DIVISIBILITY PROPERTIES OF HIGHER RANK LATTICES

MANFRED EINSIEDLER AND SHAHAR MOZES

Dedicated to Herbert Abels on the occasion of his 75 anniversary.

Abstract. We discuss a relationship between the dynamical properties of a maximal diagonalizable group A on certain arithmetic quotients and arithmetic properties of the lattice. In particular, we consider the semigroup of all integer quaternions under multiplication. For this semigroup we use measure rigidity theorems to prove that the set of elements that are not divisible by a given reduced quaternion is very small: We show that any quaternion that has a sufficiently divisible norm is also divisible by the given quaternion. Restricting to the quaternions that have norm equal to products of powers of primes from a given list (containing at least two) we show that the set of exceptions has subexponential growth.

1. Introduction

In this paper we discuss a relationship between the structure of orbits under a maximal diagonalizable group A on certain arithmetic quotients $X = \Gamma\backslash G$ and arithmetic properties of the lattice Γ.

1.1. **Quaternion algebras.** We start with the following special case that motivated this work. Let $D = \mathbb{Q}[i,j,k]$ be the Hamiltonian quaternion algebra over $\mathbb{Q}$. Let S be a finite set of primes over which D splits, i.e. $D \otimes \mathbb{Q}_p \cong \mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ for $p \in S$. (Equivalently, S consists of finitely many odd primes.) Let $\mathcal{O} = \mathbb{Z}[i,j,k] \subset D$. Recall also that there exists a canonical norm function $N : D \to \mathbb{Q}$. With this we can define the two multiplicative semigroups

$$\begin{aligned} \Lambda_{\mathcal{O}} &= \mathcal{O} \setminus \{0\} \\ \Lambda_{\mathcal{O},S} &= \{a \in \mathcal{O} : N(a) \text{ is a product of powers of primes in } S\} \end{aligned}$$

To state our theorem in this case we need a few notions. We say $a \in \Lambda_{\mathcal{O}}$ *divides* $\gamma \in \Lambda_{\mathcal{O}}$ if there exists $\alpha, \beta \in \Lambda_{\mathcal{O}}$ with $\gamma = \alpha a \beta$. We say $a \in \Lambda_{\mathcal{O}}$ is *reduced* if $\frac{1}{p}a \notin \mathcal{O}$ for all primes p.

Theorem 1.1. *Let D be the Hamiltonian quaternion algebra and let $\mathcal{O} = \mathbb{Z}[i,j,k]$. Let $a \in \Lambda_{\mathcal{O}}$ be a reduced element of odd norm. Then there exists some odd $M \geq N(a)$ such that any $\gamma \in \Lambda_{\mathcal{O}}$ with $M \mid N(\gamma)$ is divisible by a.*

We note that this stands in stark contrast with the case of the ring of integers in a quadratic field extension where the norm function does not satisfy such a property. E.g. if a is a prime in the ring of integers of a quadratic field extension

M. E. acknowledges the support by the SNF (Grant 200021-152819).

S. M. acknowledges the support by the BSF (grant 0378575) and the ISF (grants 0398362, 0399180).

such that $N(a) = a\bar{a} = p$ is a prime and $a^{-1}\bar{a}$ is not an integer, then a does not divide any power of $\bar{a}$.

In the second theorem we will restrict our attention to $\Lambda_{\mathcal{O},S}$ for a finite set of primes S as above. Notice that the above notion of divisibility automatically restricts to the divisibility within $\Lambda_{\mathcal{O},S}$, i.e. if $\gamma = \alpha a \beta$ with $a, \gamma \in \Lambda_{\mathcal{O},S}$ then also $\alpha, \beta \in \Lambda_{\mathcal{O},S}$. In this context we will use a few more definitions to express our theorem (where we will use a more geometrical language motivated by the associated buildings). Given some $a \in \Lambda_{\mathcal{O},S}$ we define the *width of* a as the minimal exponent $\mathrm{width}(a)$ of the primes in S in the factorization of $N(a)$. The condition in the theorem below that $\mathrm{width}(\gamma)$ is sufficiently big is a geometric analogue of the condition that the norm of γ is divisible by some product M of powers of primes in S. Finally we define $\mathrm{diam}(a)$, the *diameter of* $a \in \Lambda_{\mathcal{O},S}$, as the sum of the exponents in the factorization of $N(a)$.

Theorem 1.2. *Let D be the Hamiltonian quaternion algebra and $\mathcal{O} = \mathbb{Z}[i,j,k]$. Let S be a finite set of nonarchimedean places over which D splits, and assume $|S| \geq 2$. Let $a \in \Lambda_{\mathcal{O},S}$ be a reduced element. Then for every $\epsilon > 0$ there exists some $w = w(a,\epsilon)$ so that*

$$\log\left|\left\{\gamma \in \Lambda_{\mathcal{O},S} : \mathrm{diam}(\gamma) \leq R, \mathrm{width}(\gamma) \geq w, a \text{ does not divide } \gamma\right\}\right| < \epsilon R$$

for all sufficiently large R.

Let us note that if $S = \{p\}$ contains only one prime, then the above claim cannot hold. In fact, in this case the group obtained from $\Lambda_{\mathcal{O},\{p\}}$ modulo $\mathbb{Q}^\times$ contains a free subgroup of finite index and once a has sufficient width the growth rate of all elements that are not divisible by a is exponential.

In the case $|S| \geq 2$ considered above the proof will rely on measure rigidity for the action of a diagonalizable subgroup on a quotient of $\prod_{p\in S} \mathrm{PGL}_2(\mathbb{Q}_p)$ by a lattice derived from $\Lambda_{\mathcal{O},S}$. In Theorem 1.1 a measure rigidity theorem on an adelic quotient is used. The arguments behind the above theorem apply more generally, even to lattices in groups that are non-compact over $\mathbb{R}$. However, for this we have to define more general notions of divisibility.

1.2. **General definitions.** Let $\mathbb{G}$ be an algebraic semisimple group defined over $\mathbb{Q}$ of $\mathbb{Q}$-rank zero, let S be a finite set of places of $\mathbb{Q}$ (containing ∞ when $\mathbb{G}(\mathbb{R})$ is not compact), let $G = \prod_{\sigma\in S} \mathbb{G}(\mathbb{Q}_\sigma)$ be the $\mathbb{Q}_S$ -points of $\mathbb{G}$ (where $\mathbb{Q}_S = \prod_{\sigma\in S} \mathbb{Q}_\sigma$), let $A = \prod_{\sigma\in S} A_\sigma < G$ be the product of the $\mathbb{Q}_\sigma$-points of some maximal $\mathbb{Q}_\sigma$-split subtori for $\sigma \in S$, and let Γ be an arithmetic lattice in G with respect to the given $\mathbb{Q}$-structure. We will assume that $\mathbb{G}$ is split over $\mathbb{Q}_\sigma$ for all $\sigma \in S$. The S-rank of G is the sum of the $\mathbb{Q}_\sigma$-ranks of $\mathbb{G}(\mathbb{Q}_\sigma)$ (and equivalently of A_σ) for $\sigma \in S$ and equals, by our assumption, $|S|$ times the absolute rank of $\mathbb{G}$.

We shall now define several notions of divisibility for elements of Γ and show how various results and conjectures on the structure of A-orbits in $\Gamma\backslash G$ when the S-rank is at least 2 imply that for a given element $\delta \in \Gamma$ "most" elements of Γ are divisible by δ. The above notions of divisibility in quaternion algebras and Theorem 1.2 will be special cases of the following discussion.

To define the notion of divisibility we need to discuss when

$$\gamma = \alpha\beta \tag{1}$$

with $\alpha, \beta, \gamma \in \Gamma$ will be called a *factorization*. For this we would like to have a notion of complexity of elements of Γ and (1) is a factorization when the complexity of

γ is (roughly) the sum of the complexities of α and β. This complexity will be defined via a pseudo metric as follows. Let $K_\sigma < \mathbb{G}(\mathbb{Q}_\sigma)$ be a maximal compact subgroup for each $\sigma \in S$ and define $K = \prod K_\sigma < G$. Then we have a generalized Cartan decomposition $G = KAK$ of G, this relies on our assumption that $\mathbb{G}$ is split over $\mathbb{Q}_\sigma$, see [19]. For every root $\chi_\phi : A_\sigma \to \mathbb{Q}_\sigma^\times$ we define the *logarithmic root* $\phi : A_\sigma \to \mathbb{R}$ given by $\phi(a) = \log|\chi_\phi(a)|_\sigma$. For every $\sigma \in S$ let Ψ_σ be the set of logarithmic roots.

Definition 1.3. *Define for $g, h \in G$ their KAK-distance*

$$\mathrm{d}_1(g,h) = \mathrm{d}_1(h^{-1}g, e) = \sum_{\sigma\in S}\sum_{\phi\in\Psi_\sigma} |\phi(a_\sigma)|_+.$$

Here e denotes the identity element, and $a = (a_\sigma)_{\sigma\in S}$ denotes the diagonal element in the Cartan decomposition $h^{-1}g = k_1 a k_2$ and

$$|x|_+ = \begin{cases} x & x \geq 0, \\ 0 & x < 0. \end{cases}$$

We will show later in Section 2 that d_1 is a pseudo metric on G. It is clear that $\mathrm{d}_1(\cdot,\cdot)$ is left-invariant and symmetric so that $\mathrm{d}_1(h,e) = \mathrm{d}_1(h^{-1},e)$ and

$$\mathrm{d}_1(\alpha\beta, e) \leq \mathrm{d}_1(\alpha\beta,\alpha) + \mathrm{d}_1(\alpha,e) = \mathrm{d}_1(\alpha,e) + \mathrm{d}_1(\beta,e).$$

Note that $\mathrm{d}_1(k,e) = 0$ for $k \in K$ and d_1 induces a metric on G/K which we shall also denote by d_1.

Definition 1.4. *Fix $\kappa \geq 0$. Given $\alpha, \beta, \gamma \in \Gamma$ with (1) we say that this is a κ-factorization of γ if $\mathrm{d}_1(\gamma,e) \geq \mathrm{d}_1(\alpha,e) + \mathrm{d}_1(\beta,e) - \kappa$. Furthermore, we say that $\alpha \in \Gamma$ κ-divides $\gamma \in \Gamma$ if there exist $\beta_1, \beta_2 \in \Gamma$ such that*

$$\gamma = \beta_1\alpha\beta_2$$

and

$$\mathrm{d}_1(\gamma,e) \geq \mathrm{d}_1(\gamma,\beta_1\alpha) + \mathrm{d}_1(\beta_1\alpha,\beta_1) + \mathrm{d}_1(\beta_1,e) - \kappa = \mathrm{d}_1(\beta_2,e) + \mathrm{d}_1(\alpha,e) + \mathrm{d}_1(\beta_1,e) - \kappa \tag{2}$$

If $\kappa = 0$ we say simply that α divides γ.

Note that in the definition the last equality follows from the left invariance of $\mathrm{d}_1(\cdot,\cdot)$. Equivalently we might say that $\gamma = \beta_1\alpha\beta_2$ is a κ-decomposition if the discrete path from K to $\beta_1 K$ to $\beta_1\alpha K$ and finally to γK is almost geodesic in G/K with respect to d_1, i.e., the sum of the distances of these 3 steps is at most $\mathrm{d}_1(K,\gamma K) + \kappa$. If $\mathbb{G}(\mathbb{R})$ is compact we will take $\kappa = 0$, otherwise we shall always assume $\kappa > 0$.

Definition 1.5. *For an element $a \in A$ we define its* width*, respectively* diameter *to be*[1]

$$\mathrm{width}(a) = \min\{|\phi(a_\sigma)| : \sigma \in S,\, \phi \in \Psi_\sigma\},$$
$$\mathrm{diam}(a) = \sum_{\sigma\in S}\sum_{\phi\in\Psi_\sigma} |\phi(a_\sigma)|$$

[1]We note that the definition of width and diameter as defined here but in the context of Section 1.1 is bounded from above and below by multiplies of width and diameter as defined in Section 1.1.

