ and } j = i+1 \\ (-1)^N & \text{if } (i,j) = (N,1) \\ 0 & \text{otherwise} \end{cases}$$

([9], p.83). For a (long) list of defining relations between these two matrices, see [9], p.85.

5.8

Let Φ be a root system and L a lattice such that $L_0 \subset L \subset L_1$ as in 3.3.1. Let $G(\mathbb{Z})$ be the associated arithmetic group (3.3.2).

Choose a faithful representation $\rho : \mathcal{L} \to \mathrm{End}(V)$ with weight lattice L as in 3.3.1. The group $G(\mathbb{Z})$ is then generated by the endomorphisms

$$x_\alpha = \exp(\rho(X_\alpha)) \in \mathrm{End}(V)$$

([26], Th. 18, Cor. 3, Example).

Assume furthermore that Φ is irreducible, $\Phi \neq A_1$, and $L = L_1$ (so that the Chevalley group G is simple, simply connected and different from SL_2). The following relations define $G(\mathbb{Z})$ (and generalize 5.6) ([2], Satz 3.1):

$$[x_\alpha, x_\beta] = \prod_{i,j} x_{i\alpha+j\beta}^{N(\alpha,\beta;i,j)} \quad \text{when } \alpha+\beta \neq 0\,;$$

$$(x_\alpha^{-1}\, x_{-\alpha}\, x_\alpha^{-1})^4 = 1 \qquad \text{for any simple root } \alpha.$$

Here i and j run over positive integers and the integers $N(\alpha,\beta;i,j)$ are almost all zero ($N(\alpha,\beta;1,1) = N_{\alpha\beta}$ are the constants defining the Chevalley basis in 3.3.1).

6 Finite subgroups

6.1

Theorem 7 ([4] [23]). *Let Γ be an arithmetic subgroup of a linear algebraic group G over $\mathbb{Q}$. Up to conjugation, Γ contains only finitely many finite subgroups.*

Proof. Let $X = G(\mathbb{R})/K$ and $D \subset X$ be as in the proof of Theorem 6. Any finite subgroup $F \subset \Gamma$ is contained in a maximal compact subgroup K' of $G(\mathbb{R})$. Since $K' = g\,K\,g^{-1}$ is conjugate to K, the point $x = g\,K$ in X is fixed by all $\gamma \in F$.

Let $y \in D$ and $\gamma' \in \Gamma$ be such that $x = \gamma'(y)$. Then, for all $\gamma \in F$, we have

$$\gamma'^{-1}\,\gamma\,\gamma'(y) = y\,.$$

In particular $\gamma'^{-1}\,\gamma\,\gamma'(D)$ meets D and $\gamma'^{-1}\,\gamma\,\gamma'$ lies in the finite set S (Theorem 6, b)). This proves our assertion.

6.2

Theorem 8. *If Γ is an arithmetic subgroup of G, there exists a subgroup of finite index $\Gamma' \subset \Gamma$ which is torsion free.*

Proof. By definition (3.1), Γ is commensurable with $G \cap \mathrm{GL}_N(\mathbb{Z})$ for some embedding of G in $\mathrm{GL}_N(\mathbb{C})$. So it is enough to prove Theorem 8 for $\mathrm{GL}_N(\mathbb{Z})$.

It follows from the following lemma.

Lemma 9. *Let $p \geq 3$ be a prime integer and Γ the set of elements $\gamma \in \mathrm{GL}_N(\mathbb{Z})$ which are congruent to the identity modulo p. Then Γ is a torsion free subgroup of $\mathrm{GL}_N(\mathbb{Z})$.*

Proof. Clearly Γ is a subgroup of $\mathrm{GL}_N(\mathbb{Z})$. If it was not torsion free, it would contain an element of prime order, say $\ell > 1$, so there would exist a square matrix $m \in M_N(\mathbb{Z})$ not divisible by p and some integer $\alpha \geq 1$ such that

$$(1 + p^\alpha\, m)^\ell = 1\,. \tag{11}$$

From the binomial formula, we deduce from (11) that

$$\ell\, p^\alpha\, m = -\sum_{i=2}^{\ell} \binom{\ell}{i} p^{\alpha i}\, m^i\,. \tag{12}$$

When $\ell \neq p$, the exact power of p dividing $\ell\, p^\alpha\, m$ is p^α. But the right hand side of (12) is divisible by $p^{2\alpha}$, so we get a contradiction.

When $\ell = p$, $p^{\alpha+1}$ is the exact power of p dividing the left hand side of (12). When $2 \leq i < p$, p divides $\binom{p}{i}$, therefore $p^{2\alpha+1}$ divides $\binom{p}{i} p^{\alpha i}$. Finally, since $p \geq 3$, $p^{\alpha p}$ is also divisible by $p^{2\alpha+1}$. Therefore $p^{2\alpha+1}$ divides the right hand side of (12) and we get again a contradiction.

