

DIOPHANTINE APPROXIMATION ON MATRICES AND LIE GROUPS

MENNY AKA, EMMANUEL BREUILLARD, LIOR ROSENZWEIG,
NICOLAS DE SAXCÉ

ABSTRACT. We study the general problem of extremality for metric diophantine approximation on submanifolds of matrices. We formulate a criterion for extremality in terms of a certain family of algebraic obstructions and show that it is sharp. In general the almost sure diophantine exponent of a submanifold is shown to depend only on its Zariski closure, and when the latter is defined over \mathbb{Q} , we prove that the exponent is rational and give a method to effectively compute it. This method is applied to a number of cases of interest. In particular we prove that the diophantine exponent of rational nilpotent Lie groups exists and is a rational number, which we determine explicitly in terms of representation theoretic data.

CONTENTS

1. Introduction	1
2. A zero-one law	12
3. Critical exponent for the Heisenberg group	16
4. Quasi-norms, Schubert cells, and pencils	20
5. Diophantine approximation and flows on the space of lattices	25
6. The submodularity lemma	33
7. The critical exponent for rational nilpotent Lie groups	39
8. Explicit values of the critical exponent in some examples	46
References	50

1. INTRODUCTION

Pick $n + m$ vectors x_1, \dots, x_{n+m} at random in \mathbb{R}^m according to a certain distribution ν . Take integer linear combinations of the vectors and ask how close they can get to the origin in \mathbb{R}^m . One way to measure this is via the diophantine exponent, defined as:

$$\beta(x) = \inf\{\beta > 0; \|\sum_{i=1}^{m+n} p_i x_i\| > \|\mathbf{p}\|^{-\beta} \text{ for all but finitely many } \mathbf{p} \in \mathbb{Z}^{m+n}\}, \quad (1.1)$$

where $x = (x_1, \dots, x_{m+n})$, $\mathbf{p} = (p_1, \dots, p_{m+n})$ and where on both sides $\|\cdot\|$ is the supremum norm on the coordinates.

Key words and phrases. Metric diophantine approximation, homogeneous dynamics, extremal manifolds, group actions.

In the case where $x_1 = e_1, \dots, x_m = e_m$, where e_1, \dots, e_m is the canonical basis of \mathbb{R}^m , and $(x_{m+1}, \dots, x_{m+n})$ is chosen on a submanifold of $(\mathbb{R}^m)^n \simeq M_{m,n}(\mathbb{R})$, this question is the topic of *Diophantine approximation on submanifolds of matrices*, which studies the quality of approximation by integer vectors of the image of an integer vector under an $m \times n$ matrix chosen at random in some submanifold of $M_{m,n}(\mathbb{R})$.

When $m = 1$, this subject has been studied extensively, starting with a 1932 conjecture of Mahler [Mah42], which posited that the Veronese curve

$$\mathcal{M} = \{(x, x^2, \dots, x^n), x \in \mathbb{R}\}$$

is extremal, i.e. that a random point on it has the same diophantine exponent as a random point in \mathbb{R}^n chosen with respect to Lebesgue measure. This conjecture was proved by Sprindžuk [Spr64, Spr69]. We refer the reader to [Spr64, Spr69, BD99, BRV16] for background on Diophantine approximation on manifolds.

About twenty years ago, Kleinbock and Margulis [KM98] revolutionized the subject by introducing methods from the dynamics of homogeneous flows into this area. In particular they settled a conjecture of Sprindžuk by establishing that every analytic submanifold of \mathbb{R}^n that is not contained in a proper affine subspace is extremal (see [BB96] for the state of the art before their work). This method is based on certain *quantitative non-divergence estimates* for diagonal flows on the space of lattices and takes its roots in the early work of Margulis [Mar75] pertaining to the non-divergence of unipotent flows on homogeneous spaces in connection with Margulis' first proof of arithmeticity for non-uniform higher rank lattices. It was later further developed by Kleinbock in an important series of papers [Kle98b, Kle03, Kle08b, Kle10a]. We refer the reader to [Kle08a, Kle10b] for a nice introduction to these techniques.

Our first goal in this article is to answer a question of Beresnevich, Kleinbock and Margulis [BKM15] asking for the right criterion for a submanifold of matrices to be extremal. We were led to this problem after we observed that a solution would enable us to compute diophantine exponents for dense subgroups of nilpotent Lie groups, in the spirit of our previous work [ABRdS15a]. Beyond extremality, our criterion allows us to effectively compute the exponent of any rationally defined submanifold of matrices. Further in the paper, we will derive consequences for nilpotent Lie groups. The results of this paper were announced in [ABRdS15b].

*
* *

We view the $(n + m)$ -tuple x as a $m \times (m + n)$ matrix. We note in passing that the exponent $\beta(x)$ depends only on the kernel $\ker x$. Therefore diophantine approximation on submanifolds of matrices is best phrased in terms of diophantine approximation on submanifolds of the grassmannian, here the grassmannian of n -planes in \mathbb{R}^{n+m} . We will keep this observation as a guiding principle, but will always phrase everything in terms of matrices. We now describe a family of obvious obstructions to extremality.

Definition 1.1 (Pencil). Given a real vector subspace $W \leq \mathbb{R}^{m+n}$, and an integer $r \leq m$, we define the *pencil* $\mathcal{P}_{W,r}$ to be the set of matrices $x \in M_{m,m+n}(\mathbb{R})$ such that

$$\dim(xW) \leq r.$$

We say that the pencil is rational if W is rational, i.e. admits a basis in \mathbb{Q}^{m+n} .

Remark. In the $m = 1$ case, $M_{1,1+n}(\mathbb{R})$ can be identified with the space of linear forms on \mathbb{R}^{1+n} . For $W \leq \mathbb{R}^{1+n}$, the pencil $\mathcal{P}_{W,0}$ is the subspace of linear forms vanishing on W . Of course, for $r \geq 1$ we have $\mathcal{P}_{W,r} = M_{1,1+n}(\mathbb{R})$. In the general case, pencils are closed algebraic subvarieties of $M_{m,m+n}(\mathbb{R})$, but they need not be affine subspaces.

Pencils are obvious obstructions to extremality, because if W is rational, then the standard Dirichlet or pigeonhole argument shows that for every $x \in \mathcal{P}_{W,r}$

$$1 + \beta(x) \geq \frac{\dim W}{r}.$$

Indeed there are roughly $R^{\dim W}$ integer points in the ball of radius R in W , but they get mapped into a ball of radius $O(R)$ in \mathbb{R}^r , so, comparing volumes, ε -balls around each of these points cannot be all disjoint if ε is at least of order $R^{1-\dim W/r}$. Consequently, we see that if

$$\frac{\dim W}{r} > \frac{m+n}{m} \tag{1.2}$$

then the point x is not extremal, since $\frac{n}{m}$ is the diophantine exponent of a random point of $M_{m,m+n}(\mathbb{R})$ chosen with respect to Lebesgue measure.

Pencils satisfying (1.2) will be called *constraining pencils*, because they constrain the diophantine exponent away from its extremal value. A pencil is called *proper* if it is not all of $M_{m,m+n}(\mathbb{R})$. When viewed in the grassmannian (i.e. looking at the set of kernels $\ker x$, with x in a pencil), pencils are well-studied objects: they are a certain kind of *Schubert varieties* (see e.g. [GH94, ch 1.5] and Section 4.2 below).

When the Zariski closure of \mathcal{M} is defined over \mathbb{Q} , it turns out that these obvious obstructions are the only ones, and the following is our first main result.

Theorem 1.2 (Exponent for rational manifolds). *Let m, n be positive integers and \mathcal{M} be a connected analytic submanifold of $M_{m,m+n}(\mathbb{R})$. Assume that the Zariski closure of \mathcal{M} is defined over \mathbb{Q} . Then for Lebesgue almost every point $x \in \mathcal{M}$ the diophantine exponent is rational and equals*

$$\beta(x) = \max_{\mathcal{M} \subset \mathcal{P}_{W,r}} \left\{ \frac{\dim W}{r} - 1 \right\}. \tag{1.3}$$

Moreover, the maximum in the right-hand side is achieved for a rational W .

Note that the maximum in (1.3) is always achieved, because the quantity $\frac{\dim W}{r} - 1$ takes values in a finite set of rational points; the important point in the second part of the theorem is that some *rational* subspace achieves the maximum.

The theorem shows in particular that the generic value of $\beta(x)$ is constant, and can be effectively computed once the pencils containing \mathcal{M} are identified. We also note that this value is the smallest possible value for the exponent of an arbitrary point on \mathcal{M} , because of the Dirichlet or pigeonhole type argument explained above.

When speaking of Zariski closure, algebraic subsets and algebraic varieties in this paper, we will always consider these notions in real algebraic geometry and we refer the reader to the textbook [BCR98] for definitions and basic properties. By Lebesgue measure on \mathcal{M} we mean the top dimensional Hausdorff measure of the subset \mathcal{M} of $M_{m,m+n}(\mathbb{R})$. The real algebraic variety \mathcal{M} is said to be defined over \mathbb{Q} if it is the set of zeroes of a family of polynomials (in the matrix entries) with rational coefficients. We immediately conclude:

Corollary 1.3. *Let \mathcal{M} be as in Theorem 1.2. Then \mathcal{M} is extremal if and only if it is not contained in any constraining pencil.*

Theorem 1.2 and its proof hold verbatim for more general measures (than Lebesgue measure on an analytic submanifold), which we call locally good measures (see Definition 5.2.2).

The above theorem answers a question discussed at the end of the original paper of Kleinbock and Margulis [KM98, §6.2] and also raised in the problem list [Gor07, §9.1] as well as in [KMW10, p.23] and [BKM15, Problem 1]. The papers [KMW10] and [BKM15] proposed other sufficient criterions for extremality of an analytic submanifold of $M_{m,n}(\mathbb{R})$, but they just failed to be optimal. The weak non-planar condition of [BKM15] is not strong enough for example to show extremality in the applications to nilpotent groups described below. This condition is equivalent in our language to not being contained in any proper pencil, which is a strictly stronger condition (see Example 6.2.3).

We now no longer assume the Zariski closure to be defined over \mathbb{Q} . In three papers [Kle03], [Kle08b] and [Kle10a] Kleinbock studied this situation. He showed in particular that the diophantine exponent of a random point on a connected analytic submanifold of $M_{m,n}(\mathbb{R})$ achieves the same value almost everywhere. In the case where $m = 1$ he showed that this almost sure value depends only on the affine span of the submanifold in \mathbb{R}^n . In other words a submanifold inherits its exponent from its affine span. Another remarkable observation he made in [Kle08b] for \mathbb{R}^n and in [Kle10a, Theorem 1.4] for matrices, is that the diophantine exponent of a random point is also the worst diophantine exponent of any point on the submanifold. In the context of matrices, one needs to find the right replacement for the affine span. We show the following:

Theorem 1.4 (Inheritance from Plücker closure). *Let \mathcal{M} be a connected analytic submanifold of $M_{m,m+n}(\mathbb{R})$. The generic value of the diophantine exponent $\beta(x)$ depends only on the Plücker closure $\mathcal{H}(\mathcal{M})$ of \mathcal{M} . In particular it depends only on the Zariski closure of \mathcal{M} in $M_{m,m+n}(\mathbb{R})$. Moreover for Lebesgue almost every point $x \in \mathcal{M}$*

$$\beta(x) = \inf_{y \in \mathcal{M}} \beta(y) \tag{1.4}$$

The existence of a generic value for $\beta(x)$, which is the same for almost every point x of \mathcal{M} , and the identity (1.4) are due to Kleinbock [Kle10a, Theorem 1.4.a]. When we say that the generic exponent depends only on the Plücker or on the Zariski closure of \mathcal{M} , this means in particular that the generic value of the exponent of a random point of $\mathcal{H}(\mathcal{M})$ or of the Zariski closure of \mathcal{M} (considered with respect to the Lebesgue measure on these algebraic varieties) coincides with that of \mathcal{M} .

The Plücker closure of a subset S in $M_{m,m+n}(\mathbb{R})$ is the set of all matrices x whose full list of minors satisfy the same linear equations as those of S . It contains the Zariski closure of S and is contained in the Schubert closure of S , namely the intersection of all pencils containing S . See §5.2.

Theorem 1.4 has been established independently in the recent work of Das, Fishman, Simmons and Urbanski, see [DFSU15, Theorem 1.9]. In this work the authors introduce a very general class of measures, which is invariant under measure automorphisms and encompasses many fractal measures of dynamical origin, for which Theorem 1.4 is shown to hold, see the discussion after [DFSU15, Definition 1.2].

Our Theorems 1.2 and 1.5 will be proved in Section 5 for a smaller class of measures on $\text{Hom}(V, E)$ (still more general than Lebesgue measure on analytic submanifolds), which we call *locally good measures* and are basically the matrix analogue of the friendly measures introduced by Kleinbock, Lindenstrauss and Weiss in [KLW04].

We also stress that all of our results will be proved for submanifolds of $\text{Hom}(V, E)$, where V and E are finite-dimensional real vector spaces of arbitrary dimension (we will not assume $\dim V > \dim E$ as in this introduction).

We further show the following general inequality:

Theorem 1.5 (Bounds for the exponent). *Let \mathcal{M} be a connected analytic submanifold of $M_{m,m+n}(\mathbb{R})$. Then for almost every $x \in \mathcal{M}$ with respect to Lebesgue measure:*

$$\max_{\mathcal{M} \subset \mathcal{P}_{W,r}; W \text{ rational}} \left\{ \frac{\dim W}{r} - 1 \right\} \leq \beta(x) \leq \max_{\mathcal{M} \subset \mathcal{P}_{W,r}} \left\{ \frac{\dim W}{r} - 1 \right\}. \quad (1.5)$$

The maximum is taken over rational pencils on the left-hand side and arbitrary pencils on the right-hand side. In particular:

Corollary 1.6. *If \mathcal{M} is not contained in any constraining pencil, then \mathcal{M} is extremal.*

When the Zariski closure is defined over \mathbb{Q} , Theorem 1.2 reduces the determination of the exponent to a purely algebraic question: determining the maximum in (1.3). This may still be a challenging task, however the analysis is greatly simplified by the following property of the pencils realizing the maximum in (1.3).

Proposition 1.7. *There is a unique subspace $W \leq \mathbb{R}^{m+n}$ of maximal dimension such that $\mathcal{M} \subset \mathcal{P}_{W,r}$ and*

$$\frac{\dim W}{r} = \max_{\mathcal{M} \subset \mathcal{P}_{W,r}} \frac{\dim W}{r}.$$

This fact is a consequence of a very general lemma, which we call the *submodularity lemma* and runs as follows.

Lemma 1.8 (Submodularity lemma). *Let V be a finite-dimensional vector space, and suppose that $\phi : \text{Grass}(V) \rightarrow \mathbb{N}$ is a non-decreasing (for set inclusion) and submodular function, i.e. for any two vector subspaces U and W we have*

$$\phi(U + W) + \phi(U \cap W) \leq \phi(U) + \phi(W).$$

Then the maximum

$$\max_{W \in \text{Grass}(V) \setminus \{0\}} \frac{\dim W}{\phi(W)}$$

is attained at a unique subspace of maximal dimension.

In particular this applies to the right-hand side in (1.5), because the function $W \mapsto \max_{x \in \mathcal{M}} \dim xW$ is submodular.

In presence of symmetry, this lemma greatly simplifies the algebraic analysis of determining the right-hand side in (1.5) and hence the exponent. Indeed if ϕ is G -invariant for the action of some group G on the grassmanian (preserving dimension), then the submodularity lemma implies that the subspace realizing the maximum is G -invariant. This observation is used to derive Theorem 1.2 from Theorem 1.5 by means of the Galois group action on V . Here is an example illustrating the use of the submodularity lemma for another group action in combination with Theorem 1.2 :

Example 1.9 (The Veronese manifold in matrices). Let $p, s \in \mathbb{N}$. What is the infimum $\widehat{\beta}$ of all $\beta > 0$ such that for almost every $M \in M_s(\mathbb{R})$, the inequality

$$\|v_0 I + v_1 M + \cdots + v_p M^p\| \leq \|v\|^{-\beta}$$

has at most finitely many integer solutions $v \in \mathbb{Z}^{p+1}$? The Mahler conjecture proved by Sprindžuk mentioned earlier is the case $s = 1$, and then the answer is $\widehat{\beta} = p$. When $s > 1$, this problem fits the diophantine approximation on submanifolds of matrices scheme: set $V = \mathbb{R}^{m+n} = \mathbb{R}_p[X]$ the space of polynomials of degree at most p . Naturally, \mathbb{Z}^{m+n} is identified with the lattice of polynomials with integer coefficients. Set $E = \mathbb{R}^m = M_s(\mathbb{R})$, and $\mathcal{M} \subset \text{Hom}(V, E) \simeq M_{m, m+n}(\mathbb{R})$ the set of all linear maps $P \mapsto P(M)$. In terms of matrices, \mathcal{M} is just the Veronese manifold $\{(I, M, \dots, M^p) ; M \in M_s(\mathbb{R})\}$. Using Theorem 1.2 the exponent $\widehat{\beta}$ can be determined once the pencils containing \mathcal{M} are determined. But the group G of affine transformations of the real line acts on V by substitution of the variable and preserves \mathcal{M} . So in order to compute the maximum in (1.2), we only need to consider G -invariant subspaces. This is easily done, and we find that

$$1 + \widehat{\beta} = \max\left\{\frac{p+1}{s}, 1\right\}.$$

In particular the Veronese manifold is extremal if and only if $s \geq p + 1$. In this example the most constraining pencil is given by the Cayley-Hamilton relation. See Example 6.2.2 for more details. See also [Kle10a, §3.3] and [DS16], where the Veronese manifold is considered with respect to a different diophantine approximation scheme, for which it is always extremal.

Of course when the Zariski closure is not defined over \mathbb{Q} , it can happen that the almost sure exponent is not given by either side of (1.5). Then the question remains to find an appropriate hull $S(\mathcal{M})$ of \mathcal{M} whose almost

sure exponent would be the same as that of \mathcal{M} , in the spirit of Kleinbock's work [Kle03] [Kle08b] on submanifolds of \mathbb{R}^n with irrational affine span. The natural candidate is what we call the Schubert closure of \mathcal{M} , which is the intersection of the pencils containing \mathcal{M} . It is an algebraic variety, which is in general bigger than the Zariski closure of \mathcal{M} . In the classical setting of submanifolds of $M_{m,n}(\mathbb{R})$ this is the same space as the space $\mathcal{H}(\mathcal{M})$ considered by Beresnevich, Kleinbock and Margulis in [BKM15, 7.2]. The Plücker closure considered here and in [DFSU15] is in general smaller than the Schubert closure.

The results above are a first stone in a more complete study of diophantine approximation on submanifolds of matrices that we do not undertake here and would be concerned with badly approximable points (such as in [Bak76, Kle98a]), improvements of Dirichlet's theorem (see [KW08]), Khintchine-type theorems (in the spirit of [BKM01, BBKM02]), Jarnik-type theorems, etc. Let us only mention that the methods introduced in the current paper also apply to the study of multiplicative diophantine approximation as in the original work of Kleinbock and Margulis [KM98]; in particular, one can derive a satisfying criterion for a manifold to be strongly extremal. This will be explained in a forthcoming paper of the first and last authors with Das and Simmons [BDSS].

In order to apply the above results to the computation of diophantine exponents of random subgroups of nilpotent Lie groups, it is necessary (in the general case) to extend them to the setting of *quasi-norms* and consider *weighted diophantine approximation*, in which different directions are assigned possibly different weights. We now briefly describe what this means, but later in the paper we will prove our results in this generalized setting.

As above $\mathcal{M} = \Phi(U)$ is a connected analytic submanifold of $\text{Hom}(V, E)$, where V and E are two finite-dimensional real vector spaces, $U \subset \mathbb{R}^N$ is a connected open set and $\Phi : U \rightarrow \text{Hom}(V, E)$ an analytic map. We endow V and E with quasi-norms, namely

$$|v| = \max |v_i|^{\frac{1}{\alpha_i}}$$

$$|w|' = \max |w_i|^{\frac{1}{\alpha'_i}},$$

for $v = \sum_i v_i u_i \in V$ and $w = \sum_i w_i u'_i \in E$, where (u_1, \dots, u_d) is a basis of V and (u'_1, \dots, u'_e) a basis of E , and $\alpha_1 \geq \dots \geq \alpha_d > 0$ and $\alpha'_1 \geq \dots \geq \alpha'_e > 0$ are positive numbers. Next we let Δ be the lattice $\mathbb{Z}u_1 + \dots + \mathbb{Z}u_d$ and we consider the following diophantine exponent for $x \in \text{Hom}(V, E)$

$$\beta(x) := \inf\{\beta > 0 \mid \exists c > 0 : \forall v \in \Delta \setminus \{0\}, |xv|' > c|v|^{-\beta}\}. \quad (1.6)$$

Given two non-negative numbers a, b , and a subspace W of V , we define (see Section 4.4) the *pencil*

$$\mathcal{P}_{W,a,b} = \{x \in \text{Hom}(V, E) \mid \psi(\ker x \cap W) \geq a \text{ and } \phi(xW) \leq b\},$$

where ψ (resp. ϕ) is defined for a subspace $W \leq V$ (resp. $W' \leq E$) by

$$\psi(W) = \sum_{i \in I(W)} \alpha_i \quad \text{and} \quad \phi(W') = \sum_{i \in J(W')} \alpha'_i,$$

and where

$$I(W) = \{i \in \{1, \dots, d\} \mid \dim(W \cap \langle u_1, \dots, u_i \rangle) > \dim(W \cap \langle u_1, \dots, u_{i-1} \rangle)\}$$

and

$$J(W') = \{i \in \{1, \dots, e\} \mid \dim(W' \cap \langle u'_{i+1}, \dots, u'_e \rangle) < \dim(W' \cap \langle u'_i, \dots, u'_e \rangle)\}.$$

The pencil $\mathcal{P}_{W,a,b}$ is a certain closed algebraic subset of $\text{Hom}(V, E)$ associated to our choice of quasi-norms on V and E , and coincides with the pencil defined in Definition 1.1 in the unweighted case. Pencils are indeed closely related to Schubert subvarieties of the grassmannian $\text{Grass}(V)$ (see Section 4.2).

Theorem 1.10 (Weighted case). *Theorems 1.2 and 1.5 hold more generally in the weighted (quasi-norm) setting. In particular for Lebesgue almost every $x \in U$,*

$$\max_{\mathcal{M} \subset \mathcal{P}_{W,a,b}; W \text{ rational}} \frac{a}{b} \leq \beta(\Phi(x)) \leq \max_{\mathcal{M} \subset \mathcal{P}_{W,a,b}} \frac{a}{b}. \quad (1.7)$$

with equality when the Zariski closure of \mathcal{M} is defined over \mathbb{Q} .

We refer the reader to Theorems 5.1 and 5.2 for more complete statements. The \mathbb{Q} -structure on $\text{Hom}(V, E)$ used implicitly in the above theorem is the one induced by the \mathbb{Q} -span of the bases of V and E chosen to define the quasi-norms. The condition that the Zariski closure of \mathcal{M} be defined over \mathbb{Q} is satisfied for example when the map Φ itself is a polynomial map with coefficients in \mathbb{Q} (i.e. each matrix entry is such).

The dynamical method adapts well to the weighted case, as had already been observed by Kleinbock early on, for example in [Kle98b].