For a general element $g \in G$ we shall define its width, respectively diameter to be

$$\operatorname{width}(g) = \operatorname{width}(a)$$

$$\operatorname{diam}(g) = \operatorname{diam}(a) = \mathrm{d}_1(g, e)$$

where $g = k_1 a k_2$ is the Cartan decomposition of g. We define the R-ball

$$B_R^\Gamma = \{\gamma \in \Gamma : \operatorname{diam}(\gamma) < R\}.$$

Considering the product of symmetric spaces and affine Bruhat-Tits buildings associated with G we may identify the chosen Cartan subgroup of G with the product of flats and apartments invariant under it and on which it acts by translations. The geometric meaning of the width is the minimal width of the convex hull of the origin and the point a, where a subset of A is convex if it coincides with the intersection of all the half spaces bounded by the singular hyperplanes which contain the subset.

With the above notion of divisibility our main result Theorem 1.10 implies the following results for division algebras that split over $\mathbb{R}$.

Theorem 1.6. *Let D be a division algebra of prime degree over a number field $\mathbb{K}$. Let S be a finite set of places of $\mathbb{Q}$ containing the infinite ones. We define the group $\mathbb{G}$ by applying restriction of scalars to the quotient of $\mathrm{D}^\times$ by its center, assume that $\mathbb{G}$ splits at all the places of S and that the S-rank of $\mathbb{G}$ is at least 2. Let $\Gamma = \mathbb{G}\Big(\mathbb{Z}\Big[\frac{1}{p} : p \in S \setminus \{\infty\}\Big]\Big)$. Fix some $\alpha \in \Gamma$ then for every $\kappa > 0$ and $\epsilon > 0$ there exists some width $w = w(\alpha, \kappa, \epsilon)$ so that*

$$\log\big|\{\gamma \in \Gamma : \gamma \text{ is not } \kappa\text{-divisible by } \alpha,\ \operatorname{diam}(\gamma) \le R,\ \operatorname{width}(\gamma) \ge w\}\big| < \epsilon R$$

for all sufficiently large R.

Let us explicate the meaning of the lattice in the above theorem in the case where $\mathbb{K} = \mathbb{Q}$. Choose some order $\mathcal{O}_D < D$ in the division algebra D. By choosing the representation of $\mathbb{G}$ correctly with respect to $\mathcal{O}_D$ we can achieve that $\mathbb{G}(\mathbb{Z}) = \mathcal{O}_D^\times/\{\pm 1\}$ and similarly

$$\Gamma = \mathbb{G}\big(\mathbb{Z}\big[\tfrac{1}{p} : p \in S \setminus \{\infty\}\big]\big) = \big(\mathcal{O}_D\big[\tfrac{1}{p} : p \in S \setminus \{\infty\}\big]\big)^\times / \mathbb{Z}\big[\tfrac{1}{p} : p \in S \setminus \{\infty\}\big]^\times. \tag{3}$$

1.3. **Rigidity properties of higher rank Cartan actions and divisibility.** Furstenberg [11] showed in 1967 that a closed $\times 2, \times 3$-invariant subset of $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ must either be finite (consisting of rational points) or the whole space $\mathbb{T}$. Furstenberg also asked about ergodic theoretic analogues of this topological theorem, which was considered by several authors. An important insight towards this question is due to Rudolph [18], who showed that a $\times 2, \times 3$-invariant and ergodic probability measure on $\mathbb{T}$ that has positive entropy for either of the two transformations must be Lebesgue measure. Since then many analogues and generalizations have been considered, we refer to [7] for a more detailed survey of the results and to [4] for a survey of applications of these results. We would like to highlight two particular instances of generalizations to homogeneous spaces of the above phenomenon. Unfortunately, in both of these our understanding is even less complete than for the original setting given by Furstenberg; we have neither a topological theorem nor a complete classification of the invariant measures. The following theorem is contained in the work [13] of E. Lindenstrauss on the Quantum Unique Ergodicity Conjecture by Rudnick and Sarnak.

Theorem 1.7. *Let $G_i = \mathrm{SL}_2(\mathbb{K}_i)$ where $\mathbb{K}_i$ is either $\mathbb{R}$ or $\mathbb{Q}_p$ for $i = 1, 2$. Let $\Gamma < G = G_1 \times G_2$ be an irreducible lattice and set $X = G/\Gamma$. Furthermore, let $A_i < G_i$ be the maximal $\mathbb{K}_i$-split torus and let $A = A_1 \times A_2$. Suppose μ is an A-invariant and ergodic probability measure on X for which some $a \in A$ has positive entropy $h_\mu(a) > 0$. Then μ is the Haar measure on X.*

The same methods together with the methods of the work of J. Bourgain and E. Lindenstrauss [3] gives also an adelic unique ergodicity theorem, see [13, 14].

Theorem 1.8. *Let $X = \mathrm{PGL}_2(\mathbb{Q})\backslash \mathrm{PGL}_2(\mathbb{A}_\mathbb{Q})$ and let A be the full adelic diagonal subgroup of $\mathrm{PGL}_2(\mathbb{A}_\mathbb{Q})$. Then the A-action has only one invariant probability measure, namely the normalized Haar measure on X.*

For the proof of Theorem 1.1 we will need a generalization of the above to quotients defined by quaternion algebras, see Section 5.3.

The third generalization of the above phenomenon that we want to state is contained in the work [6] of the first named author with A. Katok and E. Lindenstrauss on the Littlewood conjecture in Diophantine approximation.

Theorem 1.9. *Let $G = \mathrm{SL}_p(\mathbb{R})$ for a prime[2] $p \geq 3$ and let $\Gamma < G$ be a lattice so that no diagonalizable element of Γ other than the identity has repeated eigenvalues. Let $X = \Gamma\backslash G$. Furthermore, let A be the diagonal subgroup in $\mathrm{SL}_p(\mathbb{R})$. Suppose μ is an A-invariant and ergodic probability measure on X for which some $a \in A$ has positive entropy $h_\mu(a) > 0$. Then μ is the Haar measure on X.*

Similar to Theorem 1.7 the above theorem also generalizes to products of real and p-adic groups, we refer to the discussion in Section 5.1 and [9].

We will prove that the above described rigidity properties imply the following theorem for the notion of divisibility defined in Definition 1.4.

Theorem 1.10. *Let $\mathbb{G}$ be an algebraic group defined over $\mathbb{Q}$ and let S be a finite set of places of $\mathbb{Q}$ containing ∞ if $\mathbb{G}(\mathbb{R})$ is non-compact. Assume that $\mathbb{G}$ is split over $\mathbb{Q}_\sigma$ for all $\sigma \in S$. Let $G = \prod_{\sigma\in S} \mathbb{G}(\mathbb{Q}_\sigma)$, let $A = \prod_{\sigma\in S} A_p$ be the product of the $\mathbb{Q}_\sigma$-points of maximal $\mathbb{Q}_\sigma$-diagonalizable subgroups for all $\sigma \in S$, and let Γ be an S-arithmetic lattice in G with respect to the $\mathbb{Q}$-structure $\mathbb{G}$. Suppose $X = \Gamma\backslash G$ is compact and that the Haar measure of X is the only A-invariant and ergodic probability measure on X with positive entropy for some element of A. Let $\kappa > 0$ if $\infty \in S$ respectively $\kappa = 0$ if $\infty \notin S$. Then for every $\alpha \in \Gamma$ and $\epsilon > 0$ there exists some $w = w(\alpha, \kappa, \epsilon) > 0$ such that*

$$\log\big|\{\gamma \in \Gamma : \gamma \text{ is not } \kappa\text{-divisible by } \alpha,\ \mathrm{diam}(\gamma) \leq R,\ \mathrm{width}(\gamma) \geq w\}\big| < \epsilon R \tag{4}$$

for all sufficiently large $R > 0$.

As is conjectured by Furstenberg and Margulis [15] for the dynamical systems considered above the closed A-invariant subsets should also be easy to describe: Just like for $\times 2, \times 3$ a closed invariant subset of X should be either a finite union of periodic orbits or should be all of X. If this were known, the relationship between dynamical properties and divisibility properties would give a better result.

[2] A similar theorem also holds for $G = \mathrm{SL}_n(\mathbb{R})$ for an integer $n \geq 3$, but in this more general case other algebraic orbits of intermediate groups have to be allowed. We restrict ourselves to the prime case, as in the general case our application to divisibility properties gives weaker results.

Theorem 1.11. *Let $\mathbb{G}$ be an algebraic group defined over $\mathbb{Q}$ and let S be a finite set of places of $\mathbb{Q}$ containing ∞ if $\mathbb{G}(\mathbb{R})$ is non-compact. Assume that $\mathbb{G}$ is split over $\mathbb{Q}_\sigma$ for all $\sigma \in S$. Let $G = \prod_{\sigma\in S} \mathbb{G}(\mathbb{Q}_\sigma)$, let $A = \prod_{\sigma\in S} A_p$ be the product of the $\mathbb{Q}_\sigma$-points of maximal $\mathbb{Q}_\sigma$-diagonalizable subgroups for all $\sigma \in S$, and let Γ be an S-arithmetic lattice in G with respect to the $\mathbb{Q}$-structure $\mathbb{G}$. Suppose $X = \Gamma\backslash G$ is compact and that X and finite unions of compact periodic A-orbits are the only A-invariant and closed subset of X. Let $\kappa > 0$ if $\infty \in S$ respectively $\kappa = 0$ if $\infty \notin S$. Then for every $\alpha \in \Gamma$ there exists some $c > 0$ and $w > 0$ such that*

$$\big|\{\gamma \in \Gamma : \gamma \text{ is not } \kappa\text{-divisible by } \alpha,\ \operatorname{diam}(\gamma) \le R, \operatorname{width}(\gamma) \ge w\}\big| < cR^q \tag{5}$$

where q is the S-rank of G.

In the proofs of the above theorems we will consider pieces of A-orbits in $X = \Gamma\backslash G$ associated to lattice elements in Γ that are not divisible by α. The assumption that the lattice elements are not divisible will translate to the statement that these pieces do not visit a particular open subset O_α of X associated to α. In either case we will derive a contradiction if there are indeed more lattice elements than allowed in Theorem 1.10–1.11. We will show that exponential growth of the set in (4) would give rise to an invariant probability measure on X with positive entropy, similarly we will derive (5) from the assumption that the closed A-invariant set that consists of all A-orbits disjoint from O_α must be a finite union of compact A-orbits.

1.4. **Remark.** Let us remark on the relation between the current paper and [10] which concerns the distribution of cocompact A-orbits on $\Gamma\backslash G$. The general philosophy of the latter is similar to that of the present paper: Using the main result of [6] it is shown that most A-orbits, respectively, elements of Γ satisfy certain conjectures. However, here we consider, for the notion of divisibility, only pieces of compact A-orbits (and we have no information on how large these pieces are when compared with the full A-orbit). As a result the two papers use different orderings of compact A-orbits. Here we use the geometric notion of diameter for elements of Γ whereas in [10] an arithmetic notion of discriminant is introduced to order compact A-orbits.

1.5. **Acknowledgement.** The authors thank Elon Lindenstrauss for discussions concerning this project. We are also grateful to the Israel Institute for Advanced Studies at the Hebrew University and the MSRI for the support during the special semesters in Fall 2014 respectively Spring 2015.

2. Preliminaries

Let $\mathbb{G}$ be an algebraic semisimple group defined over $\mathbb{Q}$, let S be a finite set of places of $\mathbb{Q}$ (containing ∞ when $\mathbb{G}(\mathbb{R})$ is not compact), assume that $\mathbb{G}$ is split over $\mathbb{Q}_\sigma$ for every $\sigma \in S$, and let $G = \prod_{\sigma\in S} \mathbb{G}(\mathbb{Q}_\sigma)$ be the $\mathbb{Q}_S$ -points of $\mathbb{G}$, where $\mathbb{Q}_S = \prod_{\sigma\in S} \mathbb{Q}_\sigma$. To show that the function d_1 defined above is indeed a quasi metric on G let us consider each factor $G_\sigma = \mathbb{G}(\mathbb{Q}_\sigma)$, $\sigma \in S$ separately.

