Université Grenoble Alpes

ANNALES DE
L'INSTITUT FOURIER

Michael Larsen & Dong Quan Ngoc Nguyen

Waring's problem for unipotent algebraic groups

Tome 69, nº 4 (2019), p. 1857-1877.
<http://aif.centre-mersenne.org/item/AIF_2019__69_4_1857_0>

Ann. Inst. Fourier, Grenoble
69, 4 (2019) 1857-1877

WARING'S PROBLEM FOR UNIPOTENT ALGEBRAIC GROUPS

by Michael LARSEN & Dong Quan Ngoc NGUYEN (*)

ABSTRACT. — In this paper, we formulate an analogue of Waring's problem for an algebraic group G. At the field level we consider a morphism of varieties $f\colon \mathbb{A}^1 \to G$ and ask whether every element of $G(K)$ is the product of a bounded number of elements of $f(\mathbb{A}^1(K)) = f(K)$. We give an affirmative answer when G is unipotent and K is a characteristic zero field which is not formally real.

The idea is the same at the integral level, except one must work with schemes, and the question is whether every element in a finite index subgroup of $G(\mathcal{O})$ can be written as a product of a bounded number of elements of $f(\mathcal{O})$. We prove this is the case when G is unipotent and $\mathcal{O}$ is the ring of integers of a totally imaginary number field.

RÉSUMÉ. — Dans cet article, nous formulons un analogue du problème de Waring pour un groupe algébrique G. Soit K un corps. Nous considérons un morphisme de variétés $f\colon \mathbb{A}^1 \to G$, défini sur K, et nous demandons si chaque élément de $G(K)$ est le produit d'un nombre borné d'éléments de $f(\mathbb{A}^1(K)) = f(K)$. Nous donnons une réponse affirmative quand G est unipotent et K est un corps de caractéristique 0 ce qui n'est pas formellement réel.

L'idée est la même au niveau intégral, sauf qu'il faut travailler avec des schémas, et la question est de savoir si chaque élément d'un sous-groupe d'indice fini de $G(\mathcal{O})$ peut être écrit comme un produit d'un nombre borné d'éléments de $f(\mathcal{O})$. Nous prouvons que c'est le cas lorsque G est unipotent et $\mathcal{O}$ est l'anneau d'entiers d'un corps de nombres totalement imaginaire.

Introduction

The original version of Waring's problem asks whether, for every positive integer n there exists $M := M_n$ such that every non-negative integer is of the form $a_1^n + \cdots + a_M^n$, $a_i \in \mathbb{N}$, and, if so, what is the minimum value for M_n. Since 1909, when Hilbert proved that such a bound exists, an enormous

---

Keywords: Waring's problem, easier Waring's problem, unipotent algebraic groups.
2010 *Mathematics Subject Classification:* 11P05, 20G15, 14L15.
(*) ML was partially supported by NSF Grant DMS-1401419.
DQNN was partially supported by DARPA grant N66001-17-1-4041.

literature has developed, largely devoted to determining M_n. There is also a substantial literature devoted to variants of Waring's problem. Kamke proved [11] a generalization of the theorem in which nth powers are replaced by general polynomials. In a series of papers [22, 24, 23], Wooley solved Waring's problem for vector-valued polynomials. Siegel [17, 18] treated the case of rings of integers in number fields, and since then, many papers have analyzed Waring's problem for a wide variety of rings, for instance [2, 3, 4, 6, 7, 13, 21]. Also, there has been a flurry of recent activity on "Waring's problem for groups"; the typical problem here is to prove that every element in G is a product of a small number of nth powers of elements of G (see, for instance, [1, 9, 12, 16] and the references therein.)

This paper explores the view that algebraic groups are the natural setting for Waring's problem. To this extent, it resembles the work on Waring's problem for groups of Lie type. The work on the polynomial-valued and vector-valued variants of Waring's problem also fit naturally in this framework. We will consider morphisms of varieties (resp. schemes) $f\colon \mathbb{A}^1 \to G$ defined over a field (resp. a number ring) and look at bounded generation of the groups generated by the images.

The strategy is developed in Section 2 for unipotent algebraic groups over fields of characteristic 0 which are not formally real. (Some justification for concentrating on the unipotent case is given in Lemma 1.4 below and the following remarks.) In Section 3, we solve the unipotent version of Waring's problem for totally imaginary number rings. In Section 4, we work over general characteristic 0 fields and general number rings, but consider only the "easier Waring's problem", in which one is allowed to use inverses. Our methods throughout are elementary. The only input from analytic number theory is Siegel's solution of Waring's problem over number rings.

Unfortunately, in the original situation of Waring's problem, namely the ring $\mathbb{Z}$, the additive group $\mathbb{G}_a$, and the morphism $f\colon \mathbb{A}^1 \to \mathbb{G}_a$ given by $f(x) = x^n$, our results fall short of Hilbert's theorem; we can prove only the easier Waring's problem in this case, rather than the statement that every positive integer can be represented as a bounded sum of non-negative nth powers. The difficulty, of course, is the ordering on $\mathbb{Z}$. It seems natural to ask whether, for unipotent groups over general number rings, one can characterize the set which ought to be expressible as a bounded product of images. In proving the easier Waring's problem, we simply avoid this issue.

1. Generating subvarieties

Throughout this paper, K will always be a field of characteristic 0, and G will be an algebraic group over K. A *variety* over K will be a reduced separated scheme of finite type and, in particular, need not be connected. A subvariety, closed subgroup, etc., will always be understood to be defined over K.

Definition 1.1. — *Let G be an algebraic group over a field K. A subvariety X of G is* generating *if there exists n such that every generic point of G lies in the image of the product map from $X^{\times n} := X \times \cdots \times X$ to G. A finite collection $f_i \colon X_i \to G$ of morphisms is generating if the union of Zariski closures $\bigcup_i \overline{f(X_i)}$ is generating.*

We have the following necessary and sufficient condition for a subvariety to be generating.

Proposition 1.2. — *Let G be a connected algebraic group over K and $Z \subseteq G$ a closed subvariety. Then Z is generating if and only if it satisfies the following two properties:*

(I) *Z is not contained in any proper closed subgroup of G.*
(II) *For every proper closed normal subgroup H of G, the image of $Z \to G/H$ has positive dimension.*

We first prove the following technical lemma:

Lemma 1.3. — *Let K be algebraically closed. Let X, Y be irreducible closed subvarieties of G. Assume:*

(1) $\dim(\overline{XX}) = \dim X$*;*
(2) $\dim(\overline{XYX}) = \dim X$.

Then there exists a closed subgroup H of G such that the following statements are true:

(i) *$X = xH = Hx$ for all $x \in X(K)$;*
(ii) *$Y \subset yH$ for some $y \in N_G(H)(K)$.*

Proof. — As X is irreducible, $X^{\times 2}$ is irreducible, with generic point η. The closure $\overline{X^2} = \overline{XX}$ of its image in G is therefore the closure of the image of η in G and thus irreducible. If $x \in X(K)$, then xX and Xx are closed subvarieties of X^2 of dimension $\dim X = \dim \overline{X^2}$, so $xX = X^2 = Xx$. Thus, $Xx^{-1} = x^{-1}X$.

It follows that for $x_1, x_2 \in X(K)$,

$$x_1^{-1}X = x_1^{-1}(x_2^{-1}X^2) = (x_1^{-1}X)(x_2^{-1}X) = (x_1^{-1}X^2)x_2^{-1} = Xx_2^{-1} = x_2^{-1}X.$$

Defining $H := x^{-1}X$ for $x \in X(K)$, we see that H does not depend on the choice of x and, moreover, that $H^2 = H$. As every $h \in H(K)$ can be written $x_1^{-1}x_2$, $x_1, x_2 \in X(K)$, it follows that $h^{-1} = x_2^{-1}x_1 \in H(K)$. Thus $H(K)$ is a subgroup, which since K is algebraically closed implies that H is a closed subgroup of G, which implies (i).

