Arithmetic Groups and the Lehmer Conjecture

Lam Pham and François Thilmany

ABSTRACT. We generalize a result of Sury [Sur92] and prove that uniform discreteness of cocompact lattices in higher rank semisimple Lie groups (first conjectured by Margulis [Mar91]) is equivalent to a weak form of Lehmer's conjecture. We include a short survey of related results and conjectures.

1. Introduction and main result

1.1. Margulis' arithmeticity theorem and conjecture. Let $\mathbf{G}$ be a connected semisimple $\mathbb{R}$-group with $\mathrm{rank}_{\mathbb{R}}(\mathbf{G}) \geq 2$. Then, $G = \mathbf{G}(\mathbb{R})$ is a semisimple Lie group and Margulis' celebrated *arithmeticity theorem* [Mar75] states that every irreducible lattice $\Gamma \subset G$ is *arithmetic* (see §3 for precise definitions and statements).

The starting point of this paper is the following consequence of arithmeticity for irreducible non-cocompact lattices [Mar91, IX, (4.21-A)]:

Theorem (Margulis). Assume that $\mathbf{G}$ has no $\mathbb{R}$-anisotropic factor. There is a neighbourhood $U \subset G$ of the identity such that for any irreducible non-cocompact lattice $\Gamma \subset G$, the intersection $U \cap \Gamma$ consists of unipotent elements.

Margulis [Mar91, IX, (4.21-B)] then conjectured that an analogous statement would hold for cocompact lattices. In fact, Margulis indicates that this conjecture would follow from a weaker form of Lehmer's conjecture, which we recall below (see namely Conjecture (C)).

Conjecture (A) (Margulis). Let $\mathbf{G}$ be a connected semisimple $\mathbb{R}$-group. Suppose $\mathrm{rank}_{\mathbb{R}}(\mathbf{G}) \geq 2$. Then there exists a neighborhood $U \subset \mathbf{G}(\mathbb{R})$ of the identity such that for any irreducible cocompact lattice $\Gamma \subset \mathbf{G}(\mathbb{R})$, the intersection $U \cap \Gamma$ consists of elements of finite order.

For the purpose of this paper, it will be useful to work with the following statement.

Margulis' conjecture for a family $\mathscr{T}$ of semisimple $\mathbb{R}$-groups. For each $\mathbf{G} \in \mathscr{T}$, there exists a neighborhood $U \subset \mathbf{G}(\mathbb{R})$ of the identity such that for any irreducible cocompact *arithmetic* lattice Γ in $\mathbf{G}(\mathbb{R})$, the intersection $U \cap \Gamma$ consists of elements of finite order.

Note that in view of the arithmeticity theorem, 'Margulis' conjecture for higher rank groups' is in this sense simply Conjecture (A).

Remark. An even stronger statement than Conjecture (A) holds for p-adic groups. Namely, if k is a non-archimedean local field of characteristic zero and $\mathbf{G}$ is an algebraic k-group (of dimension > 0), then

there is an open neighborhood $U \subset \mathbf{G}(k)$ of the identity such that each nontrivial element $h \in U$ generates a non-discrete subgroup [Mar91, IX, (3.5)]. In particular, every lattice in $\mathbf{G}(k)$ must intersect U *trivially*.

In contrast, in the real case one cannot omit elements of finite order from the statement of Conjecture (A). Indeed, in general one can construct a sequence $(\Gamma_m)_{m \in \mathbb{N}}$ of cocompact arithmetic lattices in $\mathbf{G}(\mathbb{R})$ and torsion elements $\gamma_m \in \Gamma_m$ tending to 1. In the case of $\mathbf{SL}_2(\mathbb{R})$ and $\mathbf{SL}_2(\mathbb{C})$, the reader can consult [MR03, §12.5] for a thorough discussion on the existence of elements of arbitrary order in cocompact lattices.

1.2. Lehmer's conjecture. Let $P \in \mathbb{C}[X]$ be a monic polynomial of degree d with roots $\alpha_1, \dots, \alpha_d \in \mathbb{C}$. The *Mahler measure* of P is

$$\mathcal{M}(P) = \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

In the following, let $\alpha_1, \dots, \alpha_{s(P)}$ be an enumeration of the roots of P in $\mathbb{C}$ which have absolute value strictly greater than 1, repeated according to their multiplicity, so that $s(P)$ denotes their count (with multiplicity) and we may rewrite $\mathcal{M}(P) = \prod_{i=1}^{s(P)} |\alpha_i|$. If $\alpha \in \overline{\mathbb{Q}}$ is an algebraic integer, the Mahler measure $\mathcal{M}(\alpha)$ of α will be defined as the Mahler measure $\mathcal{M}(P_\alpha)$ of its minimal polynomial P_α over $\mathbb{Z}$. The Mahler measure on algebraic integers is obviously invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The Mahler measure is multiplicative. By virtue of Kronecker's theorem, for P a monic, irreducible polynomial with integer coefficients, we have

$$\mathcal{M}(P) = 1 \quad \Leftrightarrow \quad P(X) = X, \text{ or } P \text{ is a cyclotomic polynomial.}$$

In 1933, Lehmer [Leh33] asked whether one could find irreducible polynomials with integer coefficients whose Mahler measure gets arbitrarily close to 1 (but is not 1). It is conjectured that this is not possible:

Conjecture (B) (Lehmer[1]). There exists $\varepsilon > 0$ such that for any (irreducible) monic polynomial P with integer coefficients, either

$$\mathcal{M}(P) = 1 \quad \text{or} \quad \mathcal{M}(P) > 1 + \varepsilon.$$

In fact, Lehmer's polynomial

$$P_{\mathrm{Lehmer}} = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1,$$

for which $\mathcal{M}(P_{\mathrm{Lehmer}}) = 1.17628...$, is suspected to attain the smallest Mahler measure greater than 1. Partial results towards Lehmer's conjecture are known; we list some of them below.

We will be concerned with the following weaker version of Lehmer's conjecture.

Conjecture (C) (weak Lehmer). For each $s \in \mathbb{N}$, there exists $\varepsilon(s) > 0$ such that for any (irreducible) monic polynomial P with integer coefficients and $s(P) \leq s$, either

$$\mathcal{M}(P) = 1 \quad \text{or} \quad \mathcal{M}(P) > 1 + \varepsilon(s).$$

For a given s, we will call the statement in Conjecture (C) *Lehmer's conjecture at level s*. In this way, Conjecture (C) could be described as "Lehmer's conjecture at all levels", and Lehmer's conjecture (B) as "Lehmer's conjecture at all levels uniformly".

1.3. Main result. Fix an absolutely (almost) simple isotropic $\mathbb{R}$-group $\mathbf{F}$ and consider, for each integer $s \geq 1$, the family of semisimple $\mathbb{R}$-groups

$$\mathscr{T}_{\mathbf{F}}^{(s)} = \left\{ \prod_{i=1}^{r} \mathbf{F} \times \prod_{i=1}^{t} \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbf{F}) \; \middle| \; r, t \in \mathbb{N}, \; r + 2t \leq s \right\}.$$

---

[1]Lehmer always insisted that he had not formulated his problem as a conjecture, although we will customarily refer to it as such.

The following theorem is the main result of this paper.

Theorem. Let $s \geq 1$. Then Margulis' conjecture for any of the families $\mathscr{T}_{\mathbf{F}}^{(s)}$ defined above[2] implies Lehmer's conjecture at level s. In consequence, Margulis' conjecture (A) is equivalent to the weak version (C) of Lehmer's conjecture.

In view of the theorem, let us emphasize that Margulis' conjecture for products of simple groups of *any fixed $\mathbb{R}$-type* and their extensions to $\mathbb{C}$ is already sufficient to imply the weak Lehmer conjecture, which in turn implies Margulis' conjecture for *all* semisimple groups (see §3). For the sake of clarity, we will first carry the argument out in detail for type A_n split in §4. To complete the proof of the theorem, we then give a comprehensive treatment of all other $\mathbb{R}$-types in §5. It is noteworthy that the argument works for every $\mathbb{R}$-type in a similar way.

It would be interesting to know whether Margulis' conjecture has implications for the full Lehmer conjecture (B), beyond Conjecture (C). Connections between the full Lehmer conjecture and linear groups have already been brought to light, for example in the work of Breuillard [Bre07] and of Breuillard–Varju [BV20].

1.4. Notation and conventions. Throughout the paper, we adopt the conventions of Bourbaki. In particular, $\mathbb{N} = \{0, 1, 2, \dots\}$ and we denote $\mathbb{N}^* = \mathbb{N} \backslash \{0\}$.

- If $P \in \mathbb{C}[x]$, $s(P)$ denotes the number of roots of P in $\mathbb{C}$ which have absolute value > 1, counted with multiplicity.
- $\mathcal{M}(P)$ denotes the Mahler measure of $P \in \mathbb{C}[x]$.
- If $\alpha \in \overline{\mathbb{Q}}$ is an algebraic integer, P_α denotes its minimal polynomial over $\mathbb{Z}$.
- $\mathcal{O}_K$ denotes the ring of integers of a number field K.
- $\mathrm{M}_n(A)$ denotes the set of $n \times n$ matrices with entries in an algebraic structure A, endowed with whichever structure is inherited from A.

2. A short history

In this section, we provide a very short (and incomplete) survey of known results and references about the arithmetic and geometry of the famous Lehmer problem. For a more extensive treatment, we refer the reader to the surveys of Smyth [Smy08, Smy15], and Ghate and Hironaka [GH01].

2.1. Some known results about the Lehmer conjecture. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic integer which is not an integer nor a root of unity, and let $d \geq 2$ denote the degree of P_α. Then, the following lower bound for $M(\alpha)$ is known:

$$(2.1.1) \quad \mathcal{M}(\alpha) > 1 + \frac{1}{4}\left(\frac{\log \log d}{\log d}\right)^3.$$

This was proved by Voutier [Vou96, Theorem], improving the bound of Dobrowolski [Dob79, Theorem 1] (who obtained a factor of $1/1200$ instead of $1/4$). Another bound due to Laurent[3] (1983), emphasizing the

---

[2]As the statement in Margulis' conjecture is insensitive to isogenies (see namely the first paragraph of §3.2), in the theorem, one could of course replace each element of the family $\mathscr{T}_{\mathbf{F}}^{(s)}$ by another semisimple group isogenous to it.

[3]In a private communication, Michel Laurent informed us that this bound was not published and that Schinzel [Sch73] proved the sharp inequality $\mathcal{M}(\alpha) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}$, for every α which is a totally real algebraic integer of degree $d \geq 2$.

number of real roots, is given by Margulis [Mar91, p. 322]: if P is a non-cyclotomic polynomial of degree $d \geq 2$ with r real roots, then

$$\mathcal{M}(\alpha) \geq c^{r^2/d \log(1+\frac{d}{r})},$$

where $c > 0$ is an absolute constant.

Recall that a polynomial $P \in \mathbb{Z}[X]$ is called *palindromic* if

$$P(X) = X^{\deg(P)} P(X^{-1}).$$

Every palindromic polynomial P of odd degree is divisible by $X + 1$, hence irreducible palindromic polynomials of degree > 1 must have even degree.