2.1. **Cartan decomposition.** Recall that G_σ admits a Cartan decomposition $G_\sigma = K_\sigma A_\sigma^+ K_\sigma$ (see [19] and [16, Thm. 2.2.1(2)]), where K_σ is a maximal compact subgroup of G_σ and A_σ^+ is a positive Weyl chamber inside the group of $\mathbb{Q}_\sigma$-points of a maximal $\mathbb{Q}_\sigma$-split torus of G_σ. We distinguish between the cases where σ is archimedean or not.

2.2. **The quasi-metric for a Lie group.** Suppose σ is archimedean. In this case we can take K_σ to be a maximal compact subgroup of G_σ such that the adjoint action of K_σ is orthogonal and the adjoint action of A_σ is self-adjoint with respect to the innner product on the Lie algebra $\mathcal{L}_\sigma$ of G_σ derived by the Cartan killing form and the Cartan involution, see [12, Sect. VI.2]. We note that if we take a wedge power $\wedge^n\mathcal{L}_\sigma$ of the Lie algebra of G_σ, then the inner product on $\mathcal{L}_\sigma$ induces an inner product on $\wedge^n\mathcal{L}_\sigma$ such that the induced actions of K_σ and A_σ are again orthogonal respectively self-adjoint. Let us write $\rho : G_\sigma \to \mathrm{GL}(\wedge^n\mathcal{L}_\sigma)$ for the induced action. Therefore, with respect to this inner product the action of any element of K_σ has operator norm one and the common eigenspaces of the action of A_σ (the weight spaces) are orthogonal with respect to each other. Observe that the orthogonal decomposition of the Lie algebra into root spaces $\mathcal{L}_\sigma = \mathcal{L}_{\sigma,0} \oplus \bigoplus_{\phi\in\Psi_\sigma} \mathcal{L}_{\sigma,\phi}$ is preserved by the adjoint action of A_σ. The restriction of a_σ to $\mathcal{L}_{s,\sigma}$ is multiplication by $\chi_\phi(a_\sigma)$. Moreover for $a_\sigma \in A_\sigma^+$ for each positive root $\phi \in \Psi_\sigma^+$, $|\chi_\phi(a_\sigma)| \geq 1$ while for all other roots the absolute value is at most 1. It follows that the operator norm of the action of a_σ on the wedge product $\wedge^n\mathcal{L}_\sigma$ is $\|\rho(a_\sigma)\| = \prod_{\phi\in\Psi_\sigma^+} |\chi_\phi(a_\sigma)|$ where n is the number of positive roots. Hence for $g_\sigma \in G_\sigma$ with $g_\sigma = k_1 a k_2$, $k_1, k_2 \in K_\sigma$, $a \in A_\sigma^+$ we have $\|\rho(g_\sigma)\| = \|\rho(a)\| = \exp(\mathrm{d}_1(g_\sigma, e))$. For any $g_\sigma, h_\sigma \in G_\sigma$ we have $g_\sigma = k_1 a k_2$, $h_\sigma = k_3 b k_4$ where $a, b \in A_\sigma^+$, $k_1, k_2, k_3, k_4 \in K_\sigma$.

$$\exp(\mathrm{d}_1(g_\sigma h_\sigma, e)) = \|\rho(g_\sigma h_\sigma)\| \leq \|\rho(g_\sigma)\|\|\rho(h_\sigma)\| = \\ \|\rho(a)\|\|\rho(b)\| = \exp(\mathrm{d}_1(g_\sigma, e)) \exp(\mathrm{d}_1(h_\sigma, e))$$

It follows from this that $\mathrm{d}_1(g_\sigma h_\sigma, e) \leq \mathrm{d}_1(g_\sigma, e) + \mathrm{d}_1(h_\sigma, e) \leq d_1(g_\sigma h_\sigma, g_\sigma) + \mathrm{d}_1(g_\sigma, e)$. I.e., the triangle inequality holds.

2.3. **The quasi-metric for a p-adic Lie group.** Let σ be now a non-archimedean place. Associated with G_σ there is an affine Bruhat-Tits building Δ_σ. One has a Cartan decomposition $G_\sigma = K_\sigma A_\sigma^+ K_\sigma$ so that there is an apartment $\Sigma_0 \subset \Delta_\sigma$ on which A_σ acts by translations and a vertex $O \in \Sigma_0$ fixed by K_σ. We may define a metric on the vertices of Δ_σ as follows: Given any two vertices $P, Q \in \Delta_\sigma$ fix an apartment Σ containing both. The apartment may be viewed as a Euclidean space. Each root $\phi \in \Psi_\sigma$ may be viewed as a linear functional on Σ and the collection of hyperplanes $L_{\phi,k} = \{x \in \Sigma : \phi(x) = k\}$, $\phi \in \Psi_\sigma$, $k \in \mathbb{Z}$ partitions Σ into its chambers. Consider the number of hyperplanes L_{ϕ_k} separating Q from P. This defines a metric $\tilde{d}(P, Q)$ on the vertices of Δ_σ. Notice that this is exactly the minimal length of a gallery of chambers from the vertex P to the vertex Q. Observe also that this metric is invariant under the action of G_σ on Δ_σ. To conclude that d_1 is indeed a quasi metric on G_σ observe that $\mathrm{d}_1(g, e) = \tilde{d}(gO, O)$.

2.4. **Diagonal subgroup.** We note that we do not wish to switch from the whole group A_σ of $\mathbb{Q}_\sigma$-points of the maximal torus to a finite index subgroup (as e.g. the connected component for $\sigma = \infty$). Instead we consider the full diagaonlizable subgroup, and define the positive Weyl chamber A_σ^+ by requiring $|\chi_\phi(a)| \geq 1$ for all positive roots $\phi \in \Psi_\sigma$ and all $a \in A_\sigma^+$. This does not affect the algebraic statements we made above but gives us slightly larger orbits for the action considered below.

We write $A_f = \prod_{\sigma\in S\setminus\{\infty\}} A_\sigma$ for the product of the diagonal subgroups at all finite places and $K_f = \prod_{\sigma\in S\setminus\infty} K_\sigma$ for the compact subgroup in the product $G_f = \prod_{\sigma\in S\setminus\{\infty\}} G_p$ of all non-Archimedean factors. Note that $A_\infty = A_\infty^\circ(A_\infty \cap K_\infty)$ and that $A_f/(A_f \cap K_f)$ is isomorphic to $\mathbb{Z}^{|S\setminus\{\infty\}|\,\mathrm{rank}\,\mathbb{G}}$.

Recall that Ψ_σ denotes the set of logarithmic roots $\phi(a) = \log|\chi_\phi(a)|$ on A_σ. We also set $\Psi_S = \bigsqcup_{\sigma\in S}\Psi_\sigma$, where we consider each $\phi \in \Psi_\sigma \subset \Psi_S$ extended trivially from the A_σ (on which it was originally defined) to all of A.

2.5. **The left-invariant metric on G and the metric on X.** For $\sigma = \infty$ we will use a left-invariant metric $d(\cdot,\cdot)$ that is locally bi-Lipshitz to a Riemannian metric on the connected component G°_∞ of G. We note that $d_1(g,e) \le cd(g,e)$ for some absolute constant and for all g close to the identity.

For $\sigma = p$ we will use any left-invariant metric on G_p with the property that K_p is the unit ball of the identity element. Hence $d_1(g,e) = 0$ for all g with $d(g,e) \le 1$.

On $G = \prod_{\sigma\in S} G_\sigma$ we then use the product metric, which is again left-invariant and denoted by $d(\cdot,\cdot)$. If now $\Gamma < G$ is arithmetic lattice in G with respect to the given $\mathbb{Q}$-structure, then the above metric also induces a metric on $X = \Gamma\backslash G$.

3. Divisibility and dynamics of A

In this section we provide the relationship between κ-divisibility and the behavior of pieces of A-orbits attached to elements of Γ. We will use this together with (measure) rigidity to show that there are few elements γ that are not κ-divisible by a fixed $\alpha \in \Gamma$.

We start by assigning to a given $\gamma \in \Gamma$ a piece of an A-orbit.

3.1. **Divisibility and open subsets of $\Gamma\backslash G$.** Let $\gamma \in \Gamma$ be arbitrary and let $\gamma = k_\gamma a_\gamma k'_\gamma$ be its Cartan decomposition (see [19]) in $G = \mathbb{G}(\mathbb{Q}_S)$. We may assume that $a = a_\gamma \in A$ belongs to the positive Weyl chamber, which shall be denoted by A^+. (I.e. $a = (a_\sigma)_{\sigma\in S}$ and each $a_\sigma \in A_\sigma$ belongs to the positive Weyl chamber of A_σ with respect to some fixed choice of positive roots.)

Using A^+ we define a partial order on A by letting $a_1 \le a_2$ if $a_2 a_1^{-1} \in A^+$, so that $A^+ = \{a \in A : a \ge e\}$. We shall call the set $\mathbb{S}_\gamma = \{a \in A : e \le a \le a_\gamma\}$ the *shape* of γ. Note that the width and diameter of γ as in Definition 1.5 are determined by its shape $\mathbb{S}_\gamma$. We shall attach to γ the subset $\Gamma k_\gamma \mathbb{S}_\gamma$ of the A-orbit $\Gamma k_\gamma A$.

We describe now how divisibility of γ by α can be interpreted in terms of the piece of the A-orbit attached to γ and an open subset O_α.

Lemma 3.1. *Let $\kappa \ge 0$ with $\kappa > 0$ if $\mathbb{G}(\mathbb{R})$ is non-compact, and let $\alpha = k_\alpha a_\alpha k'_\alpha$ be the Cartan decomposition of α. Then there is an open neighbourhood O_α of Γk_α with the following property. For any $\gamma \in \Gamma$ let $k_\gamma a_\gamma k'_\gamma$ be the Cartan decomposition of γ and define*

$$\mathbb{S}_\gamma^{-\alpha} = \{a \in A : e \le a \le a_\gamma a_\alpha^{-1}\}$$

If $\Gamma k_\gamma \mathbb{S}_\gamma^{-\alpha}$ intersects O_α then α κ-divides γ.

Proof. Note that $k_\alpha = \alpha(k'_\alpha)^{-1}a_\alpha^{-1}$. Let $\epsilon > 0$ (chosen as a function of κ below). Define $\tilde{O}_\alpha = U_1 \cap (\alpha U_2 a_\alpha^{-1})$ to be the intersection of a ϵ-neighbourhood U_1 of k_α intersected with the image $\alpha U_2 a_\alpha^{-1}$ of an ϵ-neighbourhood U_2 of $(k'_\alpha)^{-1}$. If there are no real factors of G, we let $\epsilon = 1$ and $U_1 = U_2 = K$.