6.3

From Lemma 9, Minkowski got some information on the order of the finite subgroups of $\mathrm{GL}_N(\mathbb{Z})$ ([19] 212-218, [5] § 7, Exercises 5-8). Indeed, when $p \geq 3$, any finite subgroup $F \subset \mathrm{GL}_N(\mathbb{Z})$ maps injectively into the quotient group $\mathrm{GL}_N(\mathbb{Z}/p)$, the order of which is

$$a(N,p) = (p^N - 1)(p^N - p) \cdots (p^N - p^{N-1})\,.$$

If ℓ is an odd prime, and if the reduction of p modulo ℓ^2 is a generator of $(\mathbb{Z}/\ell^2\,\mathbb{Z})^*$, the power of ℓ dividing $a(N,p)$ is exactly $\ell^{r(\ell,N)}$ with

$$r(\ell,N) = \left[\frac{N}{\ell-1}\right] + \left[\frac{N}{\ell(\ell-1)}\right] + \left[\frac{N}{\ell^2(\ell-1)}\right] + \cdots\,,$$

where $[x]$ denotes the integral part of the real number x. Conversely, it can be shown (loc. cit.) that $\mathrm{GL}_N(\mathbb{Z})$ contains a finite subgroup of order $\ell^{r(\ell,N)}$.

The same results are true when $\ell = 2$ and

$$r(2,N) = N + \left[\frac{N}{2}\right] + \left[\frac{N}{4}\right] + \cdots .$$

If we denote by $m(N)$ the product over all primes ℓ of $\ell^{r(\ell,N)}$, we conclude that $m(N)$ is the least common multiple of the cardinality of the finite subgroups of $\mathrm{GL}_N(\mathbb{Z})$. For instance

$$m(2) = 24\,,\ m(3) = 48\,,\ m(4) = 5760, \ldots$$

6.4

Let us come back to $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 10. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be any torsion free subgroup. Then Γ is a free group.*

Proof. Let $\mathcal{H}$ be the Poincaré upper half-plane. Recall from Theorem 1 that $\mathrm{SL}_2(\mathbb{Z})$ acts upon $\mathcal{H}$ with fundamental domain the set D of those $z \in \mathcal{G}$ such that $|z| \geq 1$ and $|\mathrm{Re}(z)| \leq 1/2$.

The stabilizer in $\mathrm{SL}_2(\mathbb{Z})$ of any $z \in \mathcal{H}$ is finite. Indeed $\mathcal{H} = \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$ hence the stabilizer of z is the intersection of the discrete group $\mathrm{SL}_2(\mathbb{Z})$ with a conjugate of the compact group $\mathrm{SO}_2(\mathbb{R})$. Since Γ is torsion free, it acts freely on $\mathcal{H}$ (it has no fixed point).

Let $D_0 \subset D$ be the set of points $z \in \mathcal{H}$ such that $|z| = 1$ and $|\mathrm{Re}(z)| \leq 1/2$, and

$$Y = \mathrm{SL}_2(\mathbb{Z}) \cdot D_0$$

the union of the translates of D_0 under $\mathrm{SL}_2(\mathbb{Z})$:

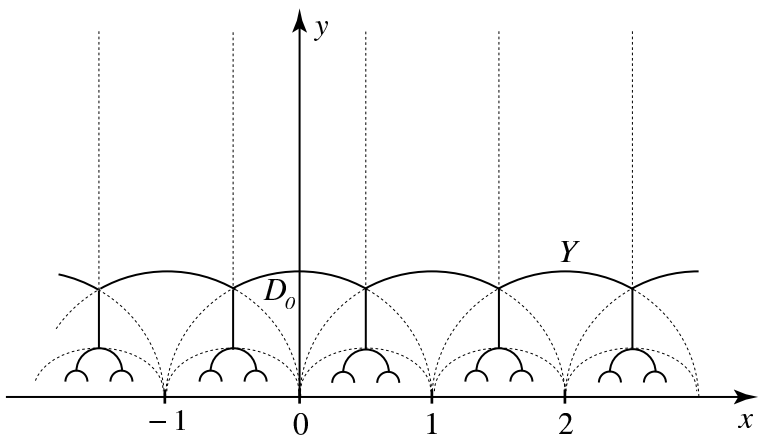

Figure 3

Proposition 11 ([24]). *The set Y is (the topological realization of) a tree.*

Proof of Proposition 11. Clearly Y is a graph, and we want to show that Y can be contracted (deformed) to a point. Consider the retraction of D onto D_0 which maps $z \in D$ to the point $z' \in D_0$ with the same abcissa as z. When $z \in D - D_0$ and $\gamma(z) \in D$ we know that $\gamma(z) = z \pm 1$ (1.2, Remark). Therefore this retraction commutes with the action of $\mathrm{SL}_2(\mathbb{Z})$ on D, and it can be extended to a retraction of $\mathcal{H} = \mathrm{SL}_2(\mathbb{Z}) \cdot D$ onto $Y = \mathrm{SL}_2(\mathbb{Z}) \cdot D_0$. Since $\mathcal{H}$ is contractible to a point, the same is true for Y. q.e.d.

To end the proof of Theorem 10 note that Γ acts freely on the tree Y, so it can be identified with the fundamental group of the quotient:

$$\Gamma = \pi_1(\Gamma \backslash Y)\,.$$

This quotient $\Gamma \backslash Y$ is a connected graph and we have:

Proposition 12. *Let $\mathcal{X}$ be a connected graph. Then $\pi_1(\mathcal{X})$ is free.*

Proof. Choose a maximal tree $T \subset \mathcal{X}$. Clearly T contains all the vertices of $\mathcal{X}$. Therefore, after contracting T, $\mathcal{X}$ becomes a "bouquet" of circles B. We get

$$\pi_1(\mathcal{X}) = \pi_1(B) = F(S)\,,$$

where S is the set of circles in B.

