COMPOSITIO MATHEMATICA

Diophantine properties of nilpotent Lie groups

Menny Aka, Emmanuel Breuillard, Lior Rosenzweig and Nicolas de Saxcé

Compositio Math. **151** (2015), 1157–1188.

doi:10.1112/S0010437X14007854

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
150 YEARS

Compositio Math. 151 (2015) 1157–1188
doi:10.1112/S0010437X14007854

Diophantine properties of nilpotent Lie groups

Menny Aka, Emmanuel Breuillard, Lior Rosenzweig and Nicolas de Saxcé

Abstract

A finitely generated subgroup Γ of a real Lie group G is said to be Diophantine if there is $\beta > 0$ such that non-trivial elements in the word ball $B_\Gamma(n)$ centered at $1 \in \Gamma$ never approach the identity of G closer than $|B_\Gamma(n)|^{-\beta}$. A Lie group G is said to be Diophantine if for every $k \geqslant 1$ a random k-tuple in G generates a Diophantine subgroup. Semi-simple Lie groups are conjectured to be Diophantine but very little is proven in this direction. We give a characterization of Diophantine nilpotent Lie groups in terms of the ideal of laws of their Lie algebra. In particular we show that nilpotent Lie groups of class at most 5, or derived length at most 2, as well as rational nilpotent Lie groups are Diophantine. We also find that there are non-Diophantine nilpotent and solvable (non-nilpotent) Lie groups.

Contents

1. Introduction

Let G be a connected real Lie group, endowed with a left-invariant Riemannian metric d. We investigate Diophantine properties of finitely generated subgroups of G. If $\Gamma = \langle S \rangle$ is a subgroup of G with finite generating set S, we define, for $n \in \mathbb{N}$,

$$\delta_\Gamma(n) = \min\{d(x,1) \mid x \in B_\Gamma(n), x \neq 1\}$$

where $B_\Gamma(n) = (S \cup S^{-1} \cup \{1\})^n$ is the ball of radius n centered at 1 for the word metric defined by the generating set S. We will say that $\Gamma = \langle S \rangle$ is *β-Diophantine* if there exists a constant $c > 0$ (depending maybe on Γ and S and d) such that, for all $n \geqslant 1$,

$$\delta_\Gamma(n) \geqslant c \cdot |B_\Gamma(n)|^{-\beta}.$$

In general, the Diophantine exponent β may depend on the choice of a generating set S. But if G is nilpotent, then it depends neither on the choice of generating set of Γ, nor on the choice of

Received 8 July 2013, accepted in final form 23 June 2014, published online 13 January 2015.
2010 Mathematics Subject Classification 22E25, 11K60 (primary), 17B01 (secondary).
Keywords: word maps, nilpotent Lie groups, Diophantine subgroup, equidistribution.

left-invariant Riemannian metric. So the notion of a β-Diophantine finitely generated subgroup of G makes sense without mention of a choice of generating set, or metric.[1] This notion naturally generalizes the classical notion of a Diophantine number in dynamical systems and number theory: $\gamma \in \mathbf{R}/\mathbf{Z}$ is a Diophantine rotation if and only if the cyclic subgroup it generates in the torus $\mathbf{R}/\mathbf{Z}$ is Diophantine in our sense.

We will say that the ambient group G is *β-Diophantine* for k-tuples if almost every k-tuple of elements of G, chosen with respect to the Haar measure of G^k, generates a β-Diophantine subgroup. We will also say that G is Diophantine for k-tuples if G is β-Diophantine for k-tuples and some $\beta = \beta(k) > 0$. Finally we say that G is Diophantine if for every integer $k \geqslant 1$ it is Diophantine for k-tuples. We will show that for every k there are Lie groups G that are Diophantine for k-tuples, but not for $(k+1)$-tuples (see Theorem 1.4). However, if G is Diophantine and nilpotent then β can always be chosen independently of k (see Theorem 1.8).

When the ambient group G is a connected abelian Lie group, the behavior of $\delta_\Gamma(n)$ depends on the rational approximations to a set of generators of Γ. This case has been much studied in the past and constitutes a classical chapter of Diophantine approximation. For example, from Dodson's generalization [Dod92] of Jarník's Theorem [Jar31], it is not difficult to compute the Hausdorff dimension of the set of β-Diophantine k-tuples in any abelian connected Lie group.

On the other hand, little is known in the non-commutative setting. Gamburd, Jakobson and Sarnak [GJS99] first identified the relevance of the Diophantine property for dense subgroups of $G = \mathrm{SU}(2)$ in their study of the spectral properties of averaging operators on $L^2(\mathrm{SU}(2))$ and the speed of equidistribution of random walks therein. In particular they stressed that, although there is a G_δ-dense set of k-tuples in SU(2) which are not Diophantine (this assertion still holds in any nilpotent Lie group as we will see, cf. Proposition 5.1), every k-tuple whose matrix entries are algebraic numbers is a Diophantine tuple. Then it is natural to conjecture (as Gamburd *et al.* did in [GHSSV09, Conjecture 29]) that almost every k-tuple in the measure-theoretic sense is Diophantine. Although this remains an open problem, Kaloshin and Rodnianski [KR01] have shown that almost every k-tuple in SU(2) generates a subgroup Γ which is weakly Diophantine in the sense that $B_\Gamma(n)$ avoids a ball of radius $e^{-C_k n^2}$ centered at 1 (the genuine Diophantine property as defined above would require this radius to be much larger, namely bounded below by some $e^{-C_k n}$). Similarly the second-named author showed in [Bre11, Corollary 1.11] (as a consequence of the uniform Tits alternative) that every k-tuple generating a dense subgroup of SU(2) satisfies a closely related weak form of the Diophantine property. Finally Bourgain and Gamburd proved in [BG08] that every (topologically generating) k-tuple in SU(2) whose matrix entries are algebraic numbers has a spectral gap in $L^2(\mathrm{SU}(2))$. Their proof uses the Diophantine property of these k-tuples in an essential way. Conjecturally almost all, and perhaps even all, topologically generating k-tuples in SU(2) have a spectral gap (cf. Sarnak's spectral gap conjecture [Sar90, p. 58]).

Recently Varjú [Var12] tackled a similar problem for the group of affine transformations of the line, the $\{ax + b\}$ group, and showed that in a certain one-parameter family of 2-tuples in this group, almost every 2-tuple is Diophantine.

In this paper we investigate Diophantine properties of finitely generated subgroups of nilpotent and solvable Lie groups. Perhaps the main surprise in our findings is that, in sharp contrast with the abelian case, not every solvable or nilpotent real Lie group is Diophantine.

[1] The left-invariant assumption is just for convenience, because any two Riemannian metrics on G are comparable in a neighborhood of the identity; however, it is important that the metric be Riemannian. Allowing the metric to be sub-Riemannian could affect the Diophantine exponents, yet not the property of being Diophantine.

We exhibit examples of connected nilpotent Lie groups G of nilpotency class 6 and higher, and of non-nilpotent connected solvable Lie groups G of derived length 3 and higher, which are not Diophantine; and, indeed, in those examples one can find, for every $k \geqslant 3$, a sequence of words w_n in k-letters, which are not laws of G, but behave like almost laws (see § 5.4) inasmuch as, for any fixed compact set K in G^k, $w_n(K) \to 1$ with arbitrarily fast speed as the length of the word $l(w_n)$ tends to $+\infty$. To put it briefly, the bad behavior of Liouville numbers with respect to Diophantine approximation by rationals can be replicated to build real Lie algebras exhibiting this bad behavior. Of course such Lie algebras are not defined over $\mathbf{Q}$.

If $\mathfrak{g}$ is a Lie algebra of step s, we define the ideal of laws on k letters $\mathcal{L}_{k,s}(\mathfrak{g})$ of $\mathfrak{g}$ as the set of all elements of the free step s nilpotent Lie algebra on k generators $\mathcal{F}_{k,s}$ that are identically zero when evaluated on k-tuples of elements of $\mathfrak{g}$. We show that the property of being Diophantine for a connected s-step nilpotent Lie group G is intimately related to the way the ideal of laws on k letters $\mathcal{L}_{k,s}(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ of G sits in the free s-step nilpotent Lie algebra $\mathcal{F}_{k,s}$ on k generators. Although $\mathcal{F}_{k,s}$ is naturally defined over $\mathbf{Q}$, the ideal of laws $\mathcal{L}_{k,s}(\mathfrak{g})$ may not be and we have a natural epimorphism of real Lie algebras:

$$\Lambda : \mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}} \to \mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})$$

where $\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}$ is the real vector space spanned by $\mathcal{L}_{k,s}(\mathfrak{g}) \cap \mathcal{F}_{k,s}(\mathbf{Q})$. It is the Diophantine properties of the kernel of Λ viewed as a real subspace of $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}$ which determines the Diophantine properties of G as a Lie group. In brief, a real subspace of a real vector space defined over $\mathbf{Q}$ is said to be Diophantine if integer points outside it cannot be too close to it (see Definition 3.10 below). It turns out that if $s \leqslant 5$, then $\mathcal{L}_{k,s}(\mathfrak{g})$ is always defined over $\mathbf{Q}$ regardless of $\mathfrak{g}$, and hence Diophantine. Recall that there is a continuous family of non-isomorphic 2-step nilpotent Lie algebras, so $\mathfrak{g}$ may not be defined over $\mathbf{Q}$ or over a number field and still give rise to a Diophantine Lie group. Similarly if G is metabelian (i.e. if $\mathcal{L}_{k,s}$ contains the ideal generated by all double commutators $[[x,y],[z,w]]$), then $\mathcal{L}_{k,s}(\mathfrak{g})$ is again defined over $\mathbf{Q}$, regardless of s and of $\mathfrak{g}$ (see Theorem 4.5 below). This follows from a study (made in the appendix) of the multiplicities of the irreducible SL_k-submodules of $\mathcal{L}_{k,s}(\mathfrak{g})$, where SL_k acts by substitution of the variables.

We now summarize the above discussion and state our results. See § 3 for precise definitions and notation. The nilpotent real Lie groups considered in this paper will always be endowed with a left-invariant Riemannian metric.

Theorem 1.1. *Let G be a connected nilpotent Lie group with Lie algebra $\mathfrak{g}$. For any integer $k \geqslant 1$, the following are equivalent.*

(1) *The group G is Diophantine for k-tuples.*

(2) *The ideal of laws on k letters of $\mathfrak{g}$, $\mathcal{L}_{k,s}(\mathfrak{g})$, is a Diophantine subspace of the free s-step nilpotent Lie algebra on k generators $\mathcal{F}_{k,s}$.*

It may seem surprising at first glance that this criterion for Diophantinity is given only in terms of Lie algebra laws as opposed to group laws. However, as is well known, nilpotent Lie groups are best analyzed through their Lie algebra and there is a simple relation between word maps in G and bracket maps in $\mathfrak{g}$ (see Lemma 3.5 below).

The proof of Theorem 1.1 relies on a Borel–Cantelli argument (analogous to the classical one showing that almost every real number is Diophantine and to the one used by Kaloshin and Rodnianski [KR01]) and sub-level sets estimates for polynomial maps, originating in the work of Remez (see Theorem 2.8) and related to the (C,α)-good functions of Kleinbock and Margulis [KM98].

This criterion immediately settles the case of nilpotent Lie groups whose Lie algebra has rational (or even algebraic) structure constants.

Corollary 1.2. *If G is a connected rational nilpotent Lie group, then it is Diophantine.*

Combining Theorem 1.1 with a study of the structure of fully invariant ideals of the free Lie algebra on k letters, we are also able to construct examples of non-Diophantine nilpotent Lie groups, and to show that such groups must have nilpotency step at least 6.

Theorem 1.3. *Fix an integer $k \geqslant 3$ (respectively $k = 2$). Then, all connected nilpotent Lie groups of step $s \leqslant 5$ (respectively $s \leqslant 6$) are Diophantine for k-tuples, but for all integers $s > 5$ (respectively $s > 6$), there exists a connected nilpotent Lie group of step s that is not Diophantine for k-tuples.*

The numbers $s = 6$ and $s = 5$ appear here for the following reason: the free s-step nilpotent Lie algebra on k letters $\mathcal{F}_{k,s}$ admits multiplicity as an SL_k-module if and only if $s \geqslant 6$ when $k \geqslant 3$ and if and only if $s \geqslant 7$ when $k = 2$. See Theorem A.2. The existence of multiplicity allows one to construct fully invariant ideals of $\mathcal{F}_{k,s}$ which are not Diophantine, hence giving rise to non-Diophantine Lie groups via Theorem 1.1.

The decomposition of $\mathcal{F}_{k,s}$ into irreducible SL_k-modules has been very much studied in the literature on free Lie algebras starting with Witt [Wit37] and Klyachko [Klj74]. See [Reu93] for a book treatment. We survey some of these results in the appendix. In particular, we recall a relatively recent formula due to Kraskiewicz and Weyman [KW01], which allows one to compute the multiplicity of any given irreducible submodule of $\mathcal{F}_{k,s}$ in terms of its Young diagram. Together with Theorem 1.1 this allows us to show the following.

Theorem 1.4. *For every integer $k \geqslant 1$, there exists a connected (nilpotent) Lie group, which is Diophantine for k-tuples, but not for $(k+1)$-tuples.*

We also give two other applications of Theorem 1.1. The first one concerns connected nilpotent Lie groups that are metabelian, i.e. solvable of derived length 2.

Theorem 1.5. *Every metabelian connected nilpotent Lie group is Diophantine.*

Again the point here is the fact that the free metabelian Lie algebra is multiplicity-free as an SL_k-module (see Lemma A.9). The second application is a construction of a solvable non-nilpotent non-Diophantine Lie group.

Proposition 1.6. *There exists a connected solvable non-nilpotent Lie group that is not Diophantine.*

For a nilpotent Lie group with Lie algebra $\mathfrak{g}$ set $d_i = \dim \mathfrak{g}^{(i)}/\mathfrak{g}^{(i+1)}$, where $\mathfrak{g}^{(i)}$ is the ith term of the central descending series. The next statement clarifies what happens to a topologically generic tuple in Diophantine and non-Diophantine nilpotent Lie groups.

Theorem 1.7. *Let G be a connected s-step nilpotent Lie group.*

(1) *Regardless of whether G is Diophantine or not, if $k > d_1$, then there is a G_δ-dense set of k-tuples in G^k which are not Diophantine.*

(2) *If G is non-Diophantine for k-tuples, then there is a proper closed algebraic subvariety of G^k outside of which every k-tuple is non-Diophantine. In particular there is an open dense subset of G^k made of non-Diophantine tuples.*

Finally we study the dependence in k, the size of the k-tuple and prove the following (see § 5.2).

THEOREM 1.8. *Let G be a connected s-step nilpotent Lie group.*

(1) *The group G is Diophantine if and only if it is Diophantine for s-tuples.*

(2) *If G is Diophantine, and β_k is the infimum of the $\beta > 0$ such that G is β-Diophantine on k-tuples, $1/d_s \leqslant \liminf \beta_k \leqslant \limsup \beta_k \leqslant s$ as $k \to +\infty$.*

The lower bound on $\liminf \beta_k$ follows from a simple pigeonhole argument (analogous to Dirichlet's principle in Diophantine approximation), while the upper bound on $\limsup \beta_k$ relies on Theorem 1.1 and the sharp Remez-type inequality derived in Theorem 2.8 together with a study of $\mathcal{L}_{k,s}(\mathfrak{g})$ as k grows.

Remark 1.9. From this theorem, we see that the exponent β seems to carry some interesting information on the group G. It is reassuring that it does not degenerate to either 0 or $+\infty$ as k grows. More importantly it makes much sense to try to determine the critical $\beta > 0$ below which almost no k-tuple is Diophantine and above which almost all are. The work of Kleinbock and Margulis [KM98] is much relevant here. For example, in the case of the Heisenberg groups, a simple application of [KM98] yields the exact value of critical β for each k. We plan to tackle this problem in a future paper.

The paper is organized as follows. After giving the general setting of our work and some preliminary lemmas in § 2, we prove Theorem 1.1 in § 3. Section 4 is devoted to the study of fully invariant ideals of the free Lie algebra and to the proof of Theorem 1.3. This section makes use of some computations on the free Lie algebra given in the appendix. The last section contains the proofs of Theorems 1.4, 1.7 and 1.8 and further remarks.