In any case, $\tilde{O}_\alpha$ is again a neighborhood of k_α. Then let $O_\alpha = \Gamma\tilde{O}_\alpha$ be the projection in $\Gamma\backslash G$. Suppose that for some $\gamma = k_\gamma a_\gamma k'_\gamma \in \Gamma$ we have

$$\Gamma k_\gamma a_1 \in \Gamma k_\gamma \mathbb{S}_\gamma^{-\alpha} \cap O_\alpha \text{ for some } a_1 \in \mathbb{S}_\gamma^{-\alpha}.$$

Then there exist $u_1 \in \tilde{O}_\alpha \subset U_1$ and $\beta_1 \in \Gamma$ so that:

$$k_\gamma a_1 = \beta_1 u_1.$$

Furthermore, there exists $u_2 \in U_2$ with

$$u_1 a_\alpha = \alpha u_2.$$

We define $\beta_2 = (\beta_1\alpha)^{-1}\gamma$ and $a_2 = (a_1 a_\alpha)^{-1} a_\gamma$. Then

$$u_2 a_2 = \alpha^{-1} u_1 a_1^{-1} a_\gamma = \alpha^{-1}\beta_1^{-1} k_\gamma a_\gamma = \alpha^{-1}\beta_1^{-1}\gamma (k'_\gamma)^{-1} = \beta_2 (k'_\gamma)^{-1}.$$

Observe that by the definition of $\mathbb{S}_\gamma^{-\alpha}$ we have that $a_2 \in A^+$. Therefore the decomposition

$$\gamma = k_\gamma a_\gamma k'_\gamma = (k_\gamma a_1 u_1^{-1})(u_1 a_\alpha u_2^{-1})(u_2 a_2 k'_\gamma) = \beta_1\alpha\beta_2$$

satisfies

$$\begin{aligned} d_1(\gamma, e) &= d_1(a_\gamma, e) \\ d_1(\beta_1, e) &= d_1(a_1 u_1^{-1}, e) = d_1(u_1^{-1}, a_1^{-1}) \le d_1(a_1, e) + c\epsilon \end{aligned}$$

for some absolute constant $c > 0$, resp. if there are no real factors for $c = 0$. Here we used the definition of $d_1(\cdot,\cdot)$, the left invariance of $d_1(\cdot,\cdot)$, the triangle inequality, and that u_1 is ϵ-close to an element of K. Similarly,

$$\begin{aligned} d_1(\alpha, e) &= d_1(a_\alpha u_2^{-1}, u_1^{-1}) \le d_1(u_2^{-1}, a_\alpha^{-1}) + c\epsilon \le d_1(a_\alpha, e) + 2c\epsilon \\ d_1(\beta_2, e) &= d_1(u_2 a_2, e) \le d_1(a_2, e) + c\epsilon \end{aligned}$$

Since $a_\gamma = a_1 a_\alpha a_2$ only involves elements of the positive Weyl chamber we have

$$d_1(a_\gamma, e) = d_1(a_1, e) + d_1(a_\alpha, e) + d_1(a_2, e)$$

and hence we conclude that γ is $\kappa = 4c\epsilon$-divisible by α. Thus we set $\epsilon = 1$ if there are no real factors and $\epsilon = \frac{\kappa}{4c}$ otherwise. □

3.2. **Counting non divisible elements of Γ and (ϵ, N)-separated points.** Every element $\gamma \in \Gamma$ defines a shape $S_\gamma \subset A$ as described in Section 3.1. When we count the elements $\gamma \in \Gamma$ which are not divisible by α we let the diameter of γ tend to infinity but make no restrictions on the shape other than that the width should be sufficiently big. However in a sense there are only polynomially many different shapes for a given diameter. This is clear if all real factors of G are compact since then $A_f/(A_f \cap K) \cong \mathbb{Z}^k$ for some $k \in \mathbb{N}$. If some real factor of G is non-compact, then we can take some regular element $a_{\text{grid}} \in A^+$ to "discretize" A^+ or rather the possible shapes within A^+ as in the following lemma.

Lemma 3.2. *Suppose for a given $\kappa \ge 0$, $\alpha \in \Gamma$, $w > 0$ and $\delta > 0$ we have*

$$|\{\gamma \in \Gamma : \alpha \text{ does not } \kappa\text{-divide } \gamma,\ \operatorname{diam}(\gamma) \le R_n,\ \operatorname{width}(\gamma) \ge w\}| \ge e^{\delta R_n}$$

for an unbounded sequence of values R_n. Then for any regular element $a_{\text{grid}} \in A_\infty^+$ there is some sequence of shapes S_{a_n} (where $a_n \in A^+$) with $\operatorname{diam} S_{a_n} < R_n$, $\lim_{n\to\infty} \operatorname{diam} S_{a_n} = \infty$ and $\operatorname{width}(S_{a_n}) \ge w$, for which

$$|\{\gamma \in \Gamma : \alpha \text{ does not } \kappa\text{-divide } \gamma,\ S_{a_n} \subseteq S_\gamma \subseteq S_{a_n a_{\text{grid}}}\}| \ge e^{\delta R_n/2} \tag{6}$$

for large enough n.

Note that the element a_{grid} is used to define a "grid" in A_∞ thus discretizing things. To make this precise fix a basis of A_∞^+ as follows. Let Ψ_∞^+ be the collection of simple positive roots of A_∞ which form a basis of the group of characters of A_∞. For any $\phi \in \Psi_\infty^+$ defined on a real simple factor G_σ take an element $a_\phi \in A_\infty^\circ \cap G_\sigma$ which satisfies $\phi(a_\phi) > 0$ but $\psi(a_\phi) = 0$ for $\psi \in \Psi_\infty^+ \setminus \{\phi\}$. Then for any $a \in A$ we have

$$a = a_\infty a_f \in a_f \prod_{\phi\in\Psi_\infty^+} a_\phi^{\frac{\phi(a)}{\phi(a_\phi)}} (A \cap K)$$

where a_∞ and a_f are the archimedean and nonarchimedean parts of a. Assuming the choice of a_ϕ has been made such that

$$a_{\mathrm{grid}} = \prod_{\phi\in\Psi_\infty^+} a_\phi$$

we can simplify the notation and the mentioned grid now consists of sets of the form:

$$D_{([a_f],(\ell_\phi)_\phi)} = a_f \Big\{ \prod_{\phi\in\Psi_S^+} a_\phi^{\ell_\phi + r_\phi} : r_\phi \in [0,1) \Big\} (A \cap K)$$

for various choices of $[a_f] \in A_f/(A_f \cap K)$ and $\ell_\phi \in \mathbb{Z}$ for all $\phi \in \Psi_\infty^+$.

Proof. of Lemma 3.2. For a given diameter R_n there are polynomially many (with respect to R_n) choices of $[a_f]$ with diameter less then R_n, and also polynomially many choices of $(\ell_\phi)_{\phi\in\Psi_\infty^+} \in \mathbb{N}_0^{|\Psi_\infty^+|}$ such that some element of the attached grid element $D_{([a_f],(\ell_\phi)_\phi)}$ has diameter less than R_n. This implies that for some choice of grid elements $D_n = D_{([a_f^{(n)}],(\ell_\phi^{(n)})_\phi)}$ we have exponential growth (with respect to R_n) of those $\gamma \in \Gamma$ considered with $a_\gamma \in D_n$. Let $a_n = a_f^{(n)} \prod_{\phi\in\Psi_\infty^+} a_\phi^{\ell_\phi^{(n)}}$. Then $a_\gamma \in D_n$ implies $S_{a_n} \subseteq S_\gamma \subseteq S_{a_n a_{\mathrm{grid}}}$, and the lemma follows. □

Recall the definition of topological entropy for a homeomorphism $T : X \to X$ of a compact metric space. A finite set $F \subset X$ is called (ϵ, N)–separated if for any two $f_1, f_2 \in F$ there exists $0 \le m < N$ such that

$$d(T^m f_1, T^m f_2) \ge \epsilon.$$

Let $S_{\epsilon,N}$ be the maximal cardinality of an (ϵ, N)–separated set in X. The topological entropy is defined by

$$\mathrm{h_{top}}(T) = \lim_{\epsilon\to 0} \limsup_{N\to\infty} \frac{\log S_{\epsilon,N}}{N}$$

It is clear the the second limit exists since $S_{\epsilon,N}$ is increasing for decreasing values of ϵ. For the same reason we do not have to consider the limit as $\epsilon \to 0$ if we only want to show that topological entropy is positive. In fact, we will choose some small enough $\epsilon > 0$ and only consider the limit superior as $N \to \infty$. Therefore, after that choice has been made we may consider ϵ as a constant and will not worry if other quantities depend on it.

We will show next how exponential growth rate of non-divisible $\gamma \in \Gamma$ as in Lemma 3.2 implies positive topological entropy for some $a \in A$ and a proper closed A invariant subset. (In the next section we will make use of the (ϵ, N)–separated set constructed and not just of the positive entropy which will be automatic.)

The element $a \in A$ for which we will get positive entropy will be one of the singular basis elements $a_\phi \in A$. For the archimedean places we already defined a_ϕ. For a non-archimedean place $\sigma \in S$ we again let Ψ_σ^+ be a set of simple positive roots, and define similarly $a_\phi \in A_\sigma$ to be an element with $\phi(a_\phi) > 0$ and $\psi(a_\phi) = 0$ for $\psi \in \Psi_\sigma^+ \setminus \{\phi\}$. We also define $\Psi_S^+ = \bigsqcup_{\sigma \in S} \Psi_\sigma^+$. Note, however, that in general the group $A_\infty \langle a_\phi : \phi \in \Psi_S^+ \rangle (A \cap K)$ will have finite index in A. So let $b_1, \dots, b_p$ be a set of coset representatives of $A / A_\infty \langle a_\phi : \phi \in \Psi_S^+ \rangle (A \cap K)$. We have now a "basis" $\{a_\phi : \phi \in \Psi_S^+\}$ of A, i.e., every $a \in A$ can be uniquely written as:

$$a = m b_i \prod_{\phi \in \Psi_S^+} a_\phi^{\ell_\phi}$$

where $m \in A \cap K$, $i \in \{1, \dots, p\}$, $\ell_\phi \in \mathbb{R}$ for archimedean places and $\ell_\phi \in \mathbb{Z}$ for non-archimedean ones. If $a \in A^+$ and the width of a is sufficiently big (depending on the choice of b_j), then $\ell_\phi \geq 0$ for all $\phi \in \Psi_S^+$. Moreover, there are some constants $c_1, c_2 > 0$ such that $\min_{\phi \in \Psi_S^+} \ell_\phi \geq c_1 \mathrm{width}(a) - c_2$.

Let us now take a finite index torsion free subgroup $\Gamma' \subset \Gamma$. Since we assume exponential growth and we only have finitely many Γ'-cosets within Γ, we may restrict to one coset without losing the exponential growth assumption. Therefore, we may assume that for any two elements $\gamma, \beta \in \Gamma$ from our list we have $\beta^{-1}\gamma \in \Gamma'$. Clearly $\Gamma' \cap K = \{e\}$ which implies that γK and βK are disjoint and have distance $\geq \rho$ (with a uniform $\rho > 0$) if $\gamma \neq \beta$ are as above.

Consider now different elements $\gamma = k_\gamma a_\gamma k_\gamma'$, $\beta = k_\beta a_\beta k_\beta' \in \Gamma$ with $\beta^{-1}\gamma \in \Gamma'$ of similar shape in the sense that $S_a \subseteq S_\gamma \subseteq S_{a a_{\mathrm{grid}}}$ and $S_a \subseteq S_\beta \subseteq S_{a a_{\mathrm{grid}}}$ for some $a \in A^+$. We show that the points k_γ and k_β are separated under the right action of a in G if a_{grid} is sufficiently small. In fact since both $a_\gamma^{-1} a$ and $a_\beta^{-1} a$ are small, say of distance $< \rho/3$ to e,

$$k_\gamma a = \gamma (k_\gamma')^{-1} a_\gamma^{-1} a$$

and

$$k_\beta a = \beta (k_\beta')^{-1} a_\beta^{-1} a$$

belong to different Γ-translates of a neighborhood of K and so have distance $\geq \rho/3$.

We would like to have an element $a \in A^+$ so that the set

$$\{\Gamma k_\gamma : \alpha \text{ does not } \kappa\text{-divide } \gamma,\ S_a \subseteq S_\gamma \subseteq S_{a a_{\mathrm{grid}}}\}$$

contains a subset of exponential size which is (ϵ, N)-separated for the action of the fixed element a. Since we do not know the shape S_a in advance we need to allow different choices for this element a.

Lemma 3.3. *Let $\kappa \geq 0$, $\alpha \in \Gamma$, $w > 0$ and $\delta > 0$ be given. Suppose there is a sequence $a_n \in A^+$ with*

$$a_\alpha^{-1} a_n = m_n b_{i_n} \prod_{\phi \in \Psi_S^+} a_\phi^{\ell_\phi(n)}$$

for which the sequence of diameters R_n of S_{a_n} is unbounded and the widths are at least w such that the set

$$E_n = \{k_\gamma : \gamma \in \Gamma,\ \alpha \text{ does not } \kappa\text{-divide } \gamma,\ S_{a_n} \subseteq S_\gamma \subseteq S_{a_n a_{\mathrm{grid}}}\}$$

has cardinality at least $e^{\delta R_n}$. Order the positive simple roots $\Psi_S^+ = \{\phi_1, \phi_2, \dots, \phi_r\}$ and choose a sufficiently small $\epsilon > 0$. Then there exists some $j = j_n \in \{1, 2, \dots, r\}$

and a subset $F_n \subset \Gamma\backslash G$ of cardinality at least $e^{\frac{\delta}{r}R_n}$ which is (ϵ, N)-separated for the action of $a = a_{\phi_j}$ and some N which is bounded from above and below by multiples of R_n. There is a rectangle T_w (depending on j and w, invariant under $A \cap K$) transverse to the direction of the acting element a which has width w in all but this direction such that $F_n T_w a^m \cap O_\alpha = \emptyset$ for $0 \le m < N$.