6.5

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be torsion free with finite index $e = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. It can be shown that 12 divides e (see 6.6 below) and that the number of generators of Γ is $1 + \frac{e}{12}$.

For instance, the subgroup of commutators

$$\Gamma = [\mathrm{SL}_2(\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z})]$$

has index 12 in $\mathrm{SL}_2(\mathbb{Z})$. It is free on the two generators $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$.

6.6

Let $N \geq 2$ and let $\Gamma \subset \mathrm{SL}_N(\mathbb{Z})$ be a torsion free normal subgroup of $\mathrm{SL}_N(\mathbb{Z})$. Any finite subgroup of $\mathrm{SL}_N(\mathbb{Z})$ maps injectively into the quotient $\mathrm{SL}_N(\mathbb{Z})/\Gamma$. Therefore the index $[\mathrm{SL}_N(\mathbb{Z}) : \Gamma]$ is divisible by $m(N)/2$, where $m(N)$ is as in 6.3. We have just seen that $\mathrm{SL}_2(\mathbb{Z})$ contains a torsion free subgroup of index $m(2)/2 = 12$. But, when $N \geq 3$, I do not know what the minimal index of a torsion free subgroup of $\mathrm{SL}_N(\mathbb{Z})$ is (a question raised by W. Nahm).

III. Rigidity

7 The congruence subgroup problem

7.1

Let $G \subset \mathrm{GL}_N(\mathbb{C})$ be a linear algebraic group over $\mathbb{Q}$ and $\Gamma \subset G(\mathbb{Q})$ an arithmetic subgroup. For any $a \geq 1$ we define a *congruence subgroup* $\Gamma(a)$ of Γ. It consists of those matrices in $\Gamma \cap \mathrm{GL}_N(\mathbb{Z})$ which are congruent to the identity modulo a. This is a subgroup of finite index in Γ.

Definition. *We say that G has property (CS) if any $\Gamma' \subset \Gamma$ of finite index contains a congruence subgroup $\Gamma(a)$.*

It can be shown that this property depends on G only and neither on the choice of Γ nor on the embedding $G \subset \mathrm{GL}_N(\mathbb{C})$.

Theorem 13.

i) ([1] [27] [18]) *If Φ is an irreducible root lattice different from A_1 and if $L = L_1$, the (simple and simply connected) Chevalley group G attached to Φ and L (see 3.3.1) has property (CS).*
ii) *The group SL_2 does not satisfy (CS) (see Corollary 18 below).*

7.2

Let us define *projective limits* of groups. Consider a partially ordered set I such that, for any i, j in I, there is some $k \in I$ with $k \geq i$ and $k \geq j$. Assume given a family of groups G_i, $i \in I$, and morphisms $\varphi_{ji} : G_j \to G_i$, when $j \geq i$, such that $\varphi_{ii} = \mathrm{id}$ and $\varphi_{ki} = \varphi_{ji} \circ \varphi_{kj}$ when $k \geq j \geq i$. By definition, the projective limit $\varprojlim_i G_i$ is the group consisting of families $(g_i)_{i \in I}$ such that $g_i \in G_i$ and $\varphi_{ji}(g_j) = g_i$ if $j \geq i$.

When $\Gamma \subset G(\mathbb{Q})$ is an arithmetic group, we can consider two projective limits. The first one is

$$\hat{\Gamma} = \varprojlim_N \Gamma/N\,,$$

where N runs over all normal subgroups of finite index in Γ. We can also define

$$\tilde{\Gamma} = \varprojlim_a \Gamma/\Gamma(a)\,,$$

where $\Gamma(a)$, $a \geq 1$, runs over all congruence subgroups of Γ. There is a surjective map

$$\hat{\Gamma} \to \tilde{\Gamma}$$

and we let $C(\Gamma)$ be the kernel of this map. The group $C(\Gamma)$ is trivial iff G has property (CS).

Note also that we have an inclusion

$$\tilde{\Gamma} \to \widetilde{\mathrm{GL}_N(\mathbb{Z})} = \mathrm{GL}_N(\mathbb{A}_f)\,,$$

where $\mathbb{A}_f = \varprojlim_a \mathbb{Z}/a\mathbb{Z}$ is the ring of finite adeles. In [1] (16.1), Bass, Milnor and Serre considered the following properties:

a) $C(\Gamma)$ is finite;
b) the image of $\hat{\Gamma} \to \mathrm{GL}_N(\mathbb{A}_f)$ contains a congruence subgroup of $\mathrm{GL}_N(\mathbb{Z})$.

They conjectured that a) and b) are true when G is simple and simply connected over $\mathbb{Q}$ (and not necessarily split). Under these assumptions, the assertion a) is known today in many cases: see [22] § 9.5, where G can also be defined over some number field. And the assertion b) is true when $G(\mathbb{R})$ is not compact, by the strong approximation theorem ([1] loc. cit., [22] Th. 7.12).

7.3

The interest of a) and b) is the following "rigidity" result ([1] Theorem 16.2):

Proposition 14. *Assume G is a semi-simple group which is simply connected (*i.e. *G does not have any nontrivial central extension), let $\Gamma \subset G(\mathbb{Q})$ be an arithmetic subgroup satisfying* a) *and* b) *in* 7.2*, and let*

$$\rho : \Gamma \to \mathrm{GL}_N(\mathbb{Q})$$

be any representation. Then there exists an algebraic group morphism

$$\varphi : G \to \mathrm{GL}_N$$

and a subgroup of finite index $\Gamma' \subset \Gamma$ such that the restrictions of ρ and φ to Γ' coincide.