2. Preliminaries

2.1 Nilpotent Lie groups

We briefly review some elementary theory of nilpotent Lie groups. Proofs of all the results mentioned below may be found in [CG90, ch. 1]. Let $\mathfrak{g}$ be a Lie algebra over $\mathbb{R}$. The *descending central series* of $\mathfrak{g}$ is defined inductively by

$$\mathfrak{g}^{(1)} := \mathfrak{g}, \mathfrak{g}^{(l+1)} := [\mathfrak{g}, \mathfrak{g}^{(l)}] = \operatorname{span}_{\mathbb{R}}\{[X, Y] : X \in \mathfrak{g}, Y \in \mathfrak{g}^{(l)}\}.$$

The algebra $\mathfrak{g}$ is said to be *nilpotent* if $\mathfrak{g}^{(s+1)} = 0$ for some $s \in \mathbb{N}$. If s is the smallest integer such that, $\mathfrak{g}^{(s+1)} = 0$, then $\mathfrak{g}$ is said to be *nilpotent of step (or class) s*.

A connected Lie group G is called nilpotent if its Lie algebra is nilpotent, or, equivalently, if it is nilpotent as a group. We have the following basic result (see [CG90, Theorem 1.2.1]).

PROPOSITION 2.1. *Let G be a connected simply connected nilpotent Lie group with Lie algebra $\mathfrak{g}$. Then, the exponential map $exp : \mathfrak{g} \to G$ is a diffeomorphism.*

As a consequence, every connected simply connected nilpotent Lie group G can be diffeomorphically identified with its Lie algebra $\mathfrak{g}$. The product operation on $G \simeq (\mathfrak{g}, *)$ is then given explicitly by the Campbell–Baker–Hausdorff formula: for all $X, Y \in \mathfrak{g}$,

$$X * Y = \sum_{n>0} \frac{(-1)^{n+1}}{n} \sum_{\substack{p_i+q_i>0 \\ 1\leqslant i\leqslant n}} \frac{(\sum_{1\leqslant i\leqslant n} p_i + q_i)^{-1}}{p_1!q_1!\cdots p_n!q_n!} (\operatorname{ad} X)^{p_1}(\operatorname{ad} Y)^{q_1}\cdots(\operatorname{ad} X)^{p_n}(\operatorname{ad} Y)^{q_n-1}Y.$$

(If $q_n = 0$, the term in the sum ends with $\cdots(\operatorname{ad} X)^{p_n-1}X$ instead of $(\operatorname{ad} X)^{p_n}(\operatorname{ad} Y)^{q_n-1}Y$; of course, if $q_n > 1$, or if $q_n = 0$ and $p_n > 1$, then the term is zero.) If G is nilpotent of step s, this

sum is finite: only commutators of length no greater than s may be non-zero. For example, for nilpotent groups of step 2, the Campbell–Baker–Hausdorff formula reads

$$X * Y = X + Y + \tfrac{1}{2}[X, Y]$$

and for nilpotent groups of step 3

$$X * Y = X + Y + \tfrac{1}{2}[X, Y] + \tfrac{1}{12}[X, [X, Y]] + \tfrac{1}{12}[Y, [Y, X]].$$

From now on, whenever we are considering a connected simply connected nilpotent Lie group G we realize it as the algebra $\mathfrak{g} = \mathrm{Lie}(G)$ equipped with the multiplication $*$ given by the Campbell–Baker–Hausdorff formula. The identity element of G will therefore be denoted by 0. Also, if $\mathfrak{g}$ is a nilpotent Lie algebra, we will denote by $(\mathfrak{g}, *)$ the corresponding connected simply connected nilpotent Lie group.

2.2 Word maps on nilpotent Lie groups

Let F_k be the free non-abelian group on k letters $x_1, \ldots, x_k$. For any group G, any word $w \in F_k$ induces a map

$$\begin{array}{rccc} w_G : & G^k & \longrightarrow & G \\ & \mathbf{g} = (g_1, \ldots, g_n) & \longmapsto & w(\mathbf{g}) \end{array}$$

where $w(\mathbf{g})$ is the element of G one gets by substituting g_i for x_i in w. A *word map ω on k letters on G* is a map that can be obtained in this way: $\omega = w_G$ for some $w \in F_k$. For Lie groups, word maps are smooth, and we will see in this subsection that, for nilpotent Lie groups, they are polynomial maps of degree bounded by the nilpotency step of G.

Definition 2.2. Let V and W be two finite-dimensional vector spaces. A map $f : V \to W$ is said to be *polynomial of degree at most d* if it is a polynomial map of degree at most d when expressed in some (or any) bases for V and W.

In the following lemma, $G = (\mathfrak{g}, *)$ is endowed with the vector space structure coming from the Lie algebra $\mathfrak{g}$.

Lemma 2.3. *Let G be a connected simply connected Lie group, nilpotent of step s. For any word $w \in F_k$, the map $w_G : G^k \to G$ is a polynomial map of degree at most s.*

Proof. The map $(X, Y) \mapsto [X, Y]$ is bilinear, and therefore any map of the form

$$(X_1, \ldots, X_k) \mapsto [X_{i_1}, [X_{i_2}, \ldots, [X_{i_{s-1}}, X_{i_s}] \ldots]]$$

is polynomial of degree at most s. Now, from the Campbell–Baker–Hausdorff formula, one sees that the word map w_G can be expressed as a linear combination of such brackets, and this proves the lemma. □

Definition 2.4 (Length of a word map). For ω a word map on k letters on G, set

$$l(\omega) := \min\{l(w); w \in F_k \text{ and } w_G = \omega\}$$

and call it the *length of ω*. Here $l(w)$ denotes the length of the word w.

Lemma 2.5 (Group of word maps). *The set $F_{k,G}$ of word maps on k letters on a group G has a natural group structure, and we have the following properties.*

(1) *The group $F_{k,G}$ is finitely generated.*

(2) *If G is a nilpotent group of step s, then so is $F_{k,G}$.*
(3) *If G is a connected Lie group, then, for almost every k-tuple $\mathbf{g} = (g_1, g_2, \dots, g_k) \in G^k$, the subgroup $\Gamma_{\mathbf{g}}$ generated by the subset $\{g_1, g_2, \dots, g_k\}$ is isomorphic to $F_{k,G}$.*

Proof. Let F_k be the abstract free group on k letters $x_1, \dots, x_k$. The group structure on $F_{k,G}$ is uniquely defined by the fact that the surjective map

$$\begin{array}{rccc} \Phi : & F_k & \to & F_{k,G} \\ & w & \mapsto & w_G \end{array}$$

is a group homomorphism. Parts (1) and (2) are clear. To justify part (3), note that if $w \notin \ker \Phi$, then the set of $\mathbf{g} \in G^k$ such that $w(\mathbf{g}) = 0$ is a proper analytic subvariety of G^k, and hence has zero Lebesgue measure. They are only countably many such w, so we see that, for almost every k-tuple $\mathbf{g} \in G^k$, the unique group homomorphism $\theta_{\mathbf{g}} : F_k \to \Gamma_{\mathbf{g}}$ mapping x_i to g_i for $i \in \{1, \dots, k\}$ has kernel exactly $\ker \Phi$. Hence $\Gamma_{\mathbf{g}}$ is isomorphic to $F_{k,G}$. □

Recall (cf. [Bas72, Gui73, Pan83]) that every finitely generated s-step nilpotent group $\Gamma = \langle S \rangle$ has polynomial growth, and, more precisely, there is an integer $\tau(\Gamma) \in \mathbf{N}$ independent of the generating set S such that $|B_\Gamma(n)| \sim c_S \cdot n^{\tau(\Gamma)}$ for some constant $c_S > 0$. The growth exponent $\tau(\Gamma)$ is given by the Bass–Guivarc'h formula:

$$\tau(\Gamma) = \sum_{k=1}^{s} k \cdot \mathrm{rk}(\Gamma^{(k)}/\Gamma^{(k+1)}), \tag{1}$$

where the $\Gamma^{(k)}$ are the terms of the central descending series of Γ and rk the (torsion-free) rank of the corresponding abelian group. We conclude that the following corollary holds.

COROLLARY 2.6 (Generic growth for a random subgroup). *Let τ_k be the growth exponent of the finitely generated group $F_{k,G}$. Then, for almost every $\mathbf{g} \in G^k$, the group $\Gamma_{\mathbf{g}}$ has growth exponent τ_k.*

2.3 Estimates on polynomial maps

The purpose of this paragraph is to derive the elementary estimates on the measure of the set of points on which a polynomial takes small values.

Let B be a convex subset of $\mathbf{R}^n$, and $f : B \to \mathbf{R}$ a real-valued polynomial function of degree at most d. For $\epsilon > 0$, we set $Z_{\epsilon,B}(f) := \{x \in B; |f(x)| \leqslant \epsilon\}$. Then, from Brudnyi and Ganzburg [GB73], we have the following.

THEOREM 2.7 (Remez-type inequality).

$$\sup_{x \in B} |f(x)| \leqslant \epsilon \cdot T_d\left(\frac{1 + (1 - |Z_{\epsilon,B}(f)|/|B|)^{1/n}}{1 - (1 - |Z_{\epsilon,B}(f)|/|B|)^{1/n}}\right)$$

where T_d is the dth Chebyshev polynomial of the first kind.

Here $|B|$ denotes the Lebesgue measure of B in $\mathbf{R}^n$. It is well known that those Remez-type inequalities imply the following estimate; we recall the proof for convenience of the reader.

PROPOSITION 2.8 (Sublevel set estimate). *Fix $n_1, n_2, d \in \mathbf{N}^*$. For any polynomial map $f : \mathbf{R}^{n_1} \to \mathbf{R}^{n_2}$ of degree at most d and any convex subset of B of $\mathbf{R}^{n_1}$, one has*

$$|\{x \in B; \|f(x)\| \leqslant \epsilon\}| \leqslant 4 \cdot n_1 \left(\frac{\epsilon}{\|f\|_B}\right)^{1/d} |B|, \tag{2}$$

where $\|f\|_B := \sup_{x\in B}\|f(x)\|$, *and* $\|f(x)\| := \max_{1\leqslant i\leqslant n_2}|f_i(x)|$ *if* $f(x) = (f_1(x),\dots, f_{n_2}(x)) \in \mathbf{R}^{n_2}$.

Proof. Clearly we may assume that $n_2 = 1$. Then the estimate follows immediately from the above Remez-type inequality after verifying the following two simple facts: first, for every $\eta \in [0,1]$, $(1+(1-\eta)^{1/n_1})/(1-(1-\eta)^{1/n_1}) \leqslant 2n_1/\eta$; and second, $T_d(x) = \frac{1}{2}((x-\sqrt{x^2-1})^d + (x+\sqrt{x^2-1})^d) \leqslant \frac{1}{2}(2^d+1)x^d \leqslant 2^d x^d$ if $x \geqslant 1$. The first calculus fact can be seen as follows: using the change of variable $z = (1-\eta)^{1/n_1}$, the desired inequality is equivalent to $(1+z)/(1-z) \leqslant 2n_1/(1-z^{n_1})$, hence to $(1+z)((1-z^{n_1})/(1-z)) \leqslant 2n_1$. Since $z \in [0,1)$ and $(1-z^{n_1})/(1-z) = 1+z+\cdots+z^{n_1-1}$, the inequality follows. □

Remark 2.9. The above bound goes back to Remez [Rem36]. See [Gan00] for some historical discussion and related references. We thank P. Varjú for providing these references. Note that the exponent $1/d$ is independent of the dimensions n_1 and n_2. This can be compared with [KM98, § 3] and [KT07, Lemma § 3.4], where a similar bound, albeit with a worse exponent $1/dn_1$ is derived. The fact that the exponent is independent of n_1 will be important in the proof of Theorem 1.8.

3. A characterization of Diophantine nilpotent Lie groups

3.1 The Borel–Cantelli lemma and condition (PUB)

Let $G = (\mathfrak{g}, *)$ be a connected simply connected nilpotent Lie group, endowed with a left-invariant Riemannian metric. Denote $n = \dim G$ and s the nilpotency step of G. Throughout we identify G with its Lie algebra $\mathfrak{g}$ via the exponential map. Then Lebesgue measure on $\mathfrak{g}$ coincides with Haar measure on G. In the following, we fix a basis of $\mathfrak{g}$ and the associated norm $\|x\| := \max\{|x_i|\}$ on $\mathfrak{g}$.

Definition 3.1 (Polynomial uniform lower bound). We will say that the group G satisfies *condition (PUB) for words in k letters* – or simply (PUB_k) – if there exist constants $C_k > 0$ and $A_k > 0$ such that

$$\forall \omega \in F_{k,G}, \quad \left(\sup_{\mathbf{g}\in B_{G^k}(0,1)} \|\omega(\mathbf{g})\|\right) \geqslant C_k \cdot l(\omega)^{-A_k}. \tag{PUB_k}$$

This condition ensures that no word map contracts too much the unit ball of G^k. In other terms, it is a polynomial uniform lower bound on the size of word maps, whence the chosen abbreviation (PUB).

Proposition 3.2. *Let G be a connected simply connected nilpotent Lie group. Then G is Diophantine for words on k letters if and only if it satisfies condition (PUB) for words on k letters. In short,*

$$\mathrm{Diophantine}_k \iff (\mathrm{PUB}_k).$$

Proof. We start by the implication ($\Rightarrow$) and prove the contrapositive. If G does not satisfy (PUB_k), then there is a sequence of words w_n in F_k whose associated word maps on G are non-trivial and satisfy $\|w_n(\mathbf{g})\| \leqslant (1/n)l(w_n)^{-n}$ for all $\mathbf{g} \in B_{G^k}(0,1)$. However, the level sets $w_n^{-1}(\{0\})$ are proper subsets of zero Haar measure in G^k. The complement of the union of all these sets therefore has full measure in G^k. No k-tuple in this complement is Diophantine, hence G is not Diophantine on k letters.

Now we turn to the converse ($\Leftarrow$). It is based on the Borel–Cantelli lemma. For a word map ω on G, and $R \geqslant 1, \beta > 0$, set

$$E_\omega(\beta) := \{\mathbf{g} \in B_{G^k}(0,R) : \|\omega(\mathbf{g})\| \leqslant |B_{\Gamma_\mathbf{g}}(l(\omega))|^{-\beta}\}.$$

Recall that $\tau_k := \tau(\Gamma_\mathbf{g})$ is the growth exponent of $\Gamma_\mathbf{g}$ for a random $\mathbf{g}$ (i.e. $|B_{\Gamma_\mathbf{g}}(n)| \sim c_k n_k^\tau$, see Corollary 2.6), that s is the nilpotency class of G and that A_k is the exponent appearing in the above definition of (PUB$_k$). We will show that if $\beta > s + A_k/\tau_k$ one has

$$\sum_{\omega \in F_{k,G}} |E_\omega(\beta)| < \infty.$$

In view of the Borel–Cantelli Lemma, this is enough to conclude that G is Diophantine for k letters. By Lemma 2.3 we know that if ω is a word map on G, then it is polynomial of degree at most s. Therefore, if it is non-trivial, we may apply Proposition 2 with $f = \omega$, $B = B_{G^k}(0,R)$ and $\epsilon = (c_k/2)l(\omega)^{-\tau_k\beta} > 0$ to get, assuming (PUB$_k$),

$$|E_\omega(\beta)| \ll \left(\frac{l(\omega)^{-\tau_k\beta}}{\|\omega\|_B}\right)^{1/s} \ll l(\omega)^{(-\tau_k\beta + A_k)/s}, \tag{3}$$

where the implied constants depend only on G, R and k. Therefore

$$\sum_{\omega \in F_{k,G}} |E_\omega(\beta)| \ll \sum_{\omega \in F_{k,G}} l(\omega)^{(-\tau_k\beta + A_k)/s}.$$

We now split this infinite sum in annuli $\{\omega \in F_{k,G}; 2^{m-1} \leqslant l(\omega) < 2^m\}$ noting that the size of each annulus is bounded above by the size of the ball of radius 2^m in $F_{k,G}$ and hence is a $O(2^{m\tau_k})$. It follows that the series converges for every $\beta > s + A_k/\tau_k$ as desired. □

Remark 3.3. The proof shows that condition (PUB$_k$) with exponent A_k implies that G is Diophantine for words in k letters, with exponent $s + A_k/\tau_k$. We will show later that the number A_k can always be bounded above independently of k. As a consequence (see Proposition 5.9), for every $\beta > s$, every Diophantine s-step nilpotent Lie group is β-Diophantine on k letters if k is large enough.