Proof. We claim that either the set ΓE_n contains an $(\epsilon, \ell_{\phi_1}(n))$–separated subset F_n of cardinality $\ge e^{\frac{\delta}{r}R_n}$ for the action of $a = a_{\phi_1}$, or $\Gamma E_n a_{\phi_1}^{\ell_{\phi_1}(n)}$ contains an $(\epsilon, \ell_{\phi_2}(n))$–separated subset of cardinality $\ge e^{\frac{\delta}{r}R_n}$ for the action of $a = a_{\phi_2}$, or $\cdots$, or $\Gamma E_n \prod_{i=1}^{r-1} a_{\phi_i}^{\ell_{\phi_i}(n)}$ contains an $(\epsilon, \ell_{\phi_r}(n))$–separated subset F_n of cardinality $\ge e^{\frac{\delta}{r}R_n}$ for the action of $a = a_{\phi_r}$.

If ΓE_n already contains an $(\epsilon, \ell_{\phi_1}(n))$-separated subset F_n for $a = a_{\phi_1}$ of cardinality $\ge e^{\frac{\delta}{r}R_n}$ then the first claim follows. Otherwise we can choose a subset $K_n \subset E_n$ of cardinality $< e^{\frac{\delta}{r}R_n}$ such that for every $f \in E_n$ there is some $g \in K_n$ with $d(\Gamma f a^m, \Gamma g a^m) < \epsilon$ for $0 \le m < \ell_{\phi_1}(n)$. For each $g \in K_n$ let $E_n(g)$ be the set of $f \in E_n$ for which this holds. Clearly one of these sets has cardinality $|E_n(g)| \ge e^{\frac{r-1}{r}\delta R_n}$. We define $E_n^{(1)} = E_n(g) a^{\ell_{\phi_1}(n)}$ and now ask whether $\Gamma E_n^{(1)}$ contains an $(\epsilon, \ell_{\phi_2}(n))$-separated subset F_n of cardinality $\ge e^{\frac{\delta}{r}R_n}$ for the action of $a = a_{\phi_2}$. Repeating this argument we end up either with a proof of the claim or a set $E_n^{(r-1)} \subset E_n \prod_{i=1}^{r-1} a_{\phi_i}^{\ell_{\phi_i}(n)}$ of cardinality $\ge e^{\frac{\delta}{r}R_n}$ which consists entirely of points that have stayed ϵ-close when each of the elements a_{ϕ_1}, $a_{\phi_1}^2$, $\ldots$, $a_{\phi_1}^{\ell_{\phi_1}(n)}$, $a_{\phi_1}^{\ell_{\phi_1}(n)} a_{\phi_2}$, $\ldots$, $\prod_{i=1}^{r-1} a_{\phi_i}^{\ell_{\phi_i}(n)}$ was applied. Either $\Gamma E_n^{(r-1)}$ is $(\epsilon, \ell_{\phi_r}(n))$-separated for the action of a_{ϕ_r} or there are two different points

$$f_1^{(r-1)} = k_\gamma \prod_{i=1}^{r-1} a_{\phi_i}^{\ell_{\phi_i}(n)}, f_2^{(r-1)} = k_\beta \prod_{i=1}^{r-1} a_{\phi_i}^{\ell_{\phi_i}(n)} \in E_n^{(r-1)}$$

such that for any $0 \le j \le \ell_{\phi_r}(n) - 1$ the points $\Gamma f_1^{(r-1)} a_{\phi_r}^j$ and $\Gamma f_2^{(r-1)} a_{\phi_r}^j$ are ϵ-close. For sufficiently small $\epsilon > 0$ (namely small enough in comparison to the injectivity radius of $\Gamma\backslash G$ and each of the maximum expansion of the actions of a_{ϕ_j}) this implies that $k_\gamma \prod_{\phi \in \Psi_S^+} a_\phi^{\ell_\phi(n)}$, $k_\beta \prod_{\phi \in \Psi_S^+} a_\phi^{\ell_\phi(n)}$ are ϵ-close. Hence also $k_\gamma a_n$ and $k_\beta a_n$ are $c\epsilon$-close. Where c is a bound on the Lipschitz constant of multiplying by a_α and $b_{i_n} \in \{b_1, \ldots, b_p\}$. Moreover since both a_γ and a_β are close to a_n (where the distance is controlled by a_{grid}) it follows that $k_\gamma a_\gamma$ and $k_\beta a_\beta$ are close. Hence if we make sure that a_{grid} and ϵ are small enough it will follow that $\beta^{-1}\gamma \in K$. Since we have passed to a torsion free lattice it follows that $\gamma = \beta$, a contradiction.

The last claim follows from Lemma 3.1. □

3.3. **Periodic κ-divisibility.** One can consider other notions of divisibility motivated geometrically by periodic orbits. In this case let $\gamma \in \Gamma$ be a semisimple element which is diagonalizable over $\mathbb{Q}_S$, i.e., for which there exists some $g_\gamma \in G$ so that $g_\gamma^{-1}\gamma g_\gamma = a \in A$. We shall assume as we may that $a \in A^+$ belongs to the positive Weyl chamber. The periodic width and periodic diameter of γ are defined via the shape $\mathbb{S}_\gamma = \mathbb{S}_a$. We shall attach to γ the subset $\Gamma g_\gamma \mathbb{S}_a$ of the (often periodic) A-orbit $\Gamma g_\gamma A$. We say that γ is *periodic κ-divisible* if the piece $\Gamma g_\gamma S_\gamma$ of the A-orbit of Γg_γ contains an element $x = \Gamma g_\gamma a_1$ with $a_1 S_\alpha \subseteq S_\gamma$ such that $x S_\alpha$ is κ-close to

the piece $\Gamma g_\alpha S_\alpha$ of the A-orbit of the point associated to α, i.e. the piece associated to γ shadows the one associated to α.

It is immediate that the above notion of periodic divisibility has the same dynamical interpretation in terms of the orbit visiting a particular open subset of $\Gamma\backslash G$ associated to α. However, in this case we have to count conjugacy classes of elements $\gamma \in \Gamma$ that are conjugated to an element of A.

For simplicity we have discussed in the previous sections only the case of κ-divisibility, but the whole discussion remains valid also for periodic κ-divisibility (with the discussed changes in the orbit associated to γ and the open subset associated to α).

4. Applying measure rigidity

In this section we are going to use the results of the previous section to prove Theorem 1.10 and Theorem 1.11. In both cases we link the number of elements that are not divisible by α to the structure of the set of all A-orbits that do not visit the particular open subset $O_\alpha \subset X$ discussed in Lemma 3.1.

4.1. **Proof of Theorem 1.10, assuming the classification of measures with positive entropy.** In Lemma 3.3 we have seen that (for a fixed w) exponentially many counterexamples to the required divisibility property gives rise to "exponentially many (ϵ, N)-separated points" for the dynamics of one of the singular elements a_ϕ. Therefore, if we assume by contradiction that the conclusion of Theorem 1.10 does not hold, then we get a sequence of finite sets F_n which are (ϵ, N)-separated for one of the singular elements satisfying $|F_n| > e^{\delta' R_n}$ for some $\delta' > 0$. Passing to a subsequence if necessary we may assume that we always consider the same element a_ϕ. As noted in Lemma 3.3 the length N of the time interval considered is bounded in terms of R_n so that $|F_n| > e^{\delta'' N}$ for some $\delta'' > 0$. Moreover, this piece of the orbit and its image under T_w (see Lemma 3.3) are disjoint to O_α. We now use the variational principle, more precisely one part of its proof. Recall that the variational principle asserts that for a homeomorphism $T : X \to X$ we have

$$\mathrm{h}_{\mathrm{top}}(T) = \sup_\mu \mathrm{h}_\mu(T)$$

where the supremum is taken over all T-invariant probability measures on X. By virtue of the statement this also applies to T-invariant subsets $Y \subset X$. However $Y = X \setminus O_\alpha$ is not T-invariant. We observe however, that the proof of the direction of the variational principle we need still applies (see for example [21]). Indeed the proof consists of showing that a sequence of measures supported on the trajectory from time 0 to time N of an (ϵ, N)-separated set give rise to a weak* limit whose entropy is at least the growth rate of the sequence of (ϵ, N)-separated points that were used. Since the (ϵ, N)-separated sets constructed as well as their trajectory up to time N is outside of the set O_α the weak* limit measure μ_α satisfies $\mu_\alpha(O_\alpha) = 0$. Moreover $(\mathrm{supp}(\mu_\alpha))T_w$ is disjoint from O_α (see Lemma 3.3). Let

$$\mu_{\alpha,W} = \frac{1}{m(T_w)} \int_{T_w} \mu_\alpha t dm(t)$$

be the average of the right translates by $t \in T_w$ (using the Haar measure m on the subgroup of A generated by T_w). By the above assertion $\mathrm{supp}(\mu_{\alpha,W})$ is disjoint from O_α and has entropy which is bounded below by $\delta' > 0$. The upper semicontinuity of entropy (see [8] and [6, Sect. 9]) implies that any weak* limit of any subsequence

of these measures will still have positive entropy. As such a weak limit will be A-invariant and give zero measure to O_α it contradicts the assumed measure rigidity for the action A-action on $\Gamma\backslash G$.

4.2. **Proof of Theorem 1.11, assuming the classification of closed invariant sets.** The main assumption in Theorem 1.11 is that proper A-invariant closed subsets are finite unions of compact orbits (as is conjectured for many homogeneous spaces). Using this we can derive the following lemma.

Lemma 4.1. *Let X and A be as in Theorem 1.11. Let $O \subset X$ be any proper non-empty open subset. Then $\{x \in X : xA \subset X \setminus O\}$ is the maximal A-invariant subset of $X \setminus O$, which is also closed. By the assumptions in the theorem there exists a collection of finitely many periodic orbits $y_1A, \dots, y_\ell A \subset X \setminus O$ with*

$$\{x \in X : xA \subset X \setminus O\} = y_1A \cup \cdots \cup y_\ell A.$$

Moreover, these periodic points satisfy, that for every $\epsilon > 0$ there exists an[3] $m \in A^+$ such that for all shapes defined using an element $a_{\mathbb{S}} \in A^+$ by

$$\mathbb{S} = \{a \in A : e \le a \le a_{\mathbb{S}}\}$$

and all points $x \in X$ with $x\mathbb{S} \subset X \setminus O$ there is a point $y \in (y_1A \cup \cdots \cup y_\ell A)$ with $d(xa, ya) < \epsilon$ for all $a \in \mathbb{S}^{(m)} = \{a \in \mathbb{S} : m \le a \le a_{\mathbb{S}}m^{-1}\}$.

Proof. We note that $Y = \{x \in X : xA \subset X \setminus O\}$ is clearly the maximal A-invariant subset of $X \setminus O$, and that Y is closed since $X \setminus O$ is closed and Y is maximal. By the assumption there exist the finite list of periodic orbits as above. We may assume that $\delta > 0$ is sufficiently small so that $y, y' \in Y$ and $d(y, y') < \delta$ implies that $y' = ya$ for some $a \in A$ with $d(a, e) < \delta$. Below we may and will assume that $\epsilon < \delta$ is sufficiently small. In particular we will assume that both are smaller than the injectivity radius of X so that $g \in G$, $x \in X$, and $d(g, e) < \delta$ implies $d(xg, x) = d(g, e)$.