Remark. Stronger results were obtained later by Margulis [18]; see below Theorem 22.

7.4

We derive from Proposition 14 several consequences.

Corollary 15. *Let G and Γ be as in Proposition* 14 *and let*

$$\Gamma \to \mathrm{Aut}(V)$$

be any representation of Γ on a finite dimensional $\mathbb{Q}$-vector space. Then V contains a lattice stable by Γ.

Proof. Let $\varphi : G \to \mathrm{Aut}(V)$ and $\Gamma' \subset \Gamma$ be chosen as in the proposition. Then $\varphi(\Gamma')$ is contained in an arithmetic subgroup of $\mathrm{Aut}(V)$ (see Proposition 3),

hence there is a lattice Λ' in V stable by Γ' (or a finite index subgroup). Let $S \subset \Gamma$ be a set of representatives of Γ modulo Γ'. The lattice

$$\Lambda = \sum_{s \in S} s(\Lambda')$$

in V is stable by Γ.

Corollary 16. *Let G and Γ be as in Proposition* 14 *and let*

$$0 \to V' \to V \to V'' \to 0$$

be an exact sequence of finite dimensional representations of Γ over $\mathbb{Q}$. This sequence splits.

Proof. Choose $\Gamma' \subset \Gamma$ such that the restriction of the exact sequence to Γ' is induced by an exact sequence of algebraic representations of G. Since G is semi-simple, hence reductive, this sequence of representations is split by a section $\sigma' : V'' \to V$ which commutes with the action of G and Γ'. If S is a set of representatives of Γ modulo Γ', the formula

$$\sigma(x) = \frac{1}{\mathrm{Card}(S)} \sum_{s \in S} s\, \sigma'\, s^{-1}(x)\,,$$

$x \in V''$, defines a Γ-equivariant splitting of the exact sequence.

Corollary 17. *When G and Γ are as in Proposition* 14*, the abelian group $\Gamma/[\Gamma,\Gamma]$ is finite.*

Proof. The quotient $\Gamma/[\Gamma,\Gamma]$ of Γ by its commutator subgroup is abelian and finitely generated. If it was infinite there would exist a nontrivial morphism

$$\chi : \Gamma \to \mathbb{Z}\,.$$

Let $V = \mathbb{Q}^2$ be equipped with the Γ-action $\Gamma \to \mathrm{Aut}(V)$ which maps γ to $\begin{pmatrix} 1 & \chi(\gamma) \\ 0 & 1 \end{pmatrix}$. We get an exact sequence

$$0 \to V' \to V \to V'' \to 0$$

where Γ acts trivially on $V' \simeq V'' \simeq \mathbb{Q}$. Since χ is nontrivial, this sequence is not trivial, and this contradicts Corollary 16.

Corollary 18. *The group* SL_2 *does not satisfy (CS).*

Proof. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be any arithmetic subgroup. We shall prove that $C(\Gamma)$ is infinite. If $\Gamma' \subset \Gamma$ is a torsion free subgroup of finite index, the morphism

$$C(\Gamma') \to C(\Gamma)$$

has finite kernel and cokernel, therefore we can assume $\Gamma' = \Gamma$. But then, by Theorem 10, Γ is free, therefore $\Gamma/[\Gamma,\Gamma]$ is a nontrivial free abelian group. The group SL_2 satisfies the strong approximation theorem, therefore b) in 7.2 is true. From Proposition 14 and Corollary 17, we conclude that a) is not true, *i.e.* $C(\Gamma)$ is infinite.

8 Kazhdan's property (T)

Let G be a topological group and π a unitary representation of G in a Hilbert space $\mathcal{H}$. We say that π *contains almost invariant vectors* when, for every $\varepsilon > 0$ and every compact subset $K \subset G$, there is a vector $v \in \mathcal{H}$, $v \neq 0$, such that

$$\|\pi(g)\, v - v\| < \varepsilon$$

for all $g \in K$.

The group G has *property (T)* when any unitary representation π which contains almost invariant vectors has an invariant vector (a $w \neq 0$ such that $\pi(g)\, w = w$ for all $g \in G$).

Theorem 19 ([13]).

i) *Assume that G is locally compact and that $\Gamma \subset G$ is a closed subgroup such that the invariant volume of $\Gamma \backslash G$ is finite. Then G has property (T) iff Γ has property (T).*
ii) *Assume Γ is discrete and has property (T). Then Γ is finitely generated and $\Gamma/[\Gamma, \Gamma]$ is finite.*

Theorem 20 ([21] Theorem 3.9, p.19). *Let G be a simple connected Lie group. Then G has property (T) iff it is not locally isomorphic to* $\mathrm{SO}(n, 1)$ *or* $\mathrm{SU}(n, 1)$*, $n \geq 2$.*

(Recall that G is simple if it does not contain any proper nontrivial closed normal connected subgroup).

We can combine Theorem 19 i), Corollary 5 ii) and Theorem 20 to show that some arithmetic groups have property (T). For instance, $\mathrm{SL}_N(\mathbb{Z})$ has property (T) iff $N \geq 3$. For an "effective" version of that result, see [12].