For $y \in Y(K)$, $\overline{XYX}$ is connected and contains $\overline{XyX}$, which has dimension $\geqslant \dim X = \dim \overline{XYX}$. Thus,

$$\overline{XYX} = \overline{XyX} = \overline{HxyxH}$$

is connected and has dimension $\dim H$. It follows that the double coset $HxyxH$ consists of a single left coset, so $xyx \in N_G(H)(K)$. By (i), x also normalizes H, and it follows that y normalizes H. Finally,

$$Y \subseteq \overline{x^{-1}XYXx^{-1}} = \overline{(x^{-1}Hx)y(xHx^{-1})} = \overline{HyH} = yH. \qquad \square$$

Using this, we can prove Proposition 1.2.

Proof. — Clearly, if $Z \subseteq H \subsetneq G$, then the same is true for $\overline{Z^n}$, and if the image of Z in G/H is finite, the same is true for $\overline{Z^n}$. This proves necessity of conditions (I) and (II).

For the sufficiency, we may assume without loss of generality that K is algebraically closed. For all $z \in Z(K)$, $Z\overline{Z^n} \subseteq \overline{Z^{n+1}}$, so $\dim \overline{Z^n}$ is a bounded non-decreasing sequence of integers. It therefore stabilizes for some n. Let X denote an irreducible component of $\overline{Z^n}$ of dimension $\dim \overline{Z^n}$ and Y any irreducible component of Z. Then $\dim X \leqslant \dim \overline{X^2} \leqslant \dim \overline{Z^n}$ and $\dim X \leqslant \dim \overline{XYX} \leqslant \dim \overline{Z^n}$, so conditions (1) and (2) of Lemma 1.3 are satisfied. Let H be the closed subgroup of G satisfying (i) and (ii) in Lemma 1.3. As H is a translate of X, it is irreducible.

If $H = G$, then X is a translate of H, so $X = G$, which means $\overline{Z^m} = G$ for all $m \geqslant n$. It thus follows that every generic point of G lies in Z^m for some $m \geqslant n$, so Z is generating, as claimed.

If $H \subsetneq G$ then $\dim H < \dim G$. If H is normal in G, then the image of Z in G/H is finite, contrary to condition (II). If H has normalizer $N \subsetneq G$, then Y is contained in N. Since N does not depend on the choice of component Y, $Z \subseteq N$, contrary to condition (I). $\square$

Henceforth, we assume G is connected. We are interested in generating collections of morphisms $\mathbb{A}^1 \to G$. By a theorem of Chevalley, Barsotti, and Rosenlicht [14], every connected algebraic group G has a closed normal subgroup H which is a linear algebraic group and such that G/H is an abelian variety. Every map from a rational curve to an abelian variety is trivial. Thus, unless G is a linear algebraic group, it is impossible for any collection of morphisms $\mathbb{A}^1 \to G$ to be generating.

Let R and U denote respectively the radical and the unipotent radical of G.

Lemma 1.4. — *If $U \subsetneq R$, then there does not exist a generating set of morphisms $\mathbb{A}^1 \to G$.*

Proof. — It suffices to prove that there is no generating set of morphisms from $\mathbb{A}^1$ to the connected reductive group G/U. Thus, we may assume without loss of generality that G is connected reductive. If the radical R is non-trivial, then the inclusion map $R \to G$ induces an isogeny of tori $R \to G/[G,G]$, so it suffices to prove that there no generating set of morphisms from $\mathbb{A}^1$ to a non-trivial torus T. Without loss of generality, we may assume that $K = \bar{K}$. Thus we may replace T by a quotient isomorphic to the multiplicative group, and it suffices to prove there is no non-constant morphism of curves from $\mathbb{A}^1$ to $\mathbb{A}^1 \backslash \{0\}$. At the level of coordinate rings, this is the obvious statement that every K-homomorphism from $K[t,t^{-1}]$ to $K[x]$ maps t to an element of K^*, or, equivalently, the fact that $K[x]^* = K^*$. □

We need only consider, then, the case that G is the extension of a semisimple group by a unipotent group, both connected. The semisimple case is perhaps even more interesting, but we know that, at least for SL_2, we cannot always expect bounded generation, since, for example, $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}[i])$ do not have bounded generation by elementary matrices [8, 20].

Since the characteristic of K is 0, if G is unipotent, it is necessarily connected [5, IV, §2, Prop. 4.1]. The derived group G' is then likewise unipotent [5, IV, §2, Prop. 2.3], and therefore connected. The quotient G/G' is unipotent [5, IV, §2, Prop. 2.3], and commutative and is therefore a vector group [5, IV, §2, Prop. 4.2]. The non-abelian Galois cohomology group $H^1(K,G')$ vanishes [15, III, Prop. 6], so the cohomology sequence for the short exact sequence $1 \to G' \to G \to G/G' \to 1$ [15, I, Prop. 38] implies $(G/G')(K) = G(K)/G'(K)$. We identify these groups. We do not distinguish between closed (vector) subgroups of G/G' at the level of algebraic groups over K and the corresponding K-subspaces of the vector space $(G/G')(K)$. If V is a subspace of G/G', we denote by VG' the inverse image of V in G, regarded as an algebraic group.

The next two results are elementary and well-known, and the proofs of these results are similar to those of [19, Thms. 2.9 and 2.12].

Lemma 1.5. — *Let G be a connected unipotent algebraic group, and let H be a proper closed subgroup of G. Then the normalizer of H in G is strictly larger than H.*

Proposition 1.6. — *If G is a unipotent group over K, then every proper closed subgroup H of G is contained in a normal subgroup N of codimension 1 in G which contains the derived group G' of G.*

From Proposition 1.2, we deduce that for unipotent groups, we have the following simple criterion.

Lemma 1.7. — *Let G be a unipotent group over K. A subvariety X of G (resp. a set $\{f_1, \dots, f_n\}$ of morphisms $\mathbb{A}^1 \to G$) is generating if and only if for each proper subspace $V \subsetneq G/G'$, such that the projection of X to G/VG' is of positive dimension (resp. the composition of some f_i with the projection $G \to G/VG'$ is non-constant.)*

Note that the question of whether a set of morphisms f_i is generating depends only on the set of compositions $\bar{f}_i$ of f_i with the quotient map $G \to G/G'$. It is also invariant under left or right translation of the f_i by any element of $G(K)$.

Lemma 1.8. — *If $\{f_1, \dots, f_n\}$ is not generating, then for all positive integers N,*

$$(f_1(K) \cup \cdots \cup f_n(K))^N \subsetneq G(K).$$

Proof. — The image of $(f_1(K) \cup \cdots \cup f_n(K))^N$ in $(G/VG')(K)$ is the same as the image of $\{f_1(0), \dots, f_n(0)\}^N$ and is therefore a finite subset of an infinite group. □

We record the following lemma, which will be needed later.