Remark 3.4. If $G = \mathbf{R}^d$, then word maps are of the form $(x_1, \ldots, x_k) \mapsto \sum_{i=1}^k n_i x_i$, with $n_i \in \mathbf{Z}$, so condition (PUB) is clearly satisfied. More generally, one can see, e.g. using the Campbell–Baker–Hausdorff formula, that word maps on rational nilpotent Lie groups have integer coefficients in an appropriate basis, so those groups certainly satisfy (PUB), and hence are Diophantine. This will also follow from the detailed analysis of condition (PUB) that we describe in 3.3.

3.2 An example: 2-step nilpotent groups

In order to motivate the discussion of the next paragraph, we start by studying the case of 2-step nilpotent groups. We will show that all of them satisfy condition (PUB) and hence are Diophantine. Note that this is not a particular case of Remark 3.4 above, as there exist non-rational nilpotent Lie groups of step two (see [Rag72, Remark 2.14, p. 38]).

Let $G = (\mathfrak{g}, *)$ be a connected simply connected nilpotent Lie group of step 2, and let $k \in \mathbb{N}$. As $F_{k,G}$ is nilpotent of step 2, by [MKS76, § 5.1], any word map $\omega \in F_{k,G}$ has a representative of the form

$$w = \prod_{i=1}^k x_i^{e_i} \prod_{1 \leqslant i < j \leqslant k} [x_i, x_j]^{f_{i,j}}. \tag{4}$$

We will show that $\|\omega\|_B := \sup_{\mathbf{g}\in B_{G^k}(0,1)} \|\omega(\mathbf{g})\|$ admits a uniform lower bound when ω ranges over the set of word maps on k letters on G. Clearly this will imply that G satisfies (PUB_k) and hence is Diophantine thanks to Proposition 3.2.

The map ω naturally induces a map on the abelianization, which under the identification $G \simeq \mathfrak{g}$ and in view of (4) is just $\bar{\omega} : \mathfrak{g}^k \to \mathfrak{g}/\mathfrak{g}^{(2)}, (x_1, \dots, x_k) \mapsto \sum_{i=1}^k e_i x_i \mod \mathfrak{g}^{(2)}$. If some e_i is non-zero, then obviously the map is not uniformly small on $B_{G^k}(0,1)$ and $\|\omega\|_B \gg 1$. If, however, all e_i are zero, then the map can be written $\omega : \mathfrak{g}^k \to \mathfrak{g}^{(2)}, (x_1, \dots, x_k) \mapsto \sum_{1\leqslant i<j\leqslant k} f_{ij} \cdot [x_i, x_j]$, where $f_{ij} \in \mathbf{Z}$. Fixing $i < j$ and letting x_m be the identity for all indices m except i and j, we see that $\|\omega\|_B \geqslant |f_{ij}| \sup_{x,y\in B_G(0,1)} \|[x, y]\|$. Since the f_{ij} are integers and not all zero, we obtain the desired uniform lower bound.

With analogous elementary methods, one can also treat the case of 3-step nilpotent groups. The idea, as in the 2-step case, consists in verifying that relations among word maps have to be rational. In particular all word maps sit inside a lattice in the space of polynomial maps $\mathfrak{g}^k \to \mathfrak{g}$, and this yields the desired uniform lower bound on their norm. Unfortunately this approach fails in step 6 and higher as we will demonstrate below.

We now turn to a more systematic study of the possible relations among word maps on a nilpotent Lie group, which will allow us, in § 4, not only to show that nilpotent groups of step up to 5 satisfy (PUB), but also to construct non-Diophantine nilpotent Lie groups of any step from 6 onwards.

3.3 Laws on nilpotent Lie algebras and the Diophantine property

Our goal in the remainder of this section will be to prove another characterization of the Diophantine property for a nilpotent Lie group G in terms of the ideal of laws of the Lie algebra $\mathfrak{g}$ (cf. Theorem 3.12 below). Recall that G is a connected simply connected nilpotent Lie group of step s. The group $F_{k,G}$ of word maps on k letters on G is by definition isomorphic to the quotient group $F_{k,s}/R_{k,s}(G)$, where $F_{k,s}$ is the free nilpotent group of step s on k generators, and $R_{k,s}(G)$ is the group of laws of G in $F_{k,s}$, i.e. the normal subgroup of $F_{k,s}$ consisting of all (classes of) words that are identically zero on G^k.

For any ring R, we denote by $\mathcal{F}_{k,s}(R)$ the free s-step nilpotent Lie algebra on the finite set $\{\mathsf{x}_1, \dots, \mathsf{x}_k\}$ over R. It is the quotient of the free Lie algebra by the ideal generated by commutators of length at least $s + 1$. For $R = \mathbf{R}$, we write $\mathcal{F}_{k,s} = \mathcal{F}_{k,s}(\mathbf{R})$. The group $F_{k,s}$ sits naturally as a lattice in $(\mathcal{F}_{k,s}, *)$, the simply connected nilpotent Lie group associated to the free nilpotent Lie algebra of step s over k generators. The precise connection between group laws and Lie algebra laws is given by the following lemma. If $\mathsf{r} \in \mathcal{F}_{k,s}$ is written as a sum of homogeneous components $\mathsf{r} = \sum_1^s \mathsf{r}_i$, each r_i being a linear combination of brackets of order i, then we set $|\mathsf{r}| := \max_1^s \|\mathsf{r}_i\|^{1/i}$, where $\|\cdot\|$ is a norm on $\mathcal{F}_{k,s}$.

Lemma 3.5. *For each $s \in \mathbb{N}^*$, there are positive integers C, D such that the following hold.*

(i) *If $w \in F_{k,s}$, then $w(e^{\mathsf{x}_1}, \dots, e^{\mathsf{x}_k}) = e^{1/C\mathsf{r}(\mathsf{x}_1,\dots,\mathsf{x}_k)}$ for some $\mathsf{r} \in \mathcal{F}_{k,s}(\mathbf{Z})$ with $|\mathsf{r}| \leqslant D \cdot l(w)$.*

(ii) *If $\mathsf{r} \in \mathcal{F}_{k,s}(\mathbf{Z})$, then $e^{C\mathsf{r}(\mathsf{x}_1,\dots,\mathsf{x}_k)} = w(e^{\mathsf{x}_1}, \dots, e^{\mathsf{x}_k})$ for some $w \in F_k$ with $l(w) \leqslant D \cdot |\mathsf{r}|$.*

Proof. For the first part, one shows by induction on $l(w)$ that $w = e^{\sum_1^s (1/a_i)\mathsf{r}_i}$, where $\mathsf{r}_i \in \mathcal{F}_{k,s}(\mathbf{Z})$ is homogeneous of degree i and $\|\mathsf{r}_i\|^{1/i} \leqslant D \cdot l(w)$. Here the a_i are positive integers which are fixed once and for all and independent of w. One picks the a_i recursively in such a way that $a_1 \dots a_{i-1} b_i$ divides a_i for each i, where b_i is the least common multiple of the denominators of the coefficients appearing in front of the brackets of order at most i in the Campbell–Baker–Hausdorff formula.

The main point to observe is that due to this choice of integers a_i if $w = e^{\sum_1^s (1/a_i)\mathsf{r}_i}$ for some values r_i, then $e^{\mathsf{x}_j} w$ remains of this form when applying the Campbell–Baker–Hausdorff formula.

The second part is proved by induction on the nilpotency class s. Suppose it holds when the nilpotency class is less than s, then write $\mathsf{r} = \mathsf{r}_{<s} + \mathsf{r}_s$ the homogeneous components of order less than s and order s respectively. From the induction hypothesis there is a word $w_{<s}$ of length $\leqslant D_{s-1}|\mathsf{r}|$ such that, for $C = C_{s-1}$, $e^{C\mathsf{r}_{<s}} = w_{<s}$ modulo commutators of order s in $F_{r,s}$. It then follows from the first part that $e^{C\mathsf{r}_{<s}} = w_{<s} e^{1/C\mathsf{r}'_s}$, where r'_s is homogeneous of order s and in $\mathcal{F}_{k,s}(\mathbf{Z})$. Moreover $|\mathsf{r}'_s| \leqslant D_s l(w_{<s}) \leqslant D_s^2|\mathsf{r}|$. Since $\mathsf{r}_{<s}$ and r'_s commute, we have $e^{C^2\mathsf{r}} = w_{<s}^C e^{\mathsf{r}'_s + C^2\mathsf{r}_s}$. It thus suffices to prove the assertion in the case when $\mathsf{r} = \mathsf{r}'_s$ is homogeneous of degree s. This follows from two observations. First if c is a commutator of order s in $\mathcal{F}_{k,s}$ with letters x_j, then e^c coincides with the group commutator of the same form in the letters e^{x_j}. Denote by n the least integer greater than $|\mathsf{r}|$. The second remark is that every positive integer $m < n^s$ can be written in base n as a sum of at most s terms of the form an^i for some integers $i = 0, \dots, s-1$ and $a \in [0, n-1]$. This shows that for every commutator shape $c(\mathsf{x}_1, \dots, \mathsf{x}_k)$ one can write e^{mc} as a product of at most s group commutators in the variables $(e^{\mathsf{x}_j})^\ell$, where $|\ell| \leqslant n$. The result follows immediately. □

For future reference, we record the following observation, which was used in the proof: if r in Lemma 3.5(ii) is a bracket commutator of order s and shape $c(\mathsf{x}_1, \dots, \mathsf{x}_k)$ (so that it belongs to $\mathcal{F}_{k,s}^{[s]}$, the ideal of homogeneous elements of degree s in $\mathcal{F}_{k,s}$), then the associated word $w \in F_k$ given by the lemma can be taken to be the commutator of order s with exactly the same shape (e.g. if $\mathsf{r}(\mathsf{x}_1, \mathsf{x}_2) = [\mathsf{x}_1, [\mathsf{x}_1, \mathsf{x}_2]]$, then $w(g_1, g_2) := (g_1, (g_1, g_2))$ works, where $(a, b) = aba^{-1}b^{-1}$ is the group commutator). This is a simple consequence of the Campbell–Baker–Hausdorff formula (see after Proposition 2.1 above). Conversely, given a commutator word w of order s, we have $w(e^{\mathsf{x}_1}, \dots, e^{\mathsf{x}_k}) = e^{\mathsf{r}(\mathsf{x}_1, \dots, \mathsf{x}_k)}$ for all x_i in $\mathcal{F}_{k,s}$, where r is the bracket commutator of the same shape.

In particular, if r belongs to $\mathcal{F}_{k,s}^{(i)}$, the ith term in the central descending series of $\mathcal{F}_{k,s}$, then w can be chosen to belong to $F_k^{(i)}$, the ith term in the central descending series of F_k. Similarly, if r belongs to $D^{(i)}(\mathcal{F}_{k,s})$, the ith term in the derived series of $\mathcal{F}_{k,s}$, then w can just as well be taken to belong to the ith term in the derived series of F_k; and, conversely, the same holds in the opposite direction, i.e. given w in $F_k^{(i)}$ (respectively $D^{(i)}(F_k)$) we may find r in $\mathcal{F}_{k,s}^{(i)}$ (respectively $D^{(i)}(\mathcal{F}_{k,s})$) satisfying the conclusion of Lemma 3.5(i).

Lemma 3.5 is fairly standard. We added a proof for the reader's convenience. More information on this topic and on the geometry of nilpotent groups, is contained in Tits' appendix to [Gro81] and in the second author's paper [Bre14, § 2].

If $\mathfrak{g}$ is an arbitrary real nilpotent Lie algebra with nilpotency class no greater than s, for each $\mathbf{X} = (X_1, \dots, X_k) \in \mathfrak{g}^k$, there is a unique Lie algebra homomorphism $\theta_{\mathbf{X}} : \mathcal{F}_{k,s} \to \mathfrak{g}$ such that, for each i, $\theta_{\mathbf{X}}(\mathsf{x}_i) = X_i$.

DEFINITION 3.6. The *ideal of laws on k letters on $\mathfrak{g}$* is defined to be

$$\mathcal{L}_{k,s}(\mathfrak{g}) := \bigcap_{\mathbf{X} \in \mathfrak{g}^k} \ker \theta_{\mathbf{X}}.$$

The quotient $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})$ is the relatively free Lie algebra in the variety of k-generated Lie algebras associated to $\mathfrak{g}$.

PROPOSITION 3.7. *The set $\mathcal{L}_{k,s}(\mathfrak{g})$ is a fully invariant ideal of $\mathcal{F}_{k,s}$, i.e. $\mathcal{L}_{k,s}(\mathfrak{g})$ is an ideal of $\mathcal{F}_{k,s}$, and it is stable under all Lie algebra endomorphisms of $\mathcal{F}_{k,s}$. Conversely, if $\mathcal{L}$ is a fully invariant*

ideal of $\mathcal{F}_{k,s}$ there exists a nilpotent Lie algebra $\mathfrak{g}$ with nilpotency class no greater than s such that $\mathcal{L}_{k,s}(\mathfrak{g}) = \mathcal{L}$.

Proof. By definition, $\mathcal{L}_{k,s}(\mathfrak{g})$ is the intersection of all ideals $\ker \theta_{\mathbf{X}}$, so it is itself an ideal. Let φ be a Lie algebra endomorphism of $\mathcal{F}_{k,s}$. For each i in $\{1, \dots, k\}$, denote $\mathsf{r}_i = \mathsf{r}_i(\mathsf{x}_1, \dots, \mathsf{x}_k)$ the image of x_i under φ. For $\mathbf{X} \in \mathfrak{g}^k$, with a slight abuse of notation, we set $\varphi(\mathbf{X}) := (\mathsf{r}_1(\mathbf{X}), \dots, \mathsf{r}_k(\mathbf{X}))$. The homomorphism of Lie algebras $\theta_{\mathbf{X}} \circ \varphi : \mathcal{F}_{k,s} \to \mathfrak{g}$ maps each x_i to $\mathsf{r}_i(\mathbf{X})$ and therefore

$$\theta_{\mathbf{X}} \circ \varphi = \theta_{\varphi(\mathbf{X})}.$$

This shows that $\mathcal{L}_{k,s}(\mathfrak{g})$ is stable under φ.

Conversely, if $\mathcal{L}$ is any ideal of the free Lie algebra $\mathcal{F}_{k,s}$, the ideal of laws in k letters of the quotient Lie algebra $\mathcal{F}_{k,s}/\mathcal{L}$ is the smallest fully invariant ideal of $\mathcal{F}_{k,s}$ containing $\mathcal{L}$. In particular if $\mathcal{L}$ is a fully invariant ideal of $\mathcal{F}_{k,s}$, then the ideal of laws of the quotient Lie algebra $\mathcal{F}_{k,s}/\mathcal{L}$ is exactly $\mathcal{L}$. □

Definition 3.8. The *ideal of rational laws on k letters on $\mathfrak{g}$* is defined to be the real vector space $\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}$ generated by $\mathcal{L}_{k,s}(\mathfrak{g}) \cap \mathcal{F}_{k,s}(\mathbf{Q})$. It is also a fully invariant ideal of $\mathcal{F}_{k,s}$.

Denoting by $(\mathfrak{g}, *)$ the simply connected Lie group associated to the Lie algebra $\mathfrak{g}$, we have the following.

Proposition 3.9. *The group of word maps $F_{k,G}$ naturally embeds into two Lie groups.*

- *It is a finitely generated subgroup of $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g}), *)$.*
- *It is a lattice in $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}, *)$.*

We defer the proof to later in this section. The discrepancy between $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}$ and $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})$ lies at the heart of the property of being Diophantine for G. We have a natural epimorphism of real Lie algebras:

$$\Lambda : \mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}} \to \mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g}). \tag{5}$$

Before we state the main result of this section we require one more definition.

Definition 3.10 (Diophantine subspace). Let V be a finite-dimensional $\mathbf{Q}$-vector space and choose a norm $\|\cdot\|$ on $V(\mathbf{R})$. A real subspace L of $V(\mathbf{R})$ is said to be Diophantine in V if there are constants $C, A > 0$ such that

$$d(v, L) \geqslant C \cdot \|v\|^{-A}$$

for every $v \in V(\mathbf{Z}) \backslash L$.