Smyth [Smy71] proved that the polynomial $P_{\text{Smyth}}(X) = X^3 - X - 1$ had the smallest Mahler measure among non-palindromic polynomials.

Theorem ([Smy71])**.** Let $\alpha \in \overline{\mathbb{Q}}$. If $\mathcal{M}(P_\alpha) < \mathcal{M}(P_{\text{Smyth}})$, then P_α is palindromic.

This effectively reduces Conjectures (B) and (C) to palindromic polynomials.

Although we will not use it, we note in passing another instance for which the Lehmer conjecture is known to hold. Borwein, Dobrowolski, and Mossinghoff [BDM07] proved that if P is a polynomial of degree d without cyclotomic factors, all of whose coefficients are odd integers, then

$$\log \mathcal{M}(P) \geq \frac{\log 5}{4} \left(1 - \frac{1}{d+1}\right).$$

2.2. The case of Salem numbers. Recall that a *Salem number* is an algebraic integer $u \in \mathbb{R}$ which is > 1 and all of whose Galois conjugates in $\mathbb{C}$ have absolute value ≤ 1, with at least one of absolute value = 1. Hence, any Salem number α satisfies $s(P_\alpha) = 1$ where P_α is the minimal polynomial of α, and it is clear that P_α is palindromic. Conversely, any irreducible palindromic polynomial $P \in \mathbb{Z}[x]$ with $s(P) = 1$ and $\deg P \geq 4$ is the minimal polynomial of a Salem number. The following conjecture is thus equivalent to Lehmer's conjecture at level $s = 1$ (see the paragraph after Conjecture (C)).

Conjecture (D) (Salem, arithmetic version)**.** There exists $\varepsilon > 0$ such that every Salem number α satisfies $\alpha > 1 + \varepsilon$.

Salem numbers constitute an important family of algebraic numbers. For example, the polynomial P_{Lehmer} with the smallest known Mahler measure (see §1.2) turns out to be the minimal polynomial of a Salem number.

A beautiful connection with discrete subgroups of Lie groups was established by Sury [Sur92]: he proved that Conjecture (D) was equivalent to the following conjecture.

Conjecture (E) (Salem, geometric version)**.** There exists a neighborhood $U \subset \mathbf{SL}_2(\mathbb{R})$ of the identity such that for any torsion-free cocompact arithmetic lattice $\Gamma \subset \mathbf{SL}_2(\mathbb{R})$, we have $\Gamma \cap U = \{e\}$.

Remark. Conjecture (E) is simply Margulis' conjecture for $\mathbf{SL}_2$, hence Theorem 1.3 for $s = 1$ includes Sury's result as a special case. In fact, Theorem 1.3 for $s = 1$ shows that Margulis' conjecture (A) for any one of the isotropic absolutely (almost) simple $\mathbb{R}$-groups (e.g. $\mathbf{SL}_n$, $\mathbf{SO}_q$, etc.) implies Conjecture (D).

2.3. Lengths of shortest geodesics in arithmetic hyperbolic orbifolds. Extending the picture to Kleinian groups, Neumann and Reid [NR92] formulated the following conjecture.

Conjecture (F) (Short geodesic conjecture)**.** There is a positive universal lower bound for the lengths of closed geodesics in arithmetic hyperbolic 2- and 3-orbifolds.

The short geodesic conjecture for hyperbolic 2-orbifolds is equivalent to Conjecture (E), hence to (D). On the other hand, the short geodesic conjecture for hyperbolic 3-orbifolds is equivalent to the following *complex Salem conjecture*. Call an algebraic integer $\alpha \in \mathbb{C}$ a *complex Salem number* if α is not real, α and its complex conjugate $\overline{\alpha}$ are the only two Galois-conjugates of α in $\mathbb{C}$ of absolute value > 1, and α has at least one conjugate of absolute value $= 1$.

Conjecture (G) (Complex Salem). There exists $\varepsilon > 0$ such that every complex Salem number α satisfies $|\alpha| > 1 + \varepsilon$.

In fact, the short geodesic conjecture for hyperbolic 3-orbifolds implies the conjecture for 2-orbifolds. This can be seen arithmetically, as the complex Salem conjecture implies the traditional Salem conjecture. Indeed, if α is a Salem number, then $P_\alpha(-x^2)$ is the minimal polynomial of a complex Salem number with the same Mahler measure as α.

For a detailed introduction to Conjecture (F), we refer the reader to the book of Maclachlan and Reid [MR03].

Remark. Similarly as for Conjecture (D), the proof of Theorem 1.3 (for $s = 2$, $r = 0$) shows that Margulis' conjecture for the restriction to $\mathbb{R}$ of any simple $\mathbb{C}$-group implies Conjecture (G).

Salem numbers can also be used to obtain a lower bound for the length of closed geodesics in noncompact arithmetic hyperbolic orbifolds of *even* dimension n. This was done by Emery, Ratcliffe and Tschantz [ERT19]. More precisely, for any integer $n \geq 2$, let $\mathcal{H}^n$ denote hyperbolic n-space, and define

$$\beta_n = \min\{\log \alpha \mid \alpha \text{ is a Salem number with } \deg P_\alpha \leq n\}.$$

For any even dimension n, if $\Gamma \subset \text{Isom}(\mathcal{H}^n)$ is a non-uniform arithmetic lattice, then the length of any closed geodesic in $\mathcal{H}^n/\Gamma$ is at least β_n [ERT19, Corollary 1.3]. It follows that Conjecture (D) is equivalent to the existence of a uniform lower bound on the length of closed geodesics in non-compact arithmetic hyperbolic orbifolds of even dimension.

2.4. Homotopy type of locally symmetric spaces. Let us conclude this section with a consequence of Conjecture (A) in the context of locally symmetric spaces. Let S be a symmetric space (e.g., $S = G/K$ where G is a semisimple Lie group, $K \subset G$ a maximal compact subgroup). Following Gelander [Gel04], an *S-manifold* is a complete Riemannian manifold locally isometric to S, i.e., a manifold of the form $\Gamma \backslash S$, where $\Gamma \subset \text{Isom}(S)$ is a discrete torsion-free subgroup. It is irreducible if Γ is an irreducible lattice. For $d, v \in \mathbb{N}$, a (d, v)-*simplicial complex* is a simplicial complex with at most v vertices, all of degree at most d. An interesting consequence of Conjecture (A) is the following conjecture of Gelander.

Conjecture (H) ([Gel04]). For any symmetric space S of noncompact type, there are constants $\alpha(S)$, $d(S)$, such that any irreducible S-manifold M (assumed to be arithmetic if $\dim(S) = 3$) is homotopically equivalent to a $(d(S), \alpha(S) \text{vol}(M))$-simplicial complex.

Conjecture (H) was recently proved by Fraczyk [Fra21, Theorem 1.16] for arithmetic 3-manifolds.

3. Margulis' arithmeticity theorem

In this section, we briefly review Margulis' arithmeticity results [Mar91, Chapter IX] in a form that will be used to show that Conjecture (C) implies Conjecture (A). Let us first recall the definitions.

Let $\mathbf{G}$ be a connected semisimple $\mathbb{R}$-group and let $\prod_{i \in I} \mathbf{G}_i$ be a decomposition of $\mathbf{G}$ as an almost direct product of almost $\mathbb{R}$-simple $\mathbb{R}$-subgroups. For any subset $J \subset I$, we write $\mathbf{G}_J = \prod_{i \in J} \mathbf{G}_i$. We denote by $\mathbf{G}^{\text{is}}$ (resp. $\mathbf{G}^{\text{anis}}$) the subgroup of $\mathbf{G}$ which is the almost direct product of the $\mathbb{R}$-isotropic (resp. $\mathbb{R}$-anisotropic) factors of $\mathbf{G}$. We also let $G = \mathbf{G}(\mathbb{R})$, $G_J = \mathbf{G}_J(\mathbb{R})$ and $G^{\text{is}} = \mathbf{G}^{\text{is}}(\mathbb{R})$.

A lattice $\Gamma \subset G$ is said to be *irreducible* if for any non-empty proper subset $J \subset I$, the index $[\Gamma : (\Gamma \cap G_J) \cdot (\Gamma \cap G_{I \setminus J})]$ is infinite.

An irreducible lattice $\Gamma \subset G$ such that $G^{\mathrm{is}} \cdot \Gamma$ is dense in G is called *arithmetic* if there exist a connected non-commutative almost $\mathbb{Q}$-simple $\mathbb{Q}$-group $\mathbf{H}$ (endowed with some $\mathbb{Z}$-structure), and an $\mathbb{R}$-epimorphism $\tau : \mathbf{H} \to \mathbf{G}$ such that:

(i) the Lie group $(\ker \tau)(\mathbb{R})$ is compact;
(ii) the subgroups $\tau(\mathbf{H}(\mathbb{Z}))$ and Γ are commensurable.

3.1. The arithmeticity theorem. We can now state Margulis' celebrated arithmeticity theorem.
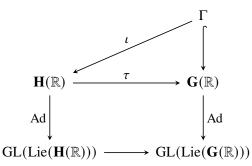
Theorem ([Mar91, IX, (1.16)])**.** Let $\mathbf{G}$ be a connected semisimple $\mathbb{R}$-group and Γ an irreducible lattice in $\mathbf{G}(\mathbb{R})$, with $\mathbf{G}^{\mathrm{is}}(\mathbb{R}) \cdot \Gamma$ dense in $\mathbf{G}(\mathbb{R})$. Suppose that $\mathrm{rank}_{\mathbb{R}} \mathbf{G} \geq 2$. Then the lattice Γ is arithmetic.

In the remainder of this section, we will assume that $\mathrm{rank}_{\mathbb{R}}(\mathbf{G}) \geq 2$, that G has no compact factors (i.e. $\mathbf{G}^{\mathrm{is}} = \mathbf{G}$) and has trivial center. Let $\Gamma \subset G$ be an irreducible lattice. Then the following facts are among the key steps of the proof of the arithmeticity theorem. We refer the reader to [Zim84, §6.1] or [Ben08, §11.5] for proofs and details.

(3.1.1)   The trace field $K = \mathbb{Q}(\mathrm{tr}\,\mathrm{Ad}\,\Gamma)$ of Γ, the field generated by the set $\{\mathrm{tr}(\mathrm{Ad}(\gamma)) \mid \gamma \in \Gamma\}$, is a number field. This follows from Margulis' superrigidity theorem, together with the fact that Γ is finitely generated.

(3.1.2)   Since Γ is Zariski-dense in $\mathbf{G}(\mathbb{R})$, $\mathbf{G}$ can be defined over K. That is, there is a K-group $\mathbf{G}'$ and a place v_0 of K such that $K_{v_0} = \mathbb{R}$, $\mathbf{G} \cong \mathbf{G}'$ as $\mathbb{R}$-groups, and the image of Γ under this isomorphism lies in $\mathbf{G}'(K)$. In the following, we will identify $\mathbf{G}$ and $\mathbf{G}'$, and simply assume that $\Gamma \subset \mathbf{G}(K)$.