Lemma 1.9. — *Let G be a unipotent group over K, G' its derived group and G'' the derived group of G'. If V is a proper subspace of G'/G'', then there exists a dense open subvariety $U_1 \subset G$ and for all $\gamma_1 \in U_1(K)$, a dense open subvariety U_2 of the form $G \setminus WG'$, such that for all $\gamma_2 \in U_2(K)$, $[\gamma_1, \gamma_2]$ does not lie in $VG''(K)$.*

Proof. — Without loss of generality, we assume K is algebraically closed. As the characteristic of K is 0, G and G' are connected, so G'/G'' is connected. The composition $G \times G \to G'/G''$ of the commutator map and the quotient map has the property that its image generates G'/G'' and is therefore not contained in V. It follows that the inverse image U of the complement of V is dense and open in $G \times G$. By Chevalley's theorem, the projection of $U \subseteq G \times G$ onto the first factor G is a constructible set containing the generic point; it therefore contains an open dense U_1. The fiber over any point $\gamma_1 \in U_1(K)$ is non-empty. The condition on γ_2 that $[\gamma_1, \gamma_2] \notin VG'$ is linear on the image of γ_2 in G/G' and is satisfied for at least one γ_2, so U_2, defined by the condition $[\gamma_1,\gamma_2]\notin VG'$ satisfies the properties claimed. □

2. The unipotent Waring Problem over nonreal fields

Definition 2.1. — *We say a field K is* nonreal *if it is of characteristic zero but not formally real (i.e., -1 is a sum of squares in K).*

The main theorem of the section is the following:

Theorem 2.2. — *If G is a unipotent algebraic group over a nonreal field K and $\{f_1,\dots,f_n\}$ is a generating set of K-morphisms $\mathbb{A}^1\to G$, then for some positive integer M,*

$$(f_1(K)\cup\cdots\cup f_n(K))^M=G(K).$$

The proof occupies the rest of this section. It depends on the following two propositions:

Proposition 2.3. — *Theorem 2.2 holds when G is a vector group.*

Proposition 2.4. — *Under the hypotheses of Theorem 2.2, there exists an integer m, a sequence of elements $g_1,\dots,g_m\in G(K)$, a sequence of positive integers $k_1,\dots,k_m$ and for each $i\in\{1,\dots,m\}$, a sequence of integers $\ell_{i,1},\dots,\ell_{i,k_i}\in[1,n]$ and of $a_{i,j},b_{i,j}\in K$, such that the K-morphisms $h_1,\dots,h_m\colon\mathbb{A}^1\to G$ defined by*

$$h_i(x):=f_{\ell_{i,1}}(a_{i,1}x+b_{i,1})\cdots f_{\ell_{i,k_i}}(a_{i,k_i}x+b_{i,k_i})g_i,\quad i=1,\dots,m$$

map $\mathbb{A}^1\to G'$ and as morphisms to G' are generating.

Assuming both propositions hold, we can prove Theorem 2.2 by induction on dimension. If G is commutative, then Proposition 2.3 applies. Otherwise, we apply Proposition 2.4 to construct $h_1,\dots,h_m$. Letting $\bar f_i$ denote the composition of f_i with $G\to G/G'$, Proposition 2.3 asserts that every element of $G(K)/G'(K)=(G/G')(K)$ is represented by a bounded product of elements of $\bar f_1(K)\cup\cdots\cup\bar f_n(K)$. For each g_i, there exists g'_i, which is a bounded product of elements of $f_1(K)\cup\cdots\cup f_n(K)$ and lies in the same $G'(K)$-coset of $G(K)$. Defining

$$h'_i(x):=g'_i f_{\ell_{i,1}}(a_{i,1}x+b_{i,1})\cdots f_{\ell_{i,k_i}}(a_{i,k_i}x+b_{i,k_i}),$$

it suffices to prove that every element of $G'(K)$ is a bounded product of elements of $h'_1(K)\cup\cdots\cup h'_m(K)$. As the h_i are generating for G', the same is true for h'_i, and the theorem follows by induction. Thus, we need only prove Propositions 2.3 and 2.4.

To prove Proposition 2.3, we begin with a special case.

Proposition 2.5. — *If K is a characteristic zero field which is not formally real and d is a positive integer, there exists an integer $N > 0$ such that every vector in K^d is a sum of N elements of*

$$X_1^d := \{(x, x^2, \dots, x^d) \mid x \in K\}.$$

Proof. — For each integer $k > 0$, let

$$X_k^d := \underbrace{X_1^d + \cdots + X_1^d}_{k}.$$

Thus $X_1^d \subseteq X_2^d \subseteq \cdots$, and we denote by X^d the limit $\bigcup_i X_i^d$. Clearly $X_i^d + X_j^d = X_{i+j}^d$ and $X_i^d X_j^d \subseteq X_{ij}^d$. Taking unions, X^d is a semiring. Let $p^{d+1}\colon X^{d+1} \to X^d$ denote the projection map onto the first d coordinates and $\pi^{d+1}\colon X^{d+1} \to K$ the projection map onto the last coordinate. In particular, $p^{d+1}(X_k^{d+1}) = X_k^d$ for all positive integers k.

It is a theorem [6, Thm. 2] that for each positive integer d there exists M such that every element in K is the sum of M dth powers of elements of K.

We proceed by induction on d. The theorem is trivial for $d = 1$. Assume it holds for d and choose M large enough that $X_M^d = X^d = K^d$ and every element of K is the sum of M $(d+1)$st powers. In particular,

$$\pi^{d+1}(X_M^{d+1}) = K. \tag{2.1}$$

If $X_M^{d+1} \subsetneq X_{M+1}^{d+1}$, then choosing $w \in X_{M+1}^{d+1} \setminus X_M^{d+1}$, there exists an element $v \in X_M^{d+1}$ such that $p^{d+1}(v) = p^{d+1}(w)$. If $u \in X_M^{d+1}$ is chosen with $p^{d+1}(u) = -p^{d+1}(v)$, then either $u + v$ or $u + w$ is non-zero, and either way there exists an element $t \in X_{2M+1}^{d+1} \setminus \{0\}$ with $p^{d+1}(t) = 0$. By (2.1),

$$\{(0, \dots, 0, x) \mid x \in K\} \subset X_{M(2M+1)}^{d+1},$$

so by the induction hypothesis, $X_{M+M(2M+1)}^{d+1} = K^{d+1}$, and we are done. We may therefore assume $X_M^{d+1} = X_{M+1}^{d+1}$, which implies $X_M^{d+1} = X^{d+1}$. Moreover, if p^{d+1} fails to be injective, the same argument applies, so we may assume that p^{d+1} is an isomorphism of semirings, and therefore an isomorphism of rings (since the target K^d is a ring).

Thus, we can regard $\pi^{d+1} \circ (p^{d+1})^{-1}$ as a ring homomorphism $\phi\colon K^d \to K$. If $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, then $\phi(e_i)$ maps to an idempotent of K, which can only be 0 or 1. Since $\phi(e_1 + \cdots + e_d) = 1$, there exists i such that $\phi(e_i) = 1$, and it follows that ϕ factors through projection onto the ith coordinate. Thus, there exists a ring endomorphism $\psi\colon K \to K$ such that for all $(x_1, \ldots, x_{d+1}) \in X^{d+1}$, $\psi(x_i) = x_{d+1}$. As $(2, 4, 8, \ldots, 2^{d+1}) \in X^{d+1}$, $\psi(2^i) = 2^{d+1}$, which is absurd. □

We now prove Proposition 2.3.