Example 3.11 (Subspaces defined over a number field). Let $K \leqslant \mathbf{R}$ be a finite field extension of $\mathbf{Q}$. If L has a basis made of vectors in $V(K)$, then L is a Diophantine subspace of V. Indeed, L is also the intersection of the kernels of linear forms $\ell_1, \dots, \ell_{\operatorname{codim} L}$ on V which are all defined over K and we are left to verify that $|\ell_i(v)| \gg \|v\|^{-A}$ for each $v \in V(\mathbf{Z}) \backslash \{\ker \ell_i\}$. This is, of course, well known, and can easily be verified from the product formula $h(x) = h(x^{-1})$ and the height bounds $h(xy) \leqslant h(x) + h(y)$ and $h(x+y) \leqslant h(x) + h(y) + \log 2$, where $h(x)$ is the absolute Weil height for the algebraic number x (cf. [BG06]).

We now have the following.

Theorem 3.12. *Let G be a connected simply connected nilpotent Lie group with Lie algebra $\mathfrak{g}$ and $k \geqslant 1$. The following are equivalent.*

(1) *The group G is Diophantine for words in k letters.*
(2) *The group $F_{k,G}$ is Diophantine as a subgroup of $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g}), *)$.*
(3) *The ideal of laws $\mathcal{L}_{k,s}(\mathfrak{g})$ is Diophantine in $\mathcal{F}_{k,s}$.*
(4) *The kernel $\ker\Lambda$ is Diophantine in $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}$.*

Note that the condition that $F_{k,G}$ be a Diophantine subgroup of $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g}), *)$ (i.e. condition (2) in Theorem 3.12) is just a reformulation of (PUB$_k$). Indeed by Lemma 3.5 for each word map $\omega \in F_{k,G}$, there is an element $\mathsf{r}_\omega \in \mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})$ such that $\omega(\mathbf{g}) = e^{\mathsf{r}_\omega(\log \mathbf{g})}$ with $l(\omega) \lesssim \|\mathsf{r}_\omega\| \lesssim l(\omega)^s$ and $\sup_{B_{G^k}(0,1)} \|\omega(\mathbf{g})\| = \sup_{\mathbf{x}\in B_{\mathfrak{g}^k}(0,1)} \|\mathsf{r}_\omega(\mathbf{x})\|$ is a norm on the Lie algebra $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})$. All norms are equivalent, so (PUB$_k$) (as formulated in Definition 3.1) precisely means that $F_{k,G}$ is Diophantine.

We are now ready to prove Proposition 3.9 and Theorem 3.12.

Proof of Proposition 3.9. As follows from Lemma 3.5, $F_{k,s}$ is a lattice in $(\mathcal{F}_{k,s}, *)$. Moreover the kernel of the natural group homomorphism $F_{k,s} \to (\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g}), *)$ coincides with $R_{k,s}(G)$. Hence $F_{k,G} = F_{k,s}/R_{k,s}(G)$ is naturally a subgroup of $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g}), *)$.

Similarly Lemma 3.5 implies that $R_{k,s}(G)$ is a lattice in $(\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}, *)$. This implies (see [Rag72, Lemma 1.16, p. 25]) that $F_{k,s}/R_{k,s}(G)$ is a lattice in $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}, *)$. □

Proof of Theorem 3.12. We just observed that part (2) is a reformulation of (PUB$_k$). Hence Proposition 3.2 shows that parts (1) and (2) are equivalent.

If $W \leqslant V$ are finite-dimensional $\mathbf{Q}$-vector spaces and L is a real subspace $W(\mathbf{R}) \leqslant L \leqslant V(\mathbf{R})$, then it follows easily from Definition 3.10 that L is Diophantine in V if and only if L/W is Diophantine in V/W. This yields the equivalence of parts (3) and (4).

We now prove the equivalence of parts (2) and (4). Let $N := (\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}, *)$ and the discrete lattice $\Gamma := F_{k,s}/R_{k,s}(G)$ inside it. Let $L := \ker\Lambda$. We need to prove that Γ is Diophantine in N/L if and only if the Lie algebra $\mathrm{Lie}(L)$ is a Diophantine subspace $\mathrm{Lie}(N)$ in the sense of Definition 3.10. This again follows easily from Lemma 3.5 and the Campbell–Baker–Hausdorff formula. Indeed, if Γ is not Diophantine in N, then for every $A > 0$ there are words w such that $w(\mathsf{x}_1, \dots, \mathsf{x}_k) = e^{\mathsf{u}_w} e^{\ell}$, where $\mathsf{u}_w \in \mathrm{Lie}(N)\backslash\{0\}$ is very small, i.e. $\|\mathsf{u}_w\| \ll l(w)^{-A}$,[(1)] and $\ell \in \mathrm{Lie}(L)$. By Lemma 3.5, this implies that there are integer points $\mathsf{r} \in \mathrm{Lie}(N)(\mathbf{Z})$ with $\|\mathsf{r}\| \ll l(w)^s$ such that $e^{\mathsf{r}} = e^{C\mathsf{u}_w} e^{C\ell}$ for a constant C. Applying the Campbell–Baker–Hausdorff formula, using the fact that $\mathrm{Lie}(L)$ is an ideal, we see that $\|\mathsf{r} - C\ell\| \ll \|\mathsf{r}\|^{-A/s}$, showing that $\mathrm{Lie}(L)$ is not Diophantine as a subspace of $\mathrm{Lie}(N)$. The reverse direction is similar and we omit it. □

Remark 3.13. Note that the proof shows that if $\mathcal{L}_{k,s}(\mathfrak{g})$ is Diophantine in $\mathcal{F}_{k,s}$ with exponent A, then G satisfies (PUB$_k$) with exponent $A_k = sA$, and therefore, by Remark 3.3, G is Diophantine in k letters with exponent $s + sA/\tau_k$.

3.4 Nilpotent Lie groups defined over an algebraic number field

A real Lie algebra $\mathfrak{g}$ is said to be defined over a proper subfield $K \leqslant \mathbf{R}$, if one can find a basis $\{X_i\}_{i=1}^d$ such that the associated structure constants of $\mathfrak{g}$ (that is the numbers c_{ijk} such that $[X_i, X_j] = \sum_{k=1}^d c_{ijk} X_k$) belong to K. We will also say that the associated connected simply connected nilpotent real Lie group is defined over K when its Lie algebra is so.

One readily checks that if the s-step nilpotent Lie algebra $\mathfrak{g}$ is defined over K, then its ideal of laws $\mathcal{L}_{k,s}(\mathfrak{g})$ is also defined over K. The following is then a direct consequence of Theorem 3.12.

COROLLARY 3.14. *If G is a connected simply connected nilpotent Lie group defined over a number field K ($[K : \mathbf{Q}] < \infty$), then G is Diophantine.*

Proof. The ideal of laws $\mathcal{L}_k(\mathfrak{g})$ is defined over the number field K, and therefore, by Example 3.11, it must be Diophantine. Theorem 3.12 then implies that the group G is Diophantine. □

3.5 Connected, but non-simply connected, nilpotent Lie groups

We explain here how the above can be adapted to handle non-simply connected, connected nilpotent Lie groups G as well.

Let $\tilde{G}$ be the universal cover of the connected nilpotent Lie group G, so that $G = \tilde{G}/Z$, where Z is a discrete subgroup of $\tilde{G}$ contained in its center. The group Z is a torsion-free abelian group, say of rank r.

A first observation is that the groups of words maps $F_{k,G}$ and $F_{k,\tilde{G}}$ are naturally isomorphic: indeed every law on G must also be a law on $\tilde{G}$ because Z is discrete in $\tilde{G}$. Second we prove the following.

Theorem 3.15. *Let G be a connected nilpotent Lie group and $\tilde{G}$ its universal cover. Then G is Diophantine on k letters if and only if $\tilde{G}$ is Diophantine on k letters.*

Proof. One direction is obvious: if G is Diophantine, then so is $\tilde{G}$. In the converse direction, we use the characterization in terms of the property (PUB$_k$) of Proposition 3.2 and modify the Borel–Cantelli argument used in the proof of this proposition. What needs to be estimated is the Haar measure of the sets $E'_\omega(\beta) := \{\mathbf{g} \in B_{\tilde{G}^k}(0,R); d(\omega(\mathbf{g}), Z) < |B_{F_{k,G}}(n)|^{-\beta}\}$. This splits into a union of at most $O(l(\omega)^{rs})$ subsets of the form $E'_\omega(\beta, z) := \{\mathbf{g} \in B_{\tilde{G}^k}(0,R); \|z^{-1}\omega(\mathbf{g})\| < |B_{F_{k,G}}(n)|^{-\beta}\}$ for $z \in Z\backslash\{0\}$. Since Z is discrete, the quantity $\sup_{\mathbf{g}\in B_{\tilde{G}^k}(0,R)} \|z^{-1}\omega(\mathbf{g})\|$ is bounded away from 0 uniformly in $z \neq 0$. Applying the Remez-type inequality (Proposition 2.8) to each polynomial map $\mathbf{g} \mapsto z^{-1}\omega(\mathbf{g})$ and using condition (PUB$_k$) for $\tilde{G}$, we obtain

$$|E'_\omega(\beta)| \leqslant |E'_\omega(\beta,0)| + \sum_{z\neq 0} |E'_\omega(\beta,z)| \ll l(\omega)^{-(\beta\tau_k - A_k)/s} + l(\omega)^{rs} l(\omega)^{-\beta\tau_k/s}$$

and the series converges as soon as $\beta > s + \max\{rs, A_k\}/\tau_k$. We conclude that G is Diophantine. □

4. Fully invariant ideals of the free Lie algebra $\mathcal{F}_k$

In this section, we complete our study of the Diophantine property for nilpotent Lie groups and explain the connection between the Diophantine property for s-step nilpotent Lie algebras and the absence of multiplicity in the ideal of laws $\mathcal{L}_{k,s}$ viewed as a module over SL_k. We then complete the proof of the results stated in the introduction.

4.1 $\mathcal{F}_{k,s}$ as an SL_k-module

Recall that $\mathcal{F}_k$ denotes the free Lie algebra on k generators and $\mathcal{F}_{k,s} = \mathcal{F}_k/\mathcal{F}_k^{(s+1)}$ the s-step free nilpotent Lie algebra. Here $\mathcal{F}_k^{(i)}$ denotes the ith term of the central descending series of $\mathcal{F}_k$. The ring $\mathrm{End}\,\mathcal{F}_{k,s}$ of Lie algebra endomorphisms of $\mathcal{F}_{k,s}$ acts naturally on $\mathcal{F}_{k,s}$, so that $\mathcal{F}_{k,s}$ has a structure of an $\mathrm{End}\,\mathcal{F}_{k,s}$-module. An $\mathrm{End}\,\mathcal{F}_k$-submodule of $\mathcal{F}_{k,s}$ is called a *fully invariant ideal* of $\mathcal{F}_{k,s}$.

Below we will show that, for $k \geqslant 3$ (respectively $k = 2$) and for all $s \geqslant 6$ (respectively $s \geqslant 7$), there exists a fully invariant ideal of $\mathcal{F}_{k,s}(\mathbf{R})$ which is not Diophantine. By Theorem 3.12 this will show existence of non-Diophantine nilpotent Lie groups.

The group SL_k acts on $\mathcal{F}_{k,s}$ by linear substitution of the free variables, and thus embeds naturally in $\mathrm{End}\,\mathcal{F}_{k,s}$.

For $s \geqslant 1$, we denote $\mathcal{F}_k^{[s]}$ the subspace of $\mathcal{F}_{k,s}$ consisting of homogeneous elements of degree s. Note that $\mathcal{F}_k^{[s]}$ is stable under the action of SL_k and that a vector subspace $V \leqslant \mathcal{F}_k^{[s]}$ is invariant under the action of SL_k if and only if it is a fully invariant ideal of $\mathcal{F}_{k,s}$. So in order to build fully invariant ideals in $\mathcal{F}_{k,s}$ we can look for SL_k-invariant subspaces of $\mathcal{F}_k^{[s]}$. Our first observation is the following.

LEMMA 4.1 (Complete reducibility). *The SL_k-module $\mathcal{F}_k^{[s]}$ is completely reducible, i.e. there are positive integers n_i such that*

$$\mathcal{F}_k^{[s]} = \bigoplus_{i=0}^{l} V_i^{n_i},$$

where each V_i is an irreducible highest-weight SL_k-module defined over $\mathbf{Q}$ and $V_i \not\simeq V_j$ if $i \neq j$.

Proof. This follows Weyl's complete reducibility theorem. See Serre [Ser06, Part I, ch. 6, § 3]. □

4.2 Multiplicity and Diophantine submodules

We now want to find under which condition $\mathcal{F}_k^{[s]}(\mathbf{R})$, the subspace of $\mathcal{F}_{k,s}(\mathbf{R})$ consisting of homogeneous elements of degree s, admits a non-Diophantine SL_k-submodule. Say that $\mathcal{F}_k^{[s]}(\mathbf{R})$ is *multiplicity free* if in the decomposition given by the above lemma, $n_i = 1$ for all i. If not, we say that $\mathcal{F}_k^{[s]}(\mathbf{R})$ admits multiplicity. The following simple observation is key to our proofs.

LEMMA 4.2. *Let $k, s \in \mathbb{N}$.*

(1) *If $\mathcal{F}_k^{[s]}(\mathbf{R})$ is multiplicity free, then it has only finitely many SL_k-submodules, all of which are defined over $\mathbf{Q}$, and hence Diophantine.*

(2) *If $\mathcal{F}_k^{[s]}(\mathbf{R})$ admits multiplicity, then it has a non-Diophantine SL_k-submodule.*

Proof. If $\mathcal{F}_k^{[s]}(\mathbf{R})$ is multiplicity free, then, using notation of Lemma 4.1, we see that every SL_k-submodule V has the form $V = \bigoplus_{i \in I} V_i$ where $I \subset \{1, \dots, n\}$. This certainly implies that they all are defined over $\mathbf{Q}$. Example 3.11 then shows that they are Diophantine.

Conversely, suppose $\mathcal{F}_k^{[s]}$ admits multiplicity. Without loss of generality, we may assume $n_1 \geqslant 2$ so that $\mathcal{F}_k^{[s]}$ admits a submodule of the form $V_1 \oplus V_1'$, with $V_1 \simeq V_1'$, both of them being defined over $\mathbf{Q}$ as subspaces of $\mathcal{F}_k$. Fix an isomorphism $\alpha : V_1 \to V_1'$ mapping $V_1 \cap \mathcal{F}_k(\mathbf{Z})$ to $V_1' \cap \mathcal{F}_k(\mathbf{Z})$. Then choose some Liouville number $\lambda \in \mathbf{R}$, i.e. some number such that the inequalities

$$0 < \left| \lambda - \frac{p}{q} \right| \leqslant q^{-q-1} \tag{6}$$

have infinitely many integer solutions in (p, q), and define

$$L_\lambda = \{x + \lambda\alpha(x) : x \in V_1\} \subset \mathcal{F}_k^{[s]}(\mathbf{R}).$$

This is an SL_k-submodule of $\mathcal{F}_k^{[s]}(\mathbf{R})$, which we claim to be non-Diophantine. To see this, take a non-zero vector $x \in V_1 \cap \mathcal{F}_k(\mathbf{Z})$, and let, for $p, q \in \mathbf{Z}$, $\mathsf{r}_{p,q} := qx + p\alpha(x) \in \mathcal{F}_k^{[s]}(\mathbf{Z})$. Then, for p, q large enough in the set of solutions to (6), we have

$$0 < d(\mathsf{r}_{p,q}, L_\lambda) \leqslant \|qx_1 + p\alpha(x_1) - q(x_1 + \lambda\alpha(x_1))\| \leqslant |p - q\lambda| \|\alpha(x_1)\| \leqslant q^{-q}. \tag{7}$$

As $\|\mathsf{r}_{p,q}\| \ll q$, this proves what we wanted. □

4.3 Applications

As we explain in the appendix, using Witt's Character Formula for the free Lie algebra, one may determine precisely when the SL_k-module $\mathcal{F}_k^{[s]}$ is multiplicity-free. The conclusion is the following (Theorem A.2).

Theorem 4.3. *The SL_k-module $\mathcal{F}_k^{[s]}$ is multiplicity-free if and only if $s \leqslant 5$ when $k \geqslant 3$ and if and only if $s \leqslant 6$ when $k = 2$.*

This will allow us to derive Theorems 1.3 and 1.5 announced in the introduction.