(3.1.3)   There is a semisimple $\mathbb{Q}$-group $\mathbf{H}$ (endowed with a $\mathbb{Z}$-structure) with trivial center, an $\mathbb{R}$-epimorphism $\tau : \mathbf{H} \to \mathbf{G}$ with $(\ker \tau)(\mathbb{R})$ compact, and a homomorphism $\iota : \Gamma \to \mathbf{H}(\mathbb{Q})$ such that $\tau \circ \iota$ is the identity, $\iota(\Gamma)$ is Zariski dense in $\mathbf{H}$ and $\iota(\Gamma)$ is commensurable with $\mathbf{H}(\mathbb{Z})$. The group $\mathbf{H}$ can be constructed as the restriction of scalars $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$ of $\mathbf{G}$ from K to $\mathbb{Q}$.

3.2. The weak Lehmer conjecture implies Margulis' conjecture. We start by indicating how Conjecture (C) implies Conjecture (A). Note that as long as the lattice Γ is arithmetic, the argument given below works equally well for groups of rank one. It shows in fact that Conjecture (C) implies Margulis' conjecture for all semisimple $\mathbb{R}$-groups (in the sense defined below the statement of Conjecture (A)). Let thus $\mathbf{G}$ be a semisimple group and Γ an irreducible arithmetic lattice in $\mathbf{G}(\mathbb{R})$.

Without loss of generality, we may assume that $\mathbf{G}$ has trivial center and is without anisotropic factors. Indeed, if $\mathbf{G}$ has center $\mathbf{C}$, and U' is a neighborhood of $(\mathbf{G}/\mathbf{C})(\mathbb{R})$ as in (A), then the preimage U of U' under the canonical map $\pi : \mathbf{G}(\mathbb{R}) \to (\mathbf{G}/\mathbf{C})(\mathbb{R})$ has the required property: if Γ is an irreducible cocompact lattice in $\mathbf{G}(\mathbb{R})$, then $\pi(\Gamma)$ is an irreducible cocompact lattice in $(\mathbf{G}/\mathbf{C})(\mathbb{R})$; hence if $\gamma \in U$, $\pi(\gamma)$ must have finite order, and since $\mathbf{C}(\mathbb{R})$ is finite, so does γ. Similarly, if $\mathbf{G} = \mathbf{G}^{\mathrm{is}} \times \mathbf{G}^{\mathrm{anis}}$ and U' is a neighborhood of $\mathbf{G}^{\mathrm{is}}$ as in (A), then the preimage U of U' under the canonical map $\pi : \mathbf{G}(\mathbb{R}) \to \mathbf{G}^{\mathrm{is}}(\mathbb{R})$ has the required property: if Γ is an irreducible cocompact lattice in $\mathbf{G}(\mathbb{R})$, then $\pi(\Gamma)$ is an irreducible cocompact lattice in $\mathbf{G}^{\mathrm{is}}(\mathbb{R})$; hence if $\gamma \in U$, $\pi(\gamma)$ has finite order m, and $\gamma^m \in \mathbf{G}^{\mathrm{anis}}(\mathbb{R}) \cap \Gamma$. As $\mathbf{G}^{\mathrm{anis}}(\mathbb{R})$ is compact and Γ is discrete, the latter is a finite group and γ has finite order.

Let $\mathbf{H}$ be the group obtained in (3.1.3), so that we have the following diagram.

Recall also from (3.1.3) that τ has compact kernel and that $\iota(\Gamma)$ is commensurable with $\mathbf{H}(\mathbb{Z})$.

Since the adjoint representation $\mathbf{H} \to \mathrm{Ad}\,\mathbf{H}$ is defined over $\mathbb{Q}$, we can find a finite-index subgroup Λ of $\mathbf{H}(\mathbb{Z})$ for which $\mathrm{Ad}(\Lambda) \subset \mathrm{Ad}(\mathbf{H})(\mathbb{Z})$ (see for example [Mar91, I, (3.1.1)]); in particular, $\mathrm{Ad}(\Lambda)$ preserves a lattice in $\mathrm{Lie}(\mathbf{H}(\mathbb{R}))$. Since Λ and $\iota(\Gamma)$ are commensurable, $\mathrm{Ad}(\iota(\Gamma))$ also stabilizes a lattice in $\mathrm{Lie}(\mathbf{H}(\mathbb{R}))$ [Mar91, IX, (4.19)]. Hence the characteristic polynomials of the elements of $\mathrm{Ad}(\iota(\Gamma))$ have integer coefficients.

Let us write $\mathbf{H}(\mathbb{R}) = F \times K$ as a direct product where K is compact and F is without compact factors. The morphism τ then induces an isogeny $F \to \mathbf{G}(\mathbb{R})$ and $d\tau$ restricts to an isomorphism $\mathrm{Lie}(F) \to \mathrm{Lie}(\mathbf{G}(\mathbb{R}))$. Let $x \in \mathbf{H}(\mathbb{R})$ and write $\mathrm{Ad}_{\mathbf{H}(\mathbb{R})}(x) = \mathrm{Ad}_F(y) \oplus \mathrm{Ad}_K(z)$ for some $y \in F$, $z \in K$. If we denote P_x, P_y, P_z the respective characteristic polynomials of $\mathrm{Ad}_{\mathbf{H}(\mathbb{R})}(x)$, $\mathrm{Ad}_F(y)$, $\mathrm{Ad}_K(z)$, we have that $P_x = P_y \cdot P_z$. Because K is compact, all roots of P_z in $\mathbb{C}$ must have absolute value 1; in consequence, $\mathcal{M}(P_z) = 1$, hence $\mathcal{M}(P_x) = \mathcal{M}(P_y)$. Moreover, P_x satisfies $s(P_x) = s(P_y) \leq \dim F = \dim \mathbf{G}$.

Now pick $\gamma \in \Gamma$ and apply the last paragraph to $x = \iota(\gamma)$. Since $\tau(\iota(\gamma)) = \gamma$ and $d\tau \circ \mathrm{Ad}(\iota(\gamma)) = \mathrm{Ad}(\gamma) \circ d\tau$, we obtain that the characteristic polynomial P_γ of $\mathrm{Ad}_{\mathbf{G}(\mathbb{R})}(\gamma)$ equals P_y. We have in turn

$$\mathcal{M}(P_\gamma) = \mathcal{M}(P_{\iota(\gamma)}) \quad \text{and} \quad s(P_\gamma) = s(P_{\iota(\gamma)}).$$

Let $f : \mathbf{G}(\mathbb{R}) \to [1, \infty[$ be defined by $f(g) = \mathcal{M}(P_g)$, where as before P_g denotes the characteristic polynomial of $\mathrm{Ad}_{\mathbf{G}(\mathbb{R})}(g)$; note that f is a continuous function. If the weak version of Lehmer's conjecture holds at level $s = \dim \mathbf{G}$, we can find $\varepsilon > 0$ such that any polynomial P with integer coefficients and $s(P) \leq \dim \mathbf{G}$ satisfies either $\mathcal{M}(P) = 1$ or $\mathcal{M}(P) > 1 + \varepsilon$. This applies to $P_{\iota(\gamma)}$ for any $\gamma \in \Gamma$: as we observed, $P_{\iota(\gamma)}$ has integer coefficients and $s(P_{\iota(\gamma)}) \leq \dim \mathbf{G}$. Thus, by the above, the open neighborhood $U = f^{-1}([1, \varepsilon[)$ of 1 in $\mathbf{G}(\mathbb{R})$ is such that $U \cap \Gamma$ consists of elements γ for which $\mathcal{M}(P_\gamma) = \mathcal{M}(P_{\iota(\gamma)}) = 1$. This means that for $\gamma \in U$, P_γ is a product of cyclotomic polynomials. Since Γ is cocompact, $\mathrm{Ad}(\gamma)$ is semisimple and thus $\mathrm{Ad}(\gamma)$, hence also γ, have finite order.

4. Proof of the main theorem for SL_n

We now proceed to prove Theorem 1.3 (in particular, that Conjecture (A) implies Conjecture (C)). To this end, we will assume Conjecture (C) fails and construct a sequence of cocompact lattices in suitable groups of the family $\mathscr{T}_{\mathbf{F}}^{(s)}$ violating Margulis' conjecture for this family. As it is more transparent, we first give the full argument for $\mathbf{F} = \mathbf{SL}_n$, i.e. for the family

$$\mathscr{T}_{\mathbf{SL}_n}^{(s)} = \left\{ \prod_{i=1}^{r} \mathbf{SL}_n \times \prod_{i=1}^{t} \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbf{SL}_n) \;\middle|\; r, t \in \mathbb{N}, \; r + 2t \leq s \right\}.$$

This is already sufficient to establish the equivalence between Conjectures (A) and (C). In the last section (§5), we then indicate the corresponding changes for $\mathbf{F}$ an arbitrary absolutely (almost) simple isotropic $\mathbb{R}$-group, completing the proof of Theorem 1.3.

4.1. Reduction to palindromic polynomials with control on the archimedean places. Given $P \in \mathbb{Z}[x]$, let us denote as before $\alpha_1, \ldots \alpha_{s(P)}$ the roots of P in $\mathbb{C}$ of absolute value > 1, and label them in such a way $\alpha_1, \ldots, \alpha_{r(P)}$ lie in $\mathbb{R}$ and $\alpha_{r(P)+1}, \ldots, \alpha_{s(P)}$ do not. In addition, let us order the latter roots so that $\overline{\alpha}_{r(P)+i} = \alpha_{(r(P)+s(P))/2+i}$ for $1 \le i \le (s(P) - r(P))/2$. For each $s' \in \mathbb{N}$, we will consider the set of polynomials

$$\mathscr{P}_{\le s'} = \{P \in \mathbb{Z}[X] \mid P \text{ is monic, irreducible, palindromic, and } s(P) \le s'\},$$

and for $r \le s \le s'$, its subsets

$$\mathscr{P}_{s,r} = \{P \in \mathscr{P}_{\le s'} \mid s(P) = s \text{ and } r(P) = r\}.$$

By construction, $\mathscr{P}_{\le s'}$ is the disjoint union $\bigcup_{s=0}^{s'} \bigcup_{r=0}^{s} \mathscr{P}_{s,r}$.

Suppose that Conjecture (C) does not hold. That is, there are $s' \in \mathbb{N}$ and a sequence $(P_m)_{m \in \mathbb{N}}$ of monic, irreducible polynomials with integer coefficients such that $s(P_m) \le s'$ and $\mathcal{M}(P_m) \to 1$ while $\mathcal{M}(P_m) > 1$. By virtue of Smyth's theorem (§2.1), we may assume that each P_m is palindromic, i.e. that $P_m \in \mathscr{P}_{\le s'}$. Moreover, up to extracting an appropriate subsequence, we may assume that $P_m \in \mathscr{P}_{s,r}$ for some fixed integers $r \le s \le s'$.[4] Of course, $s > 0$. In view of the bound (2.1.1), it must be that the sequence $(\deg P_m)_m$ is unbounded. We may thus additionally assume that $\deg P_m > 2s$. This implies the following important feature: P_m must have a root of absolute value 1. Indeed, P_m has s roots of absolute value > 1, and because P_m is palindromic, as many roots of absolute value < 1.