9 Arithmeticity

9.1

When G is semi-simple over $\mathbb{Q}$, we know from Corollary 5 ii) that any arithmetic subgroup $\Gamma \subset G(\mathbb{Q})$ has finite covolume in $G(\mathbb{R})$. A famous conjecture of Selberg asked for a converse to this assertion. It was proved by Margulis [16]. We state his theorem for simple Lie groups.

Theorem 21 ([16]). *Let H be a connected simple non-compact Lie group of rank bigger than one, and $\Gamma \subset H$ a discrete subgroup of finite covolume. Then Γ is "arithmetic".*

We need to explain what being "arithmetic" means: there exists a linear algebraic group G over $\mathbb{Q}$, an arithmetic subgroup Γ' of G, a compact Lie group K and an isomorphism of Lie groups

$$G(\mathbb{R}) \simeq H \times K$$

such that the first projection of Γ' into H has finite index in Γ.

9.2

When $H = \mathrm{PSL}_2(\mathbb{R})$ (a case of rank one), Theorem 21 is not true anymore. Indeed, let M be a compact Riemann surface. Uniformization gives an embedding of $\Gamma = \pi_1(M)$ into $\mathrm{PSL}_2(\mathbb{R})$, and the quotient $\Gamma\backslash\mathrm{PSL}_2(\mathbb{R})$ is compact. But, in general, Γ is not arithmetic.

9.3

The proof of Theorem 21 uses the following "superrigidity" theorem, and its non-archimedean analogs (see [17], [21] Theorem 6.2.1 or [29] for a general statement):

Theorem 22. *Let $\Gamma \subset H$ be as in Theorem 21. Assume that G is a semi-simple algebraic group over $\mathbb{R}$ and $f : \Gamma \to G(\mathbb{R})$ is a group morphism such that $f(\Gamma)$ is Zariski dense. Then f is the restriction to Γ of a morphism of Lie groups $H \to G(\mathbb{R})$.*

9.4

Let us conclude this survey with another result of Margulis [15], concerning all normal subgroups of a given arithmetic group:

Theorem 23. *Assume G is a linear algebraic group over $\mathbb{R}$ such that $G(\mathbb{R})$ is connected, simple, not compact and of real rank bigger than one. If $\Gamma \subset G(\mathbb{R})$ is discrete with finite covolume, any normal subgroup $N \subset \Gamma$ has finite index in Γ or it is contained in the center of Γ.*

Appendix

Following E. Cartan, Cremmer and Julia give in [8] the following description of the simple complex Lie algebra of type E_7 and its fundamental representation of dimension 56.

Let $W = \mathbb{C}^8$, with basis e_i, $1 \leq i \leq 8$, and W^* its complex dual, with dual basis e_i^*, $1 \leq i \leq 8$. For any positive integer k, we let $\Lambda^k W$ be the k-th exterior power of W, i.e. the linear subspace of $W^{\otimes k}$ consisting of fully antisymmetric tensors. A basis of $\Lambda^k W$ consists of the vectors

$$e_{i_1} \wedge \ldots \wedge e_{i_k} = \sum_{\sigma \in \mathcal{S}_k} \varepsilon(\sigma)\, e_{i_{\sigma(1)}} \otimes \ldots \otimes e_{i_{\sigma(k)}}\,,$$

with $1 \leq i_1 < i_2 < \ldots < i_k \leq 8$, where $\mathcal{S}_k$ is the permutation group on k letters and $\varepsilon(\sigma)$ is the signature of σ. The exterior product

$$\Lambda^k W \otimes \Lambda^\ell W \to \Lambda^{k+\ell} W$$

sends $(v_1 \wedge \ldots \wedge v_k) \otimes (w_1 \wedge \ldots \wedge w_\ell)$ to $v_1 \wedge \ldots \wedge v_k \wedge w_1 \wedge \ldots \wedge w_\ell$. The basis $e_1 \wedge \ldots \wedge e_8$ gives an identification $\Lambda^8 W = \mathbb{C}$ and, together with the exterior product, an isomorphism

$$(\Lambda^k W)^* = \Lambda^{8-k} W$$

for all $k \leq 8$.

On the other hand, we get a pairing

$$\Lambda^k W \otimes \Lambda^k(W^*) \to \mathbb{C}$$

by sending $(v_1 \wedge \ldots \wedge v_k) \otimes (\lambda_1 \wedge \ldots \wedge \lambda_k)$ to the determinant of the k by k matrix $(\lambda_j(v_i))_{1 \leq i,j \leq k}$. This pairing identifies $\Lambda^k(W^*)$ with $(\Lambda^k W)^*$.

Let now $V = \Lambda^2(W^*) \oplus \Lambda^2(W)$, a complex vector space of dimension 56. The complex Lie algebra $\Lambda = sl_8(\mathbb{C})$ acts upon W, hence on V.

Let $\Sigma = \Lambda^4 W$, so that $\dim_{\mathbb{C}}(\Sigma) = 70$. From the previous discussion, we get natural pairings

$$\Lambda^4 W \otimes \Lambda^2(W^*) \xrightarrow{\sim} (\Lambda^4 W)^* \otimes \Lambda^2(W^*) \to \Lambda^6(W^*) = \Lambda^2(W)$$

and

$$\Lambda^4 W \otimes \Lambda^2 W \to \Lambda^6 W = (\Lambda^2 W)^* = \Lambda^2(W^*)\,.$$

Let

$$\Sigma \otimes V \to V$$

be the action of Σ on V obtained by taking the direct sum of these maps and multiplying the result by 2.