*
* *

We now pass to the description of our results regarding diophantine approximation on nilpotent Lie groups. Inspired by the work of Gamburd, Jakobson and Sarnak [GJS99] we introduced in our previous paper [ABRdS15a] the notion of diophantine Lie group. We refer the reader to this paper for an introduction and background on the general question of diophantine approximation on Lie groups. We briefly recall here the basic definitions. We are given a connected Lie group G and a k -tuple of elements $\mathbf{g} := (g_1, \dots, g_k)$. We consider the subgroup $\Gamma_{\mathbf{g}}$ generated by g_1, \dots, g_k . Its elements can be represented by words $w(\mathbf{g})$ in the elements g_i . We ask: How close to the identity can an element γ of $\Gamma_{\mathbf{g}}$ be in terms of the minimal length $\ell(\gamma)$ of a word that represents it? The following definition is natural. Let $d(x, y)$ be a left-invariant Riemannian distance on G (or more generally a left-invariant geodesic metric) and let $V_{\mathbf{g}}(n)$ be the number of elements in $\Gamma_{\mathbf{g}}$ that can be represented by a word of length at most n .

Definition 1.11. The k -tuple $\mathbf{g} = (g_1, \dots, g_k) \in G^k$ (or the subgroup $\Gamma_{\mathbf{g}}$ they generate) is called *diophantine* if there exists $\beta > 0$ such that

$$d(\gamma, 1) > V_{\mathbf{g}}(\ell(\gamma))^{-\beta} \quad (1.8)$$

for all but at most finitely many group elements $\gamma \in \Gamma_{\mathbf{g}}$.

For example in $G = (\mathbb{R}, +)$ the pair $\mathbf{g} = (1, \alpha)$ is diophantine if and only if α is a diophantine, i.e. non-Liouville, number. It is easy to check that this definition depends only on the subgroup $\Gamma_{\mathbf{g}}$ and not on the particular generating set \mathbf{g} , nor on the choice of metric. We say that the Lie group G is *diophantine on k -letters* if almost every k -tuple in G (chosen independently at random with respect to Haar measure) is diophantine. We say that it is *diophantine* if it is diophantine on k -letters for every $k \geq 1$. When $G = \mathbb{R}^n$, then $\Gamma_{\mathbf{g}}$ is diophantine if and only if the $n \times k$ matrix whose column vectors are g_1, \dots, g_k is diophantine in the sense that its diophantine exponent (defined as in (1.1)) is finite. Hence the connection with diophantine approximation on matrices.

It is conjectured that semisimple real Lie groups are diophantine. This conjecture is open already for the smallest Lie groups, such as $SO(3, \mathbb{R})$ (see [GHS⁺09, §6]). Remez-type inequalities [BG73] combined with the Borel Cantelli lemma only yield a superexponential lower bound $\exp(-C\ell(\gamma)^2)$ for Lebesgue almost every \mathbf{g} in a semisimple Lie group (see the work of Kaloshin and Rodnianski [KR01] who handled $SU(2)$ but the method is general). It is also already an open problem to show that the affine group $\text{Aff}(\mathbb{R})$ of the real line and the group of motions of the Euclidean plane $O(2) \times \mathbb{R}^2$ are diophantine. See the work of Varjú [Var14] for a very interesting recent result in this direction.

It is fairly easy to see that any nilpotent Lie group with a rational structure (for its Lie algebra) is diophantine, but in [ABRdS15a] we constructed examples (arising only in nilpotency class 6 and higher) of non-diophantine nilpotent Lie groups. They exist because of some particular feature of the representation theory of the general linear group GL_k on the free Lie algebra on k -letters: multiplicity for the s -th homogeneous part, $s \geq 6$.

For nilpotent Lie groups the growth function $V_{\mathbf{g}}(n)$ grows polynomially like n^τ with an integer exponent τ given by the Bass-Guivarc'h formula (see [Bas72, Gui73]), and therefore changing the generating set in $\Gamma_{\mathbf{g}}$ does not result in a change of the exponent β . So it makes sense to ask for the optimal β for which (1.8) holds. We call this the exponent of the subgroup $\Gamma_{\mathbf{g}}$. This is the quantity we study here, with the help of Theorem 1.2 and Lemma 1.8.

It turns out that the optimal exponent always exists.

Theorem 1.12 (Existence of the exponent). *Let G be a connected and simply connected nilpotent real Lie group endowed with a left-invariant geodesic metric d . Then for each $k \geq 1$, there is $\widehat{\beta}_k \in [0, +\infty]$ such that for almost every k -tuple $\mathbf{g} \in G^k$ with respect to Haar measure, we have*

$$\beta(\mathbf{g}) = \widehat{\beta}_k,$$

where $\beta(\mathbf{g})$ is the infimum of all $\beta > 0$ such that (1.8) holds.

While the property of being diophantine or not for a k -generated subgroup of G does not depend on the choice of metric near the identity, the exponent does. By a geodesic metric (a.k.a length metric) we mean a distance that is defined in terms of the length of the shortest path between two points. It is well known that left-invariant geodesic metrics on connected Lie groups are all Carnot-Carathéodory-Finsler metrics induced by a norm on a generating subspace of the Lie algebra (this is Berestowski's theorem,

[Ber88]). Riemannian metrics are of course examples of such, but in the context of nilpotent Lie groups non Riemannian, Carnot-Carathéodory metrics are also very natural.

We will present two proofs of Theorem 1.12. The first is only valid when $k \geq \dim G/[G, G]$, and is based on a relatively simple general argument that relies on the ergodicity of the action of the group of automorphisms of the free Lie algebra on k -tuples of elements in \mathfrak{g} . The second proof on the other hand works for all k and necessitates to first translate the diophantine problem in terms of (weighted) diophantine approximation on submanifolds of matrices, and then use the techniques of homogeneous dynamics alluded above.

This translation will allow us to determine $\widehat{\beta}_k$ for all rational nilpotent Lie groups endowed with a rational left-invariant geodesic metric (e.g. a Riemannian metric, see §7.3 for the definition). Our main result is the following:

Theorem 1.13 (Rationality and stability of the exponent). *Let G be a connected and simply connected rational nilpotent real Lie group endowed with a rational left-invariant geodesic metric. Then for every $k \geq 1$ the exponent $\widehat{\beta}_k$ is rational. Furthermore, there exist an integer k_1 and a rational function $F_{\mathfrak{g}} \in \mathbb{Q}(X)$ with rational coefficients such that, for all $k \geq k_1$,*

$$\widehat{\beta}_k = F_{\mathfrak{g}}(k).$$

The rational function $F_{\mathfrak{g}}(X)$ is a ratio $\frac{P}{Q}$, where P and Q are both polynomials of the same degree with rational coefficients. The degree is equal to the nilpotency class of G .

The constant k_1 will be shown to depend only on $\dim \mathfrak{g}$. The value of $\widehat{\beta}_k$ for small k may not fit the general pattern $F_{\mathfrak{g}}(k)$. The fact that it does for k large is an instance of the so-called *representation stability*, as per the notion investigated by Church, Ellenberg and Farb in a series of recent papers. Here stability occurs for the action of GL_k on the free Lie algebra on k -letters, see [CF13, Corollary 5.7] for the case of interest to us.

In [ABRdS15a] we showed that a nilpotent Lie group G with Lie algebra \mathfrak{g} is diophantine on k -letters if and only if its Lie algebra of laws on k -letters $\mathcal{L}_{k,\mathfrak{g}}$ is a diophantine subspace of the free Lie algebra \mathcal{F}_k on k -letters endowed with its natural \mathbb{Q} -structure. A law of \mathfrak{g} is an element of the free Lie algebra that vanishes identically when the indeterminates are replaced with arbitrary elements of \mathfrak{g} .

The rational function $F_{\mathfrak{g}}(k)$ can be computed explicitly in terms of \mathfrak{g} and the representation theory of the GL_k -action by linear substitutions on the relatively free Lie algebra $\mathcal{F}_k/\mathcal{L}_{k,\mathfrak{g}}$. In Sections 7 and 8 we will give exact formulas in a number of examples. In particular, we compute $\widehat{\beta}_k$ for metabelian groups, for the group of unipotent upper-triangular matrices and for certain free nilpotent groups.

In [ABRdS15a, §5.2] we asked whether $\widehat{\beta}_k$ has a limit as k tends to infinity. With the above tools it is possible to answer this question, in the case where the nilpotent Lie group G is rational.

Corollary 1.14 (Rational limit). *Under the assumptions of the previous theorem*

$$\lim_{k \rightarrow +\infty} \widehat{\beta}_k$$

exists and is a rational number contained in the interval $[\frac{1}{s \dim G^{(s)}}, 1]$ (if $d(\cdot, \cdot)$ is Riemannian, the lower bound is $\frac{1}{\dim G^{(s)}}$).

Here $G^{(s)}$ is the last step in the descending central series of G .

Although we again make the assumption here that the Lie algebra \mathfrak{g} is defined over \mathbb{Q} , we believe that the above limit is always rational without such a rationality assumption, provided of course that G is diophantine:

Conjecture 1.15 (Rationality conjecture). *Suppose G is a connected nilpotent real Lie group endowed with a left-invariant geodesic metric. Assume that G is diophantine. Then the limit*

$$\lim_{k \rightarrow +\infty} \widehat{\beta}_k$$

exists and is a rational number.

Recall that G is said to be diophantine if it is diophantine on k -letters for every positive integer k . In [ABRdS15a] we constructed for each integer k a connected nilpotent Lie group that is diophantine on k letters, but not on $k + 1$ letters.

In order to apply the diophantine results for submanifolds of matrices expounded at the beginning of this introduction, we will apply Theorem 1.10 with $U = \mathfrak{g}^k$ and $V = \mathcal{F}_k / \mathcal{L}_{k, \mathfrak{g}}$, $E = \mathfrak{g}$ and $\Phi(x)$ the evaluation map at $x = (X_1, \dots, X_k) \in \mathfrak{g}^k$. The quasi-norm on V will be defined in terms of the descending central series of V and the parameters α_i will be integers. The choice of a left-invariant geodesic metric on G will yield a quasi-norm on E and Proposition 7.2.2 will show that the diophantine problem (1.8) translates precisely into (1.6). It turns out that the submodularity lemma is also of great help for this in the case of nilpotent groups. It will be used this time for the action of GL_k on $\mathcal{F}_k / \mathcal{L}_{k, \mathfrak{g}}$. This will mean that once the representation theory of $\mathcal{F}_k / \mathcal{L}_{k, \mathfrak{g}}$ viewed as a GL_k -module is understood well enough, the diophantine exponent can be computed. We will do just that in Section 8 for a number of concrete examples, for example for free nilpotent groups and for metabelian nilpotent groups.

Part of the results proved in this paper were announced in [ABRdS15b]. The paper is organized as follows. In Section 2 we give the first proof of Theorem 1.12 on the existence of the exponent via the ergodicity of the group of rational points of the group of automorphisms of the free Lie algebra acting on k -tuples. Section 3 is devoted to an important example, the Heisenberg group: we prove Theorem 1.13 for this group by an ad hoc argument using a Remez-type inequality for quadratic forms. The limitation of this method for tackling the more general nilpotent groups shows the power of the method used later on. Section 5 is devoted to the Kleinbock-Margulis method and the Dani correspondence, which allows to reformulate the diophantine approximation problem in terms of orbits in the space of

lattices. The proof of Theorem 5.1 is given in Section 5, and Theorem 5.2 is derived in Section 6, after the submodularity lemma. In Section 7 we give a second proof of Theorem 1.12 and establish the rationality of the exponent – Theorem 1.13 – in full generality using the diophantine approximation results for submanifolds of matrices developed in the previous sections. In Section 8 we compute the exponent explicitly in a number of examples using representation theory of the free Lie algebra.

Acknowledgements. It is a pleasure to thank V. Beresnevich and D. Kleinbock for interesting discussions in relation to the topics of this paper. We are also grateful to the referee for his comments. The first author acknowledges the support of ISEF, Advanced Research Grant 228304 from the ERC, and SNF Grant 200021-152819. The second author acknowledges support from ERC Grant no 617129 GeTeMo. The third author was supported by the Göran Gustafssons Stiftelse för Naturvetenskaplig och Medicinsk Forskning and Vetenskapsradet (grant no. 621-2011-5498).

2. A ZERO-ONE LAW

We now turn to the problem of diophantine approximation in nilpotent Lie groups. The purpose of this section is to show the existence of a critical exponent for any simply connected nilpotent real Lie group (not necessarily defined over \mathbb{Q}). Later, in Sections 3, 7 and 8, we will explain how to compute this exponent when the group is defined over the rationals.

In this section, G denotes an arbitrary connected simply connected nilpotent Lie group endowed with a left-invariant distance $d(\cdot, \cdot)$ inducing the topology. A finitely generated subgroup Γ of G will be called β -diophantine if there is a symmetric generating set S of Γ and a constant $c > 0$ such that for every integer n (recall that S^n denotes the set of products of n elements from S),

$$\min_{x \in S^n \setminus \{1\}} d(x, 1) \geq c \cdot |S^n|^{-\beta}. \quad (2.1)$$

By the Bass-Guivarc'h formula [Bas72, Gui73], we know that, within positive multiplicative constants, $|S^n| \simeq n^\tau$ for some integer τ depending on Γ only. It follows that if (2.1) holds for some generating set S , then it will also hold for any other generating set, possibly with a different constant c , but with the same β . We can therefore define the diophantine exponent $\beta(\Gamma)$ of a finitely generated subgroup of G by

$$\beta(\Gamma) = \inf\{\beta \mid \Gamma \text{ is } \beta\text{-diophantine}\}. \quad (2.2)$$

Theorem 2.1 (Zero-one law). *Let G be a simply connected nilpotent Lie group, whose abelianization has dimension d . Let $k \geq d$ be an integer. Given $\beta \geq 0$ the set of k -tuples $\mathbf{g} = (g_1, \dots, g_k)$ generating a group $\Gamma_{\mathbf{g}}$ that is β -diophantine is either null or co-null for the Haar measure on G^k .*

In particular, there is a number $\widehat{\beta}_k \in [0, +\infty]$ such that

$$\beta(\Gamma_{\mathbf{g}}) = \widehat{\beta}_k \quad \text{for almost every } k\text{-tuple } \mathbf{g} \in G^k.$$

This shows that Theorem 2.1 implies Theorem 1.12 from the introduction, in the case $k \geq d$. An alternative proof (including the cases $k < d$) will be given in Section 7. We record here the following open problems:

- (1) Is the set of k -tuples \mathbf{g} such that $\Gamma_{\mathbf{g}}$ is $\widehat{\beta}_k$ -diophantine null or co-null? Consistency with the case $G = \mathbb{R}$, where it is known that badly approximable tuples have zero measure, hints that the answer ought to be null, provided $k > \dim G/[G, G]$.
- (2) Is there a Jarník type theorem for k -tuples, i.e. a formula for the Hausdorff dimension of the set of k -tuples \mathbf{g} such that $\beta(\Gamma_{\mathbf{g}}) > \beta$ for any given β ?

The rest of this section is devoted to the proof of Theorem 2.1, which is based on an ergodicity argument.

2.1. Ergodic action on \mathfrak{g}^k by rational automorphisms. Let $\mathcal{F}_{k,s}$ be the free s -step nilpotent Lie algebra on k generators. The group $\text{Aut}(\mathcal{F}_{k,s})$ of linear automorphisms of $\mathcal{F}_{k,s}$ is an algebraic group defined over \mathbb{Q} . If $\alpha \in \text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ and x_1, \dots, x_k are free generators of $\mathcal{F}_{k,s}$, then for each $i = 1, \dots, k$, we let $\alpha_i = \alpha(x_i)$ and note that for every $r \in \mathcal{F}_{k,s}(\mathbb{R})$,

$$\alpha(r) = r(\alpha_1, \dots, \alpha_k)$$

Let \mathfrak{g} be an s -step nilpotent real Lie algebra. The group $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ acts on k -tuples \mathfrak{g}^k as follows:

$$\alpha \cdot (X_1, \dots, X_k) = (\alpha_1(X_1, \dots, X_k), \dots, \alpha_k(X_1, \dots, X_k)).$$

Note that this action is algebraic and preserves the measure class of the Lebesgue measure λ on \mathfrak{g}^k : For $g \in \text{Aut}(\mathcal{F}_{k,s})$, the pushforward $g_*\lambda$ is absolutely continuous with respect to λ , with density given by the Radon-Nikodym cocycle $c(g, \mathbf{X})$. Moreover, the Radon-Nikodym cocycle $c(g, \mathbf{X})$ is continuous in $(g, \mathbf{X}) \in \text{Aut}(\mathcal{F}_{k,s})(\mathbb{R}) \times \mathfrak{g}^k$. In fact $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ preserves the commutator ideal $[\mathcal{F}_{k,s}, \mathcal{F}_{k,s}]$ and thus acts on the quotient $\mathcal{F}_{k,s}/[\mathcal{F}_{k,s}, \mathcal{F}_{k,s}]$, which is isomorphic to \mathbb{R}^k . This yields a natural epimorphism from the group $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ onto $\text{GL}_k(\mathbb{R})$ with unipotent kernel; the cocycle is independent of \mathbf{X} and given by the determinant of the image of g under this epimorphism.

We are going to show:

Proposition 2.1.1 (Ergodic action by automorphisms). *If $k \geq \dim \mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]$, then the action of $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$ on \mathfrak{g}^k is ergodic.*

To prove this, we first recall:

Lemma 2.1.2. *Let G be a real Lie group, $H \leq G$ a closed subgroup and ν a quasi-invariant measure on G/H with continuous Radon-Nikodym cocycle. Then every dense subgroup of G acts ergodically on G/H .*

Proof. We need to show that if $f \in L^\infty(G/H)$ is invariant under a dense subgroup of G , then it is constant almost everywhere. Let $c : G \times G/H \rightarrow \mathbb{R}$ be the Radon-Nikodym cocycle, i.e. $\frac{d(g_*\nu)}{d\nu}(x) = c(g^{-1}, x)$. Then for every continuous and compactly supported function ϕ on G/H and every sequence of elements $g_n \in G$ converging to $g \in G$, the sequence of functions $x \mapsto \phi(g_n x)c(g_n, x)$ is uniformly converging to $\phi(gx)c(g, x)$ on G/H . It follows

that for every $f \in L^\infty(G/H)$, $\langle g_n f, \phi \rangle := \int_{G/H} f(g_n^{-1}x)\phi(x)d\nu(x)$ converges to $\langle gf, \phi \rangle$. Therefore, by duality, if $f \in L^\infty(G/H)$ is invariant under a dense subgroup of G , then for every $g \in G$ we have $gf = f$ almost everywhere. The measurable set $\Omega = \{(g, x) \in G \times G/H \mid f(g^{-1}x) \neq f(x)\}$ is such that every vertical fiber $\Omega_g := \{x \in G/H \mid f(g^{-1}x) \neq f(x)\}$ has ν -measure zero. By Fubini's theorem, Ω has measure zero, and ν -almost every horizontal fiber $\Omega^x = \{g \in G \mid f(g^{-1}x) \neq f(x)\}$ has measure zero. Fix x such that Ω^x has zero measure. The set $E = \{g^{-1} \cdot x \mid g \in G \setminus \Omega^x\}$ has full measure in G/H and f is constant on E . \square

Proof of Proposition 2.1.1. The group $\text{Aut}(\mathcal{F}_{k,s})$ is an algebraic group defined over \mathbb{Q} . Hence the group of \mathbb{Q} -points $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$ is dense in the group of \mathbb{R} -points $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ (in this case this can be checked directly on the reductive part, which is GL_k , and the unipotent part). Therefore it suffices to show that $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ admits a Zariski open orbit on \mathfrak{g}^k , when $k \geq d = \dim(\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}])$. Indeed, its complement will have Lebesgue measure zero, while the open orbit will be a homogeneous space G/H of $G := \text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ with Lebesgue measure coming from \mathfrak{g}^k as quasi-invariant measure. Lemma 2.1.2 then implies that $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$ acts ergodically.

To see that $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ admits a Zariski open orbit when $k \geq d$, observe that any two k -tuples \mathbf{X}, \mathbf{X}' of points in \mathfrak{g}^k with the property that their reductions modulo $[\mathfrak{g}, \mathfrak{g}]$ generate $\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]$ as a vector space must be in the same orbit of $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$. Indeed, since $k \geq d = \dim(\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}])$, we can find an element of $\text{GL}_k(\mathbb{R})$ such that $g\mathbf{X}$ and \mathbf{X}' have the same reduction modulo $[\mathfrak{g}, \mathfrak{g}]$. We can thus assume that $\mathbf{X}' - \mathbf{X}$ belongs to $[\mathfrak{g}, \mathfrak{g}]^k$. Now, the fact that the tuple $\mathbf{X} = (X_1, \dots, X_k)$ generates \mathfrak{g} modulo $[\mathfrak{g}, \mathfrak{g}]$ implies that every element of $[\mathfrak{g}, \mathfrak{g}]$ can be written as $\alpha(X_1, \dots, X_k)$ for some $\alpha \in [\mathcal{F}_{k,s}, \mathcal{F}_{k,s}]$. Therefore $\mathbf{X}' - \mathbf{X} = (\alpha_1(\mathbf{X}), \dots, \alpha_k(\mathbf{X}))$ for some $\alpha_i \in [\mathcal{F}_{k,s}, \mathcal{F}_{k,s}]$. But every endomorphism of $\mathcal{F}_{k,s}$ of the form $x_i \mapsto x_i + \alpha_i(x_1, \dots, x_k)$ with $\alpha_i \in [\mathcal{F}_{k,s}, \mathcal{F}_{k,s}]$ is invertible, hence belongs to $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ as desired.

To finish, simply note that when $k \geq d$, the set of k -tuples \mathbf{X} of points in \mathfrak{g}^k such that their reduction modulo $[\mathfrak{g}, \mathfrak{g}]$ spans $\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]$ is a non-empty Zariski open subset of \mathfrak{g}^k . \square

2.2. Critical exponent of a nilpotent Lie group. We will prove below Theorem 2.1. It will be a consequence of Proposition 2.1.1 and Proposition 2.2.1 below. In the statement of this proposition, we identify the connected and simply connected nilpotent Lie group G with its Lie algebra \mathfrak{g} via the exponential map $\exp : \mathfrak{g} \rightarrow G$, which is a diffeomorphism. This allows to view $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{R})$ as acting on G^k rather than \mathfrak{g}^k .

Proposition 2.2.1. *Given $\beta \geq 0$, the set of β -diophantine k -tuples in G^k is Lebesgue measurable and invariant under the action of $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$.*

Recall that two groups Γ and Γ' are *commensurable* if their intersection has finite-index in both Γ and Γ' . We divide the proof of Proposition 2.2.1 into two lemmas.

Lemma 2.2.2. *Let G be a simply connected nilpotent Lie group equipped with a left-invariant distance $d(\cdot, \cdot)$, and Γ a finitely generated subgroup of*

G. If Γ is β -diophantine, then any subgroup of G commensurable to Γ is also β -diophantine.

Proof. Let Γ be β -diophantine and Γ' commensurable to Γ . Then $\Gamma \cap \Gamma'$ has finite-index in Γ' and therefore, there exists a normal subgroup $\Gamma_0 < \Gamma \cap \Gamma'$ that has finite-index in Γ' . In particular, for some integer p , any element $\gamma \in \Gamma'$ has $\gamma^p \in \Gamma_0$. Moreover, Γ_0 is included in Γ , so it is β -diophantine. Let S and S_0 be symmetric generating sets for Γ' and Γ_0 , respectively. Since Γ_0 has finite index in Γ' , there exists a constant C such that for all integer $n \geq 1$, $\Gamma_0 \cap S^n \subset S_0^{Cn}$. Now suppose $\gamma \in \Gamma'$ is an element of $S^n \setminus \{1\}$. Then γ^p is an element of $\Gamma_0 \cap S^{pn}$ and therefore

$$\gamma^p \in S_0^{Cpn}.$$

Using that $|S_0^n|$ grows polynomially and the fact that Γ_0 is β -diophantine, this implies

$$d(\gamma^p, 1) \gg |S_0^n|^{-\beta},$$

where \gg means \geq up to a positive multiplicative constant, and in turn,

$$d(\gamma, 1) \geq \frac{1}{p} d(\gamma^p, 1) \gg |S_0^n|^{-\beta} \gg |S^n|^{-\beta}.$$

□

Our second lemma is as follows.