The discussion above shows that the negation of Lehmer's conjecture at level s' (cf. the paragraph following Conjecture (C)) amounts to the following statement.

Negation of Lehmer's conjecture at level s'. There are fixed integers $r \in \mathbb{N}$, $s \in \mathbb{N}^*$ with $r \le s \le s'$ such that:

($L_{s,r}$) for any $\varepsilon > 0$, there is a polynomial $P \in \mathscr{P}_{s,r}$ with at least one root in $\mathbb{C}$ of absolute value 1, for which $1 < \mathcal{M}(P) < 1 + \varepsilon$.

Using statement ($L_{s,r}$) as the main ingredient, for each such pair (s, r), we will construct in the semisimple $\mathbb{R}$-group

$$(\star) \qquad \mathbf{G}_{s,r} = \prod_{i=1}^{r} \mathbf{SL}_n \times \prod_{i=1}^{(s-r)/2} \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbf{SL}_n) \qquad (n \ge 2),$$

a sequence of cocompact lattices $\Gamma_m < \mathbf{G}_{s,r}(\mathbb{R})$ and a sequence of elements $\gamma_m \in \Gamma_m$ of infinite order, such that $\gamma_m \to e \in \mathbf{G}_{s,r}(\mathbb{R})$ as $m \to \infty$. This shall provide a counterexample to Margulis' conjecture for $\mathbf{G}_{s,r}$, thus proving the first part of theorem 1.3. The equivalence of Margulis' conjecture (A) and the weak version (C) of Lehmer's conjecture then follows immediately by combining this with §3.2.

4.2. The number fields K and L. Let $r \le s$ be as above. Pick a polynomial $P \in \mathscr{P}_{s,r}$, set $2d = \deg P$, and let $L = \mathbb{Q}(\alpha)$ denote the number field generated over $\mathbb{Q}$ by a root α of P. Since P is palindromic, α^{-1} is also a root of P. In particular, α^{-1} is integral over $\mathbb{Z}$, and the assignment $\tau : \alpha \mapsto \alpha^{-1}$ defines a non-trivial automorphism of L (which restricts to an automorphism of its ring of integers $\mathcal{O}_L$). Let $K = \mathbb{Q}(\alpha + \alpha^{-1})$ denote the subfield of L generated over $\mathbb{Q}$ by $\alpha + \alpha^{-1}$. Since K is the fixed field of τ, L is a quadratic extension of K whose Galois group is $\{\mathrm{id}, \tau\}$. Note that the minimal polynomial of α over K is $X^2 - (\alpha + \alpha^{-1})X + 1$.

For $1 \le i \le s$, let σ_i denote the embedding $L \to \mathbb{C}$ defined by $\sigma_i(\alpha) = \alpha_i$. By definition, L has r real embeddings $\sigma_1, \ldots, \sigma_r$ and $s - r$ complex embeddings $\sigma_{r+1}, \ldots, \sigma_s$ for which the image of α has absolute value > 1. L also has $d - s$ pairs of conjugate complex embeddings $\sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_d, \overline{\sigma}_d$ for which α maps to an element of absolute value 1. Observe that precomposition with τ sends $\{\sigma_1, \ldots, \sigma_r\}$ and $\{\sigma_{r+1}, \ldots, \sigma_s\}$ respectively to the set of real and complex embeddings of L for which the image of α has absolute value < 1. Similarly, $\sigma_i \circ \tau = \overline{\sigma}_i$ for $s+1 \le i \le d$. By construction, the embeddings σ_i and $\sigma_i \circ \tau$ for

---

[4] If s' were to be the smallest integer for which Lehmer's conjecture at level s' fails, then obviously $s = s'$.

$1 \leq i \leq d$ agree on K. This shows that $\{\sigma_1, \ldots, \sigma_d\}$ is the complete set of embeddings of K into $\mathbb{C}$ (we omit the restriction to K from the notation). The image $\sigma_i(\alpha + \alpha^{-1})$ of the generator of K belongs to $\mathbb{R}$ if and only if $\sigma_i(\alpha) \in \mathbb{R}$ or $|\sigma_i(\alpha)| = 1$. In consequence, restricted to K, the embeddings $\sigma_1, \ldots, \sigma_r$ and $\sigma_{s+1}, \ldots, \sigma_d$ are real, $\sigma_{r+1}, \ldots, \sigma_s$ are complex (coming in conjugate pairs), and K has signature $(r - s + d, (s - r)/2)$.

4.3. The K-group G. Let $h : L^n \times L^n \to L$ be the τ-hermitian form given by

$$h(x, y) = x_1 \tau(y_1) + \cdots + x_n \tau(y_n) \qquad x, y \in L^n,$$

and let $\mathbf{G} = \mathbf{SU}_h$ be the special unitary group associated to the form h. $\mathbf{G}$ is a linear algebraic K-group, whose group of K-points is (isomorphic to) the group of h-unitary matrices in $\mathrm{M}_n(L)$ of determinant 1.[5] The $K \otimes_{\mathbb{Q}} \mathbb{R}$-points of $\mathbf{G}$ can be computed easily by studying the behavior of the extension L/K and of the form h under the different embeddings $\{\sigma_1, \ldots, \sigma_d\}$ of K.

In the present setting, the extension L/K splits at the places $\sigma_1, \ldots, \sigma_r$ (since these extend to real places of L) and also at the places $\sigma_{r+1}, \ldots, \sigma_s$ (since these are complex places of K), but not at $\sigma_{s+1}, \ldots, \sigma_d$ (since there we have $L \otimes_K K_{\sigma_i} \cong \mathbb{C}$). At these last places, the hermitian form h becomes the standard hermitian form on $\mathbb{C}^n \times \mathbb{C}^n$ after identifying the completion of L/K with $\mathbb{C}/\mathbb{R}$ via σ_i ($s + 1 \leq i \leq d$). Altogether, we have

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{SL}_n(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{SL}_n(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{SU}_n(\mathbb{R}),$$

where $\mathbf{SU}_n(\mathbb{R})$ denotes the standard anisotropic special unitary group over $\mathbb{R}$.

4.4. The lattice Γ and the element γ. Let Γ be the group of h-unitary $n \times n$ matrices of determinant 1 with entries in $\mathcal{O}_L$.[6] A classical theorem of Borel and Harish–Chandra [BHC62] states that Γ is a lattice in $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ when embedded diagonally using the inequivalent archimedean places of K among $\sigma_1, \ldots, \sigma_d$. (Apply [BHC62, Theorem 7.8] to $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})$ and observe that $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(\mathbb{R}) \cong \mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$; under this isomorphism, $\mathrm{Res}_{K/\mathbb{Q}}(\mathbf{G})(\mathbb{Z})$ is commensurable to Γ.) By virtue of the strong approximation theorem (for number fields), Γ is an irreducible lattice. Moreover, if P has at least one root in $\mathbb{C}$ of absolute value 1 (i.e. if $s < d$), we claim that Γ is a cocompact lattice in $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$. Indeed, for any embedding $\sigma : K \to \mathbb{C}$ which extends to L in such a way $|\sigma(\alpha)| = 1$, the group $\mathbf{G}(K_\sigma) \cong \mathbf{SU}_n(\mathbb{R})$ is compact, and hence $\mathbf{G}$ must be K-anisotropic (as it is anisotropic over K_σ). The claim then follows from Godement's criterion [BHC62, Theorem 11.8].

Let $\mathbf{G}_{s,r}$ be the $\mathbb{R}$-group defined in 4.1($\star$). The canonical surjection $\pi : \mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \to \mathbf{G}_{s,r}(\mathbb{R})$ has compact kernel $\prod_{i=1}^{d-s} \mathbf{SU}_n(\mathbb{R})$; this implies that the image $\pi(\Gamma)$ of Γ under π is an irreducible, cocompact (provided $s < d$), lattice in $\mathbf{G}_{s,r}(\mathbb{R})$.

We set γ to be the diagonal h-unitary $n \times n$-matrix $\mathrm{diag}(\alpha, \alpha^{-1}, 1, \ldots, 1)$ in $\Gamma = \mathbf{G}(\mathcal{O}_K)$. Viewed as an element of $\mathbf{G}_{s,r}(\mathbb{R})$, the non-trivial block of $\pi(\gamma)$ is

$$\left(\begin{pmatrix} \alpha_1 & \\ & \alpha_1^{-1} \end{pmatrix}, \ldots, \begin{pmatrix} \alpha_r & \\ & \alpha_r^{-1} \end{pmatrix}, \begin{pmatrix} \alpha_{r+1} & \\ & \alpha_{r+1}^{-1} \end{pmatrix}, \ldots, \begin{pmatrix} \alpha_{(s+r)/2} & \\ & \alpha_{(s+r)/2}^{-1} \end{pmatrix} \right),$$

where we labelled the roots α_i of P in $\mathbb{C}$ as in §4.1.

4.5. The sequence $(\gamma_m')_m$ and Margulis' conjecture. Assume ($\mathrm{L}_{s,r}$) holds, set $t = (s - r)/2$ and pick a sequence $(P_m)_{m \in \mathbb{N}^*}$ of polynomials in $\mathscr{P}_{s,r}$ with at least one root of absolute value 1, satisfying

$$1 < \mathcal{M}(P_m) < \exp(\eta_{m,t}) \quad \text{with} \quad \eta_{m,t} = \frac{1}{2m^{t+1}}.$$

For each $m \in \mathbb{N}^*$, let us denote

$$\alpha_m, \quad L_m, \quad K_m, \quad h_m, \quad \mathbf{G}_m, \quad \Gamma_m, \quad \gamma_m, \quad \text{and} \quad \pi_m,$$

---

[5]In fact, since the equations defining $\mathbf{G}$ can be taken with coefficients in $\mathcal{O}_K$, $\mathbf{G}$ can also be viewed as an $\mathcal{O}_K$-group scheme.

[6]With this definition, Γ is (commensurable to) the $\mathcal{O}_K$-points of $\mathbf{G}$ when it is viewed as an $\mathcal{O}_K$-group scheme as above.

all the objects stemming from the construction in §§4.2–4.4 applied to the polynomial P_m. As above, the non-trivial block of $\pi_m(\gamma_m) \in \mathbf{G}_{s,r}(\mathbb{R})$ is

$$\left(\left(\begin{smallmatrix} \alpha_{m,1} & \\ & \alpha_{m,1}^{-1} \end{smallmatrix} \right), \ldots, \left(\begin{smallmatrix} \alpha_{m,r} & \\ & \alpha_{m,r}^{-1} \end{smallmatrix} \right), \left(\begin{smallmatrix} \alpha_{m,r+1} & \\ & \alpha_{m,r+1}^{-1} \end{smallmatrix} \right), \ldots, \left(\begin{smallmatrix} \alpha_{m,r+t} & \\ & \alpha_{m,r+t}^{-1} \end{smallmatrix} \right) \right),$$

where $\alpha_{m,i}$ are roots of P_m in $\mathbb{C}$ labelled according to §4.1.