Theorem 4.4. *Fix an integer $k \geqslant 3$ (respectively $k = 2$).*

(1) *Every connected nilpotent Lie group of step $s \leqslant 5$ (respectively $s \leqslant 6$) is Diophantine on k letters.*

(2) *For every $s \geqslant 6$ (respectively $s \geqslant 7$), there are s-step nilpotent Lie groups which are not Diophantine on k letters.*

Proof. We only deal with the case $k \geqslant 3$, because the case $k = 2$ is entirely analogous. Let G be a connected nilpotent Lie group of step $s \leqslant 5$. From Theorem 3.12, it suffices to show that $\mathcal{L}_{k,s} = \mathcal{L}_{k,s}(\mathfrak{g})$ is Diophantine in $\mathcal{F}_{k,s}$. Now $\mathcal{L}_{k,s}$ is a fully invariant ideal of $\mathcal{F}_{k,s}$ and therefore can be decomposed as

$$\mathcal{L}_{k,s} = \bigoplus_{r \geqslant 1} \mathcal{L}_{k,s}^{[r]},$$

where $\mathcal{L}_{k,s}^{[r]}$ is the set of elements of $\mathcal{L}_{k,s}$ of homogeneous degree r. For each r, $\mathcal{L}_{k,s}^{[r]}$ is an SL_k-submodule of $\mathcal{F}_{k,s}^{[r]}$. Combining Lemma 4.2 and Theorem A.2, we get that, for each $r \leqslant 5$, $\mathcal{L}_{k,s}^{[r]}$ is defined over $\mathbf{Q}$. Thus, $\mathcal{L}_{k,s}$ is defined over $\mathbf{Q}$ and hence Diophantine. This proves the first part of the theorem in the case $k \geqslant 3$.

Now let $k \geqslant 3$ and $s \geqslant 6$. From Theorem A.2 and Lemma 4.2, we may find in $\mathcal{F}_k^{[s]}(\mathbf{R})$ an SL_k-submodule L that is non-Diophantine as a subspace of $\mathcal{F}_{k,s}$. This is a fully invariant ideal of $\mathcal{F}_{k,s}$ which is not Diophantine. Let G be the connected simply connected Lie group with Lie algebra $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}$. Then G is s-step nilpotent, and its ideal of laws on k letters is $\mathcal{L}_{k,s}$ so that by Theorem 3.12, G is not Diophantine. □

The proof of Theorem 1.5 follows similar lines, the only new input is the fact, proved in Lemma A.9 below, that the free metabelian Lie algebra is multiplicity-free as an SL_k module.

Theorem 4.5. *Every connected nilpotent metabelian Lie group is Diophantine.*

Proof. Let G be such a Lie group with nilpotency step s and let $\mathfrak{g}$ be its Lie algebra. Let $\mathcal{L}_k = \mathcal{L}_k(\mathfrak{g})$ the ideal of laws on k letters in $\mathfrak{g}$. Since G is metabelian, for each r, $\mathcal{L}_k^{[r]}$ contains $\mathcal{M}_k^{[r]}$ (see the notation of Lemma A.9). It then follows from this lemma that $\mathcal{L}_k^{[r]}$ is equal either to $\mathcal{M}_k^{[r]}$ or to $\mathcal{F}_k^{[r]}$. In particular it is defined over $\mathbf{Q}$. Hence so is $\mathcal{L}_{k,s}(\mathfrak{g})$ in $\mathcal{F}_{k,s}$. By Example 3.11, it must then be Diophantine in $\mathcal{F}_{k,s}$ and Theorem 3.12 implies that G is Diophantine. □

Remark 4.6. Observe that the non-Diophantine nilpotent Lie groups constructed in Theorem 4.4 in step $s = 6$ (or $s = 7$ if $k = 2$) are solvable of derived length 3 (indeed $D^3(\mathcal{F}_k) \subset \mathcal{F}_k^{(8)}$).

We can now build a non-Diophantine solvable but not nilpotent group.

Theorem 4.7. *There exists a non-Diophantine solvable Lie group which is not nilpotent.*

Proof. Fix $s \geqslant 7$. Denote $\mathcal{M}_2 = D^2(\mathcal{F}_k)$ the second term of the derived series of $\mathcal{F}_k$. From Theorem A.2 in the appendix, we know that $\mathcal{F}_2^{[s]}$ admits multiplicity. By Lemma A.9, this implies that in fact $\mathcal{M}_2^{[s]}$ has multiplicity. From there, using a Liouville number as in the proof of Lemma 4.2, we build an SL_2-submodule $\mathcal{L}$ of $\mathcal{M}_2^{[s]}$ and a sequence $(\mathsf{r}_n)_{n\geqslant 1}$ of elements of $\mathcal{M}_2^{[s]}(\mathbf{Z})$ such that $\|\mathsf{r}_n\| \to \infty$ and, for each n,

$$0 < d(\mathsf{r}_n, \mathcal{L}) < \|\mathsf{r}_n\|^{-\|\mathsf{r}_n\|^s}. \tag{8}$$

By Lemma 3.5, we may obtain from (r_n) a sequence of words in two letters

$$w_n = e^{C\mathsf{r}_n} \mod e^{\mathcal{F}_2^{(s+1)}}$$

with $l(w_n) \leqslant C \cdot \|\mathsf{r}_n\|^s$. Moreover, given that the r_n are in $\mathcal{M}_2$, it follows from the remark made right after the proof of Lemma 3.5 that the w_n can be chosen in $M_2 = D^2(F_2)$, the second term of the derived series of the free group F_2. This implies in particular that, for any metabelian group M, all word maps $w_{n,M}$ are trivial. Now take M any metabelian non-nilpotent Lie group, e.g. the group of affine transformations of the real line, and let N be the connected simply connected nilpotent Lie group with Lie algebra $\mathcal{F}_2/(\mathcal{L} \oplus \mathcal{F}_2^{(s+1)})$. Let $G := M \times N$. The word maps $w_{n,G}$ are trivial on $M \times \{1\}$, and therefore, the bound (8) shows that, for any $\beta > 0$,

$$0 < \sup_{\mathbf{g}\in B_{G^2}(0,1)} d(w_n(\mathbf{g}), 0) \ll 4^{-\beta l(w_n)} \ll |B_{\Gamma_\mathbf{g}}(l(w_n))|^{-\beta}.$$

This shows that G cannot be Diophantine, and of course G is solvable non-nilpotent. □

5. Concluding remarks

5.1 Baire category genericity

Here we prove Theorem 1.7. It is well known that, although almost every real number is Diophantine, there is a G_δ-dense set of real numbers which are not. So topological and measure-theoretic genericity are very different notions. For k-tuples on nilpotent groups a similar phenomenon takes place.

PROPOSITION 5.1. *Let G be a connected nilpotent real Lie group. If $k > \dim G/[G,G]$, then there is a G_δ-dense set D in G^k of k-tuples which are not Diophantine.*

For the analogous result on SU(2) see [GHSSV09]. In fact D can be chosen so that the k-tuples in D are as non-Diophantine as possible, namely the speed of an approximation to 1 by a word of length n can be arbitrarily fast in n. The proof is based on the following lemma. Recall that $F_{k,G}$ is the relatively free group on k generators associated to G (see § 2.2).

LEMMA 5.2. *If there is a dense subset D_0 of G^k such that for each $\mathbf{g} \in D_0$ the induced natural map $F_{k,G} \to G$ is not injective, then there is a G_δ-dense set D of non-Diophantine k-tuples.*

Proof. Let $\omega_\mathbf{g} \in F_{k,G}\backslash\{1\}$ be such that $\omega_\mathbf{g}(\mathbf{g}) = 1$. Then $\omega_\mathbf{g}^{-1}(1)$ is a proper analytic subvariety of G^k. In particular, for every integer $n \geqslant 1$, the subset $O_{n,\mathbf{g}} := B(\mathbf{g}, e^{-nl(\omega_\mathbf{g})})\backslash\omega_\mathbf{g}^{-1}(1)$ of the open ball $B(\mathbf{g}, e^{-nl(\omega_\mathbf{g})})$ is open and its closure contains $\mathbf{g}$. Set $D := \bigcap_{n\geqslant 1}\bigcup_{\mathbf{g}\in D_0} O_{n,\mathbf{g}}$. □

Proof of Proposition 5.1. Note that we may assume that G is simply connected. Let $c \in \mathcal{F}_{k,s}^{[s]}$ be a commutator of length s not belonging to the ideal of laws $\mathcal{L}_{k,s}(\mathfrak{g})$. Let D_0 be the set of k-tuples

$(x_1, \dots, x_k)$ in G^k such that $(x_1, \dots, x_{k-1})$ span $\mathfrak{g}$ modulo $\mathfrak{g}^{(2)}$ (via the identification $G \sim \mathfrak{g}$), and such that x_k lies in the $\mathbf{Q}$-span of $(x_1, \dots, x_{k-1})$ modulo $\mathfrak{g}^{(2)}$. Since $k > \dim \mathfrak{g}/\mathfrak{g}^{(2)}$ this set is clearly dense in G^k. By the definition of D_0, and using the multi-linearity of c, if $\mathbf{g} \in D_0$, then there are integers $n_i \in \mathbf{Z}$ with $n_k \neq 0$ such that $n_k c(x_1, \dots, x_k) = \sum_{i=1}^{k-1} n_i c(x_1, \dots, x_{k-1}, x_i)$. However, viewed as an element of $\mathcal{F}_{k,s}$, the quantity

$$r(\mathsf{x}_1, \dots, \mathsf{x}_k) := n_k c(\mathsf{x}_1, \dots, \mathsf{x}_k) - \sum_{i=1}^{k-1} n_i c(\mathsf{x}_1, \dots, \mathsf{x}_{k-1}, \mathsf{x}_i)$$

does not belong to $\mathcal{L}_{k,s}$ because the sum of the $k-1$ terms on the right-hand side does not depend on x_k, while the term on the left-hand side does. By Lemma 3.5, e^r is a word w in the group elements e^{x_i} and it does not vanish entirely on G^k although it vanishes at the point $(x_1, \dots, x_k)$. Hence D_0 satisfies the requirements of Lemma 5.2 and we are done. □

If G is not Diophantine, then a much stronger statement holds.

Proposition 5.3. *Let G be a connected nilpotent Lie group, which is non-Diophantine for k-tuples. Then there is a word map $\omega \in F_{k,G} \backslash \{1\}$ such that all k-tuples $\mathbf{g} \in G^k$ such that $\omega(\mathbf{g}) \neq 1$ are non-Diophantine. In particular there is an open dense subset of G^k made of non-Diophantine k-tuples.*

Before giving the proof we make the following observation.

Lemma 5.4. *Let F be a finitely generated subgroup of a connected s-step nilpotent Lie group G and $\Gamma \leqslant F$ a subgroup. If $\min\{d(x, 1); x \in \Gamma \cap B_F(n) \backslash \{1\}\} \ll n^{-A}$ for all $A > 0$, then Γ is non-Diophantine in G.*

Proof. As is well known, every subgroup of a finitely generated nilpotent group is finitely generated, so it makes sense to require that Γ be non-Diophantine as a subgroup of G, or not. We claim that the word metric on Γ is bounded above by a fixed power of the trace on Γ of the word metric coming from F, namely $\ell_\Gamma(\gamma) \leqslant O(\ell_F(\gamma)^s)$. Clearly this implies the lemma. To see the claim let M be the Zariski closure of Γ in the Malcev closure N of F. It is a connected and closed subgroup of N [Rag72, II.2.5, II.2.6]. Given a norm $||x||$ on the Lie algebra of N, any homogeneous quasi-norm $|\cdot|_N$ on N satisfies $c|x|_N \leqslant ||x|| \leqslant C|x|_N^s$ [Bre14, Example 2.3] for some positive constants $c, C > 0$ assuming $||x|| \geqslant 1$ say. Also the same holds for a homogeneous quasi-norm $|\cdot|_M$ on M if $x \in M$. The ball-box principle (see e.g. [Bre14, Proposition 4.5] applied to the distance on N induced by the word metric on F [Bre14, Example 4.3(1)]) tells us that $|\cdot|_N$ and ℓ_F (respectively $|\cdot|_M$ and ℓ_Γ) are comparable up to multiplicative and additive constants. The claim follows. □

Proof of Proposition 5.3. Let N be the simply connected Lie group $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g}), *)$. Recall (see Proposition 3.9) that $F_{k,G}$ is a lattice in $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}, *)$ and that it embeds into N via the natural Lie homomorphism $\rho : (\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}, *) \to N$ (associated to the Lie algebra homomorphism Λ of (5)). By Theorem 3.12, $\rho(F_{k,G})$ is a non-Diophantine subgroup of N. Let $\Gamma \leqslant F_{k,G}$ be a subgroup of the form $\Gamma = \rho^{-1}(\rho(F_{k,G}) \cap L)$, where L is a connected subgroup of N, which is such that $\rho(\Gamma)$ is non-Diophantine in L. Choose Γ so that L has minimal possible dimension. Pick $\omega \in \Gamma \backslash \{1\}$.

Now let $\mathbf{g} \in G^k$ be a k-tuple such that $\omega(\mathbf{g}) \neq 1$. The choice of $\mathbf{g}$ induces a homomorphism $\phi_{\mathbf{g}} : F_{k,G} \to G$, which extends by Malcev rigidity [Rag72, Theorem 2.11] to a Lie group homomorphism from $(\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}, *)$ to G, which factors through N via ρ. This yields a

Lie group homomorphism $\widetilde{\phi_{\mathbf{g}}} : N \to G$. Now the main point is the following simple consequence of the above lemma: if a finitely generated non-Diophantine subgroup of a nilpotent Lie group maps to a Diophantine subgroup under a Lie group homomorphism, then its intersection with the kernel is already non-Diophantine. In our case $\rho(\Gamma)$ is non-Diophantine, so its image in G must also be non-Diophantine unless $\ker \widetilde{\phi_{\mathbf{g}}} \cap \rho(\Gamma)$ is non-Diophantine. By minimality of $\dim L$, if this happens, then $L \leqslant \ker \widetilde{\phi_{\mathbf{g}}}$ and so $\phi_{\mathbf{g}}(\Gamma) = 1$. However, this is impossible because we assumed that $\omega(\mathbf{g}) \neq 1$. We conclude that $\phi_{\mathbf{g}}(\Gamma)$ is non-Diophantine in G and hence so is the k-tuple $\mathbf{g}$. □

5.2 Dependence in k of the Diophantine exponent

We gather here a few additional remarks about the Diophantine exponent β, prove Theorem 1.8 and mention some related open problems. First we have the following simple observation.

Remark 5.5. Let G be a connected real Lie group G. The set of integers $k \geqslant 1$ such that G is Diophantine on k letters is an interval $[1, k_0]$, where k_0 is either a finite integer (in case G is not Diophantine) or $+\infty$ (in case it is). This is clear given that if a k-tuple $(s_1, \dots, s_k)$ in G is Diophantine, then any subtuple is again Diophantine. The following result is Theorem 1.4 from the introduction. It shows that, for any integer $k_0 \geqslant 1$, one may construct a nilpotent Lie group G that is Diophantine on k letters if and only if $k \in [1, k_0]$. We thank A. Gamburd for raising the question of the existence of such a Lie group G.

THEOREM 5.6. *For any integer $k_0 \geqslant 1$, there exists a connected nilpotent Lie group G such that G is Diophantine for words on k_0 letters, but non-Diophantine for words in $k_0 + 1$ letters.*

Proof. If $k_0 = 1, 2$, we may conclude, using Theorem 4.4, that any connected nilpotent Lie group of nilpotency step 7 (respectively 6) that is non-Diophantine on 2 (respectively 3) letters will do.

Now assume $k_0 \geqslant 3$. Let $s = k_0 + 3$. By Corollary A.13, the Young diagram with s boxes and $k_0 + 1$ rows of shape $\lambda := (2, 2, 1, \dots, 1)$ occurs with multiplicity in $\mathcal{F}^{[s]}_{k_0+1,s}$. Take E_1 and E_2 two copies of E^λ in $\mathcal{F}^{[s]}_{k_0+1,s}$ defined over $\mathbf{Q}$, and let

$$\mathcal{L} = \{(x, \lambda x) \in E_1 \oplus E_2; x \in E_1\},$$

for some Liouville number λ. Finally, define G to be the connected simply connected nilpotent Lie group with Lie algebra $\mathcal{F}_{k_0+1,s}/\mathcal{L}$. The ideal of laws of G over $k_0 + 1$ letters is just $\mathcal{L}$, and it is non-Diophantine in $\mathcal{F}_{k_0+1,s}$. Hence G is non-Diophantine for words on $k_0 + 1$ letters, by Theorem 3.12.