The action of

$$\mathcal{G} = \Lambda \oplus \Sigma$$

on V defines an embedding

$$\mathcal{G} \subset \mathrm{End}(V)\,,$$

which is the one given by formulae (B1) in [8] (the factor 2 above comes from the permutation of k and ℓ in the expression $\sum_{ijk\ell} x^{k\ell}$ of loc.cit.). The vector space $\mathcal{G}$ is stable under the Lie bracket, which is given by formulae (B2) in [8], and the action of $\mathcal{G}$ on V respects the canonical symplectic form on V coming from the pairing

$$\Lambda^2(W^*) \otimes \Lambda^2 W \to \mathbb{C}\,.$$

Therefore $\mathcal{G}$ is contained in $sp_{56}(\mathbb{C})$.

Let us now apply Chevalley's construction to this representation of $\mathcal{G}$ on V. A Cartan subalgebra of $\mathcal{G}$ is the diagonal subalgebra $\mathcal{H} \subset \Lambda$. We let

$$\varepsilon_i : \mathcal{H} \to \mathbb{C}\ , \quad 1 \le i \le 8\,,$$

be the character sending a diagonal matrix to its i-th entry. Note that $\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_8 = 0$ on $\mathcal{H}$. The action of $\mathcal{H}$ on $\mathcal{G} = \Lambda \oplus \Sigma$ is the restriction of the action of $\Lambda = sl_8(\mathbb{C})$. Therefore the roots of $\mathcal{H}$ are of two types.

The roots of "type Λ" are those given by the action of $\mathcal{H}$ on Λ. These are $\alpha = \varepsilon_i - \varepsilon_j$, for all $i \neq j$, $1 \le i, j \le 8$. The corresponding eigenspace $\mathcal{G}_\alpha$ is spanned by $X_\alpha = X_{ij}$, the matrix having 1 as (i, j) entry, all others being zero. There are 63 roots of type Λ.

The roots of "type Σ" are those given by the action of $\mathcal{H}$ on $\Sigma = \Lambda^4 W$. Given four indices $1 \le i_1 < i_2 < i_3 < i_4 \le 8$ we get the root $\alpha = \varepsilon_{i_1} + \varepsilon_{i_2} + \varepsilon_{i_3} + e_{i_4}$, with $\mathcal{G}_\alpha$ spanned by

$$X_\alpha = \frac{1}{2}\, e_{i_1} \wedge e_{i_2} \wedge e_{i_3} \wedge e_{i_4}\,.$$

There are 70 roots of type Σ. Let Φ be the set of all roots.

We claim that the vectors X_α and $H_\alpha = [X_\alpha, X_{-\alpha}]$, $\alpha \in \Phi$, form a Chevalley basis of $\mathcal{G}$. According to [11], proof of Proposition 25.2, this will follow if we prove that the Cartan involution σ satisfies

$$\sigma(X_\alpha) = -X_{-\alpha} \tag{13}$$

and that the Killing form K is such that

$$K(X_\alpha, X_{-\alpha}) = 2/(\alpha, \alpha)\,, \tag{14}$$

for every root $\alpha \in \Phi$.

The Cartan involution σ on $\mathcal{G}$ is the restriction of the Cartan involution on $\mathrm{End}(V)$, so it is the standard one on $\Lambda = sl_8(\mathbb{C})$ and we get

$$\sigma(X_{ij}) = -X_{ji}\,.$$

On the other hand, the pairings of $Z = \Lambda^4 W$ with $\Lambda^2(W^*)$ and $\Lambda^2 W$ are dual to each other. Therefore, if $x \in Z$ we have $\sigma(x) = -x^*$, where x^* is the image of x by the isomorphism

$$\Lambda^4 W \xrightarrow{\sim} (\Lambda^4 W)^* = \Lambda^4(W^*)$$

followed by the identification of W and W^* coming from the chosen bases. This sends $e_1 \wedge e_2 \wedge e_3 \wedge e_4$ to $e_5^* \wedge e_6^* \wedge e_7^* \wedge e_8^*$, and then to $e_5 \wedge e_6 \wedge e_7 \wedge e_8$. We conclude that

$$\sigma(e_1 \wedge e_2 \wedge e_3 \wedge e_4) = -e_5 \wedge e_6 \wedge e_7 \wedge e_8 \,.$$

The root corresponding to $e_5 \wedge e_6 \wedge e_7 \wedge e_8$ is

$$\varepsilon_5 + \varepsilon_6 + \varepsilon_7 + \varepsilon_8 = -(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4) \,.$$

This proves (13) for roots of type Σ.

Let us now check (14). According to the definitions in [11] 8.2 and 8.3, we have

$$(\alpha, \alpha) = K(T_\alpha, T_\alpha)$$

where $T_\alpha \in \mathcal{H}$ is defined by the equality

$$\alpha(h) = K(T_\alpha, H)$$

for all $H \in \mathcal{H}$. When $X, Y \in \Lambda$ are two 8×8 matrices of trace zero, we have, as indicated in [8] (B5),

$$K(X, Y) = 12 \operatorname{tr}(XY) \,.$$

Let $\alpha = \varepsilon_i - \varepsilon_j$ be a root of type Λ and H_{ij} the diagonal matrix such that $\varepsilon_i(H_{ij}) = 1$, $\varepsilon_j(H_{ij}) = -1$ and $\varepsilon_k(H_{ij}) = 0$ if $k \notin \{i, j\}$. For any $H \in \mathcal{H}$ we have

$$\alpha(H) = \operatorname{tr}(H_{ij}\, H) \,,$$

therefore

$$T_\alpha = H_{ij}/12$$

and

$$(\alpha, \alpha) = \frac{1}{144} K(H_{ij}, H_{ij}) = \frac{24}{144} = \frac{1}{6} \,.$$

Since $K(X_\alpha, X_{-\alpha}) = 12$, the equality (14) holds true.