Let U_m denote the inversion-invariant neighborhood of 1 in $\mathbb{C}$ given by

$$U_m = \left\{ z \in \mathbb{C} \,\middle|\, -\frac{1}{m} \le \log |z| \le \frac{1}{m} \text{ and } -\frac{2\pi}{m} \le \arg(z) \le \frac{2\pi}{m} \right\}.$$

By construction, we have $1 < |\alpha_{m,i}| \le \mathcal{M}(P_m) < \exp(\eta_{m,t})$ for $1 \le i \le r + t$. Unfortunately, it may very well be that $\alpha_{m,i} \notin U_m$. To remedy this, we will use Dirichlet's simultaneous approximation theorem (see e.g. [Sch80, II, §1, Theorem 1A]). Let us recall it under the form we will use.

Lemma (Dirichlet)**.** Let $t, m \in \mathbb{N}^*$. For any $x_1, \ldots, x_t \in \mathbb{R}/\mathbb{Z}$, there exists an integer $0 < c \le m^t$ for which cx_i lies in $[-1/m, 1/m] + \mathbb{Z}$ for all $1 \le i \le t$.

Applying the approximation theorem to the arguments of $\alpha_{m,r+1}^2, \ldots, \alpha_{m,r+t}^2$ (scaled by $1/2\pi$) yields an integer c_m with $0 < c_m \le m^t$, such that

$$\alpha_{m,i}^{2c_m} \in U_m \quad \text{for} \quad 1 \le i \le r + t.$$

Indeed, for $r + 1 \le i \le r + t$, by construction of c_m, we have $-2\pi/m \le \arg(\alpha_{m,i}^{2c_m}) \le 2\pi/m$; when $1 \le i \le r$, it is clear that $\arg(\alpha_{m,i}^2) = 0$. In both cases,

$$1 < |\alpha_{m,i}^{2c_m}| \le |\alpha_{m,i}|^{2m^t} < \exp(2m^t \cdot \eta_{m,t}) = \exp(1/m).$$

Finally, let γ_m' denote the element $\pi_m(\gamma_m^{2c_m}) \in \pi_m(\Gamma_m) \le \mathbf{G}_{s,r}(\mathbb{R})$. Because $\{U_m \mid m \in \mathbb{N}^*\}$ forms a basis of neighborhoods of 1 in $\mathbb{C}$, the discussion above (together with the continuity of the regular representation $L_{\sigma_i}^\times \to \mathbf{GL}_2(K_{\sigma_i})$) shows that $\gamma_m' \to 1 \in \mathbf{G}_{s,r}(\mathbb{R})$ as $m \to \infty$. In addition, $\pi_m(\Gamma_m)$ is an irreducible, cocompact lattice in $\mathbf{G}_{s,r}(\mathbb{R})$ by §4.4, and, as $|\alpha_{m,1}| > 1$, γ_m' has infinite order. This contradicts Conjecture (A) for the group $\mathbf{G}_{s,r}$ and concludes the proof of theorem 1.3 for $\mathbf{F} = \mathbf{SL}_n$.

5. The argument for other simple groups

In this section, we indicate the modifications to run the argument for an isotropic $\mathbb{R}$-group $\mathbf{F}$ which is either classical, or adjoint of exceptional type G_2, F_4, E_6, E_7 or E_8. As any absolutely (almost) simple isotropic $\mathbb{R}$-group is isogenous to one of these (see e.g. [Tit66b]), this is sufficient to conclude the proof of Theorem 1.3.

For brevity, we omit the parts of the argument which are analogous (if not identical) to their counterparts in §§4.1–4.5. The leitmotiv is the construction of a K-form $\mathbf{G}$ of $\mathbf{F}$ with the appropriate archimedean shape, in which the norm torus $\ker \mathrm{N}_{L/K} \le \mathrm{Res}_{L/K}(\mathbf{GL}_1)$ embeds over $\mathcal{O}_K$.

We mostly keep the notation of §§4.1–4.5. Given a root α of some $P \in \mathscr{P}_{s,r}$, the fields L and K are constructed identically as in §4.2. Let L' denote the quadratic étale K-algebra $K[X]/(X^2 + 1)$, and let τ' denote the non-trivial automorphism of L' fixing K. Whenever -1 is not a square in K (e.g. when K is a real field, which is the case if we pick P according to ($\mathsf{L}_{s,r}$)), L' is a totally complex number field; otherwise, L' is the product of two copies of K. We will denote by σ_i' one of the two τ'-conjugate extensions to L' of the embedding $\sigma_i : K \to \mathbb{C}$ ($1 \le i \le d$).

In addition, we will make use of three quaternion algebras, defined over K by the following symbols:

$$D^+ = \langle (\alpha - \alpha^{-1})^2, (\alpha - \alpha^{-1})^2 \rangle_K, \quad D^- = \langle -(\alpha - \alpha^{-1})^2, -(\alpha - \alpha^{-1})^2 \rangle_K, \quad D' = \langle -1, -1 \rangle_K,$$

and whose conjugation involutions we denote by τ^+, τ^-, and τ', respectively. (This last abuse of notation is excused by the fact the restriction of the conjugation involution of D' to any image of L' corresponds to τ'.) Note that $(\alpha - \alpha^{-1})^2$ does indeed belong to K, and that $\sigma_i((\alpha - \alpha^{-1})^2)$ is positive for $1 \le i \le r$, and negative

for $s + 1 \leq i \leq d$. Thus, the quaternion algebra D^+ (resp. D^-, D') splits over K_{σ_i} if and only if $1 \leq i \leq s$ (resp. $r + 1 \leq i \leq d$, $r + 1 \leq i \leq s$). Moreover, as $L = K(\alpha - \alpha^{-1})$, L embeds in D^+, or equivalently D^+ splits over L. Similarly, L' embeds in D'.

Once constructed, we systematically endow the K-group $\mathbf{G}$ with the $\mathcal{O}_K$-structure obtained by writing the canonical equations defining $\mathbf{G}$ over $\mathcal{O}_K$ using the basis $\{1, \alpha\}$ of L over K (and its extension to an $\mathcal{O}_K$-structure on D^+, or the canonical bases of L', D^+, D^-, D', depending on the need). Unless indicated otherwise, we then set $\Gamma = \mathbf{G}(\mathcal{O}_K)$ to be the group of solutions in $\mathcal{O}_K$ of these equations. The reader will easily verify that this integral structure has the claimed properties.

For any field extension M of K and any K-algebra A, we set $A_M = A \otimes_K M$. We also set

$$\mathbf{G}_{s,r} = \prod_{i=1}^{r} \mathbf{F} \times \prod_{i=1}^{(s-r)/2} \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbf{F}) \in \mathscr{T}_{\mathbf{F}}^{(s)},$$

and as in §4.4, π will be the projection $\mathbf{G} \to \mathbf{G}_{s,r}$ with compact kernel to be constructed below.

We now give the modifications by the $\mathbb{R}$-type of $\mathbf{F}$, following the descriptions provided by Tits [Tit66b, Table II] (except perhaps for groups of type E). The reader may also find [KMRT98] a useful reference.

5.1. Inner form of type A.
$\mathbf{F}$ is of the form $\mathbf{SL}_{n,D_0}$ for some division algebra D_0 over $\mathbb{R}$ and $n \in \mathbb{N}^*$. As the split case has already been covered, we may as well assume that $D_0 \neq \mathbb{R}$, hence D_0 is simply Hamilton's quaternion algebra. Note that in fact $n \geq 2$ since $\mathbf{F}$ is isotropic.

Consider the involution $\tau^- \otimes \tau$ on the quaternion L-algebra $D_L^- = D^- \otimes_K L$. As it coincides with τ when restricted to the center L of D_L^-, this involution is of the second kind. Let $h : (D_L^-)^n \times (D_L^-)^n \to D_L^-$ be the $\tau^- \otimes \tau$-hermitian form given by

$$h(x, y) = x_1 (\tau^- \otimes \tau)(y_1) + \cdots + x_n (\tau^- \otimes \tau)(y_n) \qquad x, y \in (D_L^-)^n,$$

and let $\mathbf{G}$ be the special unitary group $\mathbf{SU}_{h,D_L^-}$ associated to h.

The local structure of G is as follows. Of course, $\mathbf{G}$ splits at the complex places $\sigma_{r+1}, \ldots, \sigma_s$ of K. For $s + 1 \leq i \leq d$, the quaternion algebra D_L^- splits over $L_{\sigma_i} \cong \mathbb{C}$. Nonetheless, $\mathbf{G}$ remains an outer form (of $\mathbf{SL}_{2n}$) over K_{σ_i}, since $\tau^- \otimes \tau$ induces the non-trivial automorphism of the field extension $L_{\sigma_i}/K_{\sigma_i} \cong \mathbb{C}/\mathbb{R}$. In view of the coefficients of h, we deduce that $\mathbf{G}$ becomes isomorphic to $\mathbf{SU}_{2n}$ (the usual anisotropic special unitary $\mathbb{R}$-group) over $K_{\sigma_i} \cong \mathbb{R}$ for $s + 1 \leq i \leq d$. Lastly, for $1 \leq i \leq r$, we have that L is contained in K_{σ_i}. This means that

$$D_L^- \otimes_K K_{\sigma_i} \cong D^- \otimes_K (L \otimes_K K_{\sigma_i}) \cong D^- \otimes_K (K_{\sigma_i} \oplus K_{\sigma_i}) \cong D_{K_{\sigma_i}}^- \oplus D_{K_{\sigma_i}}^-,$$

with $\tau^- \otimes \tau$ inducing a flip of the two summands. Thus $\mathbf{G} \cong \mathbf{SL}_{n,D_{K_{\sigma_i}}^-}$ over K_{σ_i}, that is $\mathbf{G}$ becomes an inner form (of $\mathbf{SL}_{2n}$) over K_{σ_i}. We had already observed that $D_{K_{\sigma_i}}^-$ does not split for $1 \leq i \leq r$, hence $D_{K_{\sigma_i}}^- \cong D_0$ after identifying K_{σ_i} with $\mathbb{R}$; in turn, $\mathbf{G} \cong \mathbf{SL}_{n,D_0}$ over K_{σ_i}. Altogether, we obtain

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{SL}_{n,D_0}(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{SL}_{2n}(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{SU}_{2n}(\mathbb{R}),$$

so that $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

The element $\gamma \in \Gamma$ is taken to be $\mathrm{diag}(\alpha, \alpha^{-1}, 1, \ldots, 1)$, seen as an element of $\mathbf{G}(\mathcal{O}_K) \subset \mathbf{SL}_n(D_L^-)$. One has indeed $\alpha \cdot \tau(\alpha) = \mathrm{N}_{L/K}(\alpha) = 1$, so that γ preserves h.

5.2. Outer form of type A.
$\mathbf{F}$ is of the form $\mathbf{SU}_{h_0}$ for some hermitian form $h_0 : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ of indefinite signature, say $(p, n - p)$ with $p \geq n - p$.