We claim that the ideal of laws of G over k_0 letters is $\{0\}$, and in particular is Diophantine. This will show that G is Diophantine for words in k_0 letters by Theorem 3.12. To see the claim, observe that the ideal of laws $\mathcal{L}_{k_0,s}(\mathrm{Lie}(G))$ on k_0 letters is homogeneous, so if it is non-zero, then it must contain a weight vector (for the diagonal action $(\mathsf{x}_1, \dots, \mathsf{x}_{k_0}) \to (t_1\mathsf{x}_1, \dots, t_{k_0}\mathsf{x}_{k_0})$), say $\mathsf{r} := \mathsf{r}(\mathsf{x}_1, \dots, \mathsf{x}_{k_0}) \in \mathcal{F}_{k_0,s}$, which, being a law of $\mathrm{Lie}(G)$, must belong to $\mathcal{L}$. The weight of r is of the form $(u_1, \dots, u_{k_0})$. However, Theorem A.5 below shows that the dimension of the subspace of $\mathcal{L} \simeq E^\lambda$ made of vectors of weight $(u_1, \dots, u_{k_0})$ is the number of semi-standard tableaux of shape λ having each number $i = 1, \dots, k_0$ occurring u_i times. In particular such a tableau has at most k_0 distinct entries. However, λ has $k_0 + 1$ rows, and entries are strictly increasing in each column of a standard tableau. Hence any semi-standard tableau of shape λ must have at least $k_0 + 1$ distinct entries. This contradiction proves the claim. □

We will prove here two related results. First we show that if G is s-step nilpotent and is not Diophantine on k letters for some $k \geqslant 1$, then it is not Diophantine on s letters already. In other words we have the following.

Proposition 5.7. *An s-step nilpotent Lie group G is Diophantine if and only if it is Diophantine on s letters.*

Proof. Let $k \geqslant s$. In view of Theorem 3.12 and the above remark we are left to prove that $\mathcal{L}_{k,s}$ is Diophantine in $\mathcal{F}_{k,s}$ if $\mathcal{L}_{s,s}$ is Diophantine in $\mathcal{F}_{s,s}$. For each set B of at most s letters amongst $\mathsf{x}_1, \dots, \mathsf{x}_k$, consider the subspace V_B of $\mathcal{F}_{k,s}$ spanned by the commutators whose set of letters occurring in them is precisely B. The V_B are in direct sum, span $\mathcal{F}_{k,s}$, and they decompose further into weight spaces for the diagonal action $(t_1, \dots, t_k) \cdot c(\mathsf{x}_1, \dots, \mathsf{x}_k) := c(t_1\mathsf{x}_1, \dots, t_k\mathsf{x}_k)$ on $\mathcal{F}_{k,s}$. The weights occurring in V_B are of the form $(n_1, \dots, n_k) \in \mathbf{N}^k$, where $n_i \neq 0$ if and only if $\mathsf{x}_i \in B$. The fully invariant ideal $\mathcal{L}_{k,s}$ also decomposes as a direct sum of weight spaces, and $\mathcal{L}_{k,s} = \bigoplus_B \mathcal{L}_{k,s} \cap V_B$. Observe that for each set B of s letters $\bigoplus_{B' \subset B} V_{B'}$ is isomorphic to $\mathcal{F}_{s,s}$ and $\bigoplus_{B' \subset B} \mathcal{L}_{k,s} \cap V_{B'}$ to $\mathcal{L}_{s,s}$. The result is now a direct consequence of the following lemma. □

Lemma 5.8. *Suppose V is a finite-dimensional $\mathbf{Q}$-vector space and $V_i \leqslant V$ are $\mathbf{Q}$-subspaces such that $V = \bigoplus_i V_i$. Let $L \leqslant V(\mathbf{R})$ be a real subspace such that $L = \bigoplus_i L \cap V_i(\mathbf{R})$. Then L is Diophantine in $V(\mathbf{R})$ (with exponent $A > 0$) if and only if each $L \cap V_i(\mathbf{R})$ is Diophantine in $V_i(\mathbf{R})$ (with same exponent A).*

Proof. This is easily verified since for some choice of norm on $V(\mathbf{R})$, $\|v - l\| = \max\{\|v_i - l_i\|\}$. □

It is worthwhile to stress that the argument above shows that if $A = A_s$ is the exponent making $\mathcal{L}_{s,s}$ Diophantine in $\mathcal{F}_{s,s}$ (see Definition 3.10), then $\mathcal{L}_{k,s}$ is again Diophantine with the same exponent as a subspace of $\mathcal{F}_{k,s}$, for all $k \geqslant s$. Here is an immediate consequence of this and of the proof of Proposition 3.2.

Proposition 5.9. *Let G be a Diophantine s-step nilpotent Lie group. Then for every $\beta > s$ there is $k_0 \geqslant 1$ such that G is β-Diophantine for k-tuples for each $k \geqslant k_0$.*

Proof. Let A_k be the Diophantine exponent of $\mathcal{L}_{k,s}(\mathfrak{g})$ in $\mathcal{F}_{k,s}$, and τ_k the growth exponent of $F_{k,G}$ (see § 2.2 for notation). By Remark 3.13, the group G is β-Diophantine for k-tuples if $\beta > s + sA_k/\tau_k$. We just observed that, for any $k \geqslant s$, we have $A_k \leqslant A_s$; as the growth exponent τ_k goes to $+\infty$ as $k \to +\infty$, the result follows. □

Finally in the opposite direction, using a simple pigeonhole argument, we show that β cannot be too small.

Proposition 5.10. *Let G be an s-step nilpotent Lie group with Lie algebra $\mathfrak{g}$. Let d_s be the dimension of the last step $\mathfrak{g}^{(s)}$. For every $\epsilon > 0$ there is $k_0 \geqslant 1$ such that if, for some $k \geqslant k_0$, G is β-Diophantine for k-tuples, then $\beta > 1/d_s - \epsilon$.*

Proof. Let e_i be the rank of the ith successive quotient in the central descending series of $F_{k,G}$. Then, since $F_{k,G}$ is a lattice in $\mathcal{F}_{k,s}/\mathcal{L}_{k,s}(\mathfrak{g})_{\mathbf{Q}}$ (see Proposition 3.9), e_i is the dimension of $\mathcal{F}_{k,s}^{[i]}/\mathcal{L}_{k,s}^{[i]}(\mathfrak{g})_{\mathbf{Q}}$ for each $i = 1, \dots, s$. However, $\mathcal{L}_{k,s}^{[i]}(\mathfrak{g})_{\mathbf{Q}}$ is an SL_k-submodule of $\mathcal{F}_{k,s}$ for the action by linear substitution of the variables; and by Corollary A.4 each irreducible SL_k-module appearing in $\mathcal{F}_k^{[i]}$ has its dimension equal to a polynomial of degree i in k, when $k \geqslant s$. The number of irreducible modules that may appear in $\mathcal{F}_k^{[i]}$ is bounded in terms of i only, so each e_i is bounded above and below by a polynomial of degree i in the variable k. With some extra work it can be shown that e_i is a polynomial in k when $k \geqslant s$, but we will not need that.

Now the Bass–Guivarc'h formula (1) tells us that $\tau_k - se_s$ is a linear combination of the e_i, $i < s$. Hence it is bounded above by a polynomial in k of degree at most $s - 1$. In particular

$\lim_{k\to+\infty} se_s/\tau_k = 1$. Now there are roughly n^{se_s} word maps in the word ball of $F_{k,G}$ with radius n that lie in $F_{k,G}^{[s]}$. For a given k-tuple the images of these word maps lie in $G^{[s]}$ and are at (left-invariant Riemannian) distance $O(n)$ from the origin. Hence they lie in a part of $G^{[s]}$ of measure $O(n^{sd_s})$, because their norm in $\mathrm{Lie}(G)$ is of order $O(n^s)$ (by the ball-box principle, e.g. see [Bre14, Proposition 4.5]). By the pigeonhole principle, there must be a word of length $\leqslant 2n$ lying at (Riemannian) distance $\ll n^{-s(e_s/d_s-1)}$ from the origin. By letting k tend to $+\infty$ the result follows. □

For a Diophantine s-step nilpotent Lie group G, we can set

$$\beta_k := \inf\{\beta > 0; G \text{ is } \beta\text{-Diophantine for } k\text{-tuples}\}.$$

The above discussion shows that

$$\frac{1}{d_s} \leqslant \liminf \beta_k \leqslant \limsup \beta_k \leqslant s$$

where $d_s = \dim G^{[s]}$. At first glance it may seem surprising that these bounds hold for every Diophantine nilpotent group regardless of the Diophantine exponent A_k of $\mathcal{L}_{k,s}(\mathfrak{g})$ in $\mathcal{F}_{k,s}$.

It seems plausible that $\lim_k \beta_k$ exists and is greater than 0 for every Diophantine nilpotent Lie group. This can be verified in certain cases. For example, a Borel–Cantelli argument can be used to prove that the critical exponent for the 3-dimensional Heisenberg group is $\beta_k := 1-1/k-2/k^2$. In this case for any $\beta < \beta_k$ almost every k-tuple is not β-Diophantine. It would be interesting to compute exactly the critical exponent say for all nilpotent Lie groups defined over $\mathbf{Q}$. We plan to address some of these issues in a subsequent paper.

5.3 Speed of equidistribution

In [Bre10] the second-named author proved that finitely generated dense subgroups of connected nilpotent Lie groups are equidistributed. However, no rate of convergence was derived, in part because of the use of ergodic theory through Ratner's theorem in the proof. Of course no good error term is to be expected for general dense subgroups. Indeed even when $G = \mathbf{R}$, the 2-generated subgroup $\mathbf{Z} + \lambda\mathbf{Z}$ is equidistributed (Weyl) but no rate can be expected if say λ is irrational and yet extremely well approximable by rationals. It seems likely, however, that Diophantine dense subgroups are equidistributed with some (polynomial) rate (this is true for $\mathbf{R}$ by a standard Fourier argument), and perhaps this is even true for random subgroups in any nilpotent Lie group, Diophantine or not. This can be compared with the situation in SU(2), where we expect (cf. Sarnak's spectral gap conjecture) that every (as opposed to almost every) k-tuple equidistribute with a good rate. In this case, in stark contrast with the nilpotent case, we know by the work of the second-named author [Bre11, Corollary 1.11] that every k-tuple satisfies a weak form of the Diophantine property.

5.4 Almost laws

In showing that there are non-Diophantine nilpotent and solvable Lie groups, we proved that there are sequences of words w_n on k-tuples which are not laws of G but behave like almost laws in that, for every compact subset K of G^k, $w_n(K) \to 1$ very fast. We informally call such words almost laws. If G is any algebraic group defined over $\mathbf{Q}$, then picking a non-zero rational point it is easy to see that an almost law cannot shrink every fixed compact set faster than exponentially fast (in the length $l(w_n)$ of the word) for a general G, and faster than polynomially fast if G is nilpotent. It may be of interest to observe that the well-known shrinking property

of commutators near the identity in any Lie group G, implies that the sequence of iterated commutators $w_{n+1} = [w_n, w_{n-1}]$ shrink a fixed neighborhood of 1 at speed $e^{C\sqrt{l(w_n)}}$. Note that in [Tho13] a construction is given of a sequence of almost laws w_n such that $w_n(G^k) \to 1$ for every compact group G. We end with the following question, say for $G = \mathrm{SU}(2)$. Can one find a sequence of words w_n such that $w_n(G^k) \subset B(1, e^{-cl(w_n)})$ for some $c > 0$ as $l(w_n) \to +\infty$?

Acknowledgements
We would like to thank D. Segal and Y. de Cornulier for providing useful references about group varieties. We are also grateful to Y. Benoist, A. Gamburd, A. Gorodnik, N. Monod and P. Varjú for interesting discussions regarding various issues related to this paper. The referee's comments and careful reading were also of great help and we are happy to thank him or her. E.B. and N.S. acknowledge partial support from the European Research Council (ERC) Grant GADA 208091, ERC AdG Grant 267259, ANR-12-BS01-0011 and ANR-13-BS01-0006-01, while M.A. acknowledges the support of ISEF and Advanced Research Grant 228304 from the ERC. L.R. was supported by the Göran Gustafsson Foundation (KVA).

Appendix A. The free Lie algebra viewed as an SL_k-module

In this appendix we recall Witt's formula for the dimension of the weight spaces of the free Lie algebra on k generators. Then we use this formula to decompose the free nilpotent Lie algebra on k generators and step s into irreducible SL_k-modules for small values of k and s. We also determine precisely for which values of k and s this decomposition is multiplicity-free. As we saw in § 4, this is key to proving that nilpotent Lie groups in step at most 5 are Diophantine and to build counter-examples in higher step.

A.1 Witt's formula

Throughout the appendix, $\mathcal{F}_k$ denotes the free nilpotent Lie algebra on k generators over a field K of characteristic zero (not necessarily $\mathbf{R}$ as in the rest of the paper). Let $\mathcal{F}_k^{[s]}$ be the subspace of elements of homogeneous degree s in $\mathcal{F}_k$. The group $\mathrm{SL}_k := \mathrm{SL}_k(K)$ acts naturally on $\mathcal{F}_k^{[s]}$ by linear substitution of the free variables. Let A be the diagonal subgroup of SL_k. The representation $\mathcal{F}_k^{[s]}$ splits as a direct sum of weight spaces:

$$\mathcal{F}_k^{[s]} = \bigoplus_{\chi} V(\chi)$$

where $V(\chi)$ is the weight space associated to $\chi \in A^*$. The weights are multiplicative characters on A. Given non-negative integers $n_1, \dots, n_k$, let $\ell(n_1, \dots, n_k)$ be the dimension of the weight space with weight

$$\chi_{(n_1,\dots,n_k)} : a \mapsto \prod_i a_i^{n_i}, \tag{A1}$$

where $a \in A$ is the diagonal matrix $\mathrm{diag}(a_1, \dots, a_k)$. We will often abbreviate $\chi_{(n_1,\dots,n_k)}$ simply by $(n_1, \dots, n_k)$.

In 1937 Witt proved [Wit37, Satz 1] what is now known as the Poincaré–Birkhoff–Witt Theorem about Lie algebras and their universal enveloping algebras. In his third theorem [Wit37, Satz 3], he deduces from it two dimension formulas. The first gives the dimension of $\mathcal{F}_k^{[s]}$:

$$\dim \mathcal{F}_k^{[s]} = \frac{1}{s} \sum_{d|s} \mu(d) k^{s/d}, \tag{A2}$$

where $\mu(d)$ is the Möbius function. By Möbius inversion, this formula is equivalent to

$$\sum_{d|s} d \dim \mathcal{F}_k^{[d]} = k^s. \tag{A3}$$

The second formula of Witt refines the first and gives the dimension of the homogeneous components. It can be stated as follows.

THEOREM A.1 (Witt's character formula for the free Lie algebra). *Let $n_1, \dots, n_k$ be non-negative integers. The dimension $\ell(n_1, \dots, n_k)$ of the weight space with weight $(n_1, \dots, n_k)$ for the SL_k-action on the subspace $\mathcal{F}_k^{[s]}$ of commutators of order s in the free Lie algebra on k generators is*

$$\ell(n_1, \dots, n_k) = \frac{1}{n} \sum_{d|\gcd(n_1,\dots,n_k)} \mu(d) \frac{(\frac{n}{d})!}{(\frac{n_1}{d})! \cdot \dots \cdot (\frac{n_k}{d})!},$$

where $n = n_1 + \dots + n_k$.

In the above formula $\mu(d)$ is the Möbius function. By Möbius inversion, the formula is readily seen to be equivalent to

$$\sum_{m|\gcd(n_1,\dots,n_k)} \frac{1}{m} \ell\left(\frac{n_1}{m}, \dots, \frac{n_k}{m}\right) = \frac{((\sum_i n_i) - 1)!}{n_1! \cdot \dots \cdot n_k!}$$

for all choices of non-negative integers $n_1, \dots, n_k$.

For the reader's convenience, we reproduce Witt's proof below following Serre's treatment of Witt's first dimension formula (A3). See [Ser06, ch. 4] and also Hall's book [Hal76, ch. 11.2] for a different proof.

Proof. Let A be the free associative K-algebra on k generators (i.e. formal linear combinations of *non-commutative* monomials in k letters). Let $a(n_1, \dots, n_k)$ be the dimension of the subspace of A generated by non-commutative monomials with the letter X_i occurring n_i times.