Assume now that the second assertion of the lemma fails. Then for some $\epsilon > 0$ and for every $m \in A^+$ there exists a shape $\mathbb{S}$ and a point $x \in X$ with $x\mathbb{S} \subset X \setminus O$ so that $y \in Y = (x_1A \cup \cdots \cup x_\ell A)$ implies $d(xa, ya) \ge \epsilon$ for some $a \in \mathbb{S}^{(m)} = \{a \in \mathbb{S} : m \le a \le a_{\mathbb{S}}m^{-1}\}$. We claim that this implies that there exists some $a' \in \mathbb{S}^{(m)}$ such that $d(xa', Y) \ge \eta$ for some fixed $\eta > 0$.

If $d(xm, Y) \ge \epsilon/100$ we set $a' = m$. If however, $d(xm, ym) < \epsilon/100$ for some $y \in Y$, then we may choose $y \in Y$ such that ym has minimal distance to xm, write $xm = ymg$ for some $g \in G$ with $d(g, e) < \epsilon/100$ and decompose g into a product $g = g_A g_- g_+$ where $g_A \in A \cap B_{\epsilon/10}$, $g_- \in B_{\epsilon/10}$ is contracted by every generic elements of A^+, and $g^+ \in B_{\epsilon/10}$ is expanded by every generic elements of A^+. By our assumption there exists now some $a \in \mathbb{S}^{(m)}$ with $d(xa, ya) > \epsilon$. We may assume that ϵ is sufficiently smaller than δ, so that by continuity there must exist also some $a' \in \mathbb{S}^{(m)}$ with $d(xa', ya') \in (\epsilon, \frac{1}{2}\delta)$. We set $a'' = m^{-1}a'$ and may also assume that $d(ga'', a'') = d(xa', ya')$. However, this implies that $d(g_+a'', a'') > \epsilon/2$ and then also $d(g_+a'', a) > \eta$ for all $a \in A$ and some constant $\eta \in (0, \epsilon)$ independent of a. This in turn implies that $d(xa', yA) \ge \eta$, and so $d(x'a', Y) \ge \eta$ by our choice of δ.

[3]The reader may think of $\mathbb{S}$ as a picture, m as the thickness of the frame and the claim as saying that the painting is essentially periodic.

Fix some increasing sequence of elements $m_1 < m_2, \cdots \in A^+$ so that $\cup_{i\in\mathbb{N}} A(m_i) = A$ where $A(m_i) := \{a \in A : m_i^{-1} \leq a \leq m_i\}$. Let $\mathbb{S}_i$ be the shape associated with m_i as in the above discussion. For every i there exists some $x_i' \in X \setminus O$ whose distance to Y is bounded from below and for which $x_i' A(m_i) \subset X \setminus O$. Passing to a converging subsequence $x_{i_n}' \to x$ as $n \to \infty$ and using the fact that $A(m_i) \nearrow A$ we obtain that $xA \subset X \setminus O$. Therefore, $x \in Y \setminus (y_1 A \cup \cdots \cup y_\ell A)$ and we get a contradiction to the choice of the periodic orbits. □

To deduce Theorem 1.11 from Lemma 4.1 we proceed somewhat similarly to the proof of Theorem 1.10. Fix some $\alpha \in \Gamma$ and $\kappa \geq 0$ with $\kappa > 0$ if G has an Archimedean factor. Just as on page 11 we choose some torsion free sublattice $\Gamma' \subset \Gamma$ of finite index. It suffices to show the estimate

$$\left|\{\gamma \in \gamma_0\Gamma' : \gamma \text{ is not } \kappa\text{-divisible by } \alpha,\ \operatorname{diam}(\gamma) \leq R, \operatorname{width}(\gamma) \geq w\}\right| < cR^q$$

for each coset of $\gamma_0\Gamma'$ and some absolute constant c. We note that $\Gamma' \cap K = \{e\}$ which implies that γK and βK are disjoint and have distance $\geq \rho$ (with a uniform $\rho > 0$) if $\gamma \neq \beta \in \gamma_0\Gamma'$. We also assume that ρ is smaller than the injectivity radius on X.

The main part of the above estimate comes simply from the possible choices of shapes $\mathbb{S} \subset A$ of diameter less than R. If all G Archimedean factors of G are compact, the number of such shapes is clearly bounded from above by a multiple of R^q. If however, one factor of A is Archimedean, the number of shapes is infinite. Hence in this case, one has to introduce (similar to Section 3.2) an element of $a_{\text{grid}} \in A_\infty^+ = A^+ \cap G_\infty$ to discretize the possible shapes within A. We may assume that a_{grid} is close to the identity so that $a \in A_\infty^+$ and $e \leq a \leq a_{\text{grid}}$ implies $d(a, e) < \rho/10$.

Therefore, it suffices to show that

$$\left|\{\gamma \in \gamma_0\Gamma' : \gamma \text{ is not } \kappa\text{-divisible by } \alpha,\ S_{a_0} \subseteq S_\gamma \subseteq S_{a_0 a_{\text{grid}}}\}\right| \leq c \tag{7}$$

for some absolute constant independent of $a_0 \in A$. By Lemma 3.1 there exists a non-empty open subset O_α such that if $\Gamma k_\gamma \mathbb{S}_\gamma^{-\alpha}$ intersects O_α then Γ is κ-divisible by α.

We let $\epsilon = \rho/10$ and apply Lemma 4.1 to the set O_α. We let $Y = \{x : xA \subset X \setminus O_\alpha\} = y_1 A \cup \cdots \cup y_\ell A$ be the maximal A-invariant subset of $X \setminus O_\alpha$ and assume that $y_1', \ldots, y_k' \in Y$ are ϵ-dense. Let m be as in Lemma 4.1. Also let $x_1, \ldots, x_K \in X$ be finitely many points such that for every $x \in X$ there exists some x_i with $d(xa, x_i a) < \epsilon$ for all $a \in \mathbb{S}_m$. We claim that $c = kK^2$ satisfies (7) for all $a_0 \in A^+$ with $\operatorname{width}(a_0)$ sufficiently big so that $m^2 \in \mathbb{S}_{a_0}$.

To prove this bound we associate with every $\gamma \in \gamma_0\Gamma'$ belonging to the set on the left of (7) a triple $(x_i, y_j', x_{i'})$. The point x_i is chosen with the above property of the list $x_1, \ldots, x_K$ such that $d(\Gamma k_\gamma a, x_i a) < \epsilon$ for all $a \in \mathbb{S}_m$. The point y_j' is chosen ϵ-close to the point $y \in Y$ obtained from Lemma 4.1, so that $d(\Gamma k_\gamma a, y_j' a) < 2\epsilon$ for all $a \in \mathbb{S}_{a_0}^{(m)}$ (since the action of A on Y is isometric). Finally, $x_{i'}$ is chosen such that $d(\Gamma k_\gamma a_0 m^{-1} a, x_{i'} a) < \epsilon$ for all $a \in \mathbb{S}_m$.

If now two lattice elements γ, γ' are associated with the same triple, then we obtain

$$d(\Gamma k_\gamma a, \Gamma k_{\gamma'} a) < 4\epsilon$$

for all $a \in \mathbb{S}_m \cup \mathbb{S}_{a_0}^{(m)} \cup a_0 m^{-1} \mathbb{S}_m$. As $\rho = 10\epsilon$ is less than the injectivity radius we obtain from this

$$d(k_\gamma a_0, k_{\gamma'} a_0) < 4\epsilon.$$

Together with the restriction on the shapes of γ, γ' this gives

$$d(k_\gamma a_\gamma, k_{\gamma'} a_{\gamma'}) < 5\epsilon = \rho/2,$$

or also $d(\gamma K, \gamma' K) < \rho/2$, but then our choice of ρ implies $\gamma = \gamma'$.

5. Division algebras

5.1. **The proof of Theorem 1.6.** Let D be a division algebra of prime degree d over a number field $\mathbb{K}$. We define the group $\mathbb{G} = \mathrm{Res}_{\mathbb{K}|\mathbb{Q}} \mathrm{PD}^\times$ as follows.

First recall that $D \otimes_{\mathbb{K}} \bar{\mathbb{K}}$ is isomorphic to $\mathrm{Mat}_d(\bar{\mathbb{K}})$. We define $\mathrm{D}^\times$ to be the algebraic group that goes under this isomorphism to $\mathrm{GL}_d(\mathbb{K})$ — it is a $\mathbb{K}$-group. The center of $\mathrm{D}^\times$ corresponds to scalar matrices (and as such to the field $\mathbb{K}$). Now we let $\mathrm{D}^\times$ act on the vector space $D \otimes_{\mathbb{K}} \bar{\mathbb{K}}$ via conjugation which defines the algebraic group $\mathrm{PD}^\times$ as the image of this representation. Applying restriction of scalars we obtain $\mathbb{G} = \mathrm{Res}_{\mathbb{K}|\mathbb{Q}} \mathrm{PD}^\times$. Notice also that $\mathbb{G}(\bar{\mathbb{Q}})$ is isomorphic to the direct product of $[\mathbb{K} : \mathbb{Q}]$ copies of $\mathrm{PGL}_d(\bar{\mathbb{Q}})$.

We let S be a finite number of places of $\mathbb{Q}$, including the infinite place. For each place $\sigma \in S$ we assume that $\mathbb{G}$ splits over $\mathbb{Q}_\sigma$, which means that $\mathbb{G}(\mathbb{Q}_\sigma)$ is isomorphic to a direct product of $[\mathbb{K} : \mathbb{Q}]$ copies of $\mathrm{PGL}_d(\mathbb{Q}_\sigma)$ (and this forces $\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_\sigma$ to be also isomorphic to $\mathbb{Q}_\sigma^{[\mathbb{K}:\mathbb{Q}]}$). We make one exception to this splitting condition which will become important in Section 5.2: if $d = 2$ we allow $\mathbb{G}(\mathbb{R})$ to be compact, in which case we simply remove the infinite places from S.

We note that the $\mathbb{Q}$-points of $\mathbb{G}$ can be identified with $D^\times / \mathbb{K}^\times$. Assume for the moment that $\mathbb{K} = \mathbb{Q}$, and take now an order $\mathcal{O}_D \subset D$. Using a basis of $\mathcal{O}$ over $\mathbb{Z}$ in the representation of $\mathrm{PD}^\times$ it follows that $\mathrm{PD}^\times(\mathbb{Z})$ is isomorphic to $\mathcal{O}_D^\times$ modulo the center of $\mathrm{D}^\times$. Similarly, we get (3).

As the conclusion of Theorem 1.6 is identical to the conclusion of Theorem 1.10, it remains to justify the assumptions of Theorem 1.10.

By the Borel Harish-Chandra theorem Γ is a lattice in $G = \mathbb{G}(\mathbb{Q}_S)$ since $\mathbb{G}$ is semi-simple. If $X = \Gamma \backslash G$ is not compact, then Γ contains a nontrivial unipotent element γ. We may represent γ as the equivalence class modulo the center of some $a \in D$. Applying the Jordan decomposition of a in $\mathrm{D}^\times$ we obtain $a = a_{ss} a_u$, which forces the semi-simple part a_{ss} to belong to the center. It follows that a_u is a nontrivial unipotent element of D. However, $a_u - 1$ would then be a nonzero non-invertible element of the division algebra D. Therefore, X is compact.

By Theorem 1.9 the existence of A-invariant probability measures with positive entropy other than the Haar measure on a quotient of $\mathrm{SL}_d(\mathbb{R})$ by a lattice is ruled out if the lattice does not contain any elements with repeated eigenvalues. The proof of this theorem in [6] generalizes to allow for more general S-arithmetic quotients that we consider in this section (see also [5] for the changes needed when going from the real to the S-arithmetic setting).