The symmetric K-bilinear form b on $L \times L$ associated to the quadratic form $\mathrm{N}_{L/K}$ on L allows us to construct a τ'-hermitian form h_b on $L \otimes_K L'$ by setting

$$h_b(\ell_1 \otimes \ell_1', \ell_2 \otimes \ell_2') = b(\ell_1, \ell_2)\ell_1' \cdot \tau'(\ell_2') \qquad \ell_1, \ell_2 \in L, \ \ell_1', \ell_2' \in L'.$$

Let V denote the vector L'-space $(L \otimes_K L')^{n-p} \oplus L'^{(2p-n)}$, and let $h : V \times V \to L'$ be the τ'-hermitian form given as the orthogonal sum

$$h = h_b^{\oplus(n-p)} \oplus \langle 1 \rangle^{\oplus(2p-n)},$$

where $\langle 1 \rangle$ denotes the τ'-hermitian form $(x, y) \mapsto x\tau'(y)$. Let $\mathbf{G}$ be the special unitary group $\mathbf{SU}_h$ associated to h.

The local structure of $\mathbf{G}$ is as follows. Of course, $\mathbf{G}$ splits at the complex places $\sigma_{r+1}, \ldots, \sigma_s$ of K. At the other places, one has by construction $L'_{\sigma'_i}/K_{\sigma_i} \cong \mathbb{C}/\mathbb{R}$ with τ' inducing complex conjugation; thus $\mathbf{G}$ remains an outer form (of $\mathbf{SL}_n$) there. In addition, the quadratic form $\mathrm{N}_{L/K}$ (hence also the hermitian form h_b) has local signature $(1, 1)$ or $(2, 0)$ over K_{σ_i} for respectively $1 \leq i \leq r$ or $s + 1 \leq i \leq d$. Thus h has local signature respectively $(p, n - p)$ or $(n, 0)$ over K_{σ_i}. Altogether, we have that

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{SU}_{h_0}(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{SL}_n(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{SU}_n(\mathbb{R}),$$

so that $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

Since $\mathrm{N}_{L/K}(\alpha) = 1$, multiplication by α induces an isometry of the quadratic K-space (L, b), and hence a unitary operator u_α of the hermitian space $(L \otimes_K L', h_b)$. Let then γ be the element of $\mathbf{G}(K)$ which acts as u_α on the first component of V, and as the identity on the other components. Note that $\gamma \in \mathbf{G}(\mathcal{O}_K)$ by choice of the $\mathcal{O}_K$-structure.

5.3. Type B. $\mathbf{F}$ is of the form $\mathbf{SO}_{q_0}$ for some quadratic form q_0 on $\mathbb{R}^n$ (n odd) of indefinite signature, say $(p, n - p)$ with $p \geq n - p$.

Let V be the K-module $L^{n-p} \oplus K^{2p-n}$, and endow V with the quadratic form q over K given as the orthogonal sum

$$q = \mathrm{N}_{L/K}^{\oplus(n-p)} \oplus \langle 1 \rangle^{\oplus(2p-n)},$$

where $\langle 1 \rangle$ denotes the quadratic form $x \mapsto x^2$ on K. Let $\mathbf{G}$ be the special orthogonal group $\mathbf{SO}_q$ associated to q.

$\mathbf{G}$ splits at the complex places $\sigma_{r+1}, \ldots, \sigma_s$ of K. For $s + 1 \leq i \leq d$, the quadratic K_{σ_i}-form $\mathrm{N}_{L_{\sigma_i}/K_{\sigma_i}}$ is positive definite (since $L_{\sigma_i}/K_{\sigma_i} \cong \mathbb{C}/\mathbb{R}$), whereas for $1 \leq i \leq r$, it has signature $(1, 1)$. Thus q has local signature respectively $(n, 0)$ and $(p, n - p)$. Writing $\mathbf{SO}_n$ for the usual anisotropic special orthogonal $\mathbb{R}$-group, this means

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{SO}_{q_0}(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{SO}_n(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{SO}_n(\mathbb{R}),$$

so that $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

Since $\mathrm{N}_{L/K}(\alpha) = 1$, multiplication by α induces an isometry u_α of the quadratic K-space (L, b). We take γ to be the element of $\mathbf{G}(K)$ which acts as u_α on the first component of V, and as the identity on the other components. Note again that $\gamma \in \mathbf{G}(\mathcal{O}_K)$ by choice of the $\mathcal{O}_K$-structure.

5.4. Type C, non-split. $\mathbf{F}$ is of the form $\mathbf{SU}_{h_0, D_0}$, where D_0 is a quaternion $\mathbb{R}$-algebra and h_0 is a hermitian form (with respect to quaternion conjugation) on D_0^n, of signature say $(p, n - p)$ with $p \geq n - p$. Either D_0 is Hamilton's quaternion algebra, or D_0 splits, in which case quaternion conjugation corresponds to adjugation and $\mathbf{SU}_{h_0, D_0}$ splits to become $\mathbf{Sp}_{2n}$ regardless of the signature of h_0. We start with the case where D_0 does not split, and thus h_0 is indefinite (because $\mathbf{F}$ is isotropic).

The symmetric K-bilinear form b associated to the quadratic form $\mathrm{N}_{L/K}$ on L allows us to construct a τ'-hermitian form h_b on $L \otimes_K D'$ by setting

$$h_b(\ell_1 \otimes d'_1, \ell_2 \otimes d'_2) = b(\ell_1, \ell_2) d'_1 \cdot \tau'(d'_2) \qquad \ell_1, \ell_2 \in L, \; d'_1, d'_2 \in D'.$$

Let V be the (left) D'-module $(L \otimes_K D')^{n-p} \oplus D'^{2p-n}$, and endow V with the τ'-hermitian form h given as the orthogonal sum

$$h = h_b^{\oplus(n-p)} \oplus \langle 1 \rangle^{\oplus(2p-n)}.$$

Let $\mathbf{G}$ be the special unitary group $\mathbf{SU}_{h,D'}$ associated to h.

Of course, $\mathbf{G}$ splits at the complex places $\sigma_{r+1}, \ldots, \sigma_s$. On the other hand, $D'_{K_{\sigma_i}} \cong D_0$ when $1 \leq i \leq r$ or $s + 1 \leq i \leq d$, by construction. From the local signatures of $\mathrm{N}_{L/K}$, one computes that h has local signatures $(p, n - p)$ or $(n, 0)$ for $1 \leq i \leq r$ or $s + 1 \leq i \leq d$ respectively. In other words, writing $\mathbf{Sp}_{n,0}$ for the anisotropic $\mathbb{R}$-form of $\mathbf{Sp}_{2n}$,

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{SU}_{h_0}(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{Sp}_{2n}(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{Sp}_{n,0}(\mathbb{R}),$$

so that $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

Since $\mathrm{N}_{L/K}(\alpha) = 1$, multiplication by α induces an isometry of the quadratic K-space (L, b), and hence a unitary operator u_α of the hermitian space $(L \otimes_K D', h_b)$. Let then $\gamma \in \mathbf{G}(\mathcal{O}_K)$ act as u_α on the first component of V, and as the identity on the other components.

5.5. Type C, split. Now if D_0 is split, we consider instead the τ^+-hermitian form $h = \langle 1 \rangle^{\oplus n}$ on $(D^+)^n$. Since D^+ splits over K_{σ_i} for $1 \leq i \leq s$, so does the K-group $\mathbf{G} = \mathbf{SU}_{h,D^+}$. On the other hand, D^+ does not split at the remaining places, and the signature of h indicates that $\mathbf{G}(K \otimes \mathbb{R})$ projects appropriately onto $\mathbf{G}_{s,r}(\mathbb{R})$. It remains to observe that α can be seen as an element of D^+ through the canonical embedding of L, and viewed as such, the element $\gamma = \mathrm{diag}(\alpha, 1, \ldots, 1) \in \mathbf{GL}_n(D^+)$ actually belongs to $\mathbf{G}(\mathcal{O}_K)$ because τ^+ coincides with τ on L.

5.6. Type D. $\mathbf{F}$ is either of the form $\mathbf{SO}_{q_0}$ for some quadratic form q_0 on $\mathbb{R}^n$ (n even) of indefinite signature, or of the form $\mathbf{SU}_{h_0,D_0}$ for h_0 the standard hermitian form on D_0^n ($n \geq 2$) with respect to an involution of orthogonal type, where D_0 is Hamilton's quaternion algebra. The first case is treated exactly like type B; we thus focus on the second case.

Let ρ denote the involution of orthogonal type on D^- given by

$$\rho(x_1 + x_2 \boldsymbol{i} + x_3 \boldsymbol{j} + x_4 \boldsymbol{k}) = x_1 + x_2 \boldsymbol{i} + x_3 \boldsymbol{j} - x_4 \boldsymbol{k} \qquad x_1, x_2, x_3, x_4 \in K$$

in the canonical basis $\{1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ of D^- over K. As previously, the symmetric K-bilinear form b associated to $\mathrm{N}_{L/K}$ allows us to construct a ρ-hermitian form h_b on $L \otimes_K D^-$. Let V be the (left) D^--module $(L \otimes_K D^-) \oplus (D^-)^{n-2}$, and endow V with the ρ-hermitian form given as the orthogonal sum

$$h = h_b \oplus \langle 1 \rangle^{\oplus(n-2)}.$$

Let $\mathbf{G}$ be the special unitary group $\mathbf{SU}_{h,D^-}$.

By construction, $D^- \cong D_0$ over K_{σ_i} for $1 \leq i \leq r$, and h is easily seen to be equivalent to the standard form h_0 over D_0. For $s + 1 \leq i \leq d$ however, D^- splits over K_{σ_i}, and ρ becomes the transposition involution on $\mathrm{M}_2(K_{\sigma_i})$. Moreover, at these places the form b is positive definite; so h is again equivalent to the standard form $\langle 1 \rangle^{\oplus n}$, showing that over K_{σ_i}, $\mathbf{G} \cong \mathbf{SO}_{2n}$ is anisotropic ($s + 1 \leq i \leq d$). Altogether,

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{SU}_{h_0,D_0}(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{SO}_{2n}(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{SO}_{2n}(\mathbb{R}),$$

so that $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

Again, multiplication by α induces a unitary operator u_α on the hermitian space $(L \otimes_K D^-, h_b)$, and we take $\gamma \in \mathbf{G}(\mathcal{O}_K)$ to act as u_α on the first component of V, and as the identity on the other components.

5.7. Type G_2. $\mathbf{F}$ is of the form $\mathbf{Aut}\, O_0$, where O_0 is the split octonion $\mathbb{R}$-algebra. (Note that regardless of the base field, the only isotropic form of G_2 is the split one.)

Let O^+ be the octonion K-algebra obtained by applying the Cayley–Dickson construction to D^+ with the parameter -1. Recall that this means $O^+ = D^+ \oplus D^+\ell$, endowed with the multiplication rule

$$(a + b\ell)(c + d\ell) = (ac - \tau^+(d)b) + (da + b\tau^+(c))\ell \qquad a, b, c, d \in D^+.$$

(Recall that a split octonion algebra may be obtained by the Cayley-Dickson construction applied to a split quaternion algebra with any parameter.)

Let $\mathbf{G}$ be the K-group $\mathbf{Aut}\, O^+$.