By [Ser06, Theorem 4.2.1], the algebra A is isomorphic to the universal enveloping algebra of the free Lie algebra. Pick a basis $\{C_j\}_j$ of the free Lie algebra on k generators $X_1, \dots, X_k$ made of commutators C_j. By the Poincaré–Birkhoff–Witt Theorem, A has a basis consisting of monomials of the form

$$C^e := C_{i_1}^{e_{i_1}} \cdot \dots \cdot C_{i_k}^{e_{i_k}} \quad \text{with } i_1 < i_2 < \dots < i_k.$$

We have $\deg(C^e) = \sum_j e_{i_j} d_{i_j}$ and $\deg_{X_i}(C^e) = \sum_j e_{i_j} d_{C_{i_j}}(X_i)$, where $d_{C_j}(X_i)$ is the number of occurrences of the letter X_i in the commutator C_j.

Formula (A3) will follow by counting $a(n_1, \dots, n_k)$ in two ways. On the one hand it is clear that

$$a(n_1, \dots, n_k) = \frac{(\sum_i n_i)!}{n_1! \dots n_k!}.$$

On the other hand $a(n_1, \dots, n_k)$ is also the number of families $\{e_j\}$ such that

$$n_i = \sum_j e_j d_{C_j}(X_i)$$

for each $i = 1, \dots, k$. Therefore $a(n_1, \dots, n_k)$ is the coefficient of $t_1^{n_1} \cdot \ldots \cdot t_k^{n_k}$ in the formal power series

$$\prod_j (1 + t_1^{d_{C_j}(X_1)} \cdot \ldots \cdot t_k^{d_{C_j}(X_k)} + t_1^{2d_{C_j}(X_1)} \cdot \ldots \cdot t_k^{2d_{C_j}(X_k)} + \cdots + t_1^{md_{C_j}(X_1)} \cdot \ldots \cdot t_k^{md_{C_j}(X_k)} + \ldots)$$

which is the same as

$$\prod_j \frac{1}{1 - t_1^{d_{C_j}(X_1)} \cdot \ldots \cdot t_k^{d_{C_j}(X_k)}}.$$

Therefore we have the following identity:

$$\prod_j \frac{1}{1 - t_1^{d_{C_j}(X_1)} \cdot \ldots \cdot t_k^{d_{C_j}(X_k)}} = \sum_{n_1, \dots, n_k} \frac{(\sum_i n_i)!}{n_1! \dots n_k!} t^{n_1} \cdot \ldots \cdot t_k^{n_k} = \frac{1}{1 - (t_1 + \cdots + t_k)}.$$

Using $\log 1/(1-u) = \sum_m (1/m) u^m$, and taking logs we get

$$\sum_{n_1, \dots, n_k, m} \ell(n_1, \dots, n_k) \frac{1}{m} (t_1^{n_1} \cdot \ldots \cdot t_k^{n_k})^m = \sum_m \frac{1}{m} (t_1 + \cdots + t_k)^m.$$

Identifying the coefficients of each term we finally obtain the desired formula:

$$\sum_{m | \gcd(n_1, \dots, n_k)} \frac{1}{m} \ell\left(\frac{n_1}{m}, \dots, \frac{n_k}{m}\right) = \frac{((\sum_i n_i) - 1)!}{n_1! \cdot \ldots \cdot n_k!},$$

which, applying Möbius inversion, yields

$$\ell(n_1, \dots, n_k) = \sum_{d | \gcd(n_1, \dots, n_k)} \frac{\mu(d)}{d} \frac{((\sum_i n_i/d) - 1)!}{(n_1/d)! \cdot \ldots \cdot (n_k/d)!} = \frac{1}{n} \sum_{d | \gcd(n_1, \dots, n_k)} \mu(d) \frac{(n/d)!}{(n_1/d)! \cdot \ldots \cdot (n_k/d)!}.$$

□

A.2 Multiplicity-free theorem

Armed with Theorem A.1 we are now able to determine the decomposition of $\mathcal{F}_k^{[s]}$ into simple SL_k-modules. For small values of k and s we can give a complete description of the irreducible submodules, and for all values of k and s we determine when it is multiplicity-free.

Theorem A.2 (Multiplicity-free). *Let $\mathcal{F}_k^{[s]}$ be the subspace spanned by commutators of order s in the free Lie algebra on k generators. Then $\mathcal{F}_k^{[s]}$ is a multiplicity-free SL_k-module if and only if $s \leqslant 5$ when $k \geqslant 3$, and if and only if $s \leqslant 6$ when $k = 2$.*

Recall that irreducible representations of SL_k are parametrized by their highest weight. If $n_1 \geqslant \cdots \geqslant n_k \geqslant 0$ are non-negative integers, we denote by $E^{(n_1, \dots, n_k)}$ the irreducible representation of SL_k with highest weight $(n_1, \dots, n_k)$. If $n_{i+1} = n_{i+2} = \cdots = n_k = 0$, we will write $E^{(n_1, \dots, n_i)}$ for $E^{(n_1, \dots, n_i, 0, \dots, 0)}$.

We also recall Weyl's dimension formula for $E^{(n_1, \dots, n_k)}$, [FH91, Theorem 6.3]

$$\dim E^{(n_1, \dots, n_k)} = \prod_{1 \leqslant i < j \leqslant k} \frac{n_i - n_j + j - i}{j - i}. \tag{A4}$$

From this formula we derive the following.

LEMMA A.3. *Given $k \geqslant s \geqslant 1$ and $n_1 \geqslant \cdots \geqslant n_s$ non-negative integers such that $s = n_1 + \cdots + n_s$, the dimension of the irreducible SL_k-module $E^{(n_1,\ldots,n_k)}$ is the value at k of a polynomial of degree s and coefficients in $\mathbf{Q}$.*

Proof. Split the product in s factors $F_i := \prod_{j=i+1}^{k} (n_i - n_j + j - i)/(j - i)$ for $i = 1, \ldots, s$. Each such F_i is in fact the product of a rational number independent of k (the product of the factors arising when $i + 1 < j \leqslant s$ and the denominators of the fraction when $j = s + 1, \ldots, s + n_i$) with $(k + 1) \cdot \ldots \cdot (k + n_i)$. So each F_i is a polynomial of degree n_i in k with coefficients in $\mathbf{Q}$. The claim follows. □

Since the only weights $(n_1, \ldots, n_k)$ that can occur in $\mathcal{F}_{k,s}^{[s]}$ are such that $n_1 + \cdots + n_k = s$, we obtain the following.

COROLLARY A.4. *If $k \geqslant s$, the dimension of every irreducible SL_k-module occurring in $\mathcal{F}_{k,s}^{[s]}$ is a polynomial of degree s in k.*

If V is a finite-dimensional SL_k-module and $(n_1, \ldots, n_k)$ is its highest weight, then the irreducible SL_k-module $E^{(n_1,\ldots,n_k)}$ with highest weight $(n_1, \ldots, n_k)$ occurs as a submodule of V. Since the dimensions of the weight spaces of each irreducible SL_k-module are known, or at least can be computed, we have a procedure to decompose the original module V into a direct sum of irreducible submodules.

The dimension of the weight space of weight $(u_1, \ldots, u_k)$ in the irreducible representation with highest weight $(n_1, \ldots, n_k)$ can be determined by counting Young tableaux. Recall that to each irreducible SL_k-module $E^{(n_1,\ldots,n_k)}$, $n_1 \geqslant \cdots \geqslant n_k \geqslant 0$, is associated the Young diagram $\lambda := (n_1, \ldots, n_k)$, with n_i boxes in the ith row. A semi-standard tableau of shape λ is a filling of the Young diagram λ with positive integers (one in each box) in such a way that the rows are non-decreasing and the columns strictly increasing.

We have the following (see e.g. Fulton and Harris [FH91, p. 224]).

THEOREM A.5. *Given a Young diagram $\lambda := (n_1, \ldots, n_k)$, the dimension of the weight space of weight $(u_1, \ldots, u_k)$ in E^{λ} is the number of semi-standard tableaux of shape λ filled with integers $i \in \{1, \ldots, k\}$ such that each i occurs u_i times.*

We now turn to the proof of Theorem A.2 and start by analyzing the case when $s \geqslant 7$.

LEMMA A.6. *If $s \geqslant 7$ and $k \geqslant 2$, then $\mathcal{F}_k^{[s]}$ is not multiplicity-free.*

Proof. If a weight $\chi_{(n_1,\ldots,n_k)}$ occurs non-trivially in $\mathcal{F}_k^{[s]}$, then $\sum n_i = s$. Using Theorem A.1, we compute easily $\ell(s, 0, \ldots, 0) = 0$ and $\ell(s - 1, 1, 0, \ldots, 0) = 1$. It follows that the highest weight occurring in $\mathcal{F}_k^{[s]}$ is $(s - 1, 1, 0, \ldots, 0)$ and it occurs with multiplicity one.

Again using Theorem A.1 one computes $\ell(s-2, 2, 0, \ldots, 0)$. If s is odd, then this is $(s - 1)/2$, and if s is even, then it is $s/2 - 1$. As $s \geqslant 7$, this is at least 3. However, counting the number of associated Young diagrams, one sees that the dimension of the weight space $(s - 2, 2, 0, \ldots, 0)$ in both $E^{(s-1,1)}$ and $E^{(s-2,2)}$ is 1. Therefore, it must be that $E^{(s-2,2)}$ occurs with multiplicity at least 2 in $\mathcal{F}_k^{[s]}$. □

The rest of this subsection is devoted to the study of the cases $s = 2$ to $s = 6$. In each case, we can work out the decomposition of $\mathcal{F}_k^{[s]}$ into irreducible modules using Theorem A.1. We discovered a posteriori that this decomposition had been computed already by R. Thrall in 1942 for each s up to $s = 10$, see [Thr42, pp. 387, 388].

Case $\mathbf{s}=\mathbf{2}$. Here $\mathcal{F}_k^{[2]}$ is always irreducible and coincides with $E^{(1,1)}$. Indeed the highest weight of $\mathcal{F}_k^{[2]}$ is $(1,1,0,\dots,0)$ and comparing dimensions, we conclude that only $E^{(1,1)}$ occurs as a submodule of $\mathcal{F}_k^{[2]}$.

Case $\mathbf{s}=\mathbf{3}$. In this case $\sum_i n_i=3$, we see that the only possible values for the n_i are $(1,1,1,0,\dots,0)$ and $(2,1,0,\dots,0)$ and arbitrary permutations of such. Using Theorem A.1 we compute $\ell(1,1,1,0,\dots,0)=2$ and $\ell(2,1,0\dots,0)=1$. Since the highest weight of $\mathcal{F}_k^{[3]}$ is $(2,1,0,\dots,0)$, this implies that the irreducible representation $E^{(2,1)}$ with highest weight $(2,1,0,\dots,0)$ occurs as a sub-representation. However, by Weyl's dimension formula (A4) we have

$$\dim E^{(2,1)}=\frac{(k-1)k(k+1)}{3}=\frac{1}{3}(k^3-k).$$

Since this coincides with $\dim \mathcal{F}_k^{[3]}$ by Witt's first formula (A3), we conclude that $\mathcal{F}_k^{[3]}$ is the irreducible SL_k module,

$$\mathcal{F}_k^{[3]}=E^{(2,1)}.$$

Case $\mathbf{s}=\mathbf{4}$. Since $\sum_i n_i=4$, we see that the only possible values for the n_i are $(1,1,1,1,0\dots,0)$ and $(2,1,1,0,\dots,0)$, $(2,2,0,\dots,0)$ and $(3,1,0,\dots,0)$ arbitrary permutations of such. Using Theorem A.1 we compute $\ell(1,1,1,1,0,\dots,0)=6$, $\ell(2,1,1,0\dots,0)=3$, $\ell(2,2,0,\dots,0)=1$, and $\ell(3,1,0,\dots,0)=1$.

The highest weight of $\mathcal{F}_k^{[4]}$ is $(3,1,0,\dots,0)$, so $\mathcal{F}_k^{[4]}$ contains $E^{(3,1)}$. Now $\mathcal{F}_k^{[4]}\ominus E^{(3,1)}$ has highest weight $(2,1,1,0,\dots,0)$, so contains $E^{(2,1,1)}$. By the dimension formula,

$$\dim E^{(3,1)}=\tfrac{1}{8}(k-1)k(k+1)(k+2)=3C_{k+2}^4,$$

$$\dim E^{(2,1,1)}=\tfrac{1}{8}(k-2)(k-1)k(k+1).$$

Since they sum up to $\dim \mathcal{F}_k^{[4]}=1/4(k^4-k^2)$ we conclude that

$$\mathcal{F}_k^{[4]}=E^{(3,1)}\oplus E^{(2,1,1)}.$$

If $k=2$, then the second term is zero, and $\mathcal{F}_2^{[4]}$ is irreducible. However, if $k\geqslant 3$, then both terms are non-zero and non-isomorphic, so $\mathcal{F}_k^{[4]}$ is not irreducible and its irreducible submodules have multiplicity 1.

In fact $E^{(2,1,1)}$ is isomorphic to $\Lambda^2(\Lambda^2(K^k))$, which is the space of *metabelian* brackets, i.e. generated by the brackets $[[X_i,X_j],[X_k,X_l]]$. Those with distinct letters contribute for half of the weight space with weight type $(1,1,1,1,0,\dots,0)$.

Case $\mathbf{s}=\mathbf{5}$. Since $\sum_i n_i=5$, the only possible values for the n_i are $(4,1,0,\dots,0)$, $(3,2,0,\dots,0)$, $(3,1,1,0,\dots,0)$, $(2,2,1,0,\dots,0)$, $(2,1,1,1,0,\dots,0)$ and $(1,1,1,1,1,0\dots,0)$ and arbitrary permutations of such. Using Theorem A.1 we obtain $\ell(4,1)=1$, $\ell(3,2)=2$, $\ell(3,1,1)=4$, $\ell(2,2,1)=6$, $\ell(2,1,1,1)=12$ and $\ell(1,1,1,1,1)=24$.

In order to decompose $\mathcal{F}_k^{[5]}$ into irreducibles, we first determine the dimensions of the weight spaces of the irreducible representations of SL_k whose highest weight are in each of the above six families of weights. This is done by counting Young diagrams (or by using the sage command $symmetrica.kostka\_tafel(5)$) and we obtain Table A.1.

TABLE A.1. Dimensions of weight spaces of positive weight in the irreducible representations of SL_k of norm 5.

	Module					
Weight	$E^{(4,1)}$	$E^{(3,2)}$	$E^{(3,1,1)}$	$E^{(2,2,1)}$	$E^{(2,1,1,1)}$	$E^{(1,1,1,1,1)}$
$A=(4,1)$	1					
$B=(3,2)$	1	1				
$C=(3,1,1)$	2	1	1			
$D=(2,2,1)$	2	2	1	1		
$E=(2,1,1,1)$	3	3	3	2	1	
$F=(1,1,1,1,1)$	4	5	6	5	4	1

Comparing this data with the values for ℓ written above, we conclude that $\mathcal{F}_k^{[5]}$ is the direct sum of one copy of each one of the above six irreducible modules, except $E^{(1,1,1,1,1)}$:

$$\mathcal{F}_k^{[5]} = E^{(4,1)} \oplus E^{(3,2)} \oplus E^{(3,1,1)} \oplus E^{(2,2,1)} \oplus E^{(2,1,1,1)}.$$

If $k \geqslant 4$, then all 5 irreducible submodules are non-zero and pairwise non-isomorphic.

If $k = 3$, the last module is zero but the others are pairwise non-isomorphic:

$$\mathcal{F}_3^{[5]} = E^{(4,1)} \oplus E^{(3,2)} \oplus E^{(3,1,1)} \oplus E^{(2,2,1)}.$$

If $k = 2$, then the last three modules are zero and we get

$$\mathcal{F}_2^{[5]} = E^{(4,1)} \oplus E^{(3,2)}.$$

We conclude that the following holds.

LEMMA A.7. *In step $s = 5$ the SL_k-module $\mathcal{F}_k^{[5]}$ is multiplicity-free for all $k \geqslant 2$.*

Case $\mathbf{s = 6}$. Since $\sum_i n_i = 6$, we see that the only possible values for the n_i are $A := (5,1,0,\dots,0)$, $B := (4,2,0,\dots,0)$, $C := (4,1,1,0,\dots,0)$, $D := (3,3,0,\dots,0)$, $E := (3,2,1,0,\dots,0)$, $F := (3,1,1,1,0,\dots,0)$, $G := (2,2,2,0,\dots,0)$, $H := (2,2,1,1,0,\dots,0)$, $I := (2,1,1,1,1,0,\dots,0)$, and $J := (1,1,1,1,1,1,0\dots,0)$ and arbitrary permutations of such. We can then compute values of ℓ by Theorem A.1 and obtain the following: $\ell(A) = 1$, $\ell(B) = 2$, $\ell(C) := 5$, $\ell(D) = 3$, $\ell(E) = 10$, $\ell(F) = 20$, $\ell(G) = 14$, $\ell(H) = 30$, $\ell(I) = 60$, $\ell(J) = 120$.