Proof. — Let

$$f_j(x) = (P_{1j}(x), \ldots, P_{mj}(x)), \tag{2.2}$$

where d is the maximum of the degrees of the P_{ij} for $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$. Let N be chosen as in Proposition 2.5. We write

$$P_{ij}(x) = \sum_{k=0}^{d} a_{ijk} x^k \tag{2.3}$$

for $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$. Given $c_1, \ldots, c_m$, our goal is to find $x_{j\ell} \in K$, $1 \leqslant j \leqslant n$, $1 \leqslant \ell \leqslant N$ that satisfy the system of equations

$$\sum_{j,k,\ell} a_{ijk} x_{j\ell}^k = c_i, \ i = 1, 2, \ldots, m. \tag{2.4}$$

By Proposition 2.5, by choosing $x_{j\ell}$ suitably, we can choose the values

$$y_{jk} = \sum_{\ell=1}^{N} x_{j\ell}^k$$

independently for $1 \leqslant j \leqslant n$ and $1 \leqslant k \leqslant d$, while $y_{j0} = N$ by definition. Thus, we can rewrite the system of equations (2.4) as

$$\sum_{k=1}^{d} \sum_{j=1}^{n} a_{ijk} y_{jk} = c_i - N \sum_{j=1}^{n} a_{ij0}, \ i = 1, 2, \ldots, m. \tag{2.5}$$

This is always solvable unless there is a non-trivial relation among the linear forms on the left hand side in this system, i.e., a non-zero sequence $b_1, \ldots, b_m$ such that

$$\sum_{i=1}^{m} b_i a_{ijk} = 0$$

for all j and $k \geqslant 1$. If this is true, then

$$\sum_{i=1}^{m} b_i P_{ij} = \sum_{i} b_i a_{ij0}, \ j = 1, \ldots, n.$$

In other words, defining $\pi(t_1, \ldots, t_n) := b_1 t_1 + \cdots + b_m t_m$, $\pi \circ f_j$ is constant for all j, contrary to assumption. □

Finally, we prove Proposition 2.4.

Proof. — Suppose we have already constructed $h_1, \ldots, h_r$. Let $\bar{h}_i$ denote the composition of h_i with the projection $G' \to G'/G''$. Let W denote the vector space spanned by the set $\{\bar{h}_i(t) - \bar{h}_i(0) \mid 1 \leqslant i \leqslant r,\ t \in K\}$. Suppose $W = G'/G''$. Then for all proper subspaces $W' \subsetneq W$ there exist i and t such that $\bar{h}_i(0)$ and $\bar{h}_i(t)$ represent different classes in W/W'. It follows that the composition of h_i with the projection $G' \to G'/W'G''$ is non-constant, and therefore, $\{h_1, \ldots, h_r\}$ is a generating set of morphisms to G'.

Thus, we may assume that W is a proper subspace of G'/G''. We apply Lemma 1.9 to deduce the existence of $\gamma_1 \in G(K)$ and a proper closed subspace V of G/G' such that for all $\gamma_2 \in G(K) \setminus VG'(K)$, the commutator of γ_1 and γ_2 is not in $WG''(K)$. Let $\bar{f}_i(x)$ denote the composition of $f_i(x)$ with the quotient map $G \to G/G'$. As the f_i are generating, there exists i such that for all but finitely many values $x \in K$, $\bar{f}_i(x)$ is not in V. Without loss of generality, we assume $i = 1$.

By Proposition 2.3, there exists a bounded product

$$g = f_{s_1}(b_1) \cdots f_{s_M}(b_M),\ s_i \in \{1, 2, \ldots, n\},\ b_i \in K$$

such that

$$\bar{f}_{s_1}(b_1) + \cdots + \bar{f}_{s_M}(b_M) = \bar{\gamma}_1.$$

We write

$$\bar{f}_1(x) = v_0 + xv_1 + \cdots + x^d v_d,$$

with $v_i \in G/G'$. By Proposition 2.5, there exist $a_1, \ldots, a_N \in K$, not all zero, such that

$$\sum_{i=1}^{N} a_i^k = 0,\ k = 1, 2, \ldots, d. \tag{2.6}$$

Thus,

$$\bar{f}_1(a_1x) + \bar{f}_1(a_2x) + \bar{f}_1(a_3x) + \cdots + \bar{f}_1(a_Nx) = Nv_0,$$

which means that $x \mapsto f_1(a_1x)f_1(a_2x)\cdots f_1(a_nx)$ goes to a constant G'-coset. Without loss of generality, we may assume $a_1 \neq 0$.

Let g_{r+1} be an element of $G(K)$ which can be realized as a product of at most N values of f_i at elements of K and such that

$$f_{s_1}(b_1) \cdots f_{s_M}(b_M) f_1(a_1x) f_1(a_2x) \cdots f_1(a_Nx) g_{r+1} \tag{2.7}$$

belongs to $G'(K)$ for $x = 0$. By Proposition 2.3, such a g_{r+1} exists. We choose $h_{r+1}(x)$ to be either (2.7) or

$$f_1(a_1x) f_{s_1}(b_1) \cdots f_{s_M}(b_M) f_1(a_2x) \cdots f_1(a_Nx) g_{r+1}, \tag{2.8}$$

Either way, $h_{r+1}(0) \in G'(K)$. By (2.6), $h_{r+1}(x) \in G'(K)$ for all $x \in K$. Because the commutator $[f_1(a_1x), f_{s_1}(b_1) \cdots f_{s_M}(b_M)]$ lies in WG'' for at most finitely many x-values, at least one of (2.7) and (2.8) is non-constant (mod WG''). By induction on the codimension of W, the proposition follows. □

3. The unipotent Waring Problem over totally imaginary number rings

In this section K denotes a totally imaginary number field, $\mathcal{O}$ its ring of integers, and $\mathcal{G}$ a closed $\mathcal{O}$-subscheme of the group scheme $\mathcal{U}_k$ of unitriangular $k \times k$ matrices. Thus the generic fiber $\mathcal{G}_K$ will be a closed subgroup of $\mathcal{U}_k$ over K and therefore unipotent. Moreover, there is a filtration of $\mathcal{G}(\mathcal{O})$ by normal subgroups such that the successive quotients are finitely generated free abelian groups. In particular, it is (by definition) a finitely generated torsion-free nilpotent group, whose Hirsch number is the sum of the ranks of these successive quotients.

A set $\{f_1, \dots, f_n\}$ of $\mathcal{O}$-morphisms $\mathbb{A}^1 \to \mathcal{G}$ is said to be generating if it is so over K. The main theorem in this section is the following integral version of Theorem 2.2:

Theorem 3.1. — *If $\{f_1, \dots, f_n\}$ is a generating set of $\mathcal{O}$-morphisms $\mathbb{A}^1 \to \mathcal{G}$, then for some positive integer M,*

$$(f_1(\mathcal{O}) \cup \cdots \cup f_n(\mathcal{O}))^M$$

is a subgroup of finite index in $\mathcal{G}(\mathcal{O})$.

We begin by proving results that allow us to establish that some power of a subset of a group Γ gives a finite index subgroup of Γ.

Lemma 3.2. — *Let Γ be a group, Δ a finite index subgroup of Γ, Ξ a subset of Γ, and M a positive integer. If $\Delta \subseteq \Xi^M$, then there exists N such that Ξ^N is a finite index subgroup of Γ.*

Proof. — Without loss of generality, we assume that Δ is normal in Γ. Consider the (finite set)

$$\{(\bar{m}, \bar{\gamma}) \in \mathbb{Z}/M\mathbb{Z} \times \Gamma/\Delta \mid m \in \mathbb{N},\ \gamma \in \Xi^m\}.$$

For each element, choose a pair (m, γ), $m \in \mathbb{N}, \gamma \in \Xi^m$ representing it. Choose A to be greater than all values m appearing in such pairs. Let N be a multiple of M which is greater than $A + M$. For all positive integers k, Ξ^{kN} is a union of cosets of Δ in Γ and does not depend on k. The image of Ξ^N in Γ/Δ is therefore a subset of a finite group and closed under multiplication. It is therefore a subgroup, and the lemma follows. □

Lemma 3.3. — *Let Γ be a finitely generated nilpotent group and Δ a normal subgroup of Γ. Then every finite index subgroup Δ_0 of Δ contains a finite index subgroup Δ_0° which is normal in Γ.*

Proof. — We prove there exists a function $f\colon \mathbb{N} \to \mathbb{N}$ depending only on Γ such that for any normal subgroup Δ of Γ, every subgroup Δ_0 of Δ of index n contains a normal subgroup of Γ of index $\leqslant f(n)$ in Δ. Replacing Δ_0 with the kernel of the left action of Δ on Δ/Δ_0, we may assume without loss of generality that Δ_0 is normal in Δ. We prove the claim by induction on the total number of prime factors of n.

If $n = p$ is prime, it suffices to prove that there is an upper bound, independent of Δ, on the number of normal subgroups of Δ of index p. Let $\Gamma = \Gamma^0 \triangleright \Gamma^1 \triangleright \cdots \triangleright \Gamma^m = \{0\}$ be any central series, so $\Delta^i := \Delta \cap \Gamma^i$ is likewise a central series. We prove by induction on i that given Γ and p, $|\operatorname{Hom}(\Delta/\Delta^i, \mathbb{Z}/p\mathbb{Z})|$ is bounded independent of Δ; the case $i = m$ is our claim. Assuming this for i gives a bound on the number of homomorphisms $\phi\colon \Delta/\Delta^{i+1} \to \mathbb{Z}/p\mathbb{Z}$ which factor through Δ/Δ^i. When ϕ does not factor, $\kappa_\phi := \ker\phi \cap \Delta^i$ is of index p in Δ^i, so it is determined by a hyperplane in $(\Delta^i/\Delta^{i+1}) \otimes \mathbb{F}_p$, which is contained in the finite-dimensional vector space $(\Gamma^i/\Gamma^{i+1}) \otimes \mathbb{F}_p$. We have $0 \to \kappa_\phi \to \ker\phi \to \Delta/\Delta^i \to 0$, so $\ker\phi$ is determined as a subgroup of Δ/Δ^{i+1} by an element of

$$\operatorname{Hom}(\Delta/\Delta^i, (\Delta^i/\Delta^{i+1})/\kappa_\phi) \cong \operatorname{Hom}(\Delta/\Delta^i, \mathbb{Z}/p\mathbb{Z}).$$

If n has $\geqslant 2$ prime factors, then for some prime factor p of n, Δ_0 is a normal subgroup of index n/p of a normal subgroup Δ_p of index p in Δ. By the induction hypothesis, Δ_p contains a normal subgroup Δ_p° of Γ, of index $\leqslant f(p)$ in Δ. The index of $\Delta_0 \cap \Delta_p^\circ$ in Δ_p° divides n/p, and applying the induction hypothesis, we deduce that the existence of a normal subgroup Δ_0° of Γ of index $\leqslant \max_{i\leqslant n/p} f(i)$ in Δ_p°. □

Proposition 3.4. — *Let Γ be a finitely generated nilpotent group, Δ a normal subgroup of Γ, Ξ a subset of Γ and M_1, M_2 positive integers such that Ξ^{M_1} contains a finite index subgroup of Δ and the image of Ξ^{M_2} in Γ/Δ contains a finite index subgroup of Γ/Δ. Then there exists M_3 such that Ξ^{M_3} is a finite index subgroup of Γ.*

Proof. — Let $\langle\Xi\rangle$ denote the subgroup of Γ generated by Ξ. The intersection $\langle\Xi\rangle \cap \Delta$ is of finite index in Δ, and the image $\langle\Xi\rangle\Delta/\Delta$ is of finite index in Γ/Δ, so $\langle\Xi\rangle$ is of finite index in Γ. As a subgroup of a finitely generated nilpotent group, it is also finitely generated and nilpotent. Replacing Γ and Δ by $\langle\Xi\rangle$ and $\langle\Xi\rangle \cap \Delta$ respectively, we assume without loss of generality that Ξ generates Γ.

Replacing Ξ with Ξ^{M_1}, we may assume Ξ contains a finite index subgroup Δ_0 of Δ. By Lemma 3.3, we may assume that Δ_0 is a normal subgroup of Γ. Let $\bar{\Xi}$ denote the image of Ξ in Γ/Δ_0. If $\bar{\Xi}^N$ is a finite index subgroup of $\bar{\Gamma} := \Gamma/\Delta_0$, then Ξ^{N+1} contains the inverse image of this subgroup in Γ, and the proposition holds. Replacing Γ, Δ, Ξ by $\bar{\Gamma}$, $\bar{\Delta} := \Delta/\Delta_0$, and $\bar{\Xi}$ respectively, we reduce to the case that Δ is finite. We need only show that if $\Xi^{M_2}\Delta$ contains a finite index subgroup Γ_0 of Γ, then Ξ^N is a finite index subgroup of Γ for some N.

Replacing Ξ by $\Xi^{M_2} \cap \Gamma_0\Delta$, we may assume that $\Xi \subseteq \Gamma_0\Delta$ and Ξ meets every fiber of $\pi\colon \Gamma_0\Delta \to \Gamma_0\Delta/\Delta$. In particular, Ξ contains an element of Δ, so replacing Ξ with $\Xi^{|\Delta|}$, we may assume Ξ contains the identity, so

$$\Xi \subseteq \Xi^2 \subseteq \Xi^3 \subseteq \cdots \tag{3.1}$$

For i a positive integer, let m_i denote the maximum over all fibers of π of the cardinality of the intersection of the fiber with Ξ^i. Thus, the intersection of every fiber of π with Ξ^{i+1} is at least m_i. Since fiber size is bounded above by Δ, the sequence (3.1) must eventually stabilize. Replacing Ξ with a suitable power, we have $\Xi^2 = \Xi$. Thus Ξ is closed under multiplication. As Ξ meets every fiber of π in the same number of points, $\gamma \in \Xi$ implies $\gamma(\Xi \cap \pi^{-1}(\pi(\gamma)^{-1})) = \Xi \cap \Delta_0$, which implies $\gamma^{-1} \in \Xi$. Thus, Ξ is a subgroup of Γ of bounded index. □

Next, we prove a criterion for a subgroup of $\mathcal{G}(\mathcal{O})$ to be of finite index.

PROPOSITION 3.5. — *Let $\Gamma \subseteq \mathcal{G}(\mathcal{O}) \subset \mathcal{G}(K)$. Then the Hirsch number $h\Gamma$ of Γ satisfies*

$$h\Gamma \leqslant [K : \mathbb{Q}] \dim \mathcal{G}_K. \tag{3.2}$$

If equality holds in (3.2), then Γ is of finite index in $\mathcal{G}(\mathcal{O})$.

Proof. — Hirsch number is additive in short exact sequences. Let $G_0 := \mathcal{G}_K$, and let $G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_k = \{1\}$ be a central series. Then we have a decreasing filtration of Γ by $\Gamma_i := \Gamma \cap G_i(K)$, and each quotient Γ_i/Γ_{i+1} is a free abelian subgroup of $G_i(K)/G_{i+1}(K) \cong K^{\dim G_i/G_{i+1}}$. Every free abelian subgroup of K^r has rank $\leqslant r[K : \mathbb{Q}]$ with equality if and only if it is commensurable with $\mathcal{O}^r$. This implies (3.2).

Applying the same argument to $\mathcal{G}(\mathcal{O})$, we get

$$h\Gamma \leqslant h\mathcal{G}(\mathcal{O}) \leqslant [K : \mathbb{Q}] \dim \mathcal{G}_K.$$

If equality holds in (3.2), then $\mathcal{G}(\mathcal{O})_i/\mathcal{G}(\mathcal{O})_{i+1}$ and its subgroup Γ_i/Γ_{i+1} are commensurable, and this implies that Γ is of index

$$\prod_{i=0}^{k-1}[\mathcal{G}(\mathcal{O})_i/\mathcal{G}(\mathcal{O})_{i+1} : \Gamma_i/\Gamma_{i+1}] < \infty$$

in Γ. □

We prove Theorem 3.1 by showing that $(f_1(\mathcal{O}) \cup \cdots \cup f_n(\mathcal{O}))^M$ contains a subset which is a group of Hirsch number $[K : \mathbb{Q}] \dim \mathcal{G}_K$. We first treat the commutative case.

Proposition 3.6. — *Theorem 3.1 holds if $\mathcal{G}$ is commutative.*

Proof. — First we claim that for all $d > 0$ there exist integers $L, M > 0$ such that

$$L\mathcal{O}^d \subseteq \{(x_1 + \cdots + x_M, x_1^2 + \cdots + x_M^2, \ldots, x_1^d + \cdots + x_M^d) \mid x_i \in \mathcal{O}\}.$$

Since this is of finite index in $\mathcal{O}^d$, replacing M by a larger integer (also denoted M), we can guarantee that every element in the group generated by $\{(x, x^2, \ldots, x^d) \mid x \in \mathcal{O}\}$ can be written as a sum of M elements.

To prove the claim, we use Proposition 2.5 to show that each basis vector e_i is a sum of M elements of $\{(x, x^2, \ldots, x^d) \mid x \in K\}$. Replacing each x in the representation of e_i by Dx for some sufficiently divisible positive integer D, it follows that each $k_i e_i$ can be written as a sum of M elements of $\{(x, x^2, \ldots, x^d) \mid x \in \mathcal{O}\}$ for suitable positive integers k_i.

For each $\alpha \in \mathcal{O}$, we see from the $(i-1)$th difference of α^i (see [25, Thm. 1, p. 267]) that

$$i!\alpha = \sum_{m=0}^{i-1}(-1)^m \binom{i-1}{m} (\alpha + m)^i - \frac{1}{2}(i-1)i!. \tag{3.3}$$

Thus every element of $i!\mathcal{O}$ is in the subring $\mathcal{O}^{(i)}$ of $\mathcal{O}$ generated by ith powers of elements of $\mathcal{O}$. A theorem of Siegel (see [18, Thm. VI]) implies that there exist $N_1, N_2, \ldots$ such that every element of $\mathcal{O}^{(i)}$ is a sum of N_i ith powers of elements of $\mathcal{O}$. Thus every element of $i!\mathcal{O}$ is a sum of N_i ith powers of elements of $\mathcal{O}$, and therefore every element of $i!k_i\mathcal{O}e_i$ is a sum of MN_i elements of $\{(x, x^2, \ldots, x^d) \mid x \in \mathcal{O}\}$.

Letting L denote a positive integer divisible by $1!k_1, 2!k_2 \ldots, d!k_d$, and replacing M by $M(N_1 + \cdots + N_d)$, we can write every element of $L\mathcal{O}^d$ as a sum of M elements of $\{(x, x^2, \ldots, x^d) \mid x \in \mathcal{O}\}$.

Restricting f_j to the generic fiber, we can write it as a vector of polynomials (2.2) with the P_{ij} given by (2.3). We can solve the system (2.4) of equations in $\mathcal{O}$ whenever we can solve (2.5) in $y_{jk} \in L\mathcal{O}$. This system is always solvable in K, so it is solvable in $L\mathcal{O}$ whenever the $c_i - N\sum_j a_{ij0}$ is sufficiently divisible. Thus, there exists an integer D such that if N and the c_i are divisible by D and N is sufficiently large, then $(c_1, \ldots, c_m)$ is a sum of N terms each of which belongs to $(f_1(\mathcal{O}) \cup \cdots \cup f_n(\mathcal{O}))$. Let $\Lambda := D\mathcal{O}^m$.

Now, $\Lambda \subseteq \mathcal{G}(\mathcal{O}) \subset \mathcal{G}(K) \cong K^m$. As $\mathcal{G}(\mathcal{O})$ has a finite filtration whose quotients are finitely generated free abelian groups, it must contain Λ as a subgroup of finite index. Defining

$$X_i := \underbrace{\big(f_1(\mathcal{O}) \cup \cdots \cup f_n(\mathcal{O})\big) + \cdots + \big(f_1(\mathcal{O}) \cup \cdots \cup f_n(\mathcal{O})\big)}_{iN},$$

we have $\Lambda \subseteq X_i \subseteq \mathcal{G}(\mathcal{O})$ for all $i \geqslant 1$, and $X_{i+1} = X_1 + X_i$. It follows that X_{i+1} contains every Λ-coset in $\mathcal{G}(\mathcal{O})$ represented by any element of X_i, and therefore the sequence $X_1, X_2, \ldots$ stabilizes to a subgroup of $\mathcal{G}(\mathcal{O})$ of rank $m[K : \mathbb{Q}]$ and of finite index in $\mathcal{G}(\mathcal{O})$. $\square$

Now we prove Theorem 3.1

Proof. — We first observe that Proposition 2.4 remains true over $\mathcal{O}$; more precisely, assuming that the morphisms f_i are defined over $\mathcal{O}$, the elements g_i can be taken to be in $\mathcal{G}(\mathcal{O})$ and $a_{i,j}, b_{i,j} \in \mathcal{O}$, so the morphisms h_i are defined over $\mathcal{O}$. Instead of using Proposition 2.3, we use Proposition 3.6. The image $\bar{\gamma}_1$ of the element γ_1 guaranteed by Lemma 1.9 may not lie in the lattice $\Lambda \subset G(K)/G'(K) \cong K^m$, but some positive integer multiple of $\bar{\gamma}_1$ will do so, and the property of γ_1 with respect to V is unchanged when it is replaced by a non-trivial power. The elements a_i guaranteed by Proposition 2.5 may not lie in $\mathcal{O}$, but again we can clear denominators by multiplying by a suitable positive integer. The element g_{r+1} will exist as long as $Nv_0 \in \Lambda$. This can be guaranteed by replacing N with a suitable positive integral multiple.

Now we proceed as in the proof of Theorem 2.2, using induction on $\dim G$. By the induction hypothesis, there exists N such that $(\bigcup_i h_i(\mathcal{O}))^N$ contains a subgroup of $G'(K)$ of Hirsch number $[K : \mathbb{Q}] \dim G'$. On the other hand, by Proposition 3.6, there exists a bounded power of $(\bar{f}_1(\mathcal{O}) \cup \cdots \cup \bar{f}_n(\mathcal{O}))$ which contains a subgroup of $(G/G')(K)$ of Hirsch number $[K : \mathbb{Q}] \dim G/G'$. Here for each $1 \leqslant i \leqslant n$, $\bar{f}_i(x)$ denotes the composition of $f_i(x)$ with the quotient map $G \to G/G'$. The theorem follows from Proposition 3.4 and the additivity of Hirsch numbers. $\square$

4. The easier unipotent Waring problem

We recall that the classical "easier Waring problem" [25] is to prove that for every positive integer n there exists m such that every integer can be written in the form $\pm a_1^n \pm \cdots \pm a_m^n$, $a_i \in \mathbb{Z}$, and to determine the minimum value of m for each n.

In this section, we prove unipotent analogues of the easier Waring problem for arbitrary fields of characteristic zero and rings of integers of arbitrary number fields:

Theorem 4.1. — *If G is a unipotent algebraic group over a field K of characteristic zero and $\{f_1, \dots, f_n\}$ is a generating set of K-morphisms $\mathbb{A}^1 \to G$, then for some positive integer M,*

$$\left(\bigcup_{e_1,\dots,e_n \in \{\pm 1\}} (f_1(K)^{e_1} \cup \cdots \cup f_n(K)^{e_m}) \right)^M = G(K).$$

Theorem 4.2. — *Let K be a number field, $\mathcal{O}$ its ring of integers, and $\mathcal{G}$ a closed $\mathcal{O}$-subscheme of the group scheme $\mathcal{U}_k$ of unitriangular $k \times k$ matrices. If $\{f_1, \dots, f_n\}$ is a generating set of $\mathcal{O}$-morphisms $\mathbb{A}^1 \to \mathcal{G}$, then for some positive integer M,*

$$\left(\bigcup_{e_1,\dots,e_n \in \{\pm 1\}} f_1(\mathcal{O})^{e_1} \cup \cdots \cup f_n(\mathcal{O})^{e_n} \right)^M$$

is a subgroup of bounded index in $\mathcal{G}(\mathcal{O})$.

The proof of Theorem 4.1 depends on variants of Propositions 2.3 and 2.4.

Proposition 4.3. — *If K is a field of characteristic zero and d is a positive integer, there exists an integer $N > 0$ such that K^d can be represented as*

$$K^d = \underbrace{(X_1^d + \cdots + X_1^d)}_{N} - \underbrace{(X_1^d + \cdots + X_1^d)}_{N},$$

where

$$X_1^d := \{(x, x^2, \dots, x^d) \mid x \in K\}.$$

Proof. — This is [10, Thm. 3.2]. □

Proposition 4.4. — *Theorem 4.1 holds when G is a vector group.*

Proof. — Let

$$f_j(x) = (P_{1j}(x), \dots, P_{mj}(x)), \tag{4.1}$$

where d is the maximum of the degrees of the P_{ij} for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. Let N be chosen as in Proposition 4.3. We write

$$P_{ij}(x) = \sum_{k=0}^{d} a_{ijk} x^k \tag{4.2}$$

for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. Given $(c_1, \dots, c_m)$, our goal is to find suitable $\epsilon_{j\ell} \in \{\pm 1\}$ and $x_{j\ell} \in K$ such that

$$(c_1, \dots, c_m) = \sum_{\ell=1}^{2N} \sum_{j=1}^{n} \epsilon_{j\ell} f_j(x_{j\ell}).$$

In light of Proposition 4.3, for each $1 \leqslant j \leqslant n$, one can let $\epsilon_{j\ell} = 1$ if $1 \leqslant \ell \leqslant N$, and let $\epsilon_{j\ell} = -1$ if $N+1 \leqslant \ell \leqslant 2N$. Thus the above system is equivalent to the system of equations

$$c_i = \sum_{j=1}^{n} \sum_{k=0}^{d} a_{ijk} \left(\sum_{\ell=1}^{N} x_{j\ell}^k - \sum_{\ell=N+1}^{2N} x_{j\ell}^k \right), \ i = 1, \dots, m. \tag{4.3}$$

By Proposition 4.3, by choosing $x_{j\ell} \in K$ suitably, we can choose the values

$$y_{jk} = \sum_{\ell=1}^{N} x_{j\ell}^k - \sum_{\ell=N+1}^{2N} x_{j\ell}^k$$

independently for $1 \leqslant j \leqslant n$ and $1 \leqslant k \leqslant d$, while $y_{j0} = 0$ by definition. Thus we can rewrite the system of equations (4.3) as

$$\sum_{j=1}^{n} \sum_{k=1}^{d} a_{ijk} y_{jk} = c_i, \quad i = 1, \dots, m. \tag{4.4}$$

Arguing as in the proof of Proposition 2.3, we see that the above system of equations is always solvable unless f_j is constant modulo some proper subspace V of $\mathbb{A}^m$ for all $1 \leqslant j \leqslant n$, i.e., each $\pi \circ f_j$ is constant, where $\pi : \mathbb{A}^m \to \mathbb{A}^m / V$ is the canonical projection. This is impossible since the set of morphisms $\{f_1, \dots, f_n\}$ is generating. □

Proposition 4.5. — *Under the hypotheses of Theorem 4.1, there exists an integer m, a sequence of elements $g_1, \dots, g_m \in G(K)$, a sequence of positive integers $k_1, \dots, k_m$, for each $i \in \{1, \dots, m\}$, a sequence of integers $\ell_{i,1}, \dots, \ell_{i,k_i} \in [1, n]$, a sequence of integers $e_{i,1}, \dots, e_{i,k_i} \in \{\pm 1\}$,* *and sequences of elements $a_{i,1}, b_{i,1}, \ldots, a_{i,k_i}, b_{i,k_i} \in K$, such that for each $i \in \{1, \ldots, m\}$, the K-morphisms $h_1, \ldots, h_m \colon \mathbb{A}^1 \to G$ defined by*

$$h_i(x) := f_{\ell_{i,1}}(a_{i,1}x + b_{i,1})^{e_{i,1}} \cdots f_{\ell_{i,k_i}}(a_{i,k_i}x + b_{i,k_i})^{e_{i,k_i}} g_i$$

map $\mathbb{A}^1 \to G'$ and as morphisms to G' are generating.

Proof. — Using Proposition 4.4, and the same arguments as in Proposition 2.4, Proposition 4.5 follows immediately. □

Proof of Theorem 4.1. — The proof of Theorem 4.1 is the same as that of Theorem 2.2. Using Propositions 4.4 and 4.5, we proceed as in the proof of Theorem 2.2, using induction on $\dim(G)$, Theorem 4.1 follows immediately. □

Next, we prove an integral variant of Proposition 4.3, in greater generality than we need for Theorem 4.2:

Proposition 4.6. — *Let $\mathcal{O}$ be any integral domain whose quotient field K is of characteristic zero. For all positive integers d, there exist $\lambda \in \mathcal{O} \backslash \{0\}$ and $N \in \mathbb{Z}_{>0}$ such that*

$$\lambda \mathcal{O}^d \subseteq \underbrace{(Y_1^d + \cdots + Y_1^d)}_{N} - \underbrace{(Y_1^d + \cdots + Y_1^d)}_{N},$$

where

$$Y_1^d = \{(x, x^2, \ldots, x^d) \mid x \in \mathcal{O}\}.$$

Proof. — For each integer $k > 0$, set

$$Y_{k,k}^d = \underbrace{(Y_1^d + \cdots + Y_1^d)}_{k} - \underbrace{(Y_1^d + \cdots + Y_1^d)}_{k}.$$

Choose $N > 0$ as in Proposition 4.3. For each $1 \leqslant m \leqslant d$, the basis vector e_m can be written in the form

$$e_m = \sum_{j=1}^{N} (x_j, x_j^2, \ldots, x_j^d) - \sum_{j=1}^{N} (y_j, y_j^2, \ldots, y_j^d)$$

for some $x_j, y_j \in K$. Replacing each x_j, y_j in the above representation by $\delta x_j, \delta y_j$ for some non-zero $\delta \in \mathcal{O}$, it follows that there exists a non-zero $\kappa_m \in \mathcal{O}$ such that

$$\kappa_m e_m \in Y_{N,N}^d. \tag{4.5}$$

For each $\alpha \in \mathcal{O}$, we apply (3.3) to prove that

$$m! \kappa_m \mathcal{O} e_m \subseteq Y_{2NN_m, 2NN_m}^d.$$

Let $\lambda := d! \prod_{i=1}^{d} \kappa_i$. Replacing N by $2N(N1 + \cdots + N_d)$, we deduce that

$$\lambda \mathcal{O}^d \subseteq Y_{N,N}^d. \qquad \square$$

The next result is a variant of Proposition 3.6.

Proposition 4.7. — *Theorem 4.2 holds if $\mathcal{G}$ is commutative.*

Proof. — Let λ, N be chosen as in Proposition 4.6. Restricting f_j to the generic fiber, we can write it as a vector of polynomials (4.1) with the P_{ij} given by (4.2). We can solve the system (4.3) of equations whenever we can solve the system (4.4) in $y_{jk} \in \lambda\mathcal{O}$. This system is always solvable in K; so it is solvable in $\lambda\mathcal{O}$ whenever the c_i are sufficiently divisible. Thus there exists an integer D such that if the c_i are divisible by D and N is sufficiently large, then $(c_1, \ldots, c_m)$ is a sum of N terms, each of which belongs to $\bigcup_{e_1,\ldots,e_n \in \{\pm 1\}} (e_1 f_1(\mathcal{O}) \cup \cdots \cup e_n f_n(\mathcal{O}))$. Let $\Lambda := D\mathcal{O}^m$.

Set

$$U = \bigcup_{e_1,\ldots,e_n \in \{\pm 1\}} (e_1 f_1(\mathcal{O}) \cup \cdots \cup e_n f_n(\mathcal{O})).$$

For each $i \geqslant 1$, define

$$X_i = \underbrace{U + \cdots + U}_{iN \text{ copies of } U}.$$

We have $\Lambda \subseteq X_i \subseteq \mathcal{G}(\mathcal{O}) \subset \mathcal{G}(K) \cong K^m$ for all $i \geqslant 1$, and $X_{i+1} = X_1 + X_i$. Using the same arguments as in the proof of Proposition 3.6, Λ is a subgroup of finite index in $\mathcal{G}(\mathcal{O})$, and therefore the sequence $X_1, X_2, \ldots$ stabilizes to a subgroup of $\mathcal{G}(\mathcal{O})$ of rank $m[K : \mathbb{Q}]$, and of finite index in $\mathcal{G}(\mathcal{O})$. $\square$

We now prove Theorem 4.2.

Proof of Theorem 4.2. — We first observe that Proposition 4.5 remains true over $\mathcal{O}$; more precisely, assuming that the morphisms f_i are defined over $\mathcal{O}$, the elements g_i can be taken to be in $\mathcal{G}(\mathcal{O})$ and $a_{i,j}, b_{i,j} \in \mathcal{O}$, so the morphisms h_i are defined over $\mathcal{O}$.

Now we proceed as in the proof of Theorem 4.1, using induction on $\dim G$. By the induction hypothesis, there exists an integer $N > 0$ such that $(\bigcup_{e_1,\ldots,e_n \in \{\pm 1\}} (h_1(\mathcal{O})^{e_1} \cup \cdots \cup h_n(\mathcal{O})^{e_n}))^N$ is a subgroup of $G'(\mathcal{O})$ of Hirsch number $[K : \mathbb{Q}] \dim G'$. On the other hand, by Proposition 4.7, there exists a bounded power of $\bigcup_{e_1,\ldots,e_n \in \{\pm 1\}} (\bar{f}_1(\mathcal{O})^{e_1} \cup \cdots \cup \bar{f}_n(\mathcal{O})^{e_n})$ which is a subgroup of $(G/G')(\mathcal{O})$ of Hirsch number $[K : \mathbb{Q}] \dim G/G'$. Here for each $1 \leqslant i \leqslant n$, $\bar{f}_i(x)$ denotes the composition of $f_i(x)$ with the quotient map $G \to G/G'$. The theorem follows by Proposition 3.4 and the additivity of Hirsch numbers. $\square$

BIBLIOGRAPHY

[1] N. Avni, T. Gelander, M. Kassabov & A. Shalev, "Word values in p-adic and adelic groups", *Bull. Lond. Math. Soc.* **45** (2013), no. 6, p. 1323-1330.

[2] B. J. Birch, "Waring's problem for $\mathfrak{p}$-adic number fields", *Acta Arith.* **9** (1964), p. 169-176.

[3] M. Car, "Le problème de Waring pour les corps de fonctions", in *Journées Arithmétiques (Luminy, 1989)*, Astérisque, vol. 198-200, Société Mathématique de France, 1991, p. 77-82.

[4] T. Chinburg, "Infinite easier Waring constants for commutative rings", *Topology Appl.* **158** (2011), no. 14, p. 1844-1847.

[5] M. Demazure & P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson; North-Holland, 1970, Avec un appendice *Corps de classes local* par Michiel Hazewinkel, xxvi+700 pages.

[6] W. Ellison, "Waring's problem for fields", *Acta Arith.* **159** (2013), no. 4, p. 315-330.

[7] L. H. Gallardo & L. N. Vaserstein, "The strict Waring problem for polynomial rings", *J. Number Theory* **128** (2008), no. 12, p. 2963-2972.

[8] F. J. Grunewald & J. Schwermer, "Free nonabelian quotients of SL_2 over orders of imaginary quadratic numberfields", *J. Algebra* **69** (1981), no. 2, p. 298-304.

[9] R. M. Guralnick & P. H. Tiep, "Effective results on the Waring problem for finite simple groups", *Am. J. Math.* **137** (2015), no. 5, p. 1401-1430.

[10] B.-H. Im & M. Larsen, "Waring's problems for rational functions in one variable", `https://arxiv.org/abs/1801.06770`.

[11] E. Kamke, "Verallgemeinerungen des Waring–Hilbertschen Satzes", *Math. Ann.* **83** (1921), no. 1-2, p. 85-112.

[12] M. Larsen, A. Shalev & P. H. Tiep, "The Waring problem for finite simple groups", *Ann. Math.* **174** (2011), no. 3, p. 1885-1950.

[13] Y.-R. Liu & T. D. Wooley, "Waring's problem in function fields", *J. Reine Angew. Math.* **638** (2010), p. 1-67.

[14] M. Rosenlicht, "Some basic theorems on algebraic groups", *Am. J. Math.* **78** (1956), p. 401-443.

[15] J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics, vol. 5, Springer, 1965, With a contribution by Jean-Louis Verdier, v+212 pages.

[16] A. Shalev, "Word maps, conjugacy classes, and a noncommutative Waring-type theorem", *Ann. Math.* **170** (2009), no. 3, p. 1383-1416.

[17] C. L. Siegel, "Generalization of Waring's problem to algebraic number fields", *Am. J. Math.* **66** (1944), p. 122-136.

[18] ———, "Sums of mth powers of algebraic integers", *Ann. Math.* **46** (1945), p. 313-339.

[19] M. Suzuki, *Group theory. II*, Grundlehren der Mathematischen Wissenschaften, vol. 248, Springer, 1986, Translated from the Japanese, x+621 pages.

[20] O. I. Tavgen′, "Bounded generation of normal and twisted Chevalley groups over the rings of S-integers", in *Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989)*, Contemporary Mathematics, vol. 131, American Mathematical Society, 1992, p. 409-421.

[21] J. F. Voloch, "On the p-adic Waring's problem", *Acta Arith.* **90** (1999), no. 1, p. 91-95.

[22] T. D. Wooley, "On simultaneous additive equations. III", *Mathematika* **37** (1990), no. 1, p. 85-96.

[23] ———, "On simultaneous additive equations. I", *Proc. Lond. Math. Soc.* **63** (1991), no. 1, p. 1-34.

[24] ———, "On simultaneous additive equations. II", *J. Reine Angew. Math.* **419** (1991), p. 141-198.

[25] E. M. Wright, "An easier Waring's problem", *J. Lond. Math. Soc.* **9** (1934), no. 4, p. 267-272.

Manuscrit reçu le 26 juillet 2017,
révisé le 10 avril 2018,
accepté le 26 avril 2018.

Michael LARSEN
Department of Mathematics
Indiana University
Bloomington, Indiana 47405 (USA)
mjlarsen@indiana.edu

Dong Quan Ngoc NGUYEN
Department of Applied and Computational
Mathematics and Statistics
University of Notre Dame
Notre Dame, Indiana 46556 (USA)
dongquan.ngoc.nguyen@nd.edu