For $1 \leq i \leq s$, the algebra O^+, hence also $\mathbf{G}$, splits over K_{σ_i} because D^+ does, whereas $\mathbf{G}$ is anisotropic over K_{σ_i} for $s + 1 \leq i \leq d$, because at these places O^+ is a (nonassociative) division algebra since its norm form (which is the double of the norm form of D^+) is positive definite. Altogether, writing $\mathbf{F}^{\mathrm{anis}}$ for the anisotropic $\mathbb{R}$-group of type G_2,

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{F}(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{F}(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{F}^{\mathrm{anis}}(\mathbb{R}),$$

so that $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

One checks that given $x \in D^+$ with $\tau^+(x)x = 1$, the assignment $a + b\ell \mapsto a + (xb)\ell$ defines an automorphism u_x of O^+ (see [SV00, §2.1]). As L embeds in D^+ (with τ^+ restricting to τ), α can be seen as an element of D^+ of norm 1. The automorphism $\gamma = u_\alpha$ of O^+ then belongs to $\mathbf{G}(\mathcal{O}_K)$ (if as before, $\mathbf{G}$ is endowed with the $\mathcal{O}_K$-structure induced by an $\mathcal{O}_K$-structure on O^+ extending the basis $\{1, \alpha\}$ of $L \subset D^+$).

5.8. Preliminaries for type F_4. Recall that given a field M, an octonion algebra O over M, and parameters $c = (c_1, c_2, c_3) \in (M^\times)^3$, the set

$$\mathcal{A}_M(O, c) = \left\{ \begin{pmatrix} x_1 & y_3 & c_1^{-1}c_3\overline{y}_2 \\ c_2^{-1}c_1\overline{y}_3 & x_2 & y_1 \\ y_2 & c_3^{-1}c_2\overline{y}_1 & x_3 \end{pmatrix} \middle| x_1, x_2, x_3 \in M, y_1, y_2, y_3 \in O \right\}$$

of *(c_1, c_2, c_3)-hermitian 3×3 matrices with entries in O* (endowed with the Jordan product) forms an exceptional Jordan algebra called an *Albert algebra*. When the underlying octonion algebra is split, any choices of c_1, c_2, c_3 yield isomorphic Albert algebras, which are accordingly called *split*.

Over $\mathbb{R}$, there are three isomorphism classes of Albert algebras, represented by: the *split* Albert algebra of $(1, 1, 1)$-hermitian 3×3 matrices with entries in the split octonion $\mathbb{R}$-algebra, the algebra of $(1, 1, 1)$-hermitian 3×3 matrices with entries in Cayley's octonion algebra (which we call the *definite* Albert $\mathbb{R}$-algebra), and the algebra of $(1, 1, -1)$-hermitian 3×3 matrices with entries in Cayley's octonion algebra (which we call the *indefinite* Albert $\mathbb{R}$-algebra).

5.9. Type F_4, split. $\mathbf{F}$ is of the form $\mathbf{Aut}\, A_0$, where A_0 is the split Albert $\mathbb{R}$-algebra.

Let O^+ be the octonion K-algebra obtained by applying the Cayley–Dickson construction to D^+ with the parameter -1, and let $A^+ = \mathcal{A}_K\big(O^+, (1, 1, 1)\big)$. Let $\mathbf{G}$ be the K-group $\mathbf{Aut}\, A^+$; it is a simple group of type F_4 (see namely [SV00, Ch. 5–7] for this fact and others concerning the structure of Albert algebras).

As mentioned in §5.7, O^+ splits over K_{σ_i} for $1 \leq i \leq s$, whereas it remains a division algebra over K_{σ_i} for $s + 1 \leq i \leq d$. Thus A^+ hence $\mathbf{G}$ splits over K_{σ_i} for $1 \leq i \leq s$, while for $s + 1 \leq i \leq d$, A^+ is isomorphic over K_{σ_i} to the definite Albert $\mathbb{R}$-algebra, hence $\mathbf{G}$ is isomorphic over K_{σ_i} to the anisotropic simple $\mathbb{R}$-group $\mathbf{F}^{\mathrm{anis}}$ of type F_4. Altogether,

$$\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \prod_{i=1}^{r} \mathbf{F}(\mathbb{R}) \times \prod_{i=1}^{(s-r)/2} \mathbf{F}(\mathbb{C}) \times \prod_{i=1}^{d-s} \mathbf{F}^{\mathrm{anis}}(\mathbb{R}),$$

so that $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

Given $x \in D^+$ of norm 1, the automorphism u_x of O^+ from §5.7 extends canonically to an automorphism of A^+, still to be denoted u_x. By choice of the $\mathcal{O}_K$-structure on L, and in turn on D^+, O^+ and A^+, the automorphism $\gamma = u_\alpha$ of A^+ belongs to $\mathbf{G}(\mathcal{O}_K)$.

5.10. Type F_4, non-split. $\mathbf{F}$ is of the form $\mathbf{Aut}\, A_0$, where this time A_0 is the indefinite Albert $\mathbb{R}$-algebra.

Let O' be the octonion K-algebra obtained by applying the Cayley–Dickson construction to D' with the parameter -1, and let $A' = \mathcal{A}_K(O', (1, 1, -(\alpha - \alpha^{-1})^2))$. Let $\mathbf{G}$ be the K-group $\mathbf{Aut}\, A'$.

The octonion algebra O' is isomorphic to Cayley's octonion algebra over K_{σ_i} for all $1 \le i \le d$. The signs of the parameters defining A' vary under the different embeddings of K in such a way that for $1 \le i \le s$, A' is isomorphic over K_{σ_i} to A_0, hence also $\mathbf{G}$ to $\mathbf{F}$. For $s + 1 \le i \le d$, A' is isomorphic over K_{σ_i} to the definite Albert $\mathbb{R}$-algebra, hence $\mathbf{G}$ is isomorphic over K_{σ_i} to the anisotropic $\mathbb{R}$-form $\mathbf{F}^{\mathrm{anis}}$, as required.

Conjugation[7] by the matrix $\begin{pmatrix} (\alpha+\alpha^{-1})/2 & 0 & (\alpha-\alpha^{-1})^2/2 \\ 0 & 1 & 0 \\ 1/2 & 0 & (\alpha+\alpha^{-1})/2 \end{pmatrix} \in \mathbf{GL}_3(K)$ defines a linear map $u_\alpha \in \mathbf{GL}(A')$.

Using the fact that the above matrix preserves the diagonal quadratic form $\langle 1, 1, -(\alpha - \alpha^{-1})^2 \rangle$, it is readily seen that u_α is in fact an automorphism of the Albert algebra A'. What is perhaps less obvious is that $\gamma = u_\alpha$ belongs to an arithmetic lattice in $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$. Let Ω be the $\mathcal{O}_K$-submodule of $\mathrm{M}_3(O')$ spanned by the canonical basis. Conjugation by the matrix $\begin{pmatrix} 1 & 0 & (\alpha+\alpha^{-1})/2 \\ 0 & 1 & 0 \\ 0 & 0 & 1/2 \end{pmatrix} \in \mathbf{GL}_3(K)$ transforms Ω into Ω', which has the property that the $\mathcal{O}_K$-submodule $A' \cap \Omega'$ of A' is preserved by γ. In other words, γ belongs to $\Gamma = \mathrm{Stab}_{\mathbf{G}(K)}(A' \cap \Omega')$, which is a lattice when embedded diagonally in $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$. This can be seen easily as follows. The quadratic form $\langle 1, -(\alpha - \alpha^{-1})^2 \rangle$ is nothing but the norm form of L/K written in the K-basis $\{1, \alpha - \alpha^{-1}\}$ of L. The matrix $\begin{pmatrix} 1 & (\alpha+\alpha^{-1})/2 \\ 0 & 1/2 \end{pmatrix}$ changes basis back to the standard basis $\{1, \alpha\}$. The non-trivial block of γ in this new basis then rewrites $\begin{pmatrix} 0 & -1 \\ 1 & \alpha+\alpha^{-1} \end{pmatrix} \in \mathbf{GL}_2(\mathcal{O}_K)$, which is just the matrix of multiplication by α on L.[8] This also shows that γ is not torsion, and that $\gamma^{2c_m} \to 1$ whenever $\alpha^{2c_m} \to 1$ (as needed in the argument of §4.5).

5.11. Preliminaries for type E. In order to treat groups of type E, we briefly recall Tits' construction of the exceptional simple Lie algebras. Let B and C be *composition algebras* over a field M of characteristic $\ne 2, 3$; this means that B, C are chosen among M itself, quadratic étale algebras, quaternion algebras, or octonion algebras over M. Let J be the Jordan algebra $\mathcal{A}_M(B, (c_1, c_2, c_3))$, for some $c_1, c_2, c_3 \in M$ (defined analogously to §5.8). The set

$$\mathfrak{L}(C, J) = \mathrm{Der}(C) \oplus (C^{\circ} \otimes J^{\circ}) \oplus \mathrm{Der}(J),$$

where C° (resp. J°) denotes the kernel of the trace of C (resp. J), can be endowed with a Lie bracket which turns it into a semisimple Lie M-algebra whose absolute type is given by the *Freudenthal-Tits magic square*:

$\dim_M C$ \ $\dim_M B$	1	2	4	8
1	A_1	A_2	C_3	F_4
2	A_2	$\mathsf{A}_2 \times \mathsf{A}_2$	A_5	E_6
4	C_3	A_5	D_6	E_7
8	F_4	E_6	E_7	E_8

This construction and the magic square were discovered independently by Freudenthal and Tits. Quite remarkably, when extended appropriately to include G_2, the construction gives Lie algebras of all the exceptional types in a unified way. For a more detailed description, we refer the reader to the original articles

---

[7]Here, we only use that O' is a K-(bi)module, which splits as a direct sum of K and the K-submodule of totally imaginary octonions. Conjugation by a matrix with arbitrary entries in O' makes no sense since O' is not an associative algebra.

[8]If there were such things as *hermitian forms over octonions*, one would directly extend the norm form of L/K to O' instead of working with the form $\langle 1, -(\alpha - \alpha^{-1})^2 \rangle$. This would simplify the notation and avoid the base-change computations.

of Freudenthal [Fre54a – Fre63] and Tits [Tit66a], as well as to the lecture notes of Jacobson [Jac71] and the Book of Involutions [KMRT98, Ch. IX].

It turns out that over $\mathbb{R}$, Tits' construction produces all possible forms of simple real Lie algebras of type E or F, as C and J run through all possible combinations. We refer to [Jac71, pp. 119–121] for a summary of which input (C, J) to use for each $\mathbb{R}$-form. We will use this in the remaining cases (types E_6, E_7, E_8) to describe the group $\mathbf{F}$ and construct an appropriate form of $\mathbf{F}$ over $\mathcal{O}_K$.[9] In fact, the case F_4 treated above is also encompassed by this approach (take $C = \mathbb{R}$ and B an octonion $\mathbb{R}$-algebra); but we decided to treat F_4 beforehand because it will be used for type E, in the following way.