In order to decompose $\mathcal{F}_k^{[6]}$ into irreducibles, we first determine the dimensions of the weight spaces of the irreducible representations of SL_k whose highest weight are in each of the above ten families of weights A to J. This is done by counting Young diagrams exactly as we did in the step 5 case. Doing this counting (or using the sage command *symmetrica.kostka_tafel*(6)) we obtain the numbers given in Table A.2.

Comparing this data with the values for ℓ written above, we conclude that $\mathcal{F}_k^{[6]}$ is the direct sum of the following irreducible modules:

$$\mathcal{F}_k^{[6]} = E^{(5,1)} \oplus E^{(4,2)} \oplus (E^{(4,1,1)})^2 \oplus E^{(3,3)} \oplus (E^{(3,2,1)})^3 \oplus E^{(3,1,1,1)} \oplus (E^{(2,2,1,1)})^2 \oplus E^{(2,1,1,1,1)}.$$

Note that E^G and E^J do not occur as a submodule. If $k \geqslant 5$, then all terms are non-zero.

Table A.2. Dimensions of weight spaces of positive weight in the irreducible representations of SL_k labeled E^A to E^J.

	Module									
Weight	E^A	E^B	E^C	E^D	E^E	E^F	E^G	E^H	E^I	E^J
$A=(5,1)$	1									
$B=(4,2)$	1	1								
$C=(4,1,1)$	2	1	1							
$D=(3,3)$	1	1	0	1						
$E=(3,2,1)$	2	2	1	1	1					
$F=(3,1,1,1)$	3	3	3	1	2	1				
$G=(2,2,2)$	2	3	1	1	2	0	1			
$H=(2,2,1,1)$	3	4	3	2	4	1	1	1		
$I=(2,1,1,1,1)$	4	6	6	3	8	4	2	3	1	
$J=(1,1,1,1,1,1)$	5	9	10	5	16	10	5	9	5	1

Note that the submodules corresponding to weights involving more than k variables do not occur. Taking this remark into account we find the following.

If $k=4$,

$$\mathcal{F}_4^{[6]} = E^{(5,1)} \oplus E^{(4,2)} \oplus (E^{(4,1,1)})^2 \oplus E^{(3,3)} \oplus (E^{(3,2,1)})^3 \oplus E^{(3,1,1,1)} \oplus (E^{(2,2,1,1)})^2.$$

If $k=3$,

$$\mathcal{F}_3^{[6]} = E^{(5,1)} \oplus E^{(4,2)} \oplus (E^{(4,1,1)})^2 \oplus E^{(3,3)} \oplus (E^{(3,2,1)})^3.$$

If $k=2$,

$$\mathcal{F}_2^{[6]} = E^{(5,1)} \oplus E^{(4,2)} \oplus E^{(3,3)}.$$

We may then conclude that the following holds.

Lemma A.8. *In step $s=6$, when $k \geqslant 3$, then some irreducible SL_k-submodule of $\mathcal{F}_k^{[6]}$ appears with multiplicity $\geqslant 2$. If $k=2$, then $\mathcal{F}_2^{[6]}$ is multiplicity-free.*

This completes the proof of Theorem A.2.

A.3 The free metabelian Lie algebra

In order to prove Theorems 4.5 and 4.7, we need to describe the submodule structure of the free metabelian Lie algebra, i.e. the quotient $\mathcal{F}_k/\mathcal{M}_k$, where $\mathcal{M}_k := D^2(\mathcal{F}_k)$ is the second term of the derived series of $\mathcal{F}_k$.

Lemma A.9. *Let $\mathcal{M}_k^{[s]}$ be the homogeneous component of degree $s \geqslant 2$ of $\mathcal{M}_k$. Then*

$$\mathcal{F}_k^{[s]}/\mathcal{M}_k^{[s]} \simeq E^{(s-1,1)}.$$

Moreover, $E^{(s-1,1)}$ does not occur in the decomposition of $\mathcal{M}_k^{[s]}$ into irreducible submodules.

Proof. From the set $\{\mathsf{x}_1 < \cdots < \mathsf{x}_k\}$, construct a Hall family P for the free Lie algebra $\mathcal{F}_k$ (see Serre [Ser06, Part I, ch. IV, § 5] for definitions). Denote by P_s the elements of P of homogeneous degree s, and

$$P'_s = \{[\mathsf{x}_{i_1}, [\mathsf{x}_{i_2}, \ldots [\mathsf{x}_{i_{s-1}}, \mathsf{x}_{i_s}] \ldots]] : i_1 \geqslant i_2 \geqslant \cdots \geqslant i_{s-1}; i_s > i_{s-1}\}.$$

All other elements of P_s belong to $\mathcal{M}_k$. Hence these elements span $\mathcal{F}_k^{[s]}$ modulo $\mathcal{M}_k^{[s]}$. In fact they form a basis of $\mathcal{F}_k^{[s]}/\mathcal{M}_k^{[s]}$. Indeed, the SL_k-module $\mathcal{F}_k^{[s]}$ has highest weight $(s-1,1)$ with highest weight vector $[\mathsf{x}_1,[\mathsf{x}_1,[\ldots,[\mathsf{x}_1,\mathsf{x}_2]\ldots]\in P'_s$. So and so $\mathcal{F}_k^{[s]}/\mathcal{M}_k^{[s]}$ contains $E^{(s-1,1)}$ as an irreducible submodule. However, one verifies that the cardinality of P'_s is precisely the number of Young tableaux of shape $(s-1,1)$. Hence it is the dimension of $E^{(s-1,1)}$. This proves the first part of the lemma. Finally we already observed in the proof of Lemma A.6 that $E^{(s-1,1)}$ has multiplicity one in $\mathcal{F}_k^{[s]}$. □

COROLLARY A.10. *The free metabelian Lie algebra on k generators $\mathcal{F}_k/\mathcal{M}_k$ is multiplicity-free as an SL_k-module.*

A.4 Klyachko's theorem and the Kraskiewicz–Weyman formula

In 1973, Klyachko determined exactly which irreducible modules appear in the homogeneous component $\mathcal{F}_k^{[s]}$ of degree s of the free Lie algebra over k generators $\mathcal{F}_{k,s}$.

THEOREM A.11 (Klyachko's theorem [Klj74]). *Let $k\geqslant 2$, $s\geqslant 1$. The irreducible SL_k-module E^λ associated to the Young diagram λ appears as a submodule of $\mathcal{F}_k^{[s]}$ if and only if λ has s boxes, at most k rows and is not one of the following diagrams: a diagram with just one column $\lambda=(1,\ldots,1)$, or just one row $\lambda=(s,0,\ldots,0)$, or the two diagrams $\lambda=(2,2)$ and $\lambda=(2,2,2)$.*

We refer the reader to [Reu93] and [KS06] for two different proofs of Klyachko's theorem. This beautiful result falls short of providing a description of the multiplicities of irreducible SL_k-submodules of $\mathcal{F}_k^{[s]}$. Theorem A.12 below does just that.

Recall that if $\lambda=(\lambda_1,\ldots,\lambda_r)$ is a Young diagram with total number of boxes s, a *standard tableau* of shape λ is a filling of λ with $\{1,\ldots,s\}$ having increasing rows and increasing columns. For a standard tableau T of shape λ, with total number of boxes s, a *descent* is an index i in $\{0,\ldots,s-1\}$ such that $i+1$ is located in a lower row than i in T. We denote by $D(T)\subset\{1,\ldots,s-1\}$ the set of descents of T and define the *major index* of T as

$$\mathrm{maj}(T)=\sum_{i\in D(T)} i.$$

The following theorem is due to Kraskiewicz and Weyman [KW01] (see also [Reu93, Corollary 8.10]).

THEOREM A.12 (Kraskiewicz–Weyman formula). *Let $k\geqslant 2$, $s\geqslant 1$. The multiplicity of the Young diagram λ in the decomposition of $\mathcal{F}_k^{[s]}$ into irreducible SL_k-submodules is equal to the number of standard tableaux of shape λ with major index congruent to i mod s, where i is any fixed integer coprime to s. In particular, this number does not depend on the choice of i.*

Although it is not obvious, one can recover Theorem A.11 from Theorem A.12, see [Joh07].

Theorem A.12 allows us to show the following result about multiplicity of a specific Young diagram in the SL_k-module $\mathcal{F}_k^{[s]}$. This is needed in the proof of Theorem 5.6 only.

COROLLARY A.13. *For $s\geqslant 6$, $k\geqslant s-2$, the Young diagram $(2,2,1,\ldots,1)$ with a total number of s boxes occurs with multiplicity in $\mathcal{F}_k^{[s]}$.*

Proof. For T a standard tableau with s boxes we denote by T^* its conjugate, namely the new tableau whose ith column is the ith row of T. Note that $T*$ is also standard and that the set of

descents of T^* is just the complement in $\{1,\dots,s-1\}$ of the set of descents of T. So we have

$$\mathrm{maj}(T) = \frac{s(s-1)}{2} - \mathrm{maj}(T^*). \tag{A5}$$

If s is odd, applying the Kraskiewicz–Weyman formula with $i=1$, we see that it suffices to find two different standard tableaux of shape $(s-2,2)$ with major index congruent to $s(s-1)/2-1 = -1 \bmod s$. The major index of a standard tableau T of shape $(s-2,2)$ is equal to $x+y-2$, where x and y are the entries of the lower row of T. Taking the two standard tableaux with respective lower rows $(2,s-1)$ and $(3,s-2)$, we get what we want.

If $s=2t$ is even, then (A5) and the Kraskiewicz–Weyman formula with $i=-1$ show that we just have to find two different standard tableaux of shape $(s-2,2)$ with major index congruent to $t+1 \bmod s$. For that, we take the two standard tableaux with lower rows $(2,t+1)$ or $(3,t)$. □

Remark A.14. Note that when s is not congruent to 2 modulo 4, both 1 and $s(s-1)/2-1$ are prime to s, so that, by (A5), the multiplicity of a Young diagram λ is $\mathcal{F}_k^{[s]}$ is equal to the multiplicity of the transpose diagram λ^*.

References

Bas72 H. Bass, *The degree of polynomial growth of finitely generated nilpotent groups*, Proc. Lond. Math. Soc. (3) **25** (1972), 603–614.

BG06 E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4 (Cambridge University Press, Cambridge, 2006).

BG08 J. Bourgain and A. Gamburd, *On the spectral gap for finitely generated subgroups of* SU(2), Invent. Math. **171** (2008), 83–121.

Bre10 E. Breuillard, *Equidistribution of dense subgroups on nilpotent Lie groups*, Ergodic Theory Dynam. Systems **30** (2010), 131–150.

Bre11 E. Breuillard, *Heights on* SL_2 *and free subgroups*, in *Geometry, rigidity, and group actions*, Chicago Lectures in Mathematics (University Chicago Press, Chicago, IL, 2011), 455–493.

Bre14 E. Breuillard, *Geometry of locally compact groups of polynomial growth and shape of large balls*, Groups Geom. Dyn. **8** (2014), 669–732.

CG90 L. J. Corwin and F. P. Greenleaf, *Representations of nilpotent Lie groups and their applications. Part I*, in *Basic theory and examples*, Cambridge Studies in Advanced Mathematics, vol. 18 (Cambridge University Press, Cambridge, 1990).

Dod92 M. M. Dodson, *Hausdorff dimension, lower order and Khintchine's theorem in metric Diophantine approximation*, J. Reine Angew. Math. **432** (1992), 69–76.

FH91 W. Fulton and J. Harris, *Representation theory, A first course, readings in mathematics*, Graduate Texts in Mathematics, vol. 129 (Springer, New York, NY, 1991).

GHSSV09 A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev and B. Virág, *On the girth of random Cayley graphs*, Random Structures Algorithms **35** (2009), 100–117.

GJS99 A. Gamburd, D. Jakobson and P. Sarnak, *Spectra of elements in the group ring of* SU(2), J. Eur. Math. Soc. (JEMS) **1** (1999), 51–85.

Gan00 M. I. Ganzburg, *Polynomial inequalities on measurable sets and their applications. II. Weighted measures*, J. Approx. Theory **106** (2000), 77–109.

GB73 M. Ganzburg and J. Brudnyi, *On an extremal problem for polynomials in n variables*, Math. USSR Izv. **7** (1973), 345–356.

Gro81 M. Gromov, *Groups of polynomial growth and expanding maps*, Publ. Math. Inst. Hautes Études Sci. **53** (1981), 53–73.

Gui73 Y. Guivarc'h, *Croissance polynomiale et périodes des fonctions harmoniques*, Bull. Soc. Math. France **101** (1973), 353–379.

Hal76 M. Hall Jr, *The theory of groups* (Chelsea Publishing, New York, NY, 1976).

Jar31 V. Jarník, *Über die simultanen diophantischen approximationen*, Math. Z. **33** (1931), 505–543.

Joh07 M. Johnson, *Standard tableaux and Klyachko's theorem on Lie representations*, J. Combin. Theory Ser. A **114** (2007), 151–158.

KR01 V. Kaloshin and I. Rodnianski, *Diophantine properties of elements of* SO(3), Geom. Funct. Anal. **11** (2001), 953–970.

KM98 D. Y. Kleinbock and G. A. Margulis, *Flows on homogeneous spaces and Diophantine approximation on manifolds*, Ann. of Math. (2) **148** (1998), 339–360.

KT07 D. Kleinbock and G. Tomanov, *Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation*, Comment. Math. Helv. **82** (2007), 519–581.

Klj74 A. A. Kljačko, *Lie elements in a tensor algebra*, Sibirsk. Mat. Zh. **15** (1974), 1296–1304, 1430.

KS06 L. G. Kovács and R. Stöhr, *A combinatorial proof of Klyachko's theorem on Lie representations*, J. Algebraic Combin. **23** (2006), 225–230.

KW01 W. Kraskiewicz and J. Weyman, *Algebra of coinvariants and the action of coxeter elements*, Bayreuth. Math. Schr. **63** (2001), 265–284.

MKS76 W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, revised edition (Dover, New York, NY, 1976).

Pan83 P. Pansu, *Croissance des boules et des géodésiques fermées dans les nilvariétés*, Ergodic Theory Dynam. Systems **3** (1983), 415–445.

Rag72 M. S. Raghunathan, *Discrete subgroups of Lie groups* (Springer, 1972).

Rem36 E. Remez, *Sur une propriétée extrémale des polynômes de Tchebychef*, Comm. Inst. Sci. Kharkov **13** (1936), 93–95.

Reu93 C. Reutenauer, *Free Lie algebras* (Oxford University Press, 1993).

Sar90 P. Sarnak, *Some applications of modular forms*, Cambridge Tracts in Mathematics, vol. 99 (Cambridge University Press, 1990).

Ser06 J.-P. Serre, *Lie algebras and Lie groups*, Lecture Notes in Mathematics, vol. 1500, second edition (corrected fifth printing) (Springer, Berlin, 2006).

Tho13 A. Thom, *Convergent sequences in discrete groups*, Canad. Math. Bull. **56** (2013), 424–433.

Thr42 R. M. Thrall, *On symmetrized Kronecker powers and the structure of the free Lie ring*, Amer. J. Math. **64** (1942), 371–388.

Var12 P. P. Varjú, *Diophantine property in the group of affine transformation of the line*, Preprint (2012), arXiv:1211.3647 [math.GR].

Wit37 E. Witt, *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. **177** (1937), 152–160.

Menny Aka menashe-hai.akkaginosar@epfl.ch
Section de mathématiques, EPFL, Station 8 - Bât. MA,
CH-1015 Lausanne, Switzerland

Emmanuel Breuillard emmanuel.breuillard@math.u-psud.fr
Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11,
91405 Orsay, France

Diophantine properties of nilpotent Lie groups

Lior Rosenzweig lior.rosenzweig@gmail.com
Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden

Nicolas de Saxcé saxce@ma.huji.ac.il
Einstein Institute of Mathematics, Givat Ram, The Hebrew University,
Jerusalem, 91904, Israel