More formally, this also follows from the general classification of positive entropy measures for Cartan actions in [9]: in [9, Thm. 1.1] it is shown that an A-invariant and ergodic probability measure μ is supported on a closed orbit $\Gamma \mathbb{L}(\mathbb{Q}_S) g$ for some $g \in G$ and some reductive $\mathbb{Q}$-subgroup $\mathbb{L}$ with the same S-rank as the ambient group and whose center is $\mathbb{Q}$-anisotropic. Let us assume for the moment $\mathbb{G}$ is over $\mathbb{Q}_S$

isomoprhic to SL_d. This implies that if $\mathbb{L}$ is a proper subgroup of $\mathbb{G}$ then either $\mathbb{L}$ is a torus (and the measure must have zero entropy) or the center of $\mathbb{L}$ has to be nontrivial and all of its elements have repeated eigenvalues. In the latter case, the center of $\mathbb{L}(\mathbb{Q}_S)$ must intersect the lattice in a lattice. If the lattice does not contain any elements with repeated eigenvalues, this forces the reductive $\mathbb{Q}$-group $\mathbb{L}$ to be equal to $\mathbb{G}$. If the S-rank of $\mathbb{G}$ is greater or equal to 2 and entropy of μ is positive, then [9, Thm. 1.1] shows that μ must be invariant under a finite index subgroup of $\mathbb{G}(\mathbb{Q}_S)$. Since $\mathrm{SL}_d(\mathbb{Q}_S)$ does not have any proper finite index subgroups, this implies that μ must be the Haar measure.

We now generalize the above discussion to the case $\mathbb{G} = \mathrm{PD}^\times$ considered in this section and prove that the lattice in $G = \mathbb{G}(\mathbb{Q}_S)$ does indeed not contain non-trivial elements with repeated eigenvalues. Suppose that $a \in D$ does not belong to $\mathbb{K}$. Then $\mathbb{K}(a)$ is a proper field extension of $\mathbb{K}$. Considering D as a vector space over $\mathbb{K}(a)$ it follows that $[\mathbb{K}(a) : \mathbb{K}]$ divides $\dim_{\mathbb{K}} D$. However, as the dimension of D equals d^2 and we assumed that d is a prime, we obtain that a must generate a field extension of degree d. In other words, the minimal polynomial of a over $\mathbb{K}$ has degree d (with d distinct roots). Mapping a under the isomorphism from $D \otimes_{\mathbb{K}} \bar{\mathbb{K}}$ to $\mathrm{Mat}_d(\bar{\mathbb{K}})$ this gives a matrix for which all eigenvalues are different. Considering this element now as a lattice element in $\mathbb{G}(\mathbb{Q}_S)$, which is isomorphic to $\mathrm{PGL}_d(\mathbb{Q}_S)^{[\mathbb{K}:\mathbb{Q}]}$, we obtain a tuple of equivalence classes of matrices where the representatives have non-repeating eigenvalues. Just as in the discussion above this implies using [9, Thm. 1.1] that any A-invariant and ergodic probability measure μ with positive entropy must be invariant under a finite index subgroup of $G = \mathbb{G}(\mathbb{Q}_S) \cong \mathrm{PGL}_d(\mathbb{Q}_S)^{[\mathbb{K}:\mathbb{Q}]}$. As any finite index subgroup must contain $\mathrm{SL}_d(\mathbb{Q}_S)^{[\mathbb{K}:\mathbb{Q}]}$, and $\mathrm{SL}_d(\mathbb{Q}_S)^{[\mathbb{K}:\mathbb{Q}]} \cdot A = \mathrm{PGL}_d(\mathbb{Q}_S)^{[\mathbb{K}:\mathbb{Q}]}$ it follows that μ must once more equal the Haar measure on G. Therefore, Theorem 1.10 applies and gives Theorem 1.6.

5.2. **Quaternion algebras and finitely many primes.** We will now prove Theorem 1.2 as a corollary of Theorem 1.6. Let $D = \mathbb{Q}[i, j, k]$ be the Hamiltonian quaternion algebra over $\mathbb{Q}$. Let $\mathcal{O} = \mathbb{Z}[i, j, k]$ and let S be a set of primes with $|S| \geq 2$ such that D splits over $\mathbb{Q}_p$ (i.e. $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$, which happens precisely for all odd primes).

By (3) (which we explained above) the group of units of $D[\frac{1}{p} : p \in S]$ modulo the units of $\mathbb{Z}[\frac{1}{p} : p \in S]$ gives an irreducible lattice in the algebraic group $\mathrm{PD}^\times(\mathbb{Q}_S)$ (where we do not include ∞ in S since $\mathrm{PD}^\times(\mathbb{R})$ is compact).

We wish to explicate the injection from D into $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ for some fixed prime $p \in S$. For this we are going to use a solution $\epsilon, \eta \in \mathbb{Z}_p$ of the equation $\epsilon^2 + \eta^2 = -1$. By Hensel's lemma it suffices to solve $\epsilon^2 + \eta^2 = -1$ in $\mathbb{Z}/(p)$. If -1 is a quadratic residue modulo p then take $\eta = 0$. Otherwise we should find a solution to $-\eta^2 = \epsilon^2 + 1$ which clearly exists since not all elements of $\mathbb{Z}/(p)$ are quadratic residues. Using these two p-adic integers we map i to $\begin{pmatrix} \epsilon & \eta \\ \eta & -\epsilon \end{pmatrix}$, j to $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $k = ij$ to the corresponding product, which gives the homomorphism

$$\gamma = a + bi + cj + dk \mapsto \iota(\gamma) = \begin{pmatrix} a + b\epsilon - d\eta & b\eta + c + d\epsilon \\ b\eta - c + d\epsilon & a - b\epsilon + d\eta \end{pmatrix}.$$

It is easy to check that the norm of $\gamma \in D$ equals the determinant of its image. If $\gamma \in \mathcal{O}$, then clearly $\iota(\gamma) \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}_p)$.

We claim furthermore, that $\iota(\gamma) \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}_p)$ implies that $a, b, c, d \in \mathbb{Z}_p$. This follows from viewing the map ι as a linear transformation with determinant 4. This also implies that a reduced $\gamma \in \Lambda_{\mathcal{O}}$ is mapped to a reduced matrix (i.e. an integral matrix such that not all entries are divisible by p). It follows that the map $\gamma \mapsto [\iota(\gamma)]$ is an injective map from $\{\gamma \in \Lambda_{\mathcal{O}} : \gamma \text{ is reduced}\}$ into $\prod_{p\in S} \mathrm{PGL}_2(\mathbb{Q}_p)$.

Let $\gamma \in \Lambda_{\mathcal{O},S}$. In Theorem 1.2 the width (diameter) of γ is defined as the minimum (sum) of the exponents when writing $N(\gamma)$ as a product of powers of elements of S. In Theorem 1.6 and the proof in Section 5.1 the width (diameter) of $[\iota(\gamma)]$ is defined as in Definition 1.5. To compare these two definitions fix some $p \in S$. Note that there is (up to sign) only one root ϕ_p for the diagonal subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$. If γ is reduced, the KAK decomposition of $\iota(\gamma)$ must equal $\begin{pmatrix} p^e & 0 \\ 0 & 1 \end{pmatrix}$ for some $e \geq 0$ since $\iota(\gamma)$ is also reduced. This implies that $\phi_p([\iota(\gamma)]) = e \log p$ where e is the exponent of p in $N(\gamma)$. This shows that the two definitions of width (and diameter) are bounded by multiples of each other.

Observe that the above discussion implies also that the notions of divisibilities defined in sections 1.1 and 1.2 coincide. It follows from Theorem 1.6, using the injectivity of the map from the collection of reduced quaternions into the associated lattice in $\prod_{p\in S} \mathrm{PGL}_2(\mathbb{Q}_p)$, that:

Theorem 5.1. *Let D be the Hamiltonian quaternion algebra and $\mathcal{O} = \mathbb{Z}[i, j, k]$. Let S be a finite set of nonarchimedean places over which D splits, and assume $|S| \geq 2$. Let $a \in \Lambda_{\mathcal{O},S}$ be a reduced element. Then for every $\epsilon > 0$ there exists some $w = w(a, \epsilon)$ so that*

$$\log\left|\left\{\gamma \in \Lambda^{\mathrm{red}}_{\mathcal{O},S} : \mathrm{diam}(\gamma) \leq R, \mathrm{width}(\gamma) \geq w, a \text{ does not divide } \gamma\right\}\right| < \epsilon R$$

for all sufficiently large R, where $\Lambda^{\mathrm{red}}_{\mathcal{O},S}$ denotes the reduced quaternions in $\Lambda_{\mathcal{O},S}$.

Assume now that Theorem 1.2 does not hold. Then there exists some $\epsilon > 0$ such that for every $w > 0$ there is an increasing sequence $R_n \to \infty$ so that

$$\log\left|\left\{\gamma \in \Lambda_{\mathcal{O},S} : \mathrm{diam}(\gamma) \leq R_n, \mathrm{width}(\gamma) \geq w, a \text{ does not divide } \gamma\right\}\right| > \epsilon R_n$$

To each quaternion $\gamma \in \Lambda_{\mathcal{O},S}$ we associate a pair of integers $\psi(\gamma) = \big(N(\gamma), N(\rho(\gamma))\big)$ called its *shape pair* where $\rho(\gamma) \in \Lambda_{\mathcal{O},S}$ is the unique reduced quaternion so that $\gamma = \rho(\gamma) \cdot \prod_{p\in S} p^{e_p}$. Observe that for a given diameter R there are polynomially many possible shape pairs associated to quaternions whose diameter is at most R. Hence if Theorem 1.2 fails we have some sequence of shape pairs (x_n, y_n) so that $\log |D_n| > \epsilon R/2$ where

$$D_n = \left\{\gamma \in \Lambda_{\mathcal{O},S} \ : \ \begin{array}{l} \mathrm{diam}(\gamma) \leq R_n, \mathrm{width}(\gamma) \geq w, \\ a \text{ does not divide } \gamma, \psi(\gamma) = (x_n, y_n) \end{array}\right\}.$$

We may choose for each $\gamma \in D_n$ some reduced $\tau(\gamma) = \rho(\gamma) \cdot \gamma'$ where $\rho(\gamma)$ is the reduced part of γ and γ' is a (reduced) quaternion such that $\gamma = \rho(\gamma) \cdot \gamma' \cdot \overline{\gamma'}$. We recall that any reduced $\gamma = x_1 x_2 = y_1 y_2 \in \mathcal{O}$ with $x_1, x_2, y_1, y_2 \in \mathcal{O}$ and $N(x_1) = N(y_1)$ odd, then $x_1 = \omega y_1$ for some unit ω of $\mathcal{O}$ (cf. [17]). Therefore, for $\gamma_1, \gamma_2 \in D_n$ such that $\gamma_1 \neq \omega\gamma_2$ for all the eight units ω of $\mathcal{O}$ it follows that $\tau(\gamma_1) \neq \tau(\gamma_2)$. Note also that the width of $\tau(\gamma)$ is at least half the width of γ. Finally observe that since

a does not divide $\gamma \in D_n$ it also does not divide $\tau(\gamma)$ and we get a contradiction to Theorem 5.1.

5.3. **Quaternion algebras, the proof of Theorem 1.1.** We are going to need the following generalization of Theorem 1.8.

Theorem 5.2. *Let $D = \mathbb{Q}[i,j,k]$ be the Hamiltonian quaternion algebra. Let $X = \mathrm{PD}^\times(\mathbb{Q})\backslash \mathrm{PD}^\times(\mathbb{A}_\mathbb{Q})/M_{\infty,2}$, where $M_{\infty,2} = \mathrm{PD}^\times(\mathbb{R}\times\mathbb{Q}_2)$ and let*

$$A = \bigcup_{2,\infty\notin S \text{ finite}} \Big(\prod_{p\in S} A_p \times \prod_{3\le p\notin S} (A_p \cap K_p)\Big)$$

be the restricted direct product of the diagonal subgroups A_p of $\mathrm{PD}^\times(\mathbb{Q}_p) \cong \mathrm{PGL}_2(\mathbb{Q}_p)$ for all odd primes p, where K_p is the maximal compact open subgroup $\mathrm{PD}^\times(\mathbb{Z}_p) \cong \mathrm{PGL}_2(\mathbb{Z}_p)$. Then the A-action has only one invariant probability measure on X, namely the normalized Haar measure on X.