As is easily seen from the definition of the Lie bracket, any automorphism φ of C (resp. J) induces an automorphism $\widetilde{\varphi}$ of $\mathfrak{L}(C, J)$ by acting via conjugation on the Lie subalgebra $\mathrm{Der}(C)$ (resp. $\mathrm{Der}(J)$), acting canonically on the first (resp. second) tensor component of $C^\circ \otimes J^\circ$, and acting trivially on $\mathrm{Der}(J)$ (resp. $\mathrm{Der}(C)$). This assignment yields morphisms of algebraic groups $\mathbf{Aut}\, C \to \mathbf{Aut}\, \mathfrak{L}(C, J)$, resp. $\mathbf{Aut}\, J \to \mathbf{Aut}\, \mathfrak{L}(C, J)$, whose images commute, and which for the last row (resp. column) of the magic square correspond to the familiar embeddings G_2 (resp. F_4) $\hookrightarrow F_4, E_6, E_7, E_8$.

5.12. Type E. $\mathbf{F}$ is of the form $\mathbf{Aut}\, \mathfrak{L}(C_0, A_0)$, where C_0 is a quadratic étale, a quaternion or an octonion $\mathbb{R}$-algebra (depending on the absolute rank of $\mathbf{F}$), and A_0 is an Albert $\mathbb{R}$-algebra. There are respectively four, three and two possibilities for the isotropic $\mathbb{R}$-group $\mathbf{F}$. We list them below (labelled by the signature of their Killing form), and fix inputs (C_0, A_0) when there is more than one choice (obviously, a similar construction works with any of the choices). We begin with E_6:

(E_6^6) $C_0 \cong \mathbb{R} \oplus \mathbb{R}$ and A_0 is split (as in §5.9). In this case, $\mathbf{F}$ is split.

(E_6^{-26}) $C_0 \cong \mathbb{R} \oplus \mathbb{R}$ and A_0 is (up to isomorphism) any of the two non-split Albert $\mathbb{R}$-algebras; we pick A_0 to be indefinite (as in §5.10). In this case, $\mathbf{F}$ is the non-split inner $\mathbb{R}$-form of type E_6.

The remaining $\mathbb{R}$-forms of E_6 are outer forms. The two isotropic ones are given by:

(E_6^2) $C_0 \cong \mathbb{C}$ and A_0 split.

(E_6^{-14}) $C_0 \cong \mathbb{C}$ and A_0 is indefinite (as in §5.10).

Now for E_7:

(E_7^7) C_0 and A_0 are split. In this case, $\mathbf{F}$ is split.

(E_7^{-25}) C_0 is split and A_0 is any of the two non-split Albert $\mathbb{R}$-algebras; we pick A_0 indefinite (as in §5.10).

(E_7^{-5}) C_0 is Hamilton's quaternion algebra and A_0 is split or indefinite; we pick A_0 split.

And lastly for E_8:

(E_8^8) C_0 and A_0 are split, or alternatively C_0 is Cayley's octonion algebra and A_0 is indefinite; we pick C_0 and A_0 both split. In this case, $\mathbf{F}$ is split.

(E_8^{-24}) C_0 is Cayley's octonion algebra and A_0 is split, or alternatively C_0 is split and A_0 is any of the two non-split Albert $\mathbb{R}$-algebras; we pick the former.

Note that for each rank, exactly one combination for (C_0, A_0) is disregarded, namely the one where C_0 is not split and A_0 is definite. This combination gives the (unique) anisotropic $\mathbb{R}$-form of type E of the corresponding rank.

For each one of these possibilities, we define the K-algebras C and A as indicated in the table below. The K-algebras O^+, A^+ are those defined in §5.9, and O', A' are defined in §5.10.

$\mathbb{R}$-type	E_6^6	E_6^{-26}	E_6^2	E_6^{14}	E_7^7	E_7^{-25}	E_7^{-5}	E_8^8	E_8^{-24}
C	L	L	L'	L'	D^+	D^+	D'	O^+	O'
A	A^+	A'	A^+	A'	A^+	A'	A^+	A^+	A^+

We then let $\mathbf{G}$ be the K-group $\mathbf{Aut}\, \mathfrak{L}(C, A)$ afforded by Tits' construction.

[9]For E_6 (and perhaps for E_7), one could have used a description more resemblant to that of G_2 and F_4. However, the smallest nontrivial irreducible representation of a group of type E_8 is the adjoint representation, hence one essentially cannot avoid looking at a group of type E_8 as the automorphism groups of its Lie algebra.

In view of the behavior of the chosen algebras C and A at the archimedean places of K (described in §5.9 or §5.10), $\mathbf{G}$ is isomorphic to $\mathbf{F}$ over K_{σ_i} for $i = 1, \ldots, s$, whereas it remains anisotropic over K_{σ_i} for $i = s + 1, \ldots, d$. Thus $\mathbf{G}(K \otimes_{\mathbb{Q}} \mathbb{R})$ projects onto $\mathbf{G}_{s,r}(\mathbb{R})$ with compact kernel.

Let u_α be the automorphism of A constructed from α in §5.9 (if $A = A^+$) or in §5.10 (if $A = A'$). The induced automorphism $\gamma = \widetilde{u}_\alpha$ of $\mathfrak{L}(C, A)$ is then the required element of $\mathbf{G}(\mathcal{O}_K)$, where we use for $\mathfrak{L}(C, A)$ the $\mathcal{O}_K$-structure canonically induced by that of C and A (given in §5.9 or §5.10). Indeed, γ is not torsion since the morphism $\sim : \mathbf{Aut}\, A \to \mathbf{Aut}\, \mathfrak{L}(C, A)$ used to construct it is injective, and $\gamma^{2c_m} \to 1$ whenever $\alpha^{2c_m} \to 1$ because (the extension of) this morphism (to any completion of K) is continuous.

References

[BDM07]   Peter Borwein, Edward Dobrowolski, and Michael J. Mossinghoff. Lehmer's problem for polynomials with odd coefficients. *Ann. of Math. (2)*, 166(2):347–366, 2007.

[Ben08]   Yves Benoist. Réseaux des groupes de lie. Notes de Cours, 2008.

[BHC62]   Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75:485–535, 1962.

[Bre07]   Emmanuel Breuillard. On uniform exponential growth for solvable groups. *Pure Appl. Math. Q.*, 3(4):949–667, 2007.

[BV20]   Emmanuel Breuillard and Péter P. Varjú. Entropy of Bernoulli convolutions and uniform exponential growth for linear groups. *J. Anal. Math.*, 140(2):443–481, 2020.

[Dob79]   Edward Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34(4):391–401, 1979.

[ERT19]   Vincent Emery, John G. Ratcliffe, and Steven T. Tschantz. Salem numbers and arithmetic hyperbolic groups. *Trans. Amer. Math. Soc.*, 372(1):329–355, 2019.

[Fra21]   Mikołaj Fraczyk. Strong limit multiplicity for arithmetic hyperbolic surfaces and 3-manifolds. *Invent. Math.*, 224(3):917–985, 2021.

[Fre54a]   Hans Freudenthal. Beziehungen der E_7 und E_8 zur Oktavenebene. I. *Nederl. Akad. Wet., Proc., Ser. A*, 57:218–230, 1954.

[Fre54b]   Hans Freudenthal. Beziehungen der E_7 und E_8 zur Oktavenebene. II. *Nederl. Akad. Wet., Proc., Ser. A*, 57:363–368, 1954.

[Fre55]   Hans Freudenthal. Beziehungen der E_7 und E_8 zur Oktavenebene. III, IV. *Nederl. Akad. Wet., Proc., Ser. A*, 58:151–157, 277–285, 1955.

[Fre59]   Hans Freudenthal. Beziehungen der $\mathfrak{E}_7$ und $\mathfrak{E}_8$ zur Oktavenebene. V-IX. *Nederl. Akad. Wet., Proc., Ser. A*, 62:165–179, 180–191, 192–201, 447–465, 466–474, 1959.

[Fre63]   Hans Freudenthal. Beziehungen der $\mathfrak{E}_7$ und $\mathfrak{E}_8$ zur Oktavenebene. X, XL. *Nederl. Akad. Wet., Proc., Ser. A*, 66:457–471, 472–487, 1963.

[Gel04]   Tsachik Gelander. Homotopy type and volume of locally symmetric manifolds. *Duke Math. J.*, 124(3):459–515, 2004.

[GH01]   Eknath Ghate and Eriko Hironaka. The arithmetic and geometry of Salem numbers. *Bull. Amer. Math. Soc. (N.S.)*, 38(3):293–314, 2001.

[Jac71]   Nathan Jacobson. *Exceptional Lie algebras*. Lecture Notes in Pure and Applied Mathematics. New York: Marcel Dekker, Inc., 1971.

[KMRT98]   Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions. With a preface by J. Tits.*, volume 44. Providence, RI: American Mathematical Society, 1998.

[Leh33]   Derrick H. Lehmer. Factorization of certain cyclotomic functions. *Ann. Math. (2)*, 34:461–479, 1933.

[Mar75]   Gregory A. Margulis. Discrete groups of motions of manifolds of nonpositive curvature. In *Proceedings of the International Congress of Mathematicians (Vancouver, B.C., 1974), Vol. 2*, pages 21–34. Canad. Math. Congress, Montreal, Que., 1975.

[Mar91]   Gregory A. Margulis. *Discrete subgroups of semisimple Lie groups*, volume 17 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1991.

[MR03]   Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[NR92]   Walter D. Neumann and Alan W. Reid. Arithmetic of hyperbolic manifolds. In *Topology '90 (Columbus, OH, 1990)*, volume 1 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 273–310. de Gruyter, Berlin, 1992.

[Sch73]   Andrzej Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24:385–399, 1973.

[Sch80]   Wolfgang M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Smy71]   Chris Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.*, 3:169–175, 1971.

[Smy08]   Chris Smyth. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 322–349. Cambridge Univ. Press, Cambridge, 2008.

[Smy15]   Chris Smyth. Seventy years of Salem numbers. *Bull. Lond. Math. Soc.*, 47(3):379–395, 2015.

[Sur92]   B. Sury. Arithmetic groups and Salem numbers. *Manuscripta Math.*, 75(1):97–102, 1992.

[SV00]   Tonny A. Springer and Ferdinand D. Veldkamp. *Octonions, Jordan algebras and exceptional groups. Revised English version of the original German notes.* Berlin: Springer, revised english version of the original german notes edition, 2000.

[Tit66a] Jacques Tits. Algèbres alternatives, algèbres de Jordan et algèbres de Lie exceptionnelles. I: Construction. *Nederl. Akad. Wet., Proc., Ser. A*, 69:223–237, 1966.

[Tit66b] Jacques Tits. Classification of algebraic semisimple groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 33–62. Amer. Math. Soc., Providence, R.I., 1966.

[Vou96]   Paul Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74(1):81–95, 1996.

[Zim84]   Robert J. Zimmer. *Ergodic theory and semisimple groups*, volume 81 of *Monographs in Mathematics*. Birkhäuser Verlag, Basel, 1984.

L.P.: Department of Mathematics, Brandeis University, 415 South Street, 02453 Waltham, United States of America & The Einstein Institute of Mathematics, Edmond J. Safra Campus, Givat Ram, The Hebrew University of Jerusalem Jerusalem, 91904, Israel

Email address: lampham@brandeis.edu

F.T.: Department of mathematics, KU Leuven, Celestijnenlaan 200B, 3001 Leuven, Belgium

Email address: francois.thilmany@kuleuven.be