Lemma 2.2.3. *Let $\mathbf{X} := (X_1, \dots, X_k) \in \mathfrak{g}^k$, let $\alpha \in \text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$ and set $\mathbf{X}' := \alpha(\mathbf{X}) \in \mathfrak{g}^k$. Then the subgroup of G generated by e^{X_1}, \dots, e^{X_k} is commensurable to the subgroup generated by $e^{X'_1}, \dots, e^{X'_k}$.*

Proof. Recall that if $\gamma_1, \dots, \gamma_k$ generate a nilpotent group, then for every integer $n \geq 1$, the subgroup generated by the powers $\gamma_1^n, \dots, \gamma_k^n$ has finite index [Rag72, Lemma 4.4.]. By assumption, there is an integer N such that each NX'_i belongs to $\mathcal{F}_{k,s}(\mathbb{Z})(X_1, \dots, X_k)$, that is NX'_i is an integer linear combination of commutators in X_1, \dots, X_k . However recall [ABRdS15a, Lemma 3.5.] that there is an integer M such that $e^{Mr(X_1, \dots, X_k)}$ belongs to the subgroup generated by e^{X_1}, \dots, e^{X_k} for any $r \in \mathcal{F}_{k,s}(\mathbb{Z})$. It follows that each $(e^{X'_i})^{MN}$ belongs to the subgroup generated by e^{X_1}, \dots, e^{X_k} . Interchanging \mathbf{X} and \mathbf{X}' , the lemma follows. □

Proof of Proposition 2.2.1. It is clear from the definition that the subset of elements \mathfrak{g} such that $\Gamma_{\mathfrak{g}}$ is β -diophantine is a Borel subset. Now suppose that $\mathfrak{g} = (g_1, \dots, g_k)$ is such that $\Gamma_{\mathfrak{g}}$ is β -diophantine and let \mathfrak{g}' be in the $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$ -orbit of \mathfrak{g} . This means that $\log(\mathfrak{g})$ and $\log(\mathfrak{g}')$ are in the same $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$ -orbit. So Lemma 2.2.3 implies that $\Gamma_{\mathfrak{g}}$ and $\Gamma_{\mathfrak{g}'}$ are commensurable. Since $\Gamma_{\mathfrak{g}}$ is β -diophantine, it follows from Lemma 2.2.2 that $\Gamma_{\mathfrak{g}'}$ also is β -diophantine. □

Proof of Theorem 2.1. In view of Proposition 2.2.1, the set D_{β} of k -tuples such that $\Gamma_{\mathfrak{g}}$ is β -diophantine is measurable and invariant under the action of $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$. Since this action is ergodic by Proposition 2.1.1, we conclude that D_{β} is either null or conull. If $\widehat{\beta}_k$ denotes the infimum of all $\beta \geq 0$ for which D_{β} is conull, then D_{β} will be conull when $\beta > \widehat{\beta}_k$ and null if $\beta < \widehat{\beta}_k$. □

Remark 2.2.4. The property of being diophantine for a k -tuple \mathbf{g} does not depend only on the projection of \mathbf{g} on the abelianization of G . It is easy to construct examples showing that one may have two tuples \mathbf{g} and \mathbf{g}' such that $\mathbf{g} = \mathbf{g}'$ modulo $[G, G]$, but $\Gamma_{\mathbf{g}}$ is diophantine, while $\Gamma_{\mathbf{g}'}$ is not diophantine in G and $\Gamma_{\pi(\mathbf{g}')}$ is not diophantine in $G/[G, G]$ either, where π is the projection modulo $[G, G]$. In particular, $\text{Aut}(\mathcal{F}_{k,s})(\mathbb{Q})$ in Proposition 2.2.1 cannot be replaced by the subgroup $\text{GL}_k(\mathbb{Q})$.

Remark 2.2.5. In Theorem 2.1, the distance $d(\cdot, \cdot)$ is only assumed to be left-invariant, and need not be geodesic. The alternative argument given in Section 7, which is based on quantitative non-divergence, requires the distance to be geodesic (and hence a Carnot-Carathéodory-Finsler metric by [Ber88]).

3. CRITICAL EXPONENT FOR THE HEISENBERG GROUP

As a warm-up, we now present an explicit computation of the critical exponent of the 3-dimensional Heisenberg group. The method is elementary, using the Borel-Cantelli lemma combined with an ad-hoc Remez-type inequality for a certain family of quadratic forms (cf. Lemma 3.6 below). The relationship between this elementary method and the Kleinbock-Margulis type approach developed later in this paper will be discussed at the end of this section.

Here G will always denote the 3-dimensional Heisenberg group, consisting of 3×3 unipotent upper-triangular matrices. It will be convenient for us to view G as the space \mathbb{R}^3 , endowed with the group law

$$(x, y, z) * (x', y', z') = (x + x', y + y', z + z' + xy').$$

Recall the definition of the diophantine exponent of a finitely generated subgroup of G , made at the beginning of Section 2. We want to prove the following.

Theorem 3.1 (Critical exponent for the Heisenberg group). *Let $k \geq 2$. Then for almost every k -tuple $\mathbf{g} = (g_1, \dots, g_k)$ in G ,*

$$\beta(\Gamma_{\mathbf{g}}) = 1 - \frac{1}{k} - \frac{2}{k^2}.$$

The diophantine exponent here is computed with respect to any left-invariant Riemannian metric on G (equivalently for $\max\{|x|, |y|, |z|\}$). For the proof of Theorem 3.1, we will need a few definitions. Recall that if w is a word on k letters, i.e. an element of the free group F_k over k generators x_1, \dots, x_k , it induces a *word map*

$$w_G : \begin{array}{ccc} G^k & \rightarrow & G \\ (g_1, \dots, g_k) & \mapsto & w(g_1, \dots, g_k), \end{array}$$

where $w(g_1, \dots, g_k)$ is the element of G obtained by substituting each letter x_i by the element g_i . The group $F_{k,G}$ of word maps in k letters on G is defined to be the set of all such maps, with product law given by $w_G w'_G = (w w')_G$. The length $\ell(\omega)$ of a word map ω in $F_{k,G}$ is the minimal length of a word w such that $\omega = w_G$.

In the case of the Heisenberg group, one can describe the group of word maps very explicitly. For any two elements g and h in G , $[g, h]$ denotes the

commutator of g and h , defined by $[g, h] = ghg^{-1}h^{-1}$. The subgroup $[G, G]$ generated by commutators coincides with the center Z of G and is the set of elements $(0, 0, z)$, for $z \in \mathbb{R}$.

Proposition 3.2 (Word maps on the Heisenberg group). *Let $k \geq 2$. For each word map ω on k letters on G , there exist integers n_i , $1 \leq i \leq k$ and n_{ij} , $1 \leq i < j \leq k$ such that for all $\mathbf{g} = (g_1, \dots, g_k)$ in G^k ,*

$$\omega(\mathbf{g}) = g_1^{n_1} \dots g_k^{n_k} \prod_{1 \leq i < j \leq k} [g_i, g_j]^{n_{ij}}.$$

Moreover, the n_i and n_{ij} are uniquely determined by ω and there exists a constant $C > 0$ depending only on k such that

$$\frac{1}{C} \ell(\omega) \leq \max_{l, i, j} \{ |n_l|, |n_{ij}|^{\frac{1}{2}} \} \leq C \ell(\omega).$$

Proof. The existence of the n_i and n_{ij} is proved by elementary operations on a word representing ω , using that all commutators lie in the center of G , because G is 2-step nilpotent. To verify uniqueness, it suffices to show that no non-trivial family of integers n_l, n_{ij} yields the trivial word map; this can be checked directly, by expliciting the word maps in the (x, y, z) coordinates for G . The statement about the length of ω can also be proved directly, using the identity in G , $[g_i^n, g_j^m] = [g_i, g_j]^{nm}$. We leave the details to the reader. \square

We are now ready to prove the following theorem, which will easily imply Theorem 3.1.

Theorem 3.3. *Fix an integer $k \geq 3$.*

- *If $\alpha > k^2 - k - 2$, then for almost every k -tuple $\mathbf{g} \in G^k$, $d(\omega(\mathbf{g}), 1) \geq \ell(\omega)^{-\alpha}$ for all but finitely many $\omega \in F_{k,G}$.*
- *If $\alpha < k^2 - k - 2$, then for all $\mathbf{g} \in G^k$, there are infinitely many $\omega \in F_{k,G}$ for which $d(\omega(\mathbf{g}), 1) < \ell(\omega)^{-\alpha}$.*

We decompose the proof into two lemmas, studying first the word maps ω on G that are non-trivial modulo the center of G , i.e. those for which some n_i is non-zero.

Lemma 3.4 (Diophantine property outside the derived subgroup). *Let $k \geq 2$. If $\alpha > \frac{k}{2} - 1$, then for almost every k -tuple \mathbf{g} , we have $d(\omega(\mathbf{g}), 1) \geq \ell(\omega)^{-\alpha}$ for all but finitely many word maps ω that are non-trivial modulo the center of G .*

Proof. Suppose $\mathbf{g} = (g_1, \dots, g_k)$ is chosen at random in G^k according to the Haar measure on a compact subset. Then, the projection $\bar{\mathbf{g}} = (\bar{g}_1, \dots, \bar{g}_k)$ to $(G/Z)^k$ is a random k -tuple in $(G/Z)^k \simeq (\mathbb{R}^2)^k$, and its law is absolutely continuous with respect to the Lebesgue measure. By a standard application of the Borel-Cantelli lemma, we know that almost surely, if $\alpha > \frac{k}{2} - 1$, then

$$\|n_1 \bar{g}_1 + \dots + n_k \bar{g}_k\| \geq (\max |n_i|)^{-\alpha},$$

for all but finitely many (n_1, \dots, n_k) in \mathbb{Z}^k . This proves the lemma. \square

We now need to study word maps that are trivial modulo the center.

Lemma 3.5 (Diophantine property inside the derived subgroup). *Let $k \geq 2$. If $\alpha > k^2 - k - 2$, then for almost every k -tuple \mathbf{g} , we have $d(\omega(\mathbf{g}), 1) \geq \ell(\omega)^{-\alpha}$ for all but finitely word maps ω of the form $\omega : \mathbf{g} \mapsto \prod_{1 \leq i < j \leq k} [g_i, g_j]^{n_{ij}}$.*

Proof. Let $\omega : \mathbf{g} \mapsto \prod_{1 \leq i < j \leq k} [g_i, g_j]^{n_{ij}}$. In the (x, y, z) coordinates, the map ω is given by

$$\omega : \begin{array}{ccc} G^k & \rightarrow & G \\ (x_i, y_i, z_i)_{1 \leq i \leq k} & \mapsto & (0, 0, \sum_{1 \leq i < j \leq k} n_{ij}(x_i y_j - y_i x_j)) \end{array} .$$

If μ denotes the Lebesgue measure on the ball of radius 1 centered at 0 in G^k , Lemma 3.6 below implies that

$$\mu(\{\mathbf{g} \mid d(\omega(\mathbf{g}), 1) \leq \ell(\omega)^{-\alpha}\}) \leq \frac{2^{2k+1}}{\ell(\omega)^\alpha \max |n_{ij}|} (1 + \log(\ell(\omega)^\alpha \sqrt{2k} \max |n_{ij}|)).$$

However, by Lemma 3.2, $\ell(\omega) \simeq (\max |n_{ij}|)^{\frac{1}{2}} = \|n\|^{\frac{1}{2}}$, and therefore,

$$\mu(\{\mathbf{g} \mid d(\omega(\mathbf{g}), 1) \leq \ell(\omega)^{-\alpha}\}) \ll \frac{\log \|n\|}{\|n\|^{1+\frac{\alpha}{2}}}.$$

Since every word map trivial modulo the derived group corresponds to a unique $\frac{k(k-1)}{2}$ -tuple (n_{ij}) , we find

$$\sum_{\omega \equiv 0 \pmod{Z}} \mu(\{\mathbf{g} \mid d(\omega(\mathbf{g}), 1) \leq \ell(\omega)^{-\alpha}\}) \ll \sum_{(n_{ij}) \in \mathbb{Z}^{\frac{k(k-1)}{2}} - \{0\}} \frac{\log \|n\|}{\|n\|^{1+\frac{\alpha}{2}}} < \infty,$$

because $1 + \frac{\alpha}{2} > \frac{k(k-1)}{2}$. The lemma then follows from the Borel-Cantelli lemma. \square

We now state and prove the elementary lemma used in the above proof.

Lemma 3.6. *Let q be a quadratic form on \mathbb{R}^d , and assume that in some orthogonal basis, q can be expressed without squares as*

$$q(x) = \sum_{k < l} a_{kl} x_k x_l.$$

If μ denotes the Lebesgue measure on the ball of radius 1 centered at 0 in \mathbb{R}^d , then for all $\varepsilon > 0$

$$\mu(\{x \in \mathbb{R}^d \mid |q(x)| \leq \varepsilon\}) \leq \frac{2^{d+1} \varepsilon}{\max |a_{kl}|} \left(1 + \log^+ \left(\frac{\sqrt{d} \max |a_{kl}|}{\varepsilon} \right) \right),$$

where $\log^+ x = \max(0, \log x)$.

Proof. Choose k_0 and l_0 such that $|a_{k_0 l_0}| = \max_{k,l} |a_{kl}|$. As we may permute the indices, we may assume without loss of generality that $(k_0, l_0) = (1, 2)$. Then write

$$q(x) = x_1 \cdot \left(\sum_{l \geq 2} a_{1l} x_l \right) + y(x_2, \dots, x_d) = x_1 \langle x', a \rangle + y(x'),$$

where $x' = (x_2, \dots, x_d)$, $a = (a_{12}, \dots, a_{1d})$, and $\langle \cdot, \cdot \rangle$ denotes the usual inner product in \mathbb{R}^{d-1} . Let λ denote the Lebesgue measure on the real line. For

fixed (x_2, \dots, x_d) , observe that

$$\lambda(\{x_1 \in [-1, 1] \mid |x_1 \langle x', a \rangle - y(x')| \leq \epsilon\}) \leq 2 \min(1, \frac{\epsilon}{|\langle x', a \rangle|}).$$

Then write

$$\begin{aligned} \mu(\{x \in \mathbb{R}^d \mid q(x) \leq \epsilon\}) &\leq \int_{B_{\mathbb{R}^{d-1}}(0,1)} \lambda(\{x_1 \in [-1, 1]; |x_1 \langle x', a \rangle - y(x')| \leq \epsilon\}) dx' \\ &\leq 2 \int_{B_{\mathbb{R}^{d-1}}(0,1)} \min(1, \frac{\epsilon}{|\langle a, x' \rangle|}) dx' \\ &\leq 2^d \int_{-1}^1 \min\left(1, \frac{\epsilon}{\|a\|t}\right) dt \\ &= \frac{2^{d+1}\epsilon}{\|a\|} \left(1 + \log^+ \frac{\|a\|}{\epsilon}\right). \end{aligned}$$

Since $\max |a_{kl}| \leq \|a\| \leq \sqrt{d} \max |a_{kl}|$, we find

$$\mu(\{x \in \mathbb{R}^d \mid q(x) \leq \epsilon\}) \leq \frac{2^{d+1}\epsilon}{\max |a_{kl}|} \left(1 + \log^+ \frac{\sqrt{d} \max |a_{kl}|}{\epsilon}\right).$$

□

We can now conclude the proofs of Theorems 3.3 and 3.1.

Proof of Theorem 3.3. The first assertion follows from combining Lemmas 3.4 and 3.5, noting also that for $k \geq 2$, one has $\frac{k}{2} - 1 \leq k^2 - k - 2$.

For the second assertion, we note we have $k(k-1)/2$ commutators $[g_i, g_j]$ lying in $Z \simeq \mathbb{R}$. Therefore, given a positive integer n , Dirichlet's pigeonhole argument shows that there exist integers n_{ij} , $1 \leq i < j \leq k$ such that $|n_{ij}| \leq n^2$ and

$$\left| \sum_{i < j} n_{ij} [g_i, g_j] \right| \leq C n^{-k^2+k+2},$$

where C is a constant depending only on \mathbf{g} . Thus, for the word map $\omega : \mathbf{g} \mapsto \prod_{i < j} [g_i, g_j]^{n_{ij}}$, we get

$$d(\omega(\mathbf{g}), 1) \leq C \ell(\omega)^{-k^2+k+2}.$$

□

Proof of Theorem 3.1. By Proposition 3.2, the number of word maps of length at most n is bounded above and below by a positive constant times $n^{k+2\frac{k(k-1)}{2}} = n^{k^2}$. However, we know from [ABRdS15a, Lemma 2.5] that, for almost every k -tuple \mathbf{g} , the group $\Gamma_{\mathbf{g}}$ is isomorphic to $F_{k,G}$, so that, if $V_{\mathbf{g}}(n)$ denotes the number of elements in the ball of radius n with respect to the generating set \mathbf{g} , there exist positive constants c_1, c_2 such that

$$c_1 n^{k^2} \leq V_{\mathbf{g}}(n) \leq c_2 n^{k^2}.$$

Together with Theorem 3.3, this shows that for almost every k -tuple \mathbf{g} ,

$$\beta(\Gamma_{\mathbf{g}}) = \frac{k^2 - k - 2}{k^2} = 1 - \frac{1}{k} - \frac{2}{k^2}.$$

□

Remark 3.0.6. Let

$$\begin{aligned} \varphi : G^k &\rightarrow \mathbb{R}^{\frac{k(k-1)}{2}} \\ (x_i, y_i, z_i) &\mapsto (x_i y_j - y_i x_j)_{1 \leq i < j \leq k} \end{aligned}$$

Lemma 3.5 is equivalent to saying that the pushforward under φ of the Haar measure on (a ball of) G^k is extremal. So an alternative proof consists in using the Kleinbock-Margulis theorem [KM98, Theorem A]: all one is left to check is that the image of φ is not contained in a hyperplane.

In the rest of this paper, this will be our approach to compute the critical exponent of an arbitrary connected simply connected rational nilpotent Lie group. Clearly there is little hope to use a direct elementary approach in the spirit of Lemma 3.5 to handle general nilpotent groups. We will reduce the problem to studying the extremality of certain maps from G^k to G . If the target space of these maps were one-dimensional, the Kleinbock-Margulis theory would in general be enough. However this is typically not the case and one is thus naturally led to develop a suitable matrix analogue of their theory, which is what we do in the next two sections. The translation to a problem about (weighted) diophantine approximation on submanifolds of matrices is expounded in Section 7.

4. QUASI-NORMS, SCHUBERT CELLS, AND PENCILS

The main goal of the next three sections is to establish Theorems 1.2 and 1.5 from the introduction, which address a problem raised by Kleinbock and Margulis in [KM98, 6.2] and studied in [KMW10] and [BKM15]. The proof will be split into two parts, which correspond to Sections 5 and 6, respectively. First, the upper bound and the fact that the almost sure exponent depends only on the Zariski closure will be proved as Theorem 5.3.1 below, which is a consequence of the quantitative non-divergence estimates on the space of lattices, and the proof will be given in the slightly more general setup of locally good measures. Second, we shall show that equality holds when the Zariski closure is defined over \mathbb{Q} . This will be Theorem 6.2.1, and will be obtained as a consequence of the *submodularity lemma* proved in Section 6. In the present section, we describe the geometric objects involved in our diophantine problem, and explain what Dirichlet's pigeonhole argument, giving the lower bound on the exponent, becomes in this general setting.

As before, V and E are two finite-dimensional real vector spaces, and Δ is a lattice in V . Given a measure ν (say a probability measure) on $\text{Hom}(V, E)$, we want to study the diophantine properties with respect to Δ of a random point x in $\text{Hom}(V, E)$ chosen according to the distribution ν . For the application to nilpotent groups that we develop in Section 7, we need to compute the diophantine exponent of an element x in $\text{Hom}(V, E)$, which is defined in terms of certain quasi-norms on V and E .

Definition 4.1. A *quasi-norm* (resp. *local quasi-norm*) on V is a map $V \rightarrow \mathbb{R}_+$, $v \mapsto |v|$, for which there exist $C > 0$, a basis u_1, \dots, u_d of V and positive real numbers $\alpha_1, \dots, \alpha_d$ such that

$$\frac{1}{C}|v| \leq \max_{1 \leq i \leq d} |u_i^*(v)|^{1/\alpha_i} \leq C|v| \quad (4.1)$$

outside a neighborhood of the origin (resp. in a neighborhood of the origin), where u_1^*, \dots, u_d^* is the dual basis.

Given a quasi-norm $|\cdot|$ on V and a local quasi-norm $|\cdot|'$ on E , we define the *diophantine exponent* of x in $\text{Hom}(V, E)$ by

$$\beta(x) = \inf\{\beta > 0 \mid \exists c > 0 : \forall v \in \Delta \setminus \{0\}, |x(v)|' \geq c|v|^{-\beta}\}. \quad (4.2)$$

Remark 4.0.7. At a first reading it is fair to assume that $|\cdot|$ and $|\cdot|'$ are chosen to be genuine norms on V and E .

4.1. Quasi-norms and local quasi-norms. For later use, we now record some elementary properties of quasi-norms and local quasi-norms. We say that two quasi-norms (resp. local quasi-norms) are *comparable* (or *equivalent*) if their ratio is bounded and bounded away from zero outside a neighborhood of the origin (resp. in a neighborhood of the origin). Let V and E be real vector spaces of respective dimension d and e , and fix $|\cdot|$ a quasi-norm on V and $|\cdot|'$ a local quasi-norm on E . As in Definition 4.1, we fix bases $(u_i)_{1 \leq i \leq d}$ and $(u'_i)_{1 \leq i \leq e}$ for V and E , together with positive real numbers $\alpha_1, \dots, \alpha_d$ and $\alpha'_1, \dots, \alpha'_e$ such that

$$\frac{1}{C}|v| \leq \max_{1 \leq i \leq d} |u_i^*(v)|^{1/\alpha_i} \leq C|v|$$

outside a neighborhood of 0 in V , and

$$\frac{1}{C}|v|' \leq \max_{1 \leq i \leq e} |u_i'^*(v)|^{1/\alpha'_i} \leq C|v|'$$

in a neighborhood of 0 in E .

1. If we reorder the vectors u_i so that $\alpha_1 \geq \dots \geq \alpha_d > 0$ and let $V_i = \langle u_1, \dots, u_{i-1} \rangle$, we obtain a full flag $0 = V_1 < V_2 < \dots < V_d < V$, and $|v|$ is comparable to

$$\max_{1 \leq i \leq d} d(v, V_i)^{\frac{1}{\alpha_i}}, \quad (4.3)$$

where $d(v, V_i)$ is the distance to V_i in some fixed Euclidean structure on V . Similarly, if $\alpha'_1 \geq \dots \geq \alpha'_e > 0$, then $|v|'$ is comparable to

$$\max_{1 \leq i \leq e} d(v, V_i')^{\frac{1}{\alpha'_i}}, \quad (4.4)$$

where $V_i' = \langle u'_{i+1}, \dots, u'_e \rangle$. For the rest of the paper, we assume that $\alpha_1 \geq \dots \geq \alpha_d$ and $\alpha'_1 \geq \dots \geq \alpha'_e$.