The proof of Theorem 5.2 is essentially the same as the proof of Theorem 1.8, but unfortunately the above theorem does not exist in the literature in this form. Roughly speaking the invariance under the diagonal subgroup at all odd primes can be used to prove that the measure must have positive entropy. In the proof of Theorem 1.8 in [14] entropy for the real diagonal flow is used, which has to be replaced in the proof of Theorem 5.2 by say the 3-adic diagonal flow. A detailed proof will appear together with some generalizations in the paper [2].

As A is amenable and X is compact, unique ergodicity has immediate consequences regarding density of orbits.

Corollary 5.3. *Let X and A be as in Theorem 5.2. Let $O \subset X$ be a non-empty open subset. Then there exists a compact subset $F \subset A$ such that for every $x \in X$ the set xF intersects O nontrivially.*

Proof. Let $F_n < A$ be a sequence of Følner sets and suppose that the corollary fails for each of the sets F_n. Then there exists for every n some x_n such that x_nF_n is disjoint to O. Let μ_n be the push-forward of the Haar measure of A restricted to F_n under the map $a \in F_n \mapsto xa$. We normalize μ_n to be a probability measure. By Tychonoff-Alaoglu there exists a weak* limit point μ, which will be an A-invariant probability measure on X (since the latter is compact). By Theorem 5.2 $\mu = m_X$ is the Haar measure on X, which contradicts our construction of the sequence μ_n. □

Proof of Theorem 1.1. Let $\alpha \in \mathcal{O}$ be a reduced element of odd norm. Let S_0 be the set of odd primes that divide $N(a)$. We recall that $\alpha \in \Lambda_{\mathcal{O},S_0}$ gives rise to a lattice element $[\alpha] = [\iota(\alpha)] \in \mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S_0])$. We also recall from the last section that if $[\alpha]$ divides $[\gamma]$ for some other reduced $\gamma \in \Lambda_{\mathcal{O},S_0}$, then α divides γ in $\mathcal{O}$.

By Lemma 3.1 there exists some nontrivial open subset

$$O_\alpha \subset X_{S_0} = \mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S_0])\backslash \mathrm{PD}^\times(\mathbb{Q}_{S_0})$$

such that any reduced $\gamma \in \Lambda_{\mathcal{O},S_0}$ with a nonempty intersection

$$O_\alpha \cap \big(\mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S_0])k_{[\gamma]}\mathbb{S}^{-[\alpha]}_{[\gamma]}\big)$$

satisfies that $[\alpha]$ divides $[\gamma]$ (and so α divides γ).

Since for any odd N there exists some reduced $\gamma \in \mathcal{O}$ with $N(\gamma) = N$ it follows that the projection map π_{S_0} from

$$X = \mathrm{PD}^\times(\mathbb{Q}) \backslash \mathrm{PD}^\times(\mathbb{A}_\mathbb{Q})/M_{\infty,2} \cong \mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S_0]) \backslash \mathrm{PD}^\times\Big(\mathbb{Q}_{S_0} \times \prod_{3 \le p \notin S_0} \mathbb{Z}_p\Big)$$

to $\mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S_0]) \backslash \mathrm{PD}^\times(\mathbb{Q}_{S_0})$ is well-defined and onto. Using it we define the open subset $O = \pi_{S_0}^{-1} O_\alpha \subset X$. We now apply Corollary 5.3 and find some compact subset $F \subset A$ such that $xF \cap O$ is nonempty for all $x \in X$. By definition of the restricted direct product there exists now some set of odd primes $S \supset S_0$ such that

$$F \subset A_S = \prod_{p \in S} A_p \times \prod_{3 \le p \notin S} (A_p \cap K_p).$$

Furthermore, there exists some integer M' which is a product of powers of primes in S such that for any reduced $\gamma \in \Lambda_{\mathcal{O},S}$ with $M \mid N(\gamma)$ we have that some translate of F is contained in $\mathbb{S}_{[\gamma]}^{-[\alpha]}$. This implies that[4]

$$\mathrm{PD}^\times(\mathbb{Q}) k_{[\gamma]} \Big(\mathbb{S}_{[\gamma]}^{-[\alpha]} \times \prod_{3 \le p \notin S} (A \cap K_p)\Big)$$

intersects O nontrivially, or equivalently

$$\big(\mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S]) k_{[\gamma]} \mathbb{S}_{[\gamma]}^{-[\alpha]}\big) \cap \big(\mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S]) \pi_{S,S_0}^{-1} O_\alpha\big)$$

is nonempty. Here π_{S,S_0} denotes the projection map

$$\mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S]) \backslash \mathrm{PD}^\times(\mathbb{Q}_S) \to \mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S_0]) \backslash \mathrm{PD}^\times(\mathbb{Q}_{S_0}).$$

By Lemma 5.4 this implies that α divides γ.

To summarize we have found some odd M (which is a product of powers of primes in S) such that $\gamma \in \Lambda_{\mathcal{O},S}$ reduced and $M \mid N(\gamma)$ implies that $\alpha \mid \gamma$. If $\gamma \in \mathcal{O}$ is now arbitrary with $M^2 \mid N(\gamma)$ and odd norm, we denote the reduced part of γ by $\rho(\gamma)$. We may also find some reduced $\gamma' \in \mathcal{O}$ such that $\rho(\gamma) \cdot \gamma'$ is reduced and $\gamma = \rho(\gamma) \cdot \gamma' \cdot \bar{\gamma'}$. Clearly $M \mid N(\rho(\gamma)\gamma')$ so that the above implies $\alpha \mid \rho(\gamma)\gamma'$ and so also $\alpha \mid \gamma$.

In case $N(\gamma)$ is even, we claim that $\gamma = \gamma'\eta$ where γ' has odd norm and the norm of η is a power of 2. With the claim and the above, the theorem follows quickly. To prove the claim, let $\gamma = a + bi + cj + dk$. We may assume a, b, c, d are not all even, for otherwise we may simply use as our initial η the appropriate power of 2. By looking at $N(\gamma)$ modulo 8 we see that $N(\gamma)$ is at most divisible by 4 and either two or all of the coefficients are now odd. By multiplying by a unit on the right we may assume that a is odd. We also assume that b is odd (the other cases are similar). Now multiply

$$\begin{aligned}(a + bi + cj + dk)(1 + i) &= (a - b) + (a + b)i + (c - d)j + (c + d)k = \\ &= (a' + b'i + c'j + d'k)2 = (a' + b'i + c'j + d'k)(1 - i)(1 + i),\end{aligned}$$

and note that a', b', c', d' are integers. Dividing by $(1+i)$ we have shown that we can split γ into γ' and η where $N(\gamma') = \frac{1}{2}N(\gamma)$. If necessary we repeat the argument (once). □

It remains to prove the following lemma.

[4]Here we extend $k_{[\gamma]}$ in some way to an element of $\mathrm{PD}^\times(\prod_{p \ge 3} \mathbb{Z}_p)$.

Lemma 5.4. *Let O_α be the set from Lemma 3.1 for some reduced $\alpha \in \Lambda_{\mathcal{O},S_0}$ as in the above proof. Replacing S_0 by $S \supset S_0$ the set $\pi^{-1}_{S,S_0} O_\alpha$ also satisfies the conclusion of Lemma 3.1 for all $[\gamma]$ with $\gamma \in \Lambda_{\mathcal{O},S}$ reduced.*

Proof. As $\mathrm{PD}^\times(\mathbb{R})$ is compact, we may set $\kappa = 0$ in the discussion of Section 3.1. Let us write K_S for the maximal compact open subgroup of $\mathrm{PD}^\times(\mathbb{Q}_S)$ for any finite set S of odd primes.

As noted in the proof of Lemma 3.1 the open set O_α may be chosen in our case as $\mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S_0])\big(K_{S_0} \cap [\alpha] K_{S_0} a^{-1}_{[\alpha]}\big)$. With this choice

$$\pi^{-1}_{S,S_0} O_\alpha = \mathrm{PD}^\times(\mathbb{Z}[1/p : p \in S])\big(K_S \cap [\alpha] K_S a^{-1}_{[\alpha]}\big),$$

since at the primes $p \in S \setminus S_0$ we have $[\alpha] \in K_p$ and the component of $a_{[\alpha]}$ at p equals the identity. The lemma follows from Lemma 3.1. □

References

[1] H. Abels, G. Margulis, *Coarsely geodesic metrics on reductive groups. Modern dynamical systems and applications*, 163–183, Cambridge Univ. Press, Cambridge, 2004.

[2] M. Björklund, M. Einsiedler, A. Ghosh, *On adelic unique ergodicity of diagonal flows*, in preparation.

[3] J. Bourgain, E. Lindenstrauss, *Entropy of quantum limits.* Comm. Math. Phys. 233 (2003), no. 1, 153171.

[4] M. Einsiedler, *Applications of measure rigidity of diagonal actions*, Proceedings of the International Congress of Mathematicians Hyderabad, India, 2010,

[5] M. Einsiedler and A. Katok, *Rigidity of measures – the high entropy case, and non-commuting foliations*, Probability in mathematics. Israel J. Math. 148 (2005), 169–238.

[6] M. Einsiedler, A. Katok, E. Lindenstrauss, *Invariant measures and the set of exceptions to Littlewood's conjecture*, Ann. of Math. (2) 164 (2006), no. 2, 513–560.

[7] M. Einsiedler, E. Lindenstrauss, *Diagonalizable flows on locally homogeneous spaces and number theory.* International Congress of Mathematicians. Vol. II, 1731–1759, Eur. Math. Soc., Zrich, 2006.

[8] M. Einsiedler, E. Lindenstrauss, *Diagonal actions on locally homogeneous spaces.* Homogeneous flows, moduli spaces and arithmetic, 155–241, Clay Math. Proc., 10, Amer. Math. Soc., Providence, RI, 2010.

[9] M. Einsiedler, E. Lindenstrauss, *On measures invariant under tori on quotients of semisimple groups.* Ann. of Math. (2) 181 (2015), no. 3, 993–1031.

[10] M. Einsiedler, E. Lindenstrauss, Ph. Michel, A. Venkatesh, *Distribution of periodic torus orbits on homogeneous spaces.* Duke Math. J. 148 (2009), no. 1, 119–174.

[11] H. Furstenberg, *Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation,* Math. Systems Theory 1 1967 1–49.

[12] A.W. Knapp, *Lie groups beyond an introduction*, Second edition. Progress in Mathematics, 140. Birkhuser Boston, Inc., Boston, MA, 2002. xviii+812 pp. ISBN: 0-8176-4259-5

[13] E. Lindenstrauss, *Invariant measures and arithmetic quantum unique ergodicity*, Ann. of Math. (2) 163 (2006), no. 1, 165–219.

[14] E. Lindenstrauss, *Adelic dynamics and arithmetic quantum unique ergodicity*, Current developments in mathematics, 2004, 111139, Int. Press, Somerville, MA, 2006.

[15] G.A. Margulis, *Dynamical and ergodic properties of subgroup actions on homogeneous spaces with applications to number theory*, A plenary address presented at the International Congress of Mathematicians held in Kyoto, August 1990. ICM-90. Mathematical Society of Japan, Tokyo

[16] G.A. Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 17. Springer-Verlag, Berlin, 1991. x+388 pp. ISBN: 3-540-12179-X

[17] G. Pall, *On the factorization of generalized quaternions*, Duke Math. J. 4 (1938), no. 4, 696–704.

[18] D. Rudolph, *$\times 2$ and $\times 3$ invariant measures and entropy.* Ergodic Theory Dynam. Systems 10 (1990), no. 2, 395–406.

[19] J. Tits. *Reductive groups over local fields.* Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1, pp. 2969, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.
[20] G. Tomanov, *Actions of maximal tori on homogeneous spaces.* Rigidity in dynamics and geometry (Cambridge, 2000), 407–424, Springer, Berlin, 2002.
[21] P. Walters, *An introduction to ergodic theory*, Graduate Texts in Mathematics, 79. Springer-Verlag, New York-Berlin, 1982. ix+250 pp. ISBN: 0-387-90599-5

Manfred Einsiedler, D-Math, ETH, Rämistrasse 101, 8092 Zürich, Switzerland

Shahar Mozes, Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel