A NON-ABELIAN VARIANT OF THE CLASSICAL MORDELL-LANG CONJECTURE

DRAGOS GHIOCA AND YIFENG HUANG

Abstract. We obtain a non-abelian variant of both the classical Mordell-Lang conjecture and of the dynamical Mordell-Lang problem in the context of finite-dimensional division algebras.

1. Introduction

Throughout this paper, we let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Also, in this paper, any subvariety of an algebraic variety is a closed subvariety.

1.1. The Mordell-Lang conjecture.

This classical problem was settled in the case of algebraic tori by Laurent [Lau84] and then in the case of abelian varieties by Faltings [Fal91]. We state below the result of Vojta [Voj96, Theorem 0.2] which covers all semiabelian varieties. Note that a semiabelian variety is a commutative algebraic group, which is an extension of an abelian variety by an algebraic torus.

Theorem 1.1. *Let G be a semiabelian variety defined over a field K of characteristic 0, let $\Gamma \subseteq G(K)$ be a finitely generated subgroup, and let $V \subseteq G$ be a K-subvariety. Then $\Gamma \cap V(K)$ is a finite union of cosets of subgroups of Γ.*

It is worth noting that the structure of the intersection of a subvariety V of G with a finitely generated subgroup of G becomes significantly wilder when G is an arbitrary algebraic group (even the case of an extension of an abelian variety by a copy of $\mathbb{G}_a$ is difficult); for more details, see [GHSZ19].

Theorem 1.1 can be reformulated as follows. Consider a finite set of generators $\gamma_1, \dots, \gamma_r$ for Γ; then the set of all r-tuples $(n_1, \dots, n_r) \in \mathbb{Z}^r$ with the property that

$$n_1\gamma_1 + n_2\gamma_2 + \cdots + n_r\gamma_r \in V(K) \tag{1.1}$$

is a finite union of cosets of subgroups of $\mathbb{Z}^r$ (see also Theorem 3.1 and its proof for a similar reformulation in the case of algebraic tori). This alternative reformulation of the classical Mordell-Lang conjecture suggests a more general dynamical question.

1.2. The dynamical Mordell-Lang problem.

First, we note that in arithmetic dynamics, given a quasiprojective variety X endowed with a self-map Φ, for any $n \in \mathbb{N}_0$, one uses the notation Φ^n to denote the n-th compositional iterate of Φ (where Φ^0 is the identity map). For any point $x \in X$, we define the orbit of x under Φ as follows:

$$\mathcal{O}_\Phi(x) = \{\Phi^n(x) \colon n \in \mathbb{N}_0\}.$$

One can view the finitely generated subgroup $\Gamma \subseteq G(K)$ from Theorem 1.1 as the image of the identity $0 \in G$ under the action of the subgroup of automorphisms of the quasiprojective variety G spanned by the finitely many translation maps $x \mapsto x+\gamma_i$, where the points $\gamma_1, \dots, \gamma_r$ generate Γ. Therefore, replacing now the semiabelian variety G by an arbitrary quasiprojective variety X and working with the semigroup spanned by finitely many endomorphisms of X, one could formulate a very broad question, which is coined in arithmetic dynamics as the dynamical Mordell-Lang problem.

Question 1.2. Let X be a quasiprojective variety defined over a field K of characteristic 0, let $V \subseteq X$ be a subvariety, let $\alpha \in X(K)$, let $r \in \mathbb{N}$ and let $\varphi_1, \dots, \varphi_r$ be endomorphisms of X. Is it true that the set $\mathcal{S}$ of all r-tuples $(n_1, \dots, n_r) \in \mathbb{N}_0^r$ for which

$$(\varphi_1^{n_1} \circ \varphi_2^{n_2} \circ \cdots \circ \varphi_r^{n_r})(\alpha) \in V(K) \tag{1.2}$$

is a finite union of cosets of subsemigroups of $\mathbb{N}_0^r$?

Theorem 1.1 (see also equation (1.1)) yields a positive answer to Question 1.2 when X is a semiabelian variety and each φ_i is translation map on X; also, there are a few other known instances when Question 1.2 has a positive answer (see [Mel21, Mel22], for example). An important special case of Question 1.2 is when $X = Y \times Y$ (for another quasiprojective variety Y), V is the diagonal subvariety of X, while $r = 2$ and the corresponding endomorphisms are of the form

$$\varphi_1 = (f_1, \mathrm{id}_Y) \text{ and } \varphi_2 = (\mathrm{id}_Y, f_2),$$

for some endomorphisms f_1 and f_2 of Y. Then considering a point $\alpha := (\alpha_1, \alpha_2) \in Y \times Y$, then the dynamical Mordell-Lang problem in this case reduces to understanding the intersection of the two orbits $\mathcal{O}_{f_1}(\alpha_1)$ and $\mathcal{O}_{f_2}(\alpha_2)$. The problem of intersection of orbits attracted a great deal of interest and several important special cases were settled (see [GN17, GTZ08, GTZ12, Rou20, SV13]).

However, as shown in [GTZ11, Section 6], the dynamical Mordell-Lang problem has a negative answer for arbitrary regular self-maps φ_i on an abelian variety X (even when the maps φ_i are commuting group endomorphisms). Furthermore, in [SY14], Scanlon and Yasufuku construct a broad class of examples showing that the structure of the set $\mathcal{S}$ from Question 1.2 can be quite wild in the case the maps φ_i are endomorphisms of semiabelian varieties.

On the other hand, in the special case $r = 1$, Question 1.2 is known to hold in several instances (see [BGT10, BGKT12, Fak14, GT09, Xie17], among many other results). There are known even partial results regarding quantitative versions of this problem (see [BGKT10, OS15]); most importantly, there are no known counterexamples to Question 1.2 when $r = 1$. In this special case of the orbit of a point under a single endomorphism Φ, Question 1.2 is widely believed to be true for all dynamical systems (X, Φ) and it is known as the dynamical Mordell-Lang conjecture (see [BGT16], for more details on this problem).

Furthermore, both the problem of intersection of orbits and the dynamical Mordell-Lang conjecture have either applications or variants appearing in quite diverse settings (sometimes going beyond the world of algebraic dynamics), such as:

- inclusion of ideals of K-algebras under the iterated action of an automorphism (see [BL15]);
- homologically transverse subvarieties of a variety endowed with a given endomorphism (see [BSS17]);
- p-adic analytic maps (see [BGKT10, Section 7]);
- orbits of subvarieties of a given variety endowed with an endomorphism (see [LL19]);
- finitely presented k-algebras of linear growth (see [Pio19]);

- trajectories of balls inside rectangular billiards (see [CZ23]);
- real analytic dynamical systems (see [Sca11]);
- intersection of orbits of points under the action of two non-linear endomorphisms of the Riemann sphere (see [Wan17]).

The goal of our paper is to prove a variant of Question 1.2 in the context of division algebras, i.e., we prove that the dynamical Mordell-Lang problem has a positive answer in the context of division algebras. On the other hand, it is worth noting that the examples from [GTZ11, Section 6] show that the dynamical Mordell-Lang problem has a negative answer for the matrix algebra over an arbitrary field; hence, it is somewhat surprising that we can establish a positive result for a *nonabelian* variant of the dynamical Mordell-Lang problem.

Next, we introduce the necessary notation for our main result.

1.3. **Basic notation for division algebras.** Throughout this paper, let K be a field of characteristic 0, and D be a finite-dimensional division algebra over K. For each element $f \in D$, we define its norm by

$$\|f\| = \mathrm{Norm}_{D/K}(f) := \mathrm{Norm}_{K(f)/K}(f)^{[D:K(f)]} \in K. \tag{1.3}$$

In this subsection only, let $m := [D : K]$. Then D can be (non-canonically) identified with the K-points of the m-dimensional affine space $\mathbb{A}^m(K)$. Indeed, we let $y_1, \dots, y_m$ be a given K-basis for D and then each point $x \in D$ is written uniquely as $x = \sum_{i=1}^m x_i \cdot y_i$ for some $x_i \in K$; thus, $x \in D$ can also be viewed as the point $(x_1, \dots, x_m) \in \mathbb{A}^m(K)$. Therefore, a (closed) K-subvariety V of D is cut out by a system of polynomial equations

$$P_1(x_1, \dots, x_m) = \cdots = P_\ell(x_1, \dots, x_m) = 0 \tag{1.4}$$

for some given polynomials $P_1, \dots, P_\ell \in K[t_1, \dots, t_m]$. A point of D, written as $\sum_{i=1}^m x_i \cdot y_i$ (for some $x_1, \dots, x_m \in K$), lies on V if and only if $(x_1, \dots, x_m)$ satisfies equation (1.4).

We set up some notions that are independent of the choice of a K-basis for D. A map $P : D \to K$ is said to be a *homogeneous K-polynomial of degree d* if there is a K-multilinear map

$$\Theta : \underbrace{D \times \cdots \times D}_{d} \to K$$

such that $P(x) = \Theta(x, \dots, x)$ for all $x \in D$.[1] A map $F : D \to K$ is said to be a *K-polynomial* if F is a pointwise sum of finitely many homogeneous K-polynomials of various degrees. More concretely, given any choice of (ordered) basis $\{y_1, \dots, y_m\}$ for D/K and a map $F : D \to K$, there is a unique function $f : K^m \to K$ such that

$$F\left(\sum_{i=1}^m x_i y_i\right) = f(x_1, \dots, x_m) \text{ for all } x_1, \dots, x_m \in K.$$

Then it can be directly verified that F is a K-polynomial if and only if there is a polynomial $P \in K[t_1, \dots, t_m]$ such that $f(x_1, \dots, x_m) = P(x_1, \dots, x_m)$ for all $x_1, \dots, x_m \in K$, and note that P is necessarily unique since K is of characteristic zero. Moreover, F is homogeneous of degree d if and only if $P(t_1, \dots, t_m)$ is homogeneous of degree d. With these notions set up,

[1] The choice of Θ is not unique unless we impose symmetry condition, but we do not need this consideration for this paper.

we can simply say that a closed K-subvariety V of D is by definition a subset of D cut out by a system of equations

$$F^{(1)}(x) = \cdots = F^{(l)}(x) = 0, \tag{1.5}$$

where $F^{(j)} : D \to K$ are K-polynomials. We will crucially use this rephrasing in Subsection 4.1.

1.4. **Our results.**

We prove the following result.

Theorem 1.3. *Let K be a field of characteristic 0, let D be a finite-dimensional division algebra over K, let $r \in \mathbb{N}$ and $f_1, \dots, f_r \in D^\times$. Then for any K-subvariety V of D, we have that*

$$\mathcal{S} := \{(n_1, \dots, n_r) \in \mathbb{Z}^r \colon f_1^{n_1} f_2^{n_2} \cdots f_r^{n_r} \in V\} \tag{1.6}$$

is a finite union of cosets of subgroups of $\mathbb{Z}^r$.

Theorem 1.3 is a variant of the dynamical Mordell-Lang problem since once could consider for each f_i from Theorem 1.3 the corresponding translation map φ_i on D given by $\varphi_i(x) = f_i \cdot x$; then the set $\mathcal{S}$ from (1.6) is precisely the set

$$\{(n_1, \dots, n_r) \in \mathbb{Z}^r \colon \left(\varphi_1^{n_1} \circ \varphi_2^{n_2} \cdots \circ \varphi_r^{n_r}\right)(1) \in V\}. \tag{1.7}$$

Also, in the special case D is itself a field, then due to the commutativity of the field, we have that the set of all elements $f_1^{n_1} f_2^{n_2} \cdots f_r^{n_r}$ is actually the subgroup of $D^\times$ generated by $f_1, \dots, f_r$, thus connecting our result to the classical Mordell-Lang conjecture.

We also prove several finiteness results in our context, i.e., under additional hypotheses on the elements $f_1, \dots, f_r \in D^\times$ and the variety V from Theorem 1.3, we prove the set $\mathcal{S}$ from (1.6) is finite (see our Theorems 2.2 and 6.4). Furthermore, in Section 6 we obtain another finiteness result (see Theorem 6.2), which was raised naturally in the previous work of the second author [Hua20].

1.5. **Plan for our paper.**

We start in Section 2 by stating Theorem 2.2 in which (under suitable hypotheses) we obtain that the set $\mathcal{S}$ of r-tuples from equation (1.6) is finite. Also, in Section 2, we present several examples, which show the relevance of the hypotheses in our Theorem 2.2. In addition, we show (see Proposition 2.5) that we cannot obtain a variant of the Mordell-Lang theorem for intersections of *finitely generated subgroups* of $D^\times$ with subvarieties V of D.

We continue by proving several useful results in Section 3, which will later be employed in our proofs. Our technical propositions range from a re-statement of Laurent's [Lau84, Théorème 2] classical result (see Theorem 3.1) to a general result regarding an infinite system of equations over a field of characteristic 0 (see Lemma 3.3). We also state and prove an elementary combinatorial result regarding elements in cosets of subgroups of $\mathbb{Z}^r$ (see Lemma 3.2).

We prove Theorem 1.3 in Section 4. Our strategy is to translate the condition from Theorem 1.3 that

$$f_1^{n_1} f_2^{n_2} \cdots f_r^{n_r} \in V$$

to an exponential equation (see Subsection 4.1, especially equation (4.4)). Then the conclusion in Theorem 1.3 follows using Theorem 3.1.

We continue by proving Theorem 2.2 in Section 5. Our proof strategy is similar to the one employed for deducing Theorem 1.3. Furthermore, under the additional hypotheses from

Theorem 2.2, we show that the set $\mathcal{S}$ from equation (1.6) cannot contain a coset of an infinite subgroup of $\mathbb{Z}^r$; though elementary, Lemma 3.2 is instrumental for our argument.

We conclude by stating and proving two additional finiteness results (Theorems 6.4 and 6.2) in Section 6. Theorem 6.4 follows along a similar approach as the one used in the proof of Theorem 2.2. Finally, Theorem 6.2 follows by combining the results of [Hua20, Theorem 1.2] with our Theorem 6.4.

Acknowledgments. We thank the anonymous referee for numerous very useful comments and suggestions.

2. Another theorem and further remarks regarding our results

In Subsection 2.1 we will state our second main result (Theorem 2.2). Then we introduce the classical quaternions in Subsection 2.2 and we present various examples in Subsection 2.3 showing the relevance of the hypotheses in our results.

2.1. Our second main result.

Before stating our result, we need a definition.

Definition 2.1.
- (i) We say a collection of elements $s_1, \dots, s_r \in K^\times$ is **multiplicatively independent** if $n_1, \dots, n_r \in \mathbb{Z}$ and $s_1^{n_1} \cdot \dots \cdot s_r^{n_r} = 1$ imply $n_1 = \dots = n_r = 0$.
- (ii) We say a collection of elements $f_1, \dots, f_r \in D^\times$ has **multiplicatively independent norms** if $\|f_1\|, \dots, \|f_r\|$ are multiplicatively independent.

Theorem 2.2. *Let D be a finite-dimensional division algebra over a field K of characteristic 0, let V be a K-subvariety of D not passing through zero, let $f_1, \dots, f_r \in D^\times$, and let $\mathcal{S}$ be the set:*

$$\mathcal{S} = \{(n_1, \dots, n_r) \in \mathbb{Z}^r \colon f_1^{n_1} \cdot \dots \cdot f_r^{n_r} \in V\}. \tag{2.1}$$

If $f_1, \dots, f_r$ have multiplicatively independent norms, then $\mathcal{S}$ is finite.

Theorem 2.2 was inspired by the work of the second author [Hua20], who searched for variants of the S-unit equation in a nonabelian setting (see [Sch90] for the classical setting of the S-unit equation). We will see in Examples 2.3 and 2.4 that the conclusion in Theorem 2.2 fails if we remove its hypotheses. Our examples live in the world of the classical quaternions, which we will introduce next.

2.2. The quaternions.

We denote by $\mathbb{H}$ the usual quaternion algebra over $\mathbb{R}$, i.e., $\mathbb{H} := \mathbb{R} \oplus \mathbb{R} \cdot i \oplus \mathbb{R} \cdot j \oplus \mathbb{R} \cdot k$, with the standard multiplication law

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

We also denote by $\mathbb{H}_a$ the subring of algebraic quaternions, i.e., the set of all elements $a + b \cdot i + c \cdot j + d \cdot k \in \mathbb{H}$ with $a, b, c, d \in \overline{\mathbb{Q}} \cap \mathbb{R}$. Note that in our notation (1.3),

$$\|a + bi + cj + dk\| = (a^2 + b^2 + c^2 + d^2)^2. \tag{2.2}$$

In the following examples, we work with the usual Euclidean norm $|f| := \|f\|^{1/4}$. This is purely for the sake of convenience, as we note that $|f_1|, \dots, |f_r|$ are multiplicatively independent if and only if $\|f_1\|, \dots, \|f_r\|$ are.

2.3. **Examples.** We first note that the conclusion in Theorem 2.2 fails if V were to pass through 0.

Example 2.3. We can take $D = \mathbb{H}_a$, Γ be the cyclic subgroup generated by 2, and V be the hyperplane consisting of all points $x_1 + x_2 \cdot i + x_3 \cdot j + x_4 \cdot k \in \mathbb{H}_a$ with $x_2 = 0$; then the entire group Γ is contained in V.

Furthermore, the norm condition (or a version thereof) is necessary in Theorem 2.2, as shown by the following example.

Example 2.4. Take $K = \mathbb{R}, D = \mathbb{H}$, $V = \{a + bi + cj + dk : a + d = 1\}$, $f_1 = 3 + 4i$, and $f_2 = (3+4j)/25$. An easy computation (employing the fact that $i^2 = -1$) shows that for each positive integer n, we have:

$$f_1^n = \left(\sum_{0\le \ell\le n/2}\binom{n}{2\ell}(-1)^\ell 3^{n-2\ell}4^{2\ell}\right) + \left(\sum_{0\le s\le (n-1)/2}\binom{n}{2s+1}(-1)^s 3^{n-2s-1}4^{2s+1}\right)\cdot i.$$

Therefore, letting

$$a_n = \sum_{0\le \ell\le n/2}\binom{n}{2\ell}(-1)^\ell 3^{n-2\ell}4^{2\ell} \text{ and } b_n = \sum_{0\le s\le (n-1)/2}\binom{n}{2s+1}(-1)^s 3^{n-2s-1}4^{2s+1},$$

we obtain that $f_1^n = a_n + b_n \cdot i$. Furthermore, using that the norm of f_1 equals 5 and therefore, the norm of f_1^n equals 5^n, we get that

$$5^{2n} = |f_1^n|^2 = a_n^2 + b_n^2. \tag{2.3}$$

An identical computation (employing this time that $j^2 = -1$) yields that $f_2^n = \frac{a_n + b_n j}{5^{2n}}$. Then a simple computation inside the quaternion ring yields that

$$f_1^n \cdot f_2^n = \frac{a_n^2 + a_n b_n i + a_n b_n j + b_n^2 k}{5^{2n}}. \tag{2.4}$$

Equation (2.3) yields that $f_1^n f_2^n \in V$ for all $n \in \mathbb{N}_0$; furthermore, these elements are all distinct. Indeed, if $f_1^n f_2^n = f_1^m f_2^m$ for some integers $n > m \ge 0$, then we would get that

$$f_1^\ell f_2^\ell = 1 \text{ for } \ell := n - m.$$

However, inspecting the computation of the general form of $f_1^n f_2^n$ from equation (2.4), we see that $f_1^\ell f_2^\ell = 1$ would yield $a_\ell^2 = 5^{2\ell}$ and $b_\ell = 0$, i.e., $f_1^\ell = \pm 5^\ell$. However, $g_1 := \frac{3+4i}{5}$ is not a root of unity since the minimal polynomial of g_1 over $\mathbb{Z}$ is $5x^2 - 6x + 5$, which *cannot* divide a cyclotomic polynomial (in $\mathbb{Z}[x]$) since it is not a monic polynomial.

So, there exist indeed infinitely many elements in V of the form $f_1^n f_2^n$. On the other hand, we also note that the hypothesis from Theorem 2.2 is not verified since $|f_1| \cdot |f_2| = 1$, i.e., f_1 and f_2 do not have multiplicatively independent norms.

The following result shows that Example 2.4 provides also an example in which the intersection between a subgroup Γ of $D^\times$ with a K-subvariety of D is *not* a finite union of cosets of subgroups of Γ.

Proposition 2.5. *Let $K = \mathbb{R}$ and $D = \mathbb{H}$, $V = \{a + bi + cj + dk : a + d = 1\}$, $f_1 = 3 + 4i$, and $f_2 = (3 + 4j)/25$. Let Γ be the subgroup of $D^\times$ generated by f_1 and f_2. Then $\Gamma \cap V$ is not a finite union of cosets of subgroups of Γ.*

Proposition 2.5 shows that one cannot expect the same conclusion (of Mordell-Lang type) when we intersect a finitely generated subgroup of the multiplicative group of a K-division algebra with a K-subvariety of D. Therefore, our Theorem 1.3 is the most one can expect towards a variant of the classical Mordell-Lang problem in the context of division algebras.

Proof of Proposition 2.5. Let $U := \Gamma \cap V$. We argue by contradiction and therefore, assume U is a union of finitely many right-cosets of subgroups of Γ along with finitely many left-cosets of subgroups of Γ. Since $f_1^n f_2^n \in U$ for each $n \in \mathbb{N}_0$ (according to Example 2.4), then there exists such a right-coset, or a left-coset of a subgroup of Γ which contains two distinct elements $f_1^n f_2^n$ and $f_1^m f_2^m$ (with $n > m > 0$). Without loss of generality (the exact same argument works also considering a left-coset), we may assume

$$f_1^n f_2^n,\ f_1^m f_2^m \in \gamma \cdot H \text{ for some } \gamma \cdot H \subseteq U.$$

But then $f_2^{-m} f_1^{-m} \cdot f_1^n f_2^n \in H$ and therefore,

$$f_1^n f_2^n \cdot (f_2^{-m} f_1^{-m} \cdot f_1^n f_2^n) \in \gamma \cdot H.$$

We let $\ell := n - m$; note that $n > \ell > 0$. So, we have that

$$f_1^n f_2^\ell f_1^\ell f_2^n \in V. \tag{2.5}$$

We compute (exactly as in Example 2.4) that

$$f_1^n = a_n + i \cdot b_n \text{ with } a_n^2 + b_n^2 = 5^{2n} \tag{2.6}$$

$$f_2^n = \frac{a_n + j \cdot b_n}{5^{2n}} \tag{2.7}$$

$$f_1^\ell = a_\ell + i \cdot b_\ell \text{ with } a_\ell^2 + b_\ell^2 = 5^{2\ell} \tag{2.8}$$

$$f_2^\ell = \frac{a_\ell + j \cdot b_\ell}{5^{2\ell}}. \tag{2.9}$$

Then equations (2.6) and (2.7) yield

$$f_1^n f_2^\ell = \frac{a_n a_\ell + i \cdot b_n a_\ell + j \cdot a_n b_\ell + k \cdot b_n b_\ell}{5^{2\ell}}, \tag{2.10}$$

while equations (2.8) and (2.9) yield

$$f_1^\ell f_2^n = \frac{a_\ell a_n + i \cdot b_\ell a_n + j \cdot b_n a_\ell + k \cdot b_\ell b_n}{5^{2n}}. \tag{2.11}$$

In order to check equation (2.5), we need to compute the components for 1 and for k, when we multiply $f_1^n f_2^\ell$ with $f_1^\ell f_2^n$; note that each quaternion is uniquely defined by the components of the 4 elements: $1, i, j, k$, but due to the definition of the variety V, only the components for 1 and k are relevant for checking that some element of Γ lands in V. So, the component corresponding to 1 in $f_1^n f_2^\ell f_1^\ell f_2^n$ equals

$$\frac{a_n^2 a_\ell^2 - b_n^2 b_\ell^2 - 2a_n b_n a_\ell b_\ell}{5^{2(n+\ell)}}, \tag{2.12}$$

while the component corresponding to k in $f_1^n f_2^\ell f_1^\ell f_2^n$ equals

$$\frac{b_n^2 a_\ell^2 - a_n^2 b_\ell^2 + 2a_n b_n a_\ell b_\ell}{5^{2(n+\ell)}}. \tag{2.13}$$

Using equations (2.12) and (2.13), we get that $f_1^n f_2^\ell f_1^\ell f_2^n \in V$ if and only if

$$\left(a_n^2 a_\ell^2 - b_n^2 b_\ell^2 - 2a_n b_n a_\ell b_\ell\right) + \left(b_n^2 a_\ell^2 - a_n^2 b_\ell^2 + 2a_n b_n a_\ell b_\ell\right) = 5^{2(n+\ell)}, \tag{2.14}$$

which yields

$$a_n^2 a_\ell^2 - b_n^2 b_\ell^2 + b_n^2 a_\ell^2 - a_n^2 b_\ell^2 = 5^{2(n+\ell)}, \tag{2.15}$$

and factoring the left-hand side yields

$$(a_n^2 + b_n^2)(a_\ell^2 - b_\ell^2) = 5^{2(n+\ell)}, \tag{2.16}$$

Since $a_n^2 + b_n^2 = 5^{2n}$ from equation (2.6), we have

$$a_\ell^2 - b_\ell^2 = 5^{2\ell}. \tag{2.17}$$

But since $a_\ell^2 + b_\ell^2 = 5^{2\ell}$ from equation (2.8), we get $b_\ell = 0$.

However, this is impossible because it would mean that $(3+4i)^\ell = a_\ell \in \mathbb{R}$ (note that $\ell > 0$ and also the fact that in Example 2.4, we explained that $(3+4i)/5$ is not a root of unity). This contradiction shows that indeed, the intersection between Γ and V is *not* a finite union of cosets of subgroups of Γ. This concludes our proof of Proposition 2.5. □

We conclude this Section by noting that in the context of subgroups of $D^\times$, it is also very difficult to formulate a general finiteness statement similar to our Theorem 2.2. In particular, we cannot expect the same conclusion in Theorem 2.2 if we replace the set of all elements

$$f_1^{n_1} \cdots f_r^{n_r} \text{ (as we vary } n_1, \dots, n_r \in \mathbb{Z})$$

with the group Γ spanned by $f_1, \dots, f_r$ (even if $f_1, \dots, f_r$ have multiplicatively independent norms); this is shown in our next Example.

Example 2.6. Again working inside $D := \mathbb{H}$ and considering the $\overline{\mathbb{R}}$-subvariety $V = \{a + bi + cj + dk \colon a + d = 1\}$, we let now Γ be the subgroup of $D^\times$ spanned by $f_1 = 3 + 4i$ and by $g = 1 + i + j - k$. We note that f_1 and g have multiplicatively independent norms (since 5 and 2 are multiplicatively independent). However, we show next that the intersection of V with Γ is actually infinite.

Indeed, letting $f_2 := 3 + 4j$, we observe first that

$$f_1 g = g f_2 \text{ because } i \cdot g = g \cdot j.$$

This means that $f_2 = g^{-1} f_1 g \in \Gamma$. But then, as shown by Example 2.4, we obtain that $V \cap \Gamma$ is infinite (since $f_1^n f_2^n \in \Gamma \cap V$ for each $n \in \mathbb{N}_0$).

3. Preliminary results

In this Section 3, we gather three technical results to be employed in our proofs.