2. (subspace) If $W \leq V$ is a subspace, then the restriction of $|\cdot|$ to W is a quasi-norm, associated to the flag $0 = V_1 \cap W \leq \dots \leq V_d \cap W \leq W$ in the sense that $|w|$ is comparable to

$$\max_{1 \leq i \leq d} d(w, V_i \cap W)^{1/\alpha_i},$$

when $w \in W$. This is easily seen, since $d(w, W \cap V_i)$ is comparable to $d(w, V_i)$ when w varies in W . Similarly, the restriction of $|\cdot|'$ to a subspace F in E is a local quasi-norm, associated to the flag $0 = V_e' \cap F \leq \dots \leq V_1' \cap F \leq F$.

3. (quotient) If $W \leq V$ is a subspace, then $|\cdot|$ induces a quasi-norm on V/W by setting, for $\bar{v} := v \bmod W$,

$$|\bar{v}| := \inf_{w \in W} |v + w|.$$

It is easy to see that this indeed defines a quasi-norm V/W . It is associated to the flag $\{V_i/(V_i \cap W)\}$ of V/W , in the sense that it is comparable to

$$\max_{1 \leq i \leq d} d(\bar{v}, V_i/(V_i \cap W))^{1/\alpha_i},$$

where $V_i/(V_i \cap W) \leq V/W$. To see this, note that W has an adapted complement, namely a subspace W' such that $(W \cap V_i) \oplus (W' \cap V_i) = V_i$ for every $i = 1, \dots, d$, and that $|\bar{v}|$ is comparable to the restriction of $|v|$ to W' .

4. (triangle inequality) There is $C > 0$ such that

$$|v + w| \leq C(|v| + |w|)$$

for every v, w in V outside a neighborhood of the origin in V , and

$$|v + w|' \leq C(|v|' + |w|')$$

for every v, w inside a neighborhood of the origin in E .

5. (volume of large balls) From the quasi-norm $|\cdot|$ on V , we define a function $\psi : \text{Grass}(V) \rightarrow \mathbb{R}_+$ by

$$\psi(W) = \sum_{i \in I(W)} \alpha_i,$$

where

$$I(W) = \{i \in \{1, \dots, d\} \mid \dim(V_{i+1} \cap W) = \dim(V_i \cap W) + 1\},$$

with the convention that $V_{d+1} = V$ and $\alpha_{d+1} = 0$. Clearly ψ is non-decreasing because I is. Moreover $-\psi$ is submodular (cf. Lemma 6.1.2). This is easily seen, since reorganizing the sum yields

$$\psi(W) = \sum_{i=1}^d (\alpha_i - \alpha_{i+1}) \dim(V_{i+1} \cap W), \quad (4.5)$$

and $\alpha_i \geq \alpha_{i+1}$. Moreover, ψ determines the volume of the ball of radius Q restricted to W : for all $Q > 1$,

$$\text{vol}\{w \in W \mid |w| \leq Q\} \simeq Q^{\psi(W)}.$$

Here and hereafter, we write $x \simeq y$ if there exist positive constants $c, C > 0$ such that $cx \leq y \leq Cx$. The constants c and C are allowed to depend on W and $|\cdot|$, but *not* on Q . Note also that if W' is an adapted complement to W in V , then

$$I(W') = \{1, \dots, d\} \setminus I(W) = \{i \in \{1, \dots, d\} \mid \dim(\frac{V_{i+1}}{V_{i+1} \cap W}) = \dim(\frac{V_i}{V_i \cap W}) + 1\},$$

and hence $\psi(W') = \psi(V) - \psi(W)$ and

$$\text{vol}\{\bar{v} \in V/W \mid |\bar{v}| \leq Q\} \simeq Q^{\psi(V) - \psi(W)}.$$

6. (volume of small balls) We also define a function $\phi : \text{Grass}(E) \rightarrow \mathbb{R}_+$ by

$$\phi(F) = \sum_{i \in J(F)} \alpha'_i,$$

where

$$J(F) = \{i \in \{1, \dots, e\} \mid \dim(V'_i \cap F) = \dim(V'_{i-1} \cap F) - 1\},$$

with the convention that $V'_0 = E$. Then ϕ is non-decreasing (because J is) and submodular (cf. Lemma 6.1.2). This is easily seen, since $\alpha'_i \geq \alpha'_{i+1}$, and reorganizing the sum yields

$$\phi(F) = \sum_{i=1}^e (\alpha'_i - \alpha'_{i+1}) (\dim F - \dim(V'_i \cap F)). \quad (4.6)$$

Moreover, ϕ determines the volume of the ball of radius ε restricted to F : within multiplicative constants (depending on F and $|\cdot|'$ only), for all $\varepsilon \in (0, 1)$,

$$\text{vol}\{w \in F \mid |w|' \leq \varepsilon\} \simeq \varepsilon^{\phi(F)}.$$

4.2. Schubert varieties. Schubert varieties are certain distinguished closed algebraic subsets of the Grassmannian. See [GH94] for the complex case and [BCR98] for the real case. In this subsection we briefly recall their definition, because the pencils defined in the introduction give rise to Schubert varieties via the map $x \mapsto \ker x$ and because they will appear in the definition of locally good measures below.

As before V is a d -dimensional real vector space and $0 = V_1 < V_2 < \dots < V_d < V_{d+1} = V$ is a full flag of subspaces. Let n be an integer with $1 \leq n \leq d$ and let $\sigma = (\sigma_1, \dots, \sigma_n)$ be a sequence of integers such that $1 \leq \sigma_1 < \sigma_2 < \dots < \sigma_n \leq d$. Let $\text{Grass}_n(V)$ be the Grassmannian of n -dimensional subspaces of V . Recall that $\text{Grass}_n(V)$ can be realized as a closed (affine) algebraic subset of $M_{d,d}(\mathbb{R})$ by assigning to each subspace the orthogonal projection onto it. The *Schubert cell* of type σ associated to the full flag $\{V_i\}_i$ is the subset $e(\sigma)$ of all subspaces W in $\text{Grass}_n(V)$ such that $\dim(V_{\sigma_i+1} \cap W) = \dim(V_{\sigma_i} \cap W) + 1$ for each $i = 1, \dots, n$, or equivalently in the notation of the previous subsection, such that $I(W) = \{\sigma_1, \dots, \sigma_n\}$.

The cell $e(\sigma)$ is a subset of $\text{Grass}_n(V)$, and it is easy to see that its closure is a union of other cells, namely:

$$\overline{e(\sigma)} = \bigcup_{\tau \leq \sigma} e(\tau),$$

where we define the partial order $\tau \leq \sigma$ by requiring that $\tau_i \leq \sigma_i$ for each $i = 1, \dots, n$. This closure $\overline{e(\sigma)}$ is called the *Schubert variety* of type σ .

It is worth mentioning that subsets of the form $\{W \in \text{Grass}_n(V); \dim(W \cap V_j) \geq i\}$ for some indices i, j are Schubert subvarieties and that the Schubert subvarieties associated to the full flag $\{V_i\}_i$ are precisely the intersections of subsets of this form.

Note that $\dim(W \cap V_j) \geq i$ if and only if the family of vectors obtained by projecting a fixed basis of V_j onto the orthogonal complement of W has rank $< j - i$. In particular this subset of the Grassmannian is a closed algebraic

subset and hence so are all Schubert subvarieties. Moreover the Schubert cell $e(\sigma)$ is Zariski open (and dense) in the Schubert subvariety $\overline{e(\sigma)}$.

4.3. Dirichlet's principle. As before, V and E are real vector spaces of respective dimensions d and e , and Δ is a lattice in V . We fix a quasi-norm $|\cdot|$ on V associated to a full flag $0 = V_1 < V_2 < \dots < V_d < V$ and a d -tuple $\alpha_1 \geq \dots \geq \alpha_d > 0$ via (4.3), and a local quasi-norm $|\cdot|'$ on E defined by (4.4) using a decreasing full flag $E > V'_1 > V'_2 > \dots > V'_e = 0$ and an e -tuple $\alpha'_1 \geq \dots \geq \alpha'_e > 0$. To this data are associated the volume exponents functions $\psi : \text{Grass}(V) \rightarrow \mathbb{R}_+$ and $\phi : \text{Grass}(E) \rightarrow \mathbb{R}_+$ defined in points 5. and 6. of the Subsection 4.1.

Recall that the diophantine exponent of a homomorphism $x \in \text{Hom}(V, E)$ with respect to these quasi-norms is defined by

$$\beta(x) = \inf\{\beta > 0 \mid \exists c > 0 : \forall v \in \Delta \setminus \{0\}, |xv|' \geq c|v|^{-\beta}\}. \quad (4.7)$$

A subspace $W \leq V$ is called Δ -rational if $W \cap \Delta$ is a lattice in W .

Proposition 4.3.1 (Dirichlet's principle). *For every $x \in \text{Hom}(V, E)$ and every Δ -rational subspace $W \leq V$,*

$$\beta(x) \geq \frac{\psi(W \cap \ker x)}{\phi(xW)}.$$

Proof. This is a version of the classical Dirichlet argument using the pigeon-hole principle. If Q is a large parameter, the ball of radius Q in W for the quasi-norm $|\cdot|$ contains roughly (up to multiplicative constants) $Q^{\psi(W)}$ points of Δ , which are mapped to a ball in xW (for the quotient quasi-norm on $xV \simeq V/\ker x$) of volume $Q^{\psi(W) - \psi(W \cap \ker x)}$. On the other hand, the volume of a ball of radius ε for the restriction of $|\cdot|'$ to $xW \leq E$ is comparable to $\varepsilon^{\phi(xW)}$. Using the triangle inequality 4. from the previous subsection, we see that not all ε -balls in xW around the images of $Q^{\psi(W)}$ integer points can be disjoint if $\varepsilon^{\phi(xW)} Q^{\psi(W)} \gg Q^{\psi(W) - \psi(W \cap \ker x)}$. The proposition follows. \square

Remark 4.3.2. Anticipating the next sections, we note here that given any $x \in \text{Hom}(V, E)$, the maps $W \mapsto -\psi(W \cap \ker x)$ and $W \mapsto \phi(xW)$ are both submodular (see §6.1). This is formal from the submodularity of $-\psi$ and ϕ . Also they are non-increasing and non-decreasing respectively for set inclusion. So the hypotheses of the submodularity lemma (Lemma 6.1.2) are fulfilled.

4.4. Pencils. Given two non-negative numbers a, b , and a subspace W of V , we define the *pencil* $\mathcal{P}_{W,a,b}$ associated to our choice of quasi-norms on V and E to be the algebraic subset

$$\mathcal{P}_{W,a,b} = \{x \in \text{Hom}(V, E) \mid \psi(\ker x \cap W) \geq a \text{ and } \phi(xW) \leq b\},$$

where ψ (resp. ϕ) is defined for a subspace $W \leq V$ (resp. $W' \leq E$) by

$$\psi(W) = \sum_{i \in I(W)} \alpha_i \quad \text{and} \quad \phi(W') = \sum_{i \in J(W')} \alpha'_i,$$

where as before

$$I(W) = \{i \in \{1, \dots, d\} \mid \dim(W \cap \langle u_1, \dots, u_i \rangle) > \dim(W \cap \langle u_1, \dots, u_{i-1} \rangle)\}$$

and

$$J(W') = \{i \in \{1, \dots, e\} \mid \dim(W' \cap \langle u'_{i+1}, \dots, u'_e \rangle) < \dim(W' \cap \langle u'_i, \dots, u'_e \rangle)\}.$$

We easily see that pencils are closed algebraic subvarieties of $\text{Hom}(V, E)$. Moreover $\{\ker x \mid x \in \mathcal{P}_{W,a,b}, \dim \ker x = k\}$ is a Schubert subvariety of $\text{Grass}_k(V)$ (see §4.2).

For an irreducible closed algebraic subset \mathcal{M} in $\text{Hom}(V, E)$, we define

$$\tau(\mathcal{M}) = \max_{W \leq V} \left\{ \frac{a}{b} \mid \mathcal{M} \subset \mathcal{P}_{W,a,b} \right\} \quad (4.8)$$

and

$$\tau_{\mathbb{Q}}(\mathcal{M}) = \max_{W \leq V, \Delta\text{-rational}} \left\{ \frac{a}{b} \mid \mathcal{M} \subset \mathcal{P}_{W,a,b} \right\}. \quad (4.9)$$

Remark 4.4.1. When all weights α_i and α'_i are equal to 1, then ψ and ϕ are just the dimension functions. Hence in this case our pencil $\mathcal{P}_{W,a,b}$ is just the pencil $\mathcal{P}_{W,r}$ defined in the introduction, with r equal to the integer part of the minimum of b and $\dim W - a$.

5. DIOPHANTINE APPROXIMATION AND FLOWS ON THE SPACE OF LATTICES

In this section we prove the results about diophantine approximation on submanifold of matrices stated in the introduction. We will do so in the general weighted setting using the quasi-norms defined in the previous section. More precisely we will show the following results (using the notation defined in (4.7), (4.8) and (4.9)).

Theorem 5.1 (Exponent for submanifolds of matrices). *Let E, V be two real vectors spaces equipped with quasi-norms and $\mathcal{M} = \Phi(U) \subset \text{Hom}(V, E)$ a connected analytic submanifold. Then there is $\widehat{\beta} \in [0, +\infty]$ such that for Lebesgue almost every $x \in U$*

$$\beta(\Phi(x)) = \widehat{\beta}.$$

Moreover $\widehat{\beta}$ depends only on the Zariski closure of \mathcal{M} , and

$$\tau_{\mathbb{Q}}(\mathcal{M}) \leq \widehat{\beta} \leq \tau(\mathcal{M}).$$

and

Theorem 5.2 (Rational manifolds). *In the setting of the previous theorem, assume that the Zariski closure of \mathcal{M} is defined over \mathbb{Q} , then*

$$\tau_{\mathbb{Q}}(\mathcal{M}) = \widehat{\beta} = \tau(\mathcal{M}).$$

In particular $\widehat{\beta}$ is a rational number if the α_i, α'_i are rational.

The \mathbb{Q} -structure on $\text{Hom}(V, E)$ used implicitly in the above theorem is the one induced by the \mathbb{Q} -span of the bases of V and E chosen to define the quasi-norms.

The above statements account for Theorems 1.2, 1.5 and 1.10 from the introduction. Theorem 1.4 will be proved below as Theorem 5.2.6 (together with its consequences 5.2.10 and 5.2.11.)

5.1. The Dani correspondence. We now recall the connection between diophantine approximation and flows on homogeneous spaces, in particular the so-called quantitative non-divergence estimate, which originates in the work of Margulis [Mar75] and Dani [Dan85] and first arose in the groundbreaking work of Kleinbock and Margulis [KM98] on diophantine approximation on manifolds.

A Dani correspondence is a statement which relates a diophantine exponent to the rate of escape of a certain flow on the space of lattices. In this subsection we present a Dani correspondence for matrices that is valid in the quasi-norm setting. A similar correspondence was worked out by Kleinbock and Margulis already in the matrix context in their work on logarithm laws [KM99, Theorem 8.5].

We keep the notation of the previous subsection and let $x \in \text{Hom}(V, E)$. If $I(\ker x) = \{i_1 < i_2 < \dots < i_n\}$, then

$$0 < V_{i_1+1} \cap \ker x < V_{i_2+1} \cap \ker x < \dots < V_{i_n+1} \cap \ker x = \ker x$$

is a full flag in $\ker x$. Similarly, if $J(xV) = \{i'_1 < \dots < i'_m\} \subset \{1, \dots, e\}$ is the set of indices i for which $\dim(xV \cap V'_i) = \dim(V'_{i-1} \cap xV) - 1$, then

$$\ker x < x^{-1}(xV \cap V'_{i'_m+1}) < \dots < x^{-1}(xV \cap V'_{i'_2+1}) < x^{-1}(xV \cap V'_{i'_1+1}) = V$$

is a full flag from $\ker x$ to V . Concatenating these two flags, we obtain a full flag in V :

$$F_x : 0 < F_x^{(1)} < \dots < F_x^{(d)} = V.$$

We choose an adapted basis $\{e_i^{(x)}\}_i$ of V so that $e_i^{(x)} \in F_x^{(i)} \setminus F_x^{(i-1)}$, and we define a d -tuple (a_1, \dots, a_d) of positive numbers by setting

$$a_i = \begin{cases} \alpha_j & \text{if } F_x^{(i)} = V_{j+1} \cap \ker x \text{ for some } j \in I(\ker x) \\ \alpha'_j & \text{if } F_x^{(i)} = x^{-1}(xV \cap V'_{j+1}) \text{ for some } j \in J(xV). \end{cases}$$

Finally given $\beta > 0$ we define a one-parameter subgroup $\{\tilde{g}_t^{(x,\beta)}\}_{t \in \mathbb{R}}$ of $\text{GL}(V)$ by

$$\tilde{g}_t^{(x,\beta)} e_i^{(x)} = \begin{cases} e^{-a_i t} e_i^{(x)} & \text{if } i \leq n, \\ e^{\beta a_i t} e_i^{(x)} & \text{if } i > n, \end{cases}$$

where $n = \dim \ker x$. Observe that $a_i \geq a_{i+1}$ for every $i < n$ and $a_i \leq a_{i+1}$ for every $i > n$.

Proposition 5.1.1 (Dani correspondence). *For $x \in \text{Hom}(V, E)$ the diophantine exponent for quasi-norms defined in (4.7) is given by*

$$\beta(x) = \inf\{\beta > 0 \mid \exists c > 0 : \forall t > 0, \forall v \in \Delta \setminus \{0\}, \|\tilde{g}_t^{(x,\beta)} v\| \geq c\},$$

where $\|\cdot\|$ is a fixed Euclidean norm on V .

Proof. We show that given β and x , $\tilde{g}_t^{(x,\beta)} v$ is uniformly bounded away from zero when $t > 0$ and $v \in \Delta \setminus \{0\}$ if and only if $|xv|' \cdot |v|^\beta$ is uniformly bounded away from zero for all non-zero $v \in \Delta$.

Note that $\ker x = \langle e_i^{(x)}, i \leq n \rangle$, and that we may restrict attention to vectors v such that xv is small, for otherwise there is nothing to prove. We may write $v = v' + v''$, where $v' = \sum_{i \leq n} v_i e_i^{(x)}$ and $v'' = \sum_{i > n} v_i e_i^{(x)}$ and note, using the triangle inequality 5. of §4.1, that $|v|$ is comparable within

multiplicative constants to $|v'|$ since v'' can be assumed bounded. So we are left to check that

$$\max\{\max_{i \leq n} |v_i e^{-a_i t}|, \max_{i > n} |v_i e^{\beta a_i t}|\}$$

is bounded away from zero uniformly in $t > 0$ and $v \in \Delta \setminus \{0\}$ if and only if $|xv|' \cdot |v|^\beta$ is bounded away from zero for v in $\Delta \setminus \{0\}$. This is straightforward since $|xv|'$ is comparable to $\max_{i > n} |v_i|^{1/a_i}$, while $|v|$ is comparable to $|v'|$ and hence to $\max_{i \leq n} |v_i|^{1/a_i}$. \square

For the next subsection, it will be convenient to use a slightly different flow $g_t^{(x, \beta)}$ in place of $\tilde{g}_t^{(x, \beta)}$ so as to make the dependence on x explicit while preserving the validity of the Dani correspondence. For this, we fix (independently of x) bases (u_i) of V and (u'_i) of E that are adapted to the flags $\{V_i\}$ and $\{V'_i\}$, so that $V_i = \langle u_1, \dots, u_{i-1} \rangle$ and $V'_i = \langle u'_{i+1}, \dots, u'_e \rangle$ and assume $x \in \text{Hom}(V, E)$ is given as a $e \times d$ matrix $(x_{ij})_{i,j}$ in these bases. We denote by x_i^* , $1 \leq i \leq e$ the rows of x , which we view as linear forms on V . The indices in the set $J(xV) = \{i'_1 < \dots < i'_m\}$ are obtained by

$$i'_j = \min\{i \in \{1, \dots, e\} \mid \text{rk}(x_1^*, \dots, x_i^*) = j\}.$$

By construction, the family of linear forms $x_{i'_m}^*, \dots, x_{i'_1}^*$ has rank $m = \dim xV$. We obtain the elements $i_1 < \dots < i_n$ of the set $I(\ker x)$ in the following way:

$$i_j = \min\{i \in \{1, \dots, d\} \mid \text{rk}(u_1^*, \dots, u_i^*, x_{i'_m}^*, \dots, x_{i'_1}^*) = m + j\}.$$

Now, consider the matrix $x' \in \text{GL}_d(\mathbb{R})$ given in rows by

$$x' = \begin{pmatrix} u_{i_1}^* \\ \vdots \\ u_{i_n}^* \\ x_{i'_m}^* \\ \vdots \\ x_{i'_1}^* \end{pmatrix}.$$

We denote by $a_t^{(\beta)}$ the diagonal matrix

$$a_t^{(\beta)} := \text{diag}(e^{-a_1 t}, \dots, e^{-a_n t}, e^{\beta a_{n+1} t}, \dots, e^{\beta a_{n+m} t}),$$

and define $g_t^{(x, \beta)}$ by the matrix

$$g_t^{(x, \beta)} := a_t^{(\beta)} x'. \quad (5.1)$$

Remark 5.1.2. Note that, with this notation, $F_x^{(i)} = x'^{-1} V_{i+1}$ and our former definition $\tilde{g}_t^{(x, \beta)}$ was simply $\tilde{g}_t^{(x, \beta)} = x'^{-1} a_t^{(\beta)} x'$. The Dani correspondence (Proposition 5.1.1 above) still holds for $\tilde{g}_t^{(x, \beta)}$ in place of $g_t^{(x, \beta)}$, because the shortest vectors of $x'^{-1} a_t^{(\beta)} x' \Delta$ and $a_t^{(\beta)} x' \Delta$ have comparable sizes, up to a positive multiplicative constant depending on x only and not on t .

With this construction, the map $x \mapsto g_t^{(x, \beta)}$ is a polynomial map on any set where $I(\ker x)$ and $J(xV)$ are constant. This last condition is equivalent to requiring that $\ker x$ and xV respectively stay in some a fixed Schubert

cell of the grassmannians $\text{Grass}(V)$ and $\text{Grass}(E)$, defined with respect to the flags $\{V_i\}$ and $\{V'_i\}$.

5.2. Quantitative non-divergence. For the remainder of this subsection, V and E are two filtered real vector spaces endowed with quasi-norms as introduced in §4.3. In this context, we adapt the strategy introduced by Kleinbock and Margulis [KM98] to study diophantine approximation on manifolds. The results presented in this subsection are closely related to further work of Kleinbock [Kle08b, Kle10a], who proved in particular the existence of an almost sure exponent and the fact that it is the smallest exponent.

Let ν be a Borel measure on a metric space X . Given an open set $U \subset X$, the measure ν is D -doubling (or D -Federer) on U if every ball B centered at $x \in U \cap \text{Supp}(\nu)$ and contained in U satisfies

$$\nu(\frac{1}{3}B) \geq \frac{1}{D}\nu(B), \quad (5.2)$$

where $\frac{1}{3}B$ is the ball centered at the center of B whose radius is a third of the radius of B . Given two positive constants C and α , we say that a real-valued function f on X is (C, α) -good on U with respect to the measure ν if it satisfies, for any ball $B \subset U$ and any $\varepsilon > 0$,

$$\nu(\{x \in B; |f(x)| \leq \varepsilon\}) \leq C \left(\frac{\varepsilon}{\|f\|_{\nu, B}} \right)^\alpha \nu(B), \quad (5.3)$$

where $\|f\|_{\nu, B} = \sup_{x \in B \cap \text{Supp} \nu} |f(x)|$. By convention, we also agree that if f is identically zero on the support of ν , then it is (C, α) -good with respect to ν for any values of C and α .

The heart of the Kleinbock-Margulis approach to study diophantine approximation on manifolds is the following key result, which can be seen as a Remez-type inequality (see [BG73] or [ABRdS15a, Thm 2.7]) for functions taking values in the space of lattices. It originates in the work of Margulis [Mar71] on non-divergence of unipotent flows, which was later greatly generalized in work of Dani [Dan85] and Kleinbock-Margulis [KM98]. The following version is borrowed from [Kle08b] (see also [Kle10b]).

Theorem 5.2.1. [Kle08b, Theorem 2.2] *Let X be a Besicovitch metric space. Let $U \subset X$ be an open subset and ν a Radon measure on U which is D -doubling on U for some $D > 0$. Let $C, \alpha > 0$ be positive constants and $h : U \rightarrow \text{GL}_d(\mathbb{R})$ be a continuous map. Let $\rho \in (0, 1]$ and let $B = B(z, r)$, $z \in \text{Supp}(\nu)$, be an open ball such that $B(z, 3^d r)$ is contained in U . Assume that for each v_1, \dots, v_k in $\mathbb{Z}^d \setminus \{0\}$, $1 \leq k \leq d$,*

- *the function $x \mapsto \|h(x)\mathbf{w}\|$ is (C, α) -good for ν on $B(z, 3^d r)$, and*
- *if $\mathbf{w} \neq 0$, then $\sup_{y \in B \cap \text{Supp}(\nu)} \|h(y)\mathbf{w}\| > \rho^k$,*

where $\mathbf{w} = v_1 \wedge v_2 \wedge \dots \wedge v_k$.

Then for every $\varepsilon \in (0, \rho]$, we have that

$$\nu(\{x \in B; h(x)\mathbb{Z}^d \in \Omega_\varepsilon\}) \leq C' \left(\frac{\varepsilon}{\rho} \right)^\alpha \nu(B),$$

where $C' > 0$ depends only on D, C, α and the Besicovitch constant of X .

In the above theorem, the letter Ω_ε denotes the part of the space of lattices $\text{GL}_d(\mathbb{R})/\text{GL}_d(\mathbb{Z})$ made of lattices in \mathbb{R}^d admitting a non-zero vector

of length at most ε . When one restricts attention to unimodular lattices, the set Ω_ε is thought of as “the cusp” of Ω , because as $\varepsilon \rightarrow 0$ these sets form a nested sequence of neighborhoods of infinity. This fact is known as Mahler’s criterion [Rag72, Cor. 10.9].

In fact the theorem is stated only for $\mathrm{SL}_d(\mathbb{R})$ -valued maps in [Kle08b], but it is valid as well – with the same proof – for $\mathrm{GL}_d(\mathbb{R})$ -valued maps. In older versions of this non-divergence result (such as in [KLW04]) the second assumption involved a lower bound of the form ρ . Kleinbock’s observation [Kle08b] that one can relax this assumption to a lower bound ρ^k is crucial when one wants to study diophantine exponents of measures that might not be extremal; it will be essential in the proofs of our formulas for the exponent.

Recall also that a metric space X is called *Besicovitch* if there exists an integer C such that we have the following property: suppose $A \subset X$ and for each $a \in A$ we are given a non-empty open ball B_a centered at a ; then there exists a countable subset $A' \subset A$ such that $A \subset \bigcup_{a \in A'} B_a$ and any intersection of C distinct balls B_a , $a \in A'$, is empty. In the definition below, the flow $g_t^{(y,\beta)}$ on $\mathrm{GL}(V)$ is the one constructed at the end of §5.1, and we denote by \mathcal{W}_Δ^k the set of non-zero pure integral k -vectors, i.e. those $\mathbf{w} \in \wedge^k V \setminus \{0\}$ that can be written $\mathbf{w} = v_1 \wedge \cdots \wedge v_k$ where each v_i is an element of Δ .

Definition 5.2.2. Let ν be a Radon measure on $\mathrm{Hom}(V, E)$ and $x \in \mathrm{Supp}(\nu)$. We will say that the measure ν is *locally good at x* if there exists a neighborhood U_x of x and positive constants C, D and α such that

- there exists $n \leq d$ and a Schubert cell $e(\sigma) \subset \mathrm{Grass}_n(V)$ such that for all y in $U_x \cap \mathrm{Supp} \nu$, $\ker y$ belongs to $e(\sigma)$ (see §4.2).
- there exists $m \leq e$ and a Schubert cell $e(\sigma') \subset \mathrm{Grass}_m(E)$ such that for all y in $U_x \cap \mathrm{Supp} \nu$, yV belongs to $e(\sigma')$ (see §4.2).
- ν is D -doubling on U_x
- for all $t, \beta > 0$, all $k \geq 0$ and all \mathbf{w} in \mathcal{W}_Δ^k , the map $y \mapsto \|g_t^{(y,\beta)} \mathbf{w}\|$ is (C, α) -good on U_x with respect to ν .

Remark 5.2.3. The first two conditions ensure that the map $y \mapsto g_t^{(y,\beta)}$ is continuous on a neighborhood of x in $\mathrm{Supp} \nu$.

Remark 5.2.4. The set of points where ν is locally good is an open subset of $\mathrm{Supp}(\nu)$.

With the quantitative non-divergence result (Theorem 5.2.1) we can derive the following statement. The argument in the proof is taken from Kleinbock [Kle10a].

Theorem 5.2.5 (Existence of a local exponent). *If a Radon measure ν on $\mathrm{Hom}(V, E)$ is locally good at x , then there is a neighborhood B_x of x such that for ν -almost every point $y \in B_x$,*

$$\beta(y) = \inf_{z \in B_x} \beta(z). \quad (5.4)$$

If B_x is a neighborhood such that (5.4) holds, we define the local diophantine exponent of ν at x by

$$\widehat{\beta}_\nu(x) = \inf_{z \in B_x} \beta(z).$$

Proof. If B_x is any neighborhood of x , it is trivial that for all y in B_x , $\beta(y) \geq \inf_{z \in B_x} \beta(z)$. Conversely, assume ν is locally good at x , and let $C, D, \alpha > 0$ and $B_x = B(x, r)$ be a ball around x such that the conditions of Definition 5.2.2 hold on $U_x := B(x, 3^d r)$. We claim that for almost every y in B_x , $\beta(y) \leq \inf_{z \in B_x} \beta(z)$. To see this, fix $z \in B_x$ and $\beta > \beta(z)$, so that, by Proposition 5.1.1, there exists $c > 0$ such that

$$\forall t > 0, \forall k, \forall \mathbf{w} \in \mathcal{W}_\Delta^k, \quad \|g_t^{(z, \beta)} \mathbf{w}\| \geq c.$$

Of course, this implies that

$$\forall t > 0, \forall k, \forall \mathbf{w} \in \mathcal{W}_\Delta^k, \quad \sup_{y \in B_x} \|g_t^{(y, \beta)} \mathbf{w}\| \geq c.$$

For $\eta > 0$, apply Theorem 5.2.1 with $U = U_x$, $B = B_x$, $\rho = c$, $h : y \mapsto g_t^{(y, \beta)}$, and $\varepsilon = e^{-\eta t}$. For any $t > 0$ such that $e^{-\eta t} < c$, we find that

$$\nu(\{y \in B_x \mid g_t^{(y, \beta)} \Delta \in \Omega_{e^{-\eta t}}\}) \leq C' \left(\frac{e^{-\eta t}}{c}\right)^\alpha \nu(B_x).$$

Therefore,

$$\sum_{t \in \mathbb{N}} \nu(\{y \in B_x \mid g_t^{(y, \beta)} \Delta \in \Omega_{e^{-\eta t}}\}) < \infty$$

and, by the Borel-Cantelli lemma and Proposition 5.1.1 again, for almost every y in B_x , $\beta(y) \leq \beta + \eta$. Letting $\eta \rightarrow 0$, $\beta \rightarrow \beta(z)$, and taking the infimum over z in B_x , we get, for almost every y in B_x ,

$$\beta(y) \leq \inf_{z \in B_x} \beta(z).$$

□

Given a non-negative parameter β , we say that the measure ν satisfies the condition (\mathcal{C}_β) at x if the following holds:

$$\forall r > 0, \exists c > 0 : \forall k \in \{1, \dots, \dim V\}, \forall t > 0, \forall \mathbf{w} \in \mathcal{W}_\Delta^k, \quad (\mathcal{C}_\beta) \\ \sup_{y \in B(x, r) \cap \text{Supp } \nu} \|g_t^{(y, \beta)} \mathbf{w}\| \geq c.$$

It follows from Theorem 5.2.5 and Proposition 5.1.1 that if ν is locally good at x , then

$$\widehat{\beta}_\nu(x) = \inf\{\beta > 0 \mid \nu \text{ satisfies } (\mathcal{C}_\beta) \text{ at } x\}. \quad (5.5)$$

We now use this observation to show that the local exponent $\widehat{\beta}_\nu(x)$ of a locally good measure at x is determined by the local Zariski closure at x of the support of ν . More precisely, fix two bases for V and E , and given x in $\text{Hom}(V, E)$, consider $\theta(x) \in \mathbb{R}^N$ the N -tuple of all minors of x , where $N = \sum_{k=1}^e \binom{d}{k} \binom{e}{k} = \binom{e+d}{d} - 1$. For a subset S in $\text{Hom}(V, E)$, we define the *Plücker closure* of S by

$$\mathcal{H}(S) = \{x \in \text{Hom}(V, E) \mid \theta(x) \in \text{Span}(\theta(y); y \in S)\},$$

and finally, if ν is a locally good measure at x in $\text{Hom}(V, E)$, we let

$$\mathcal{H}_\nu(x) = \bigcap_{r>0} \mathcal{H}(B(x, r) \cap \text{Supp } \nu) \quad (5.6)$$

be the *local Plücker closure* at x .

Theorem 5.2.6 (Inheritance). *Let ν, ν' be Radon measures on $\text{Hom}(V, E)$, and assume that ν is locally good at x and ν' locally good at x' . If $\mathcal{H}_\nu(x) \subset \mathcal{H}_{\nu'}(x')$, then $\widehat{\beta}_\nu(x) \geq \widehat{\beta}_{\nu'}(x')$.*

Proof. Let S be a compact subset of $\text{Hom}(V, E)$, and assume that for all x in S , the subspaces $\ker x$ and xV belong to some fixed Schubert cells in $\text{Grass}(V)$ and $\text{Grass}(E)$. We will say that S satisfies (\mathcal{C}_β) if

$$\begin{aligned} \exists c > 0 : \forall k \in \{1, \dots, \dim V\}, \forall t > 0, \forall \mathbf{w} \in \mathcal{W}_\Delta^k, \\ \sup_{y \in S} \|g_t^{(y, \beta)} \mathbf{w}\| \geq c. \end{aligned} \quad (\mathcal{C}_\beta(S))$$

The expression $g_t^{(y, \beta)} \mathbf{w}$ is a linear function of the minors of $g_t^{(y, \beta)}$. By (5.1), it is also a linear function of the minors of y , and therefore, for some constant $C > 0$ depending only on S ,

$$\sup_{y \in S} \|g_t^{(y, \beta)} \mathbf{w}\| \leq \sup_{y \in \mathcal{H}(S) \cap B} \|g_t^{(y, \beta)} \mathbf{w}\| \leq C \cdot \sup_{y \in S} \|g_t^{(y, \beta)} \mathbf{w}\|,$$

where B is a fixed compact neighborhood of 0 in $\text{Hom}(V, E)$ containing S (note that both expressions on the right-hand side are norms on the finite-dimensional space of linear maps between $\theta(\mathcal{H}(S))$ and $\wedge^k V$). It follows that the condition $(\mathcal{C}_\beta(S))$ depends only on $\mathcal{H}(S)$. To conclude the proof of the theorem, it suffices to use equality (5.5), and to note that the measure ν satisfies (\mathcal{C}_β) at x if and only if $(\mathcal{C}_\beta(B(x, r) \cap \text{Supp } \nu))$ holds for every $r > 0$. \square

Remark 5.2.7. Note that if S is a subset of $\text{Hom}(V, E)$, then $\mathcal{H}(S)$ is a Zariski closed subset containing S , so in particular it contains the Zariski closure $Z(S)$ of S , i.e. the intersection of all closed real algebraic subsets of $\text{Hom}(V, E)$ containing S . Since by definition $\mathcal{H}(S) = \mathcal{H}(\mathcal{H}(S))$ we also get $\mathcal{H}(S) = \mathcal{H}(Z(S))$.

Remark 5.2.8 (local Zariski closure). The local Zariski closure of ν at x is defined to be the intersection of the Zariski closures of $B(x, r) \cap \text{Supp}(\nu)$ in $\text{Hom}(V, E)$ for all $r > 0$. By noetherianity the local Zariski closure (resp. the local Plücker closure) coincides with the Zariski closure (resp. the Plücker closure) of $B(x, r) \cap \text{Supp}(\nu)$ whenever r is sufficiently small. Observe in particular that $\mathcal{H}_\nu(x)$ depends only on the local Zariski closure at x .

Hence we obtain the following corollary:

Corollary 5.2.9. *Let ν, ν' be Radon measures on $\text{Hom}(V, E)$, and assume that ν is locally good at x and ν' locally good at x' . If the local Zariski closures coincide, then $\widehat{\beta}_\nu(x) = \widehat{\beta}_{\nu'}(x')$.*

As a corollary of this inheritance theorem, we can define the diophantine exponent of an algebraic subset of $\text{Hom}(V, E)$. Here, and throughout the paper, when speaking of Zariski closure, algebraic subsets and algebraic

varieties, we will always consider these notions in real algebraic geometry and we refer the reader to the textbook [BCR98] for definitions and basic properties. By Lebesgue measure on an algebraic set \mathcal{M} we mean the top-dimensional Hausdorff measure on the subset \mathcal{M} of $\text{Hom}(V, E)$.

Corollary 5.2.10 (Exponent of an algebraic subset). *Let \mathcal{M} be an irreducible algebraic subset in $\text{Hom}(V, E)$. There exists $\widehat{\beta}(\mathcal{M})$ such that, for almost every x in \mathcal{M} with respect to the Lebesgue measure,*

$$\beta(x) = \widehat{\beta}(\mathcal{M}).$$

Proof. Let x be a non-singular point on \mathcal{M} such that $\ker x$ and xV lie in the interior of the smallest Schubert subvariety (of $\text{Grass}(V)$ and $\text{Grass}(E)$ respectively) containing $\{\ker y; y \in \mathcal{M}\}$ and $\{yV; y \in \mathcal{M}\}$. Since \mathcal{M} is irreducible, by [BCR98, §3.2], this makes a set of full measure in \mathcal{M} . Take an analytic parametrization $\Phi : U \rightarrow \text{Hom}(V, E)$ of \mathcal{M} in a neighborhood of x , and let ν be the pushforward under Φ of the Lebesgue measure on U . Note that ν is equivalent to the Lebesgue measure on \mathcal{M} in a neighborhood of x . Restricting U if necessary, we see using [Kle10a, Proposition 2.1] that there exist constants (C, α) and a neighborhood U_x of x such that all functions $y \mapsto \|g_t^{(y, \beta)} \mathbf{w}\|$ are (C, α) -good on U_x with respect to ν . So ν is locally good at x , and by Theorem 5.2.5, for ν -almost all y in a neighborhood of x , $\beta(y) = \widehat{\beta}_\nu(x)$. At a non-singular x as above the local Zariski closure is \mathcal{M} itself ([BCR98, Proposition 3.3.14]). So by Corollary 5.2.9, $\widehat{\beta}_\nu(x)$ is independent of the choice of x . This proves the corollary. \square

Remark 5.2.11. We can also conclude that $\widehat{\beta}(\mathcal{M}) = \widehat{\beta}(\mathcal{H}(\mathcal{M}))$. Indeed the local Plücker closure at a random point of \mathcal{M} is $\mathcal{H}(\mathcal{M})$, and so is the local Plücker closure at a random point of $\mathcal{H}(\mathcal{M})$. We actually believe that more is true, namely that $\widehat{\beta}(\mathcal{M}) = \widehat{\beta}(\mathcal{S}(\mathcal{M}))$, where $\mathcal{S}(\mathcal{M})$ is the *Schubert closure* of \mathcal{M} , namely the intersection of all pencils containing \mathcal{M} .

The pushforward of the Lebesgue measure under an analytic map $U \rightarrow \text{Hom}(V, E)$, where U is a open domain in \mathbb{R}^N is locally good at every point, so we have the following important corollary to Theorem 5.2.5. This result is due to Kleinbock [Kle10a] in the case where $|\cdot|$ and $|\cdot|'$ are norms, and the proof is essentially the same, once the correspondence of §5.1 has been established.

Corollary 5.2.12 (Exponent of an analytic manifold). *Let $\Phi : U \rightarrow \text{Hom}(V, E)$ be an analytic map on a connected open set $U \subset \mathbb{R}^N$. There exists $\widehat{\beta} \in [0, \infty]$ such that, for almost every x in U ,*

$$\beta(\Phi(x)) = \widehat{\beta}.$$

Moreover $\widehat{\beta} = \widehat{\beta}(\mathcal{M})$, where \mathcal{M} is the Zariski closure of $\{\Phi(u); u \in U\}$.

Proof. Since Φ is analytic, \mathcal{M} is irreducible, and there exists a subset of full measure $U' \subset U$ such that, for all x in U' , the local Zariski closure at x (i.e. the intersection of the Zariski closures of all neighborhoods of x) is equal to \mathcal{M} . For such an x the pushforward under Φ of the Lebesgue measure on a neighborhood of x is locally good at x ([Kle10a, Proposition 2.1]) so that $\beta(\Phi(y)) = \widehat{\beta}(\mathcal{M})$ for almost every y in a neighborhood of x . \square

5.3. Pencils and extremality. Given two non-negative numbers a, b and a subspace W of V , recall that we have defined the *pencil* $\mathcal{P}_{W,a,b}$ associated to our choice of quasi-norms on V and E to be the set

$$\mathcal{P}_{W,a,b} = \{x \in \text{Hom}(V, E) \mid \psi(\ker x \cap W) \geq a \text{ and } \phi(xW) \leq b\}.$$

And the numbers $\tau(\mathcal{M})$ and $\tau_{\mathbb{Q}}(\mathcal{M})$ have been defined in (4.8) and (4.9).

Theorem 5.3.1. *Let E, V be two real vector spaces equipped with quasi-norms and $\mathcal{M} \leq \text{Hom}(V, E)$ an irreducible algebraic subset. Then*

$$\tau_{\mathbb{Q}}(\mathcal{M}) \leq \widehat{\beta}(\mathcal{M}) \leq \tau(\mathcal{M}).$$

Proof. The left-hand side follows from Dirichlet's principle proved in Proposition 4.3.1. Let us verify the right-hand side. Let $\beta > \tau(\mathcal{M})$. By Theorem 5.2.5, it suffices to show that $\beta > \widehat{\beta}_{\nu}(x)$ for every non-singular point x of \mathcal{M} which lies in the interior of the smallest Schubert subvariety containing \mathcal{M} . Equivalently, from (5.5), it is enough to check that (\mathcal{C}_{β}) holds at x . Note that we may replace $g_t^{(x,\beta)}$ by $\tilde{g}_t^{(x,\beta)}$ in the definition of (\mathcal{C}_{β}) , because x' remains bounded in a neighborhood of x in \mathcal{M} . Clearly then a sufficient condition for (\mathcal{C}_{β}) to hold is that $\mathbf{w} \mapsto \sup_{y \in B(x,r) \cap \mathcal{M}} \|\pi_0^{(y,\beta)}(\mathbf{w})\|$ does not vanish for any $r > 0$, when \mathbf{w} ranges among pure k -vectors of norm 1, and $\pi_0^{(y,\beta)}$ is the projection onto the sum of the eigenspaces of $\tilde{g}_t^{(y,\beta)}$ with non-negative eigenvalue with kernel the sum of the other eigenspaces.

Now, if W is the subspace of V associated to the k -vector \mathbf{w} , then the largest eigenvalue occurring in the decomposition of \mathbf{w} into eigenvectors of $\tilde{g}_t^{(y,\beta)}$ is $\beta\phi(yW) - \psi(\ker y \cap W)$. Therefore, if (\mathcal{C}_{β}) fails to hold, there exist $r > 0$ and a subspace $W \leq V$ such that $B(x, r) \cap \mathcal{M}$ is entirely contained in the set

$$\{y \in \text{Hom}(V, E) \mid \beta\phi(yW) - \psi(\ker y \cap W) < 0\},$$

which is the (finite) union of all pencils $\mathcal{P}_{W,a,b}$ such that $\beta b - a < 0$. Recall that neighborhoods of non-singular points are Zariski-dense in \mathcal{M} [BCR98, Proposition 3.3.14]. From the irreducibility of \mathcal{M} it follows that \mathcal{M} is entirely contained in a single pencil $\mathcal{P}_{W,a,b}$ for a pair a, b with $\beta b - a < 0$, which is contrary to our assumption that $\beta > \tau(\nu)$. \square

Proof of Theorem 5.1. Combine Corollary 5.2.12 with Theorem 5.3.1. \square

6. THE SUBMODULARITY LEMMA

In view of Theorem 5.3.1, the following question is natural: Under what condition on the irreducible algebraic subset $\mathcal{M} \subset \text{Hom}(V, E)$ is the maximum defining $\tau(\mathcal{M})$ in (4.8) attained on a Δ -rational subspace W ? We will show here that a sufficient condition is that \mathcal{M} be defined over the rationals. This is the content of Theorem 6.2.1. The method will also show that if \mathcal{M} is invariant under some group G of linear automorphisms, then $\tau(\mathcal{M})$ is attained on a G -invariant subspace W . This observation will be essential for the application to nilpotent Lie groups developed in Section 7.

6.1. Statement and proof of the submodularity lemma. Let V be a d -dimensional vector space (over some field). Let ϕ and ψ be two real-valued functions on the Grassmannian of V , with the following properties:

- (1) $\phi \geq 0$, $\phi(0) = 0$.
- (2) ϕ and ψ are non-decreasing for set inclusion.
- (3) ϕ and $-\psi$ are *submodular*, i.e. for any two vector subspaces U and W we have

$$\begin{aligned}\phi(U + W) + \phi(U \cap W) &\leq \phi(U) + \phi(W), \\ \psi(U + W) + \psi(U \cap W) &\geq \psi(U) + \psi(W).\end{aligned}$$

We let

$$q(x) = \frac{\psi(x)}{\phi(x)}$$

with the convention that $q(x) = 0$ if $\psi(x) = 0$ and $q(x) = \text{sign}(\psi(x))\infty$ if $\phi(x) = 0$ but $\psi(x) \neq 0$. We are interested in the supremum S of q on the entire Grassmannian. Note that $S \in \mathbb{R} \cup \{\pm\infty\}$.

Lemma 6.1.1 (Submodularity lemma). *The supremum*

$$S = \sup_{x \in \text{Grass}(V)} q(x)$$

is attained, and there is a unique subspace x_0 of maximal dimension such that

$$S = q(x_0).$$

Proof. We perform a preliminary reduction: we are going to reduce to the case where $\phi(x) > 0$ when $x \neq 0$ and $S > q(0)$. For this we make the following initial observation. Let W be the sum of all subspaces x such that $\phi(x) = 0$. Then $\phi(W) = 0$. Indeed, using that ϕ is non-decreasing and submodular, if $\phi(x) = \phi(y) = 0$, then $0 \leq \phi(x \cap y) \leq \phi(x) = 0$, so that $\phi(x \cap y) = 0$, while $0 \leq \phi(x + y) \leq \phi(x) + \phi(y) = 0$, so $\phi(x + y) = 0$.

It follows that for every $x \in \text{Grass}(V)$, $\phi(x + W) = \phi(x)$. Indeed $\phi(x) \leq \phi(x + W) \leq \phi(x) + \phi(W) = \phi(x)$. Also $\psi(x + W) \geq \psi(x)$. So $q(x + W) \geq q(x)$. In particular $S = \sup_{x \supset W} q(x)$. We may thus restrict ϕ and ψ to those subspaces of V that contain W . This gives rise to new functions ϕ' and ψ' on the quotient space V/W , which clearly satisfy the same properties.

So we have reduced the proof to the case where $W = 0$, i.e. $\phi(x) > 0$ unless $x = 0$. If $\psi(0) > 0$, then $q(0) = +\infty$, while $q(x) < +\infty$ if $x \neq 0$, so the conclusion of the lemma holds with $x_0 = 0$. Therefore we may assume that $\psi(0) \leq 0$. This implies that $q(0) < S$, provided ψ is not identically zero. Indeed, if $\psi(0) < 0$, then $q(0) = -\infty$, while $q(x) > -\infty$ if $x \neq 0$, so $S > q(0)$. While if $\psi(0) = 0$, then $q(0) = 0$, while $S > 0$ provided ψ is not identically zero. If ψ is identically zero, the conclusion of the lemma holds with $x_0 = V$.

So we have proved our initial claim and we thus assume without loss of generality that ψ is not identically zero, that $q(0) < S$, and that $\phi(x) > 0$ if $x \neq 0$. This enables us to assert that $S = S_1$, where we have denoted, for $k = 1, \dots, d$,

$$S_k = \sup\{q(x); \dim x \geq k\}.$$

Let k_0 be the maximal $k \geq 1$ such that $S_k = S$. If $k_0 = d$, then $S = q(V)$ and the conclusion of the lemma holds with $x_0 = V$. If not we have $S_{k_0+1} < S$.

Pick $\varepsilon > 0$ such that $S - S_{k_0+1} > 2\varepsilon$, and pick $x_0 \in \text{Grass}(V)$ such that $\dim(x_0) \geq k_0$ and $q(x_0) > S - \varepsilon$. Note that $\dim(x_0) = k_0$, for otherwise $\dim(x_0) \geq k_0 + 1$ and thus $q(x_0) \leq S_{k_0+1} < S - 2\varepsilon < S - \varepsilon$, a contradiction to our choice of x_0 .

Now let y_0 be another choice of subspace such that $\dim(y_0) \geq k_0$ and $q(y_0) > S - \varepsilon$. For the same reason $\dim(y_0) = k_0 = \dim(x_0)$. But

$$\begin{aligned} \psi(x_0 + y_0) &\geq \psi(x_0) + \psi(y_0) - \psi(x_0 \cap y_0) \\ &\geq (S - \varepsilon)(\phi(x_0) + \phi(y_0)) - S\phi(x_0 \cap y_0) \\ &\geq S(\phi(x_0) + \phi(y_0) - \phi(x_0 \cap y_0)) - \varepsilon(\phi(x_0) + \phi(y_0)) \\ &\geq S\phi(x_0 + y_0) - \varepsilon(\phi(x_0) + \phi(y_0)) \\ &\geq S\phi(x_0 + y_0) - 2\varepsilon(\phi(x_0 + y_0)) = (S - 2\varepsilon)\phi(x_0 + y_0) \end{aligned}$$

where we have used submodularity of $-\psi$ in the first line, positivity of ϕ in the second line, submodularity of ϕ in the fourth line and monotonicity of ϕ in the last line. Hence:

$$q(x_0 + y_0) \geq S - 2\varepsilon > S_{k_0+1}.$$

Therefore $\dim(x_0 + y_0) \leq k_0$. This means that $x_0 = y_0$. Hence we have proved that $q(x) > S - \varepsilon$ and $\dim(x) \geq k_0$ implies that x is unique. In particular $S = q(x_0)$, and the lemma follows. \square

Corollary 6.1.2. *Let G be a group acting on the Grassmannian, and assume that the action preserves dimension. If ϕ and ψ are invariant under G , then the supremum S is attained on a G -invariant subspace.*

Proof. Indeed x_0 and gx_0 will have the same dimension and will both achieve the supremum S , so by uniqueness $x_0 = gx_0$, for every $g \in G$. \square

Remark 6.1.3. The proof works verbatim more generally for functions defined on a graded lattice of finite length, in place of $\text{Grass}(V)$, i.e. a partially ordered set with a smallest element (0) and a largest element (V) such that every pair of elements admits unique lower and upper bounds, and which is equipped with an integer-valued rank function $r(x)$, which is ≥ 0 and takes only finitely many values and is such that if $x < y$ and there is no z with $x < z < y$, then $r(y) = r(x) + 1$.

6.2. Applications of the submodularity lemma. We go back to the setting of Section 4. Thus, V and E are finite-dimensional real vector spaces, endowed with quasi-norms $|\cdot|$ and $|\cdot|'$ with associated flags $\{V_i\}$ and $\{V'_i\}$. The lattice $\Delta \leq V$ induces a \mathbb{Q} -structure on V . Recall that by a \mathbb{Q} -structure we mean a \mathbb{Q} -vector subspace which generates the ambient space over \mathbb{R} and whose dimension over \mathbb{Q} is the dimension over \mathbb{R} of the ambient space. Let us assume that the flag $\{V_j\}$ is made of Δ -rational subspaces, and endow E with a \mathbb{Q} -structure for which each V'_j is rational. This endows $\text{Hom}(V, E)$ with a natural \mathbb{Q} -structure.

Theorem 6.2.1 (Exponent of a rational algebraic subset). *Assume that the irreducible algebraic subset $\mathcal{M} \leq \text{Hom}(V, E)$ is defined over \mathbb{Q} . Then*

$$\widehat{\beta}(\mathcal{M}) = \tau(\mathcal{M}) = \tau_{\mathbb{Q}}(\mathcal{M}) = \max_{W \subset V, \Delta\text{-rational}} \left\{ \frac{a}{b} ; \mathcal{M} \subset \mathcal{P}_{W,a,b} \right\}.$$

Proof. From Theorem 5.3.1, it is enough to show that $\tau(\mathcal{M}) = \tau_{\mathbb{Q}}(\mathcal{M})$. By definition

$$\tau(\mathcal{M}) = \max_{W \leq V} \frac{\psi_{\mathcal{M}}(W)}{\phi_{\mathcal{M}}(W)} \quad \text{and} \quad \tau_{\mathbb{Q}}(\mathcal{M}) = \max_{W \leq V, W \Delta\text{-rational}} \frac{\psi_{\mathcal{M}}(W)}{\phi_{\mathcal{M}}(W)}. \quad (6.1)$$

where

$$\psi_{\mathcal{M}}(W) = \min_{x \in \mathcal{M}} \psi(W \cap \ker x) \quad \text{and} \quad \phi_{\mathcal{M}}(W) = \max_{x \in \mathcal{M}} \phi(xW). \quad (6.2)$$

These functions are defined a priori on the real grassmannian $\text{Grass}(V)$, but they also make sense on the grassmannian of the complexified space $V^{\mathbb{C}}$, where x is now viewed as a linear map from $V^{\mathbb{C}}$ to $E^{\mathbb{C}}$, and the flags $\{V_j\}$ and $\{V'_i\}$ are also complexified. The Galois group $\text{Gal}(\mathbb{C}|\mathbb{Q})$ acts on $\text{Grass}(V^{\mathbb{C}})$ and preserves $\psi_{\mathcal{M}}$ and $\phi_{\mathcal{M}}$, because \mathcal{M} is defined over \mathbb{Q} as well as the flags $\{V_j\}$ and $\{V'_i\}$. The functions $\psi_{\mathcal{M}}$ and $\phi_{\mathcal{M}}$ are both non-decreasing and non-negative functions. Moreover $-\psi_{\mathcal{M}}$ and $\phi_{\mathcal{M}}$ are submodular. This follows from the submodularity of $W \mapsto -\psi(W \cap \ker x)$ and $W \mapsto \phi(xW)$ for a given x proved in Subsection 4.1, from the irreducibility of \mathcal{M} and from the fact that for each W there is a Zariski-open set of x in \mathcal{M} such that $\psi_{\mathcal{M}}(W) = \psi(W \cap \ker x)$ (resp. $\phi_{\mathcal{M}}(W) = \phi(xW)$). We may thus apply the submodularity lemma (Lemma 6.1.2) and conclude that the maximum in the definition of $\tau(\mathcal{M})$ is attained for a rational W . \square

This completes the proof of Theorem 5.2. A different application of the submodularity lemma will be given in Section 7, in the proof of Theorem 1.13 from the introduction.

For now, we just give another simple example where the submodularity lemma applies, and allows to compute the diophantine exponent of an algebraic subset of matrices. For the example below, and until the end of this section, we shall only consider diophantine approximation for genuine norms on V and E .

Example 6.2.2 (The Veronese curve in algebras). Consider the Veronese curve \mathcal{V} in \mathbb{R}^n given by the parametrization $x \mapsto (x, \dots, x^n)$. The Mahler conjecture proved by Sprindžuk says that the curve \mathcal{V} is extremal, or in other words, that for almost every $x \in \mathbb{R}$, for all $\varepsilon > 0$, the inequality

$$|v_0 + v_1x + \dots + v_nx^n| \geq \|v\|^{-(\beta+\varepsilon)} \quad (6.3)$$

has only finitely many integer solutions $v \in \mathbb{Z}^{n+1}$, where here $\beta = n$.

We can consider the analogous problem, where \mathbb{R} is replaced by an arbitrary finite-dimensional \mathbb{R} -algebra E with unit (e.g. $E = M_m(\mathbb{R})$). Given $x \in E$, we may consider integer linear combinations of $1, x, \dots, x^n$. We may then ask for the minimal $\beta > 0$ such that for almost every $x \in E$ and for every $\varepsilon > 0$, the inequality (6.3) (with a norm in place of the absolute value on the left-hand side) has at most finitely many integer solutions $v \in \mathbb{Z}^{n+1}$.

To fit this problem into our setting, we let $V = \mathbb{R}_n[X]$ the space of polynomials of degree at most n and Δ the lattice of polynomials with integer

coefficients. Consider the submanifold \mathcal{M} of $\text{Hom}(V, E)$ that consists of the evaluations maps $P \mapsto P(x)$ for $x \in E$. It is defined over \mathbb{Q} , so, by Theorem 6.2.1, its exponent, which is exactly the β we are looking for, is equal to

$$\tau(\mathcal{M}) = \max \left\{ \frac{\psi(W)}{\phi(W)}; W \leq V \right\},$$

where

$$\phi(W) = \max_{x \in E} \dim W(x) \quad \text{and} \quad \psi(W) = \min_{x \in E} \dim W - \dim W(x).$$

Here $W(x) \leq E$ denotes the image of W under the evaluation map $P \mapsto P(x)$. Now, let G be the group of affine transformations of the real line and let it act on V by substitution of the variable. The maps ϕ and $-\psi$ are submodular and G -invariant, so by Lemma 6.1.2, τ achieves its value on one of the G -invariant subspaces, which are exactly the subspaces $V_i \leq V$, $i = 0, \dots, n$ of polynomials of degree at most i . Let m be the maximal dimension of one-generator subalgebras $\mathbb{R}[x] \leq E$, for $x \in E$. Evaluating V_i at an x with minimal polynomial of degree m , we see that, for $i < m$, $\phi(V_i) = i + 1$ and $\psi(V_i) = 0$. On the other hand, we always have $\phi(W) \leq m$ and $\psi(W) \geq \dim W - m$, so we find

$$\frac{\psi(V_i)}{\phi(V_i)} = \begin{cases} 0 & \text{if } i < m \\ \frac{i+1-m}{m} & \text{if } i \geq m. \end{cases}$$

This shows that the desired diophantine exponent β is equal to $\max\{0, \frac{n+1-m}{m}\}$.

Example 6.2.3 (Weak non-planarity and extremality). Consider the unweighted case (i.e. $\alpha_i = \alpha'_i = 1$). A submanifold $\mathcal{M} \subset \text{Hom}(V, E)$ is called *weakly non-planar* if it is not contained in any proper pencil $\mathcal{P}_{W,r} \subsetneq \text{Hom}(V, E)$. This notion was introduced, using slightly different words, by Beresnevich, Kleinbock and Margulis [BKM15] who showed that every locally good weakly non-planar measure on $\text{Hom}(V, E)$ is extremal. The converse however does not hold, and we now provide an example.

Let $k \geq 4$ be an integer and $X = (\mathbb{R}^3)^k$. Consider the finite-dimensional space V of polynomial maps f from X to $E = \mathbb{R}^3$ given by

$$f(u_1, \dots, u_k) = \sum_{1 \leq i < j \leq k} a_{ij} u_i \wedge u_j$$

where \wedge is the usual wedge product in \mathbb{R}^3 and $a_{ij} \in \mathbb{R}$. Let \mathcal{M} be the Zariski closure in $\text{Hom}(V, E)$ of the image of X by the map $\Phi : x \mapsto (f \mapsto f(x))$.

Let W be the subspace of V generated by the $u_1 \wedge u_j$, $j = 2, \dots, k$. For any $x = (u_1, \dots, u_k)$ with $u_1 \neq 0$, the space $W(x)$ is included in the orthogonal of u_1 and hence has dimension at most 2. Therefore, $\mathcal{M} \subset \mathcal{P}_{W,2}$ is not weakly non-planar.

However, it is easy to see that $\text{GL}_k(\mathbb{R})$ acts irreducibly on V by substitution of the variables. By the submodularity lemma we conclude that V is the unique subspace realizing the maximum in $\tau(\mathcal{M})$. Therefore \mathcal{M} is not contained in any constraining pencil and thus \mathcal{M} must be extremal by Corollary 1.6.

Example 6.2.4 (A criterion of Kleinbock-Margulis-Wang). Here we recover by means of Corollary 1.6 a criterion due to Kleinbock, Margulis and Wang

[KMW10, Theorem 7.1(b)] for the extremality of measures on two-by-two matrices. Following their terminology, we say that an algebraic subset $\mathcal{M} \subset M_{2,2}(\mathbb{R})$ is *row-nonplanar* if for all non-zero $v \in \mathbb{R}^2$, the map $M \mapsto Mv$ is not constant on \mathcal{M} .

Theorem 6.2.5. [KMW10, Theorem 7.1 (b)] *Let \mathcal{M} be an algebraic subset in $M_{2,2}(\mathbb{R})$ and assume that both \mathcal{M} and its image ${}^t\mathcal{M}$ under the transpose map are row-nonplanar. Then the submanifold*

$$\widetilde{\mathcal{M}} = \{(I_2|M); M \in \mathcal{M}\} \subset M_{2,4}(\mathbb{R})$$

is extremal.

Proof. Corollary 1.6, all we have to do is to check that for all non-zero subspace $W < V = \mathbb{R}^4$, there exists a point $x \in \widetilde{\mathcal{M}}$ such that $\dim x(W) \geq \frac{\dim W}{2}$. We study all possible values for $\dim W$. Suppose first $\dim W = 1, 2$. Since \mathcal{M} is row-nonplanar, there exists $x \in \widetilde{\mathcal{M}}$ such that $x(W)$ is non-zero, which implies $\dim x(W) \geq 1 \geq \frac{\dim W}{2}$. Now if $\dim W = 3$, denote by v_1, \dots, v_4 the coordinates in V , and suppose first that W is given by an equation $v_1 = \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4$. The matrix of the restriction of $(I_2|M)$ to W is given in some basis by

$$\begin{pmatrix} \lambda_2 & a + \lambda_3 & b + \lambda_4 \\ 1 & c & d \end{pmatrix},$$

where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We have to show that all three columns are not always proportional. The minors corresponding to the pairs of columns (1, 2) and (1, 3) are $d_{12} = c\lambda_2 - a - \lambda_3$ and $d_{13} = d\lambda_2 - b - \lambda_4$, i.e.

$$\begin{pmatrix} d_{12} \\ d_{13} \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} -1 \\ \lambda_2 \end{pmatrix} - \begin{pmatrix} \lambda_3 \\ \lambda_4 \end{pmatrix}.$$

Since the image of \mathcal{M} under the transposition is row-nonplanar, d_{12} and d_{13} cannot both vanish identically on \mathcal{M} , so that there exists $x \in \widetilde{\mathcal{M}}$ with $\dim x(W) = 2$. The remaining cases, where W is defined by $v_2 = \lambda_3 v_3 + \lambda_4 v_4$, $v_3 = \lambda_4 v_4$ or $v_4 = 0$ are treated similarly. \square

Example 6.2.6 (Every submanifold is extremal for a random lattice). The upper bound in Theorem 1.5 can be strict. Of course, if the maximum in $\tau(\mathcal{M})$ is attained on a Δ -rational subspace, then this upper bound is the true value of $\widehat{\beta}(\mathcal{M})$, but otherwise it may not be, and we give here a family of examples illustrating this fact. Note that the definition of $\tau(\mathcal{M})$ is independent of the lattice Δ , whereas it is likely that varying the lattice will change the value of $\widehat{\beta}(\mathcal{M})$. We prove:

Proposition 6.2.7 (Random lattice). *Let \mathcal{M} be an irreducible algebraic set in $\text{Hom}(V, E)$, and denote by m the maximal rank of an element of \mathcal{M} . Suppose we pick the lattice $\Delta < V$ at random according to Haar measure on the space of (say unimodular) lattices in V . Then $\widehat{\beta}(\mathcal{M}) = \frac{\dim V - m}{m}$ with respect to almost every lattice Δ .*

Proof. Let $\beta_\Delta(x)$ be the number defined in (4.7). Fix a lattice Δ_0 in V once and for all. By Fubini's theorem, it is enough to prove that for almost

every $x \in \mathcal{M}$, $\beta_{g\Delta_0}(x) = \frac{\dim V - m}{m}$ for almost every $g \in \mathrm{SL}(V)$. Indeed, the set of pairs $(x, g) \in \mathcal{M} \times \mathrm{SL}(V)$, for which $\beta_{g\Delta_0}(x) = \frac{\dim V - m}{m}$ is a Borel set and Fubini's theorem applied to the product measure $\nu \otimes dg$, where dg is a Haar measure on $\mathrm{SL}(V)$ then implies that for almost every Δ we have $\beta_\Delta(x) = \frac{\dim V - m}{m}$ for almost every $x \in \mathcal{M}$.

Fix $x \in \mathcal{M}$ such that $\mathrm{rk} x = m$ (this happens for x in a Zariski dense open subset of \mathcal{M} and hence for almost every x in \mathcal{M} .) Consider the map from $\mathrm{SL}(V)$ to $\mathrm{Hom}(V, E)$ given by $\phi_x : g \mapsto xg^{-1}$. The pushforward ν_x of the Haar measure on a neighborhood U of some g_0 by the map ϕ_x is locally good. Let \mathcal{M}_x be the Zariski closure of the support of ν_x . It contains all points of the form xg^{-1} , $g \in \mathrm{SL}(V)$. Now suppose W is a subspace of V . Since $\mathrm{rk} x = m$, we may choose $g \in \mathrm{SL}(V)$ such that $\dim(xg^{-1})(W) = \min\{m, \dim W\}$. This shows that $\tau(\mathcal{M}_x) = \frac{\dim V}{m}$. Moreover, equality is attained for $W = V$, which is Δ_0 -rational, so Theorem 5.2 shows that for almost every y in \mathcal{M}_x , $\beta_{\Delta_0}(y) = \frac{\dim V - m}{m}$. In particular, for almost every g in U ,

$$\beta_{g\Delta_0}(x) = \beta_{\Delta_0}(xg^{-1}) = \frac{\dim V - m}{m}.$$

□

Remark 6.2.8. The above proposition implies that for almost every W in the Grassmannian of k -planes in V , the pencil $\mathcal{P}_{W,r}$ is extremal, even if $\frac{\dim W}{r} > \frac{\dim V}{\dim E}$, provided it contains a matrix of maximal rank (i.e. provided $\dim W - r \leq \dim V - \dim E$). Indeed, $\widehat{\beta}_{g\Delta_0}(\mathcal{P}_{W,r}) = \widehat{\beta}_{\Delta_0}(\mathcal{P}_{gW,r})$.

7. THE CRITICAL EXPONENT FOR RATIONAL NILPOTENT LIE GROUPS

In this section we shall prove Theorems 1.12 and 1.13. Our method is based on the results of the previous sections regarding diophantine approximation on submanifolds of matrices.

Let G denote an arbitrary simply connected nilpotent real Lie group, with Lie algebra \mathfrak{g} of nilpotency class s . We endow G with a left-invariant geodesic metric $d(\cdot, \cdot)$. It is well known [Ber88] that these are exactly the left-invariant Carnot-Carathéodory-Finsler metrics on G . These metrics are obtained by the same construction as the left-invariant Riemannian metrics on G , except that instead of a Euclidean norm on \mathfrak{g} , we start with an arbitrary norm on a generating subspace V^1 of \mathfrak{g} . Denoting inductively, for $i \geq 1$, $V^{i+1} = V^i + [V^1, V^i]$, every Carnot-Carathéodory-Finsler metric on G associated to V^1 is comparable near the identity (up to multiplicative constants) to

$$d(\exp(X), 1) \simeq |X|' := \max_{i=1, \dots, s} \mathrm{dist}(X, V^{i-1})^{\frac{1}{i}}, \quad (7.1)$$

where $V^0 = 0$ by convention, dist is some fixed Euclidean distance on the Lie algebra, s is the nilpotency class of \mathfrak{g} and $X \in \mathfrak{g}$ lies in a neighborhood of the origin. Hence the function $X \mapsto d(\exp(X), 1)$ is a local quasi-norm (see Definition 4.1).

7.1. Growth of a generic subgroup and group of words maps. Let $k \geq 1$ and a k -tuple $\mathbf{g} = (g_1, \dots, g_k)$ of elements of G . Recall that the

subgroup $\Gamma_{\mathbf{g}}$ generated by \mathbf{g} is β -diophantine if there exists $c > 0$ such that, for every integer n ,

$$\min_{x \in S^n \setminus \{1\}} d(x, 1) \geq c \cdot |S^n|^{-\beta},$$

where $S = \{1, g_1^{\pm 1}, \dots, g_k^{\pm 1}\}$ and S^n is the set of elements that can be obtained as a word of length n in the elements of S . This definition involves the volume $V_{\mathbf{g}}(n) = |S^n|$ of the ball of radius n in the subgroup generated by $S = \{1, g_1^{\pm 1}, \dots, g_k^{\pm 1}\}$.

It turns out [ABRdS15a, Lemma 2.5] that for a generic k -tuple \mathbf{g} (generic with respect to Haar measure on G^k) the isomorphism class of the subgroup $\Gamma_{\mathbf{g}} = \langle S \rangle$ is always the same. It is isomorphic to the *group of word maps on k letters* $F_{k,G}$ of G , introduced in [ABRdS15a]. We briefly recall this notion. Any element w in the free group F_k on k letters x_1, \dots, x_k determines a word map $w_G : G^k \rightarrow G$ given by replacing each letter x_i by an element of G . The group $F_{k,G}$ is defined to be the set of all such word maps, with composition law given by $w_G w'_G = (w w')_G$, where $w w'$ denotes the product of w and w' in F_k . It can also be viewed as the relatively free group in the variety of k -generated subgroups of G .

Since $F_{k,G}$ is a fixed nilpotent group, the Bass-Guivarc'h formula [Bas72, Gui73] tells us that, up to multiplicative constants, for a generic k -tuple \mathbf{g} in G ,

$$V_{\mathbf{g}}(n) \simeq n^{\eta_G(k)} \quad (7.2)$$

where $\eta_G(k)$ is a positive integer that can be expressed in terms of the ranks of the successive quotients of the central descending series of $F_{k,G}$, see (7.7) below.