Assume now that $\alpha = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4$, $X_\alpha = \frac{1}{2}\, e_1 \wedge e_2 \wedge e_3 \wedge e_4$ and $X_{-\alpha} = \frac{1}{2}\, e_5 \wedge e_6 \wedge e_7 \wedge e_8$. According to (B5) in [8] we have

$$K(X_\alpha, X_{-\alpha}) = \frac{2}{24} \frac{1}{4} (4!)(4!) = 12 \,.$$

Let H' be the diagonal matrix such that $\varepsilon_i(H') = 1/2$ when $1 \le i \le 4$ and $\varepsilon_i(H') = -1/2$ when $5 \le i \le 8$. Given any H in $\mathcal{H}$ we have

$$\operatorname{tr}(H'H) = \frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 - \varepsilon_5 - \varepsilon_6 - \varepsilon_7 - \varepsilon_8)(H) = \alpha(H)\,.$$

Therefore $T_\alpha = H'/12$ and

$$(\alpha, \alpha) = \frac{1}{144}\, K(H', H') = \frac{12}{144} \times \frac{8}{4} = \frac{1}{6}\,.$$

Therefore (14) is true for α.

The Lie algebra $\mathcal{G}$ is simple of type E_7. Indeed, a basis of its root system Φ consist of $\alpha_1 = \varepsilon_1 - \varepsilon_2$, $\alpha_2 = \varepsilon_4 + \varepsilon_5 + \varepsilon_6 + \varepsilon_7$, $\alpha_3 = \varepsilon_2 - \varepsilon_3$, $\alpha_4 = \varepsilon_3 - \varepsilon_4$, $\alpha_5 = \varepsilon_4 - \varepsilon_5$, $\alpha_6 = \varepsilon_5 - \varepsilon_6$ and $\alpha_7 = \varepsilon_6 - \varepsilon_7$. Its Dynkin diagram is the one of E_7 ([11], 11.4).

Let us now consider the representation ρ of $\mathcal{G}$ on V. Its weight vectors are $e_i^* \wedge e_j^* \in \Lambda^2(W^*)$ and $e_i \wedge e_j \in \Lambda^2 W$, $1 \le i < j \le 8$, with corresponding weights $-\varepsilon_i - \varepsilon_j$ and $\varepsilon_i + \varepsilon_j$. The root lattice L_0 of E_7 has index 2 in its weight lattice L_1 ([11], 13.1). Since the weights of ρ are not in L_0 they must span the lattice L_1. Therefore, the Chevalley group G generated by the endomorphisms $\exp(t\rho(X_\alpha))$, $t \in \mathbb{C}$, $\alpha \in \Phi$, is the simply connected Chevalley group of type E_7. Its set of real points $G(\mathbb{R})$ is the real Lie group spanned by the endomorphisms $\exp(t\rho(X_\alpha))$, $t \in \mathbb{R}$, $\alpha \in \Phi$ ([26], § 5, Th. 7, Cor. 3), i.e. the split Lie group $E_{7(+7)}$.

Let $M \subset V$ be the standard lattice, with basis $e_i^* \wedge e_j^*$ and $e_i \wedge e_j$, $1 \le i < j \le 8$. The group $E_7(\mathbb{Z}) = E_{7(+7)} \cap \mathrm{Sp}_{56}(\mathbb{Z})$ is the stabilizer of M in G. So, according to [26], § 8, Th. 18, Cor. 3, to check that $E_7(\mathbb{Z}) = G(\mathbb{Z})$, all we need to prove is that the lattice M is admissible, i.e. stable by the endomorphisms $\rho(X_\alpha)^n/n!$ for all $n \ge 1$ and $\alpha \in \Phi$.

When $\alpha = \varepsilon_i - \varepsilon_j$ is of type Λ, $\rho(X_\alpha) = X_{ij}$ has square zero and stabilizes the standard lattice M. Assume finally that $\alpha = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4$, hence $X_\alpha = \frac{1}{2}\, e_1 \wedge e_2 \wedge e_3 \wedge e_4$. By definition of the action of Z on $V = \Lambda^2(W^*) \oplus \Lambda^2 W$, $\rho(X_\alpha)$ sends $e_i \wedge e_j$ to $\pm\, e_k^* \wedge e_\ell^*$ when $5 \le i < j$, $k < \ell$ and $\{i, j, k, \ell\} = \{5, 6, 7, 8\}$. When $i < 5$, $\rho(X_\alpha)(e_i \wedge e_j) = 0$. Similarly, when $i < j \le 4$, $\rho(X_\alpha)$ sends $e_i^* \wedge e_j^*$ to $\pm\, e_k \wedge e_\ell$ with $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$, and $\rho(X_\alpha)(e_i^* \wedge e_j^*) = 0$ if $j > 4$. From this it follows that the endomorphism $\rho(X_\alpha)$ has square zero and stabilizes M. Therefore $E_7(\mathbb{Z}) = G(\mathbb{Z})$.

References

1. H. Bass, J.W. Milnor, J.-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Publ. Math. Inst. Hautes Etud. Sci.* **33**, 59-137 (1967).
2. H. Behr, Explizite Präsentation von Chevalleygruppen über $\mathbb{Z}$, *Math. Z.* **141**, 235-241 (1975).
3. A. Borel, *Introduction aux groupes arithmétiques*, Paris, Hermann & Cie. 125 p. (1969).
4. A. Borel, Arithmetic properties of linear algebraic groups, *Proc. Int. Congr. Math. 1962*, 10-22 (1963).
5. N. Bourbaki, *Éléments de mathématique*, Fasc. XXXVII: Groupes et algèbres de Lie; Chap. II: Algèbres de Lie libres; Chap. III: Groupes de Lie; *Actualités scientifiques et industrielles* 1349, Paris, Hermann. 320 p. (1972).
6. D. Carter, G. Keller, Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$, *Am. J. Math.* **105**, 673-687 (1983).
7. C. Chevalley, Certains schémas de groupes semi-simples, *Semin. Bourbaki* **13** (1960/61), No. 219 (1961).
8. E. Cremmer, B. Julia., The $SO(8)$ supergravity. Nucl.Phys.B **159**,141-212 (1979).
9. H.S.M. Coxeter, W.O.J. Moser, *Generators and relations for discrete groups*, 4th ed., Erg. der Math. und ihrer Grenzg. **14** Berlin-Heidelberg-New York, Springer-Verlag, IX, 169 p.
10. C.M. Hull, P.K. Townsend, Unity of Superstrings Dualities, Nucl.Phys.B **438**, 109-137 (1995).
11. J.E. Humphreys, *Introduction to Lie algebras and representation theory*, 3rd printing, Rev. Graduate Texts in Mathematics **9**. New York - Heidelberg - Berlin, Springer-Verlag, XII, 171 p.
12. M. Kassabov, Kazhdan Constants for $\mathrm{SL}_n(\mathbb{Z})$, math.GR/0311487 (2003) 22 p.
13. D.A. Kazhdan, Connection of the dual space of a group with the structure of its closed subgroups, *Funct. Anal. Appl.* **1**, 63-65 (1967); translation from *Funkts. Anal. Prilozh.* **1**, No.1, 71-74 (1967).
14. S. Lang, *Algebra*, Reading, Mass., Addison-Wesley Publishing Company, Inc., XVIII, 508 p.
15. G.A. Margulis, Finiteness of factor groups of discrete subgroups, *Funkts. Anal. Prilozh.* **13**, No.3, 28-39 (1979).
16. G.A. Margulis, Arithmeticity of the irreducible lattices in the semi-simple groups of rank greater than 1, *Invent. Math.* **76**, 93-120 (1984).
17. Margulis, *Discrete subgroups of semisimple Lie groups*, Erg. Math. und ihrer Grenzg., 3. Folge, **17**, Berlin etc.: Springer-Verlag. ix, 388 p.
18. H. Matsumoto, Sur les sous-groupes arithmétiques des groupes semi-simples déployés, *Ann. Sci. Ec. Norm. Supér.*, IV, Sér. 2, 1-62 (1969).
19. J.W. Milnor, *Introduction to algebraic K-theory*, Annals of Mathematics Studies **72**, Princeton, N. J., Princeton University Press and University of Tokyo Press, XIII, 184 p.
20. H. Minkowski, Gesamm. Abh., Leipzig-Berlin, Teubner, 1911 (Bd I, S. 212-218).

21. A.L. Onishchik, (ed.); E.B. Vinberg, (ed.); R.V. Gamkrelidze, (ed.), Lie groups and Lie algebras II. Transl. from the Russian by John Danskin, *Encyclopaedia of Mathematical Sciences* **21**, Berlin, Springer, 223 p.
22. V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, Transl. from the Russian by Rachel Rowen, Pure and Applied Mathematics (New York), **139**, Boston, MA, Academic Press, xi, 614 p.
23. M.S. Raghunathan, *Discrete subgroups of Lie groups*, *Erg. der Math. und ihrer Grenzg.* **68**, Berlin-Heidelberg-New York, Springer-Verlag, VIII, 227 p.
24. J.-P. Serre, *A course in arithmetic*, Translation of "Cours d'arithmétique", 2nd corr. print, Graduate Texts in Mathematics, **7**, New York, Heidelberg, Berlin, Springer-Verlag, IX, 115 p.
25. J.-P. Serre, *Trees*, Transl. from the French by John Stillwell, Corrected 2nd printing of the 1980 original, Springer Monographs in Mathematics, Berlin, Springer, ix, 142 p.
26. R. Steinberg, *Lectures on Chevalley groups*, Yale, 1967.
27. L.N. Vaserstein, On the congruence problem for classical groups, *Funct. Anal. Appl.* **3**, 244-246 (1969).
28. W.C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics **66**, New York, Heidelberg, Berlin, Springer-Verlag, XI, 164 p.
29. R.J. Zimmer, *Ergodic theory and semisimple groups*, Monographs in Mathematics **81**, Boston-Basel-Stuttgart, Birkhäuser, X, 209 p.