Now, given a k -tuple \mathbf{g} of elements of G , we can define another diophantine exponent, denoted $\alpha(\mathbf{g})$, as follows. It is the infimum of all $\alpha > 0$ such that for all but finitely many $\omega \in F_{k,G}$ we have:

$$d(\omega(\mathbf{g}), 1) \geq \ell(\omega)^{-\alpha}, \quad (7.3)$$

where $\ell(\omega)$ is the length of an element $\omega \in F_{k,G}$, i.e. the minimal length of a word w such that $w_G = \omega$. Recall that the diophantine exponent of the subgroup $\Gamma_{\mathbf{g}}$ was defined in Section 2 by

$$\beta(\Gamma_{\mathbf{g}}) = \inf\{\beta > 0 \mid \Gamma_{\mathbf{g}} \text{ is } \beta\text{-diophantine}\}.$$

It follows from the above observations about $V_{\mathbf{g}}(n)$ that, for almost every k -tuple \mathbf{g} in G ,

$$\alpha(\mathbf{g}) = \eta_G(k) \beta(\Gamma_{\mathbf{g}}). \quad (7.4)$$

7.2. From words to Lie brackets. In this subsection, we describe the correspondence between words on G and laws on its Lie algebra \mathfrak{g} .

We first define the Lie algebra $\mathcal{F}_{k,\mathfrak{g}}$ of bracket maps on k letters on \mathfrak{g} . Let \mathcal{F}_k be the free Lie algebra on k generators. Each element r in \mathcal{F}_k yields a map

$$\begin{aligned} r : \quad \mathfrak{g}^k &\rightarrow \mathfrak{g} \\ (X_1, \dots, X_k) &\mapsto r(X_1, \dots, X_k) \end{aligned}$$

where $r(X_1, \dots, X_k)$ is the evaluation of the formal bracket r at the point (X_1, \dots, X_k) in \mathfrak{g}^k . By definition, the Lie algebra $\mathcal{F}_{k,\mathfrak{g}}$ consists of all maps from \mathfrak{g}^k to \mathfrak{g} obtained in the above manner. It is naturally isomorphic to

the quotient Lie algebra $\mathcal{F}_k/\mathcal{L}_{k,\mathfrak{g}}$ where $\mathcal{L}_{k,\mathfrak{g}}$ is the *ideal of laws* on k letters on the Lie algebra \mathfrak{g} . Recall that a law on k letters is an element $r \in \mathcal{F}_k$ such that $r(X_1, \dots, X_k) = 0$ for all X_1, \dots, X_k in \mathfrak{g} .

Note that the free Lie algebra \mathcal{F}_k has a natural \mathbb{Q} -structure induced by the subring $\mathcal{F}_k(\mathbb{Z})$ of integer linear combinations of brackets monomials. We can thus consider the *ideal of rational laws* $\mathcal{L}_{k,\mathfrak{g},\mathbb{Q}}$, which is the real span of the intersection of $\mathcal{L}_{k,\mathfrak{g}}$ with $\mathcal{F}_k(\mathbb{Z})$. It thus inherits a rational structure, which induces a rational structure on the quotient space $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}} = \mathcal{F}_k/\mathcal{L}_{k,\mathfrak{g},\mathbb{Q}}$. We will say that r is an element of $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}(\mathbb{Z})$ if it is the projection on $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$ of an element of $\mathcal{F}_k(\mathbb{Z})$.

Remark 7.2.1. Certainly if \mathfrak{g} itself is defined over the rationals, then so is $\mathcal{L}_{k,\mathfrak{g}}$, but the converse does not hold. For example, it followed from the analysis made in [ABRdS15a, Appendix A] that the ideal of laws is always defined over \mathbb{Q} if \mathfrak{g} is a nilpotent Lie algebra of step at most 5, or if \mathfrak{g} is both nilpotent and metabelian.

The Lie algebra $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$ has a graded structure

$$\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}} = \bigoplus_{i=1}^s \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}^{[i]},$$

where $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}^{[i]}$ is the homogeneous part of $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$ consisting of brackets of degree i . For $r = \sum r_i$ with $r_i \in \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}^{[i]}$, we let

$$|r| = \max_{i=1,\dots,s} \|r_i\|^{\frac{1}{i}}, \quad (7.5)$$

where $\|\cdot\|$ is a fixed norm on $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$.

Lemma 7.2.2. *Let \mathfrak{g} be a real nilpotent Lie algebra and G the simply connected Lie group with Lie algebra \mathfrak{g} . There are positive integers C, D such that*

- If $\omega \in F_{k,G}$, then there exists $r \in \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}(\mathbb{Z})$ with $|r| \leq D\ell(\omega)$ such that for all X_1, \dots, X_k in \mathfrak{g} , $\omega(e^{X_1}, \dots, e^{X_k}) = e^{\frac{1}{C}r(X_1, \dots, X_k)}$.
- If $r \in \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}(\mathbb{Z})$, then there exists $\omega \in F_{k,G}$ with $\ell(\omega) \leq D|r|$ and for all X_1, \dots, X_k in \mathfrak{g} , $e^{Cr(X_1, \dots, X_k)} = \omega(e^{X_1}, \dots, e^{X_k})$.

Proof. This was proved in [ABRdS15a, Lemma 3.5] for the free Lie algebra \mathcal{F}_k and the free group F_k . The relative version stated here follows without difficulty, using that $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}} = \mathcal{F}_k/\mathcal{L}_{k,\mathfrak{g},\mathbb{Q}} = \bigoplus_i \mathcal{F}_k^{[i]}/\mathcal{L}_{k,\mathfrak{g},\mathbb{Q}}^{[i]}$. \square

Recall that $|X|'$ denotes the local quasi-norm on \mathfrak{g} defined in (7.1). The above lemma has the following immediate consequence.

Proposition 7.2.3. *Let G be a simply connected nilpotent Lie group, with Lie algebra \mathfrak{g} . Let $\mathbf{g} = (e^{X_1}, \dots, e^{X_k})$ be a k -tuple in G . The exponent $\alpha(\mathbf{g})$ defined in (7.3) is also the infimum of all $\alpha > 0$ such that*

$$|r(X_1, \dots, X_k)|' \geq |r|^{-\alpha} \quad (7.6)$$

holds for all but finitely many $r \in \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}(\mathbb{Z})$.

It also follows from Lemma 7.2.2 that the group of word maps $F_{k,G}$ is included as a lattice in the simply connected rational nilpotent Lie group whose Lie algebra is $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$ [ABRdS15a, Proposition 3.9]. The Bass-Guivarc'h formula for the growth exponent of $F_{k,G}$ from (7.2) now reads:

$$\eta_G(k) = \sum_{i=1}^s i \dim \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}^{[i]}. \quad (7.7)$$

Each $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}^{[i]}$ is a module for the action of GL_k under linear substitution. We will see below that, as a consequence, $\dim \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}^{[i]}$ is a degree i polynomial in k with rational coefficients, when k is large enough. It follows that, for k large, $\eta_G(k)$ is given by a degree s polynomial in k . Therefore, in view of (7.4), we now focus on computing $\alpha(\mathfrak{g})$ for a random tuple \mathfrak{g} .

7.3. Existence of the exponent. We now use the results of Section 5 to study the diophantine problem described by (7.6), and prove Theorem 1.12 from the introduction, which we recall here:

Theorem 7.3.1 (Existence of the exponent). *Let G be a connected and simply connected nilpotent real Lie group endowed with a left-invariant geodesic metric d . For each $k \geq 1$, there is $\widehat{\beta}_k \in [0, +\infty]$ such that for almost every k -tuple $\mathfrak{g} \in G^k$ with respect to Haar measure, we have*

$$\beta(\Gamma_{\mathfrak{g}}) = \widehat{\beta}_k.$$

Proof. We set $E = \mathfrak{g}$, $V = \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$, $\Delta = \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}(\mathbb{Z})$ and we define the local quasi-norm $|X|'$ on $E = \mathfrak{g}$ by (7.1) and the quasi-norm $|r|$ on V by (7.5). We let $U = \mathfrak{g}^k$ and

$$\begin{aligned} \Phi : U &\rightarrow \mathrm{Hom}(V, E) \\ \mathfrak{g} &\mapsto (\Phi(\mathfrak{g}) : r \mapsto r(\mathfrak{g})). \end{aligned}$$

Now we are in the setting of Corollary 5.2.12 from Section 5 and hence $\alpha(\mathfrak{g})$ is almost everywhere constant. In view of (7.4) this shows that $\beta(\mathfrak{g})$ is also well-defined and constant almost everywhere. \square

We denote by $\widehat{\alpha}_k$ the almost sure value of $\alpha(\mathfrak{g})$ for $\mathfrak{g} \in \mathfrak{g}^k$. Hence (7.4) becomes:

$$\widehat{\alpha}_k = \eta_G(k) \widehat{\beta}_k. \quad (7.8)$$

If we assume moreover that G and the geodesic metric are rational, we may even conclude that α_k is rational. We define a *rational* nilpotent Lie group as a nilpotent Lie group G with Lie algebra \mathfrak{g} endowed with a rational structure induced by a basis \mathcal{B} with rational structure constants. A left-invariant geodesic metric on a rational nilpotent Lie group G is said to be *rational* if the associated subspaces V^i – defined at the beginning of this section – are rational. For this, it is enough to require that V^1 is rational.

Theorem 7.3.2 (Rationality of the exponent). *Let G be a connected and simply connected rational nilpotent real Lie group, and $d(\cdot, \cdot)$ a rational left-invariant geodesic metric on G . Then, for all $k \geq 1$,*

$$\widehat{\beta}_k \in \mathbb{Q}.$$

Proof. We use the notation of the previous proof. If \mathfrak{g} is rational, then the Zariski closure \mathcal{M} of $\Phi(U)$ is defined over \mathbb{Q} . Indeed, complexifying E , V and Φ we see that $\sigma(\Phi(\mathfrak{g})) = \Phi(\sigma(\mathfrak{g}))$, for all $\sigma \in \text{Gal}(\mathbb{C}|\mathbb{Q})$. Therefore, Theorem 6.2.1 applies and we get that $\widehat{\alpha}_k = \tau_{\mathbb{Q}}(\mathcal{M})$. Now note that the exponents α_i and α'_i defining our quasi-norms are integers. As a result, the functions ψ and ϕ are integer-valued, and thus $\widehat{\alpha}_k \in \mathbb{Q}$. \square

7.4. The relatively free Lie algebra as a GL_k -module. In order to prove the second part of Theorem 1.13, we need some understanding of the GL_k -submodules of $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$. The action of the linear group GL_k on the free Lie algebra \mathcal{F}_k on k letters is by substitution of the variables. It turns out that the decomposition of each homogeneous component $\mathcal{F}_k^{[i]}$ into simple GL_k -modules is representation stable in the sense of Church, Ellenberg and Farb, see [CF13, Corollary 5.7]. This can be made more precise as follows. We set

$$\mathcal{F}_k^{\leq s} = \bigoplus_1^s \mathcal{F}_k^{[i]}$$

the subspace of the free Lie algebra on k letters spanned by brackets of order at most s .

Proposition 7.4.1. *Let $k \geq s$. The forgetful map*

$$\begin{aligned} F_s: \mathcal{F}_k^{\leq s} &\rightarrow \mathcal{F}_s^{\leq s} \\ r(x_1, \dots, x_k) &\mapsto r(x_1, \dots, x_s, 0, \dots, 0) \end{aligned}$$

establishes a bijective correspondence between GL_k -submodules of $\mathcal{F}_k^{\leq s}$ and GL_s -submodules of $\mathcal{F}_s^{\leq s}$. Moreover, if $W \leq \mathcal{F}_k^{\leq s}$ is a GL_k -submodule with the following decomposition into irreducible submodules

$$W = \bigoplus_{\lambda} E^{\lambda}(k)^{n_{\lambda}}, \quad (7.9)$$

then $F_s(W)$ decomposes, with the same multiplicities, as

$$F_s(W) = \bigoplus_{\lambda} E^{\lambda}(s)^{n_{\lambda}},$$

where $E^{\lambda}(k)$ is the irreducible representation of GL_k with Young diagram λ .

Remark 7.4.2. The Young diagrams appearing in either decomposition have at most s boxes. Furthermore F_s sends $\mathcal{L}_{k,\mathfrak{g}}$ to $\mathcal{L}_{s,\mathfrak{g}}$ and $\mathcal{L}_{k,\mathfrak{g},\mathbb{Q}}$ to $\mathcal{L}_{s,\mathfrak{g},\mathbb{Q}}$, if \mathfrak{g} is any Lie algebra of nilpotency class s . In particular, as k grows, $\mathcal{F}_{k,\mathfrak{g},\mathbb{Q}}$ has only boundedly many irreducible GL_k -submodules counting multiplicity in its decomposition, all obtained by the above process from the decomposition of $\mathcal{F}_{s,\mathfrak{g},\mathbb{Q}}$ into irreducible GL_s -submodules.

Proof. Note that elements of $\mathcal{F}_k^{\leq s}$ are linear combinations of brackets having at most s letters, and that $\mathcal{F}_k^{\leq s}$ decomposes into weight spaces for the diagonal action

$$(t_1, \dots, t_k) \cdot c(x_1, \dots, x_k) = c(t_1 x_1, \dots, t_k x_k).$$

If $W \leq \mathcal{F}_k^{(s)}$ is an irreducible GL_k -module, then it is generated by a highest weight vector, whose weight λ is of the form (n_1, \dots, n_k) with $n_i = 0$ if $i > s$. The corresponding GL_s -submodule $F_s(W)$ is generated by the same highest weight vector. It is therefore an irreducible GL_s -module with the same Young diagram. The result follows. \square

Given a Young diagram λ , by the Weyl dimension formula, the dimension $d_\lambda(k)$ of the irreducible GL_k -module associated to λ is:

$$d_\lambda(k) = \prod_{1 \leq i < j \leq k} \frac{\lambda_i - \lambda_j + j - i}{j - i}.$$

In particular, if i is the total number of boxes of λ , then $d_\lambda(k)$ is a degree i polynomial in k with rational coefficients. The number of boxes of $E^\lambda \leq \mathcal{F}_k^{\leq s}$ is the number of letters appearing in the brackets of the associated submodule of $\mathcal{F}_k^{\leq s}$. In particular, we obtain:

Corollary 7.4.3. *For $i = 1, \dots, s$, the map $k \mapsto \dim \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}^{[i]}$ is a polynomial in k of degree i with rational coefficients, provided $k \geq s$. From (7.7) the same holds for the growth exponent $\eta_G(k)$. More generally, there is a finite family F of rational polynomials of degree at most s such that for $k \geq s$, if W is any GL_k -submodule in $\mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}$ then $\dim W = P(k)$ for some $P \in F$.*

7.5. Stability of the exponent. We now prove the second part of Theorem 1.13 from the introduction, which we recall here, for convenience.

Theorem 7.5.1 (Stability of the exponent). *Let G be a connected and simply connected rational nilpotent real Lie group, and $d(\cdot, \cdot)$ a rational left-invariant geodesic metric on G . There exists a rational function $F_{\mathfrak{g}} \in \mathbb{Q}(X)$ with rational coefficients such that, for k large enough,*

$$\widehat{\beta}_k = F_{\mathfrak{g}}(k).$$

Proof. We already know from Corollary 7.4.3 that, for $k \geq s$, $\eta_G(k)$ is given by a degree s polynomial in k with rational coefficients. So in view of (7.8), we need only prove that $\widehat{\alpha}_k$ is given by a rational function, for large k . We saw in §7.3 that $\widehat{\alpha}_k = \tau_{\mathbb{Q}}(\mathcal{M})$, where $\tau_{\mathbb{Q}}(\mathcal{M})$ is given by (4.9) and takes the form (6.1) of the ratio of submodular functions, $-\psi_{\mathcal{M}}$ and $\phi_{\mathcal{M}}$ defined on the grassmannian $\mathrm{Grass}(V)$, where $V = \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}$.

The group GL_k acts by linear substitution on V and it preserves the flag of subspaces

$$V_i = \bigoplus_{j \geq i} \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}^{[j]} \quad (7.10)$$

defining the quasi-norm $|r|$ in (7.5), so the function ψ is GL_k -invariant. Noting that $gW \cap \ker \Phi(u) = g(W \cap \ker \Phi(g^{-1}u))$ for any $g \in \mathrm{GL}_k$, $u \in \mathfrak{g}^k$ and $W \leq V$, we conclude that $\psi_{\mathcal{M}}$ is GL_k -invariant. Similarly $\phi_{\mathcal{M}}$ is GL_k -invariant. We can therefore apply the submodularity Lemma 6.1.2, and conclude that there is a GL_k -invariant Δ -rational subspace $W \leq V$ such that

$$\widehat{\alpha}_k = \frac{\psi_{\mathcal{M}}(W)}{\phi_{\mathcal{M}}(W)}. \quad (7.11)$$

Combining (7.5) with (4.5) and (7.1) with (4.6) we obtain $\psi_{\mathcal{M}}$ and $\phi_{\mathcal{M}}$ explicitly in the form:

$$\psi_{\mathcal{M}}(W) = \sum_{i=1, \dots, s} (\dim(W \cap V_i) - \dim((W \cap V_i)(\mathbf{x}))) \quad (7.12)$$

$$\phi_{\mathcal{M}}(W) = \sum_{i=0, \dots, s-1} \dim \pi_i(W(\mathbf{x})) \quad (7.13)$$

for all $\mathbf{x} \in \mathfrak{g}^k$ in a Zariski open subset, where $\pi_i : \mathfrak{g} \rightarrow \mathfrak{g}/V^i$. Recall that $V_i \leq V = \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}$ is defined in (7.10) above, and $V^i \leq \mathfrak{g}$ at the beginning of this section; also note that this notation is not perfectly coherent with the notation in Section 5, where $\{V_i\}$ and $\{V'_i\}$ are *full* flags.

According to Proposition 7.4.1 and Corollary 7.4.3 the dimension of GL_k -invariant subspaces of $V = \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}$ can achieve only boundedly many values, each given by a polynomial in k with rational coefficients and degree at most s . It then follows from the special form (4.5) taken by ψ that $\psi_{\mathcal{M}}$ can only take boundedly many values, each of which is one of boundedly many polynomials in k of degree at most s and with rational coefficients. We conclude that the same holds for $\hat{\alpha}_k$, since ϕ is integer valued and bounded in terms of $\dim \mathfrak{g}$ only. When k is large enough (larger than a constant depending only on the size of the coefficients of these polynomials, hence only on $\dim \mathfrak{g}$), this maximum will be achieved by a single polynomial with rational coefficients and of degree at most s . In fact the degree will be exactly s , because of the Dirichlet lower bound and the fact that already with $W = \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}^{[s]}$, the function $k \mapsto \frac{\psi_{\mathcal{M}}(W)}{\phi_{\mathcal{M}}(W)}$ is a degree s polynomial. This completes the proof. \square

Now that we have finished proving Theorem 1.13, we briefly explain how to derive Corollary 1.14.

Proof of Corollary 1.14. The existence of the limit follows immediately from the theorem. To prove the upper bound, note that ϕ takes integer values, while ψ is bounded above by $s \dim \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}$, as follows from (4.5). However, according to the Bass-Guivarc'h formula (7.7), $\eta_G(k)$ is asymptotic to $s \dim \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}$. This shows the upper bound. For the lower bound, note that $\tau_{\mathbb{Q}}(\mathcal{M})$ is a maximum over the subspaces W ; evaluating at $W = \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}^{[s]}$, we get $\psi_{\mathcal{M}}(W) = s(\dim \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}^{[s]} - \dim \mathfrak{g}^{[s]})$ and $\phi_{\mathcal{M}}(W) \leq s \dim \mathfrak{g}^{[s]}$.

When $d(\cdot, \cdot)$ is Riemannian, all α'_i are 1 and then $\phi(W) \leq \dim \mathfrak{g}^{[s]}$. This ends the proof. We will see explicit examples in the next section, where both upper and lower bounds are attained for $\lim_k \hat{\beta}_k$, see also Remark 8.4.3. \square

Remark 7.5.2 (Irrational \mathfrak{g}). If $\mathcal{L}_{k, \mathfrak{g}}$ is not rational, then there is a non-trivial subspace $W \leq \mathcal{F}_{k, \mathfrak{g}, \mathbb{Q}}$ for which $\phi_{\mathcal{M}}(W) = 0$, and in particular $\tau(\mathcal{M}) = +\infty$, so we cannot conclude anything in this case. However if $\mathcal{L}_{k, \mathfrak{g}}$ is rational and even if \mathfrak{g} is not, we can assert that the conclusion of Theorem 1.13 holds in certain cases. For example it holds whenever $\mathcal{F}_{k, \mathfrak{g}}$ is multiplicity-free as a GL_k -module. Indeed in this case every GL_k -invariant subspace is rational (because GL_k is \mathbb{Q} -split). Since we know that the maximum in $\tau(\mathcal{M})$ is attained at a GL_k -invariant subspace, we obtain again $\tau(\mathcal{M}) = \tau_{\mathbb{Q}}(\mathcal{M})$ in

this case. We will make use of this observation in some of the examples below.

Remark 7.5.3 (The exponent is attained in the last step). Let

$$L = \{r \in \mathcal{F}_{k,\mathfrak{g},\mathbb{Q}} \mid r(\mathfrak{g}^k) \subset \mathfrak{g}^{(s)}\}.$$

When k is large enough, the GL_k -invariant rational subspace W realizing the maximum of $\psi_{\mathcal{M}}/\phi_{\mathcal{M}}$ in (7.11) can be chosen to belong to L . This can be seen easily by writing $W = W_0 \oplus W'_0$ with $W_0 = W \cap L$ for a GL_k -invariant W'_0 (which exists by complete reducibility of the GL_k action). Then from (7.12) it follows that $\psi_{\mathcal{M}}(W) - \psi_{\mathcal{M}}(W_0)$ is a polynomial of degree at most $s - 1$ in k , while $\phi_{\mathcal{M}}(W) > \phi_{\mathcal{M}}(W_0)$ unless $W = W_0$. From these two inequalities we see that, for large enough k ,

$$\frac{\psi_{\mathcal{M}}(W)}{\phi_{\mathcal{M}}(W)} \leq \frac{\psi_{\mathcal{M}}(W_0)}{\phi_{\mathcal{M}}(W_0)}.$$

8. EXPLICIT VALUES OF THE CRITICAL EXPONENT IN SOME EXAMPLES

In this final section, we illustrate Theorems 1.13 and 1.14 and work out an explicit value for the critical exponent $\widehat{\beta}_k$ in several examples. For definiteness we always assume in this section that the metric on G is Riemannian.

8.1. Nilpotent Lie groups of step 2. In this paragraph, G is a connected simply connected non-abelian nilpotent Lie group of step 2. We denote by d_i , $i = 1, 2$ the dimension of $\mathfrak{g}^{[i]}$. Here $\mathfrak{g}^{[1]} = \mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]$ and $\mathfrak{g}^{[2]} = [\mathfrak{g}, \mathfrak{g}]$.

It is easy to check that $d_2 \leq \frac{d_1(d_1-1)}{2}$. Moreover, by [ABRdS15a, Appendix A], $\mathcal{F}_{k,\mathfrak{g}}^{[1]}$ and $\mathcal{F}_{k,\mathfrak{g}}^{[2]}$ are both irreducible GL_k -modules of dimension k and $k(k-1)/2$ respectively. In particular Remark 7.5.2 applies and this implies that $\widehat{\alpha}_k = \frac{k(k-1)}{d_2} - 2$. Since $\eta_G(k) = k + k(k-1) = k^2$ according to (7.7), we get:

Theorem 8.1.1 (Step 2 nilpotent Lie groups). *Let G be a connected simply connected non-abelian nilpotent Lie group of step 2. Set $d_1 = \dim G/[G, G]$ and $d_2 = \dim[G, G]$ and let $k \geq d_1$ be an integer. The critical exponent for k -tuples in G is*

$$\widehat{\beta}_k = \frac{1}{d_2} - \frac{1}{d_2 k} - \frac{2}{k^2}.$$

In the special case of the 3-dimensional Heisenberg group, $d_2 = 1$ and we thus recover the computation made in Section 3.

8.2. Metabelian nilpotent Lie groups. Suppose now, more generally, that G is a simply connected metabelian nilpotent Lie group, that is we assume that $[G, G]$ is abelian. This does not constrain the nilpotency class. No assumption of rationality on G is made. It is shown in [ABRdS15a, §A.3] that $\mathcal{F}_{k,\mathfrak{g}}^{[i]}$ is irreducible as a GL_k -module for each i and isomorphic to $E^{(i-1,1)}(k)$. Hence Remark 7.5.2 applies. In particular, for k large we obtain:

$$\widehat{\alpha}_k = s \frac{\dim E^{(s-1,1)}(k)}{\dim G^{(s)}} - s.$$

On the other hand, the Bass-Guivarc'h formula reads:

$$\eta_G(k) = k + \sum_{i=2}^s i \dim E^{(i-1,1)}(k).$$

Using Weyl's dimension formula, we may compute $\dim E^{(i-1,1)}(k) = (i-1) \binom{i+k-2}{i}$ a polynomial of degree i in k .

Theorem 8.2.1 (Metabelian nilpotent groups). *When k is large enough the critical exponent is given by $\widehat{\beta}_k = \widehat{\alpha}_k / \eta_G(k)$ with the above polynomial expressions for $\widehat{\alpha}_k$ and $\eta_G(k)$. In particular,*

$$\lim_{k \rightarrow \infty} \widehat{\beta}_k = \frac{1}{\dim G^{(s)}}.$$

8.3. Unipotent upper triangular matrices. We now deal with the case of the group U_s of upper triangular unipotent $(s+1) \times (s+1)$ matrices. Its Lie algebra is the Lie algebra $\mathfrak{g} = \mathfrak{u}_s$ of upper triangular matrices with zero diagonal, and our first task will be to determine, for any positive integer k , the Lie algebra $\mathcal{F}_{k,\mathfrak{g}}$ of bracket maps on \mathfrak{g} on k letters. The result is the following.

Proposition 8.3.1. *Let k be a positive integer, and let $\mathfrak{g} = \mathfrak{u}_s$ be the Lie algebra of upper triangular $(s+1) \times (s+1)$ matrices with zero diagonal terms. The Lie algebra $\mathcal{F}_{k,\mathfrak{g}}$ of bracket maps on \mathfrak{g} on k letters is isomorphic to the free s -step nilpotent Lie algebra $\mathcal{F}_{k,s}$.*

An alternative formulation of Proposition 8.3.1 is in terms of the nilpotent group of unipotent upper triangular matrices:

Corollary 8.3.2. *Let U_s be the group of upper triangular unipotent $(s+1) \times (s+1)$ matrices, and let k be any positive integer. Then U_s contains the free nilpotent group of step s on k generators as a finitely generated subgroup.*

Proof of Proposition 8.3.1. Let $k \geq s$ be a positive integer and let \mathcal{F}_k denote the free Lie algebra on the k generators x_1, x_2, \dots, x_k . We have to check that $\mathfrak{g} = \mathfrak{u}_s$ has no non-trivial relation of degree less than or equal to s in \mathcal{F}_k . First, by the proof of [Bah87, Theorem 3, page 99] we note that if \mathfrak{g} satisfies a non-trivial relation, then it also satisfies a non-trivial multilinear relation whose degree is not larger. Now, if r is such a multilinear relation in \mathfrak{g} , then so is each of its homogeneous components, so we may assume r has degree one in each x_i , $1 \leq i \leq t$. In fact, we may also assume $t = s$, otherwise, we replace r by $[[r, x_{t+1}], \dots, x_s]$. So we just have to see that \mathfrak{g} has no multilinear relation in s variables.

Let \mathcal{H}_s be the vector space of all elements of \mathcal{F}_k of degree s that are multilinear in (x_1, x_2, \dots, x_s) . We want to check that the canonical map $\theta : \mathcal{H}_s \rightarrow \mathcal{F}_{k,\mathfrak{g}}$ is injective. By Witt's Formula [Hal76, Theorem 11.2.2],

$$\dim \mathcal{H}_s = (s-1)! \tag{8.1}$$

For σ a permutation of $\{1, 2, \dots, s\}$ fixing 1, we denote

$$m_\sigma = [\dots [[x_1, x_{\sigma(2)}], x_{\sigma(3)}], \dots, x_{\sigma(s)}].$$

This gives us a family (m_σ) of $(s-1)!$ elements in \mathcal{H}_s . We will show that its image $(\theta(m_\sigma))$ under θ is linearly independent in $\mathcal{F}_{k,\mathfrak{g}}$; together with (8.1), this will prove the theorem.

For $1 \leq i, j \leq s+1$ we denote by $E_{i,j}$ the matrix whose only non-zero entry is 1, in position (i, j) . For $1 \leq i \leq s$, we also let $e_i = E_{i,i+1}$. Using the relations $[E_{i,j}, E_{k,l}] = \delta_{jk}E_{il}$, one can compute the values of the $\theta(m_\sigma)$ on permutations of the s -tuple (e_i) , and get, for any two permutations σ and τ of $\{1, 2, \dots, s\}$, both fixing 1:

$$\theta(m_\sigma)(e_1, e_{\tau(2)}, \dots, e_{\tau(s)}) = \begin{cases} E_{s+1,s+1} & \text{if } \sigma = \tau^{-1} \\ 0 & \text{otherwise.} \end{cases}$$

This implies in particular that the family $(\theta(m_\sigma))$ is linearly independent, so we are done. \square

From Proposition 8.3.1, it is not difficult to compute the critical exponent for the group $G = U_s$ of unipotent upper triangular matrices. Indeed, if $r \in \mathcal{F}_k$ is a law of $\mathfrak{g}/\mathfrak{g}^{(s)}$, then $[x_{k+1}, r]$ is a law of \mathfrak{g} , hence has all its homogeneous components of degree at least $s+1$ according to Proposition 8.3.1. Hence $r \in \mathcal{F}_k^{[s]}$. Therefore Remark 7.5.3 applies and in computing the maximum $\tau(\mathcal{M})$ we may restrict attention to subspaces W in $\mathcal{F}_k^{[s]}$. For such W , $\psi_{\mathcal{M}}(W) = s(\dim W - \dim W(\mathfrak{g}^k))$ and $\phi_{\mathcal{M}}(W) \leq 1$, so we get

$$\widehat{\alpha}_k = s(\dim \mathcal{F}_k^{[s]} - 1) = \sum_{d|s} \mu(d)k^{s/d} - s$$

where we used Witt's formula [Hal76, Theorem 11.2.2] in the last equality. From the Bass-Guivarc'h formula (7.7) and Witt's formula again, we also compute

$$\eta_G(k) = \sum_1^s i \dim \mathcal{F}_k^{[i]} = \sum_1^s \sum_{d|i} \mu(d)k^{i/d} = \sum_{i \leq s} M\left(\frac{s}{i}\right)k^i, \quad (8.2)$$

where $M(x) = \sum_{n \leq x} \mu(n)$ is the Mertens function, and thus obtain:

Theorem 8.3.3 (Critical exponent for U_s). *Let U_s be the nilpotent group of unipotent upper triangular $(s+1) \times (s+1)$ matrices. Then for k large, the critical exponent for k -tuples in U_s is*

$$\widehat{\beta}_k = \frac{\sum_{d|s} \mu(d)k^{s/d} - s}{\sum_{i \leq s} M\left(\frac{s}{i}\right)k^i}$$

with $M(x) = \sum_{n \leq x} \mu(n)$ the Mertens function. In particular, $\lim_k \widehat{\beta}_k = 1$.

Note that the limit also follows directly from Theorem 1.14 since for $G = U_s$, we have $\dim G^{(s)} = 1$.

8.4. Free nilpotent Lie algebras. In this paragraph \mathfrak{g} will denote the free nilpotent Lie algebra $\mathcal{F}_{d,s}$ of step s on d generators. We will assume throughout that $d \geq s$.

Note that \mathfrak{g} has a natural structure of GL_d -module. Given a Young diagram λ , we denote by $d_\lambda(d)$ the dimension of the irreducible GL_d -representation $E^\lambda(d)$ associated to λ .

Theorem 8.4.1 (Critical exponent for free nilpotent groups). *Let G be the connected simply connected Lie group with Lie algebra $\mathfrak{g} = \mathcal{F}_{d,s}$. Assume that $d \geq s$. Then, if k is large enough, the critical exponent for k -tuples in G is*

$$\widehat{\beta}_k = \frac{s}{\binom{d+1}{s}} \cdot \frac{\binom{k+1}{s} - \binom{d+1}{s}}{\sum_{i \leq s} M\left(\frac{s}{i}\right) k^i}$$

where $M(x) = \sum_{n \leq x} \mu(n)$ is the Mertens function.

Passing to the limit, we get:

Corollary 8.4.2 (Limiting value). *For $d \geq s$, we have the following limit for the critical exponent for $\mathfrak{g} = \mathcal{F}_{d,s}$:*

$$\lim_{k \rightarrow +\infty} \widehat{\beta}_k = \frac{1}{(s-1)! \binom{d+1}{s}}.$$

Remark 8.4.3. This shows that the strict inequality $\frac{1}{\dim \mathfrak{g}^{(s)}} < \lim_k \widehat{\beta}_k < 1$ can happen.

We now pass to the proof of Theorem 8.4.1. Our Lie algebra \mathfrak{g} has the following special property: for each $k \geq s$ the laws of $\mathfrak{g}/\mathfrak{g}^{(s)}$ are either laws of \mathfrak{g} or are contained in $\mathcal{F}_{k,\mathfrak{g}}^{[s]}$ (i.e. if $r \in \mathcal{F}_{k,\mathfrak{g}}$ and $r(\mathfrak{g}^k) \leq \mathfrak{g}^{(s)}$, then $r \in \mathcal{F}_{k,\mathfrak{g}}^{[s]}$). So it follows from Remark 7.5.3 that the maximum value of $\tau_{\mathbb{Q}}(\mathcal{M})$ is attained at a rational GL_k -invariant subspace W that is contained in $\mathcal{F}_{k,\mathfrak{g}}^{[s]}$. For such a subspace $\psi_{\mathcal{M}}(W) = s(\dim W - \phi_{\mathcal{M}}(W))$ and $\phi_{\mathcal{M}}(W) = \dim W(\mathbf{x})$, where $W(\mathbf{x})$ is the image of W in \mathfrak{g} under evaluation at a generic \mathbf{x} in \mathfrak{g}^k . Note that if $k \geq s$, then, for \mathbf{x} in a dense Zariski open set in \mathfrak{g}^k , the space $W(\mathbf{x})$ is independent of \mathbf{x} , equal to the span $W_{\mathfrak{g}}$ of all $r(\mathbf{x}_1, \dots, \mathbf{x}_k)$, $r \in W$, $\mathbf{x}_1, \dots, \mathbf{x}_k \in \mathfrak{g}$. Thus,

$$\frac{1}{s} \widehat{\alpha}_k = \max \left\{ \frac{\dim W}{\dim W_{\mathfrak{g}}} - 1; W \leq \mathcal{F}_{k,\mathfrak{g}}^{[s]} \text{ rational } \mathrm{GL}_k\text{-module} \right\}.$$

Recall Proposition 7.4.1, which describes precisely the GL_k -submodules of $\mathcal{F}_{k,\mathfrak{g}}^{[s]}$. An immediate consequence of this proposition is the following simpler expression:

$$\frac{1}{s} \widehat{\alpha}_k = \max_{\lambda} \left\{ \frac{d_{\lambda}(k)}{d_{\lambda}(d)} \right\} - 1, \quad (8.3)$$

where the maximum is taken over all Young diagrams λ that appear in the decomposition of $\mathfrak{g}^{(s)}$ as a GL_d -module. The following theorem of Klyachko describes this set of diagrams:

Theorem 8.4.4 (Klyachko [Klj74, Reu93]). *Let $\mathfrak{g} = \mathcal{F}_{d,s}$. Then, except for (s) and $(1, 1, \dots, 1)$, with the further exceptions of $\lambda = (2, 2)$, when $s = 4$, and $\lambda = (2, 2, 2)$ when $s = 6$, all Young tableaux with s boxes and at most d rows appear in the decomposition of $\mathfrak{g}^{[s]}$ into irreducible GL_d -modules.*

We thus need to maximize $\frac{d_{\lambda}(k)}{d_{\lambda}(d)}$ over all diagrams with s boxes, at most d rows, and different from the above exceptions. For this we prove the following lemma:

Lemma 8.4.5. *Let μ and λ be two Young diagrams with at most d rows and having the same number of boxes. If μ can be obtained from λ by moving some boxes downwards, then for any $k \geq d$,*

$$\frac{d_\mu(k)}{d_\mu(d)} \geq \frac{d_\lambda(k)}{d_\lambda(d)}.$$

Proof. Without loss of generality we may assume that μ is obtained from λ by moving only one box downwards, i.e. $\mu_i = \lambda_i$, except for $\mu_r = \lambda_r - 1$ and $\mu_s = \lambda_s + 1$ for some indices $r < s$. Using Weyl's dimension formula:

$$d_\lambda(k) = \prod_{1 \leq i < j \leq k} \frac{\lambda_i - \lambda_j + j - i}{j - i},$$

we get

$$\frac{d_\lambda(k) d_\mu(d)}{d_\mu(k) d_\lambda(d)} = \prod_{d < j \leq k} \frac{\lambda_r + j - r}{\lambda_r + j - s} \frac{\lambda_s + j - r - 1}{\lambda_s + j - r}.$$

But $\lambda_s \leq \lambda_r$, and hence each factor in the above product is at most 1. \square

Combined with Klyachko's theorem, this lemma allows us to compute $\widehat{\alpha}_k$. The Young diagram λ present in $\mathfrak{g}^{(s)}$ and achieving the maximal value in (8.3) is the diagram with s boxes of the form $\lambda_0 := (2, 1, \dots, 1)$, because we have assumed $s \leq d$. Using Weyl's dimension formula, it is easy to compute

$$d_{\lambda_0}(k) = (s-1) \binom{k+1}{s}.$$

When $k \geq d \geq s$, the relatively free Lie algebra $\mathcal{F}_{k,\mathfrak{g}}$ coincides with the free Lie algebra $\mathcal{F}_{k,s}$ of step s . In particular, the growth exponent $\eta_G(k)$ is given by (8.2). Given that $\widehat{\beta}_k = \widehat{\alpha}_k / \eta_G(k)$, this concludes the proof of Theorem 8.4.1.

REFERENCES

- [ABRdS15a] M. Aka, E. Breuillard, L. Rosenzweig, and N. de Saxcé. Diophantine properties of nilpotent Lie groups. *Compos. Math.*, 151(6):1157–1188, 2015.
- [ABRdS15b] M. Aka, E. Breuillard, L. Rosenzweig, and N. de Saxcé. On metric Diophantine approximation in matrices and Lie groups. *C. R. Math. Acad. Sci. Paris*, 353(3):185–189, 2015.
- [Bah87] Yu. Bahturin. *Identical Relations in Lie Algebras*. VNU Science Press, 1987.
- [Bak76] R. C. Baker. Metric Diophantine approximation on manifolds. *J. London Math. Soc. (2)*, 14(1):43–48, 1976.
- [Bas72] H. Bass. The degree of polynomial growth of finitely generated nilpotent groups. *Proc. London Math. Soc.*, 25:603–614, 1972.
- [BB96] V. Beresnevich and V. Bernik. On a metrical theorem of W. Schmidt. *Acta Arith.*, 75(3):219–233, 1996.
- [BBKM02] V. Beresnevich, V. Bernik, D. Kleinbock, and G. Margulis. Metric Diophantine approximation: the Khintchine-Groshev theorem for nondegenerate manifolds. *Mosc. Math. J.*, 2(2):203–225, 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday.
- [BCR98] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*. Springer, 1998.
- [BD99] V. I. Bernik and M. M. Dodson. *Metric Diophantine approximation on manifolds*, volume 137 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1999.

- [BDSS] Emmanuel Breuillard, Tushar Das, Nicolas de Saxcé, and David Simmons. Strongly extremal manifolds. *in preparation*.
- [Ber88] V.N. Berestovskii. Homogeneous manifolds with an intrinsic metric. i. *Sibirsk. Math. Zh.*, 29(6):17–29, 1988.
- [BG73] Ju. A. Brudnyi and M. I. Ganzburg. A certain extremal problem for polynomials in n variables. *Izv. Akad. Nauk SSSR Ser. Mat.*, 37:344–355, 1973.
- [BKM01] V. Bernik, D. Kleinbock, and G. A. Margulis. Khintchine-type theorems on manifolds: the convergence case for standard and multiplicative versions. *Internat. Math. Res. Notices*, 9:453–486, 2001.
- [BKM15] V. Beresnevich, D. Kleinbock, and G. Margulis. Non-planarity and metric Diophantine approximation for systems of linear forms. *J. Théor. Nombres Bordeaux*, 27(1):1–31, 2015.
- [BRV16] V. Beresnevich, F. Ramirez, and S. Velani. Metric diophantine approximation: aspects of recent work. *preprint arXiv:1601.01948*, 2016.
- [CF13] T. Church and B. Farb. Representation theory and homological stability. *Adv. Math.*, 245:250–314, 2013.
- [Dan85] S. G. Dani. Divergent trajectories of flows on homogeneous spaces and Diophantine approximation. *J. Reine Angew. Math.*, 359:55–89, 1985.
- [DFSU15] T. Das, L. Fishman, D. Simmons, and M. Urbański. Extremality and dynamically defined measures, part I: Diophantine properties of quasi-decaying measures. *preprint arXiv:1504.04778*, 2015.
- [DS16] T. Das and D. Simmons. A proof of the matrix version of Baker’s conjecture in diophantine approximation. *preprint arXiv:1510.09195*, 2016.
- [GH94] Ph. Griffiths and J. Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1994. Reprint of the 1978 original.
- [GHS⁺09] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, and B. Virag. On the girth of random Cayley graphs. *Random Structures Algorithms*, 35(1):100–117, 2009.
- [GJS99] A. Gamburd, D. Jacobson, and P. Sarnak. Spectra of elements in the group ring of $SU(2)$. *J. Eur. Math. Soc. (JEMS)*, 1(1):51–85, 1999.
- [Gor07] Alexander Gorodnik. Open problems in dynamics and related fields. *J. Mod. Dyn.*, 1(1):1–35, 2007.
- [Gui73] Y. Guivarc’h. Croissance polynomiale et périodes des fonctions harmoniques. *Bull. Sc. Math. France*, 101:353–379, 1973.
- [Hal76] Marshall Hall, Jr. *The theory of groups*. Chelsea Publishing Co., New York, 1976. Reprinting of the 1968 edition.
- [Kle98a] D. Kleinbock. Bounded orbits conjecture and Diophantine approximation. In *Lie groups and ergodic theory (Mumbai, 1996)*, volume 14 of *Tata Inst. Fund. Res. Stud. Math.*, pages 119–130. Tata Inst. Fund. Res., Bombay, 1998.
- [Kle98b] D. Kleinbock. Flows on homogeneous spaces and Diophantine properties of matrices. *Duke Math. J.*, 95(1):107–124, 1998.
- [Kle03] D. Kleinbock. Extremal subspaces and their submanifolds. *Geom. Funct. Anal.*, 13(2):437–466, 2003.
- [Kle08a] D. Kleinbock. Diophantine properties of measures and homogeneous dynamics. *Pure Appl. Math. Q.*, 4(1, Special Issue: In honor of Grigory Margulis. Part 2):81–97, 2008.
- [Kle08b] D. Kleinbock. An extension of quantitative nondivergence and applications to Diophantine exponents. *Trans. Amer. Math. Soc.*, 360(12):6497–6523, 2008.
- [Kle10a] D. Kleinbock. An ‘almost all versus no’ dichotomy in homogeneous dynamics and Diophantine approximation. *Geom. Dedicata*, 149:205–218, 2010.
- [Kle10b] D. Kleinbock. Quantitative nondivergence and its Diophantine applications. In *Homogeneous flows, moduli spaces and arithmetic*, volume 10 of *Clay Math. Proc.*, pages 131–153. Amer. Math. Soc., Providence, RI, 2010.
- [Klj74] A. A. Kljačko. Lie elements in a tensor algebra. *Sibirsk. Mat. Ž.*, 15:1296–1304, 1430, 1974.

- [KLW04] D. Kleinbock, E. Lindenstrauss, and B. Weiss. On fractal measures and Diophantine approximation. *Selecta Math.*, 10(4):479–523, 2004.
- [KM98] D. Y. Kleinbock and G. A. Margulis. Flows on homogeneous spaces and Diophantine approximation on manifolds. *Ann. of Math. (2)*, 148(1):339–360, 1998.
- [KM99] D. Kleinbock and G. Margulis. Logarithm laws for flows on homogeneous spaces. *Invent. Math.*, 138:431–494, 1999.
- [KMW10] D. Kleinbock, G. Margulis, and J. Wang. Metric Diophantine approximation for systems of linear forms via dynamics. *Int. J. Number Theory*, 6(5):1139–1168, 2010.
- [KR01] V. Kaloshin and I. Rodnianski. Diophantine properties of elements of $SO(3)$. *Geom. Funct. Anal.*, 11(5):953–970, 2001.
- [KW08] D. Kleinbock and B. Weiss. Dirichlet’s theorem on Diophantine approximation and homogeneous flows. *J. Mod. Dyn.*, 2(1):43–62, 2008.
- [Mah42] K. Mahler. Über das Mass der Menge aller S -Zahlen. *Math. Ann.*, 106:131–139, 1942.
- [Mar71] G. A. Margulis. The action of unipotent groups in a lattice space. *Mat. Sb. (N.S.)*, 86(128):552–556, 1971.
- [Mar75] G. A. Margulis. On the action of unipotent groups in the space of lattices. In *Lie groups and their representations (Proc. Summer School, Bolyai, János Math. Soc., Budapest, 1971)*, pages 365–370. Halsted, New York, 1975.
- [Rag72] M. S. Raghunathan. *Discrete subgroups of Lie groups*. Springer-Verlag, 1972.
- [Reu93] C. Reutenauer. *Free Lie Algebras*. Oxford University Press, 1993.
- [Spr64] V. G. Sprindžuk. More on Mahler’s conjecture. *Dokl. Akad. Nauk SSSR*, 155:54–56, 1964.
- [Spr69] V. G. Sprindžuk. *Mahler’s problem in metric number theory*. Translated from the Russian by B. Volkmann. Translations of Mathematical Monographs, Vol. 25. American Mathematical Society, Providence, R.I., 1969.
- [Var14] P. P. Varjú. Diophantine property in the group of affine transformations of the line. *Acta Sci. Math. (Szeged)*, 80(3-4):447–458, 2014.

M.A. DEPARTEMENT MATHÉMATIK, ETH ZÜRICH, RÄMISTRASSE 101, 8092 ZÜRICH, SWITZERLAND

E-mail address: `menashe-hai.akka@math.ethz.ch`

MATHEMATISCHES INSTITUT, 62 EINSTEINSTRASSE, UNIVERSITÄT MÜNSTER, MÜNSTER, GERMANY

E-mail address: `emmanuel.breuillard@uni-muenster.de`

DEPARTMENT OF MATHEMATICS, ORT BRAUDE COLLEGE, P.O.BOX 78, KARMIEL 21982, ISRAEL

E-mail address: `liorr@braude.ac.il`

CNRS – UNIVERSITÉ PARIS-NORD, LAGA, 93430 VILLETANEUSE, FRANCE

E-mail address: `desaxce@math.univ-paris13.fr`