3.1. The classical Mordell-Lang.

One of our key tools is the classical Mordell-Lang theorem for tori, proven by Laurent [Lau84, Théorème 2]; we state a slight reformulation of Theorem 1.1, which is better suited for our application.

Theorem 3.1 (Mordell-Lang)**.** *Let $N, r \in \mathbb{N}$, let L be a field of characteristic 0, let V be an algebraic subvariety of $\mathbb{G}_m^N$, and $\varphi : \mathbb{Z}^r \to \mathbb{G}_m^N(L)$ be a group homomorphism. Then the set $\{(n_1, \dots, n_r) \in \mathbb{Z}^r \colon \varphi(n_1, \dots, n_r) \in V(L)\}$ is a finite union of cosets of subgroups of $\mathbb{Z}^r$.*

Proof. Let $\Gamma = \varphi(\mathbb{Z}^r)$. By [Lau84, Théorème 2], $V \cap \Gamma$ is a finite union of sets of the form $\gamma_i(H_i(\overline{K}) \cap \Gamma)$, where γ_i are elements of Γ and H_i are algebraic subtori of T. Let ν_i be any element of $\varphi^{-1}(\gamma_i)$. Then the desired set is

$$\varphi^{-1}(V) = \varphi^{-1}(V \cap \Gamma) = \varphi^{-1}\left(\bigcup_i \gamma_i(H_i \cap \Gamma)\right) \tag{3.1}$$

$$= \bigcup_i \varphi^{-1}(\gamma_i(H_i \cap \Gamma)) \tag{3.2}$$

$$= \bigcup_i (\nu_i + \varphi^{-1}(H_i \cap \Gamma)), \tag{3.3}$$

so we are done since $\varphi^{-1}(H_i \cap \Gamma)$ is a subgroup of $\mathbb{Z}^r$. □

3.2. **Cosets of subgroups of $\mathbb{Z}^m$.** The following result shows that the infinite intersection of $\mathbb{N}^m$ with a coset of a subgroup H of $\mathbb{Z}^m$ is always explained by the existence of a nontrivial element in $H \cap \mathbb{N}^m$.

Lemma 3.2. *If H is a subgroup of $\mathbb{Z}^m$ such that a coset of it $\underline{c} + H$ has infinite intersection with $\mathbb{N}^m$, then H must contain a nontrivial element from $\mathbb{N}^m$.*

Proof. The proof is by induction on m, where the case $m = 1$ is trivial. So we assume the statement is true for m and then prove it for $m + 1$.

We pick an element $\underline{x}_1 \in (\underline{c}+H) \cap \mathbb{N}^{m+1}$. If there exists another element $\underline{x}_2 \in (\underline{c}+H) \cap \mathbb{N}^{m+1}$ such that each entry of $\underline{x}_2$ is not less than the corresponding entry of $\underline{x}_1$, then the difference $\underline{x}_2 - \underline{x}_1$ is in H and as desired. So, let us assume that for each element $\underline{x}_2 \neq \underline{x}_1$ from $(\underline{c} + H) \cap \mathbb{N}^{m+1}$, there exists some entry in $\underline{x}_2$ less than the corresponding entry from $\underline{x}_1$. By the pigeonhole principle, we may assume that there exist infinitely many elements $\underline{x}_2, \underline{x}_3, \dots \in (\underline{c} + H) \cap \mathbb{N}^{m+1}$ such that the first entry in $\underline{x}_i$ (for $i \geq 2$) is smaller than the first entry in $\underline{x}_1$. Then by another application of the pigeonhole principle, we may assume $\underline{x}_2, \underline{x}_3, \dots$ have the same first entry, which we denote by j.

Now, consider the intersection $(\underline{c} + H) \cap (\{j\} \times \mathbb{Z}^m)$; this is another coset of a subgroup of $\mathbb{Z}^{m+1}$ (because it is the intersection of two cosets of subgroups), which we call $\underline{c}_1 + H_1$. More precisely, H_1 is the subgroup of H consisting of all elements of H whose first entry equals 0. Also, $(\underline{c}_1 + H_1) \cap \mathbb{N}^{m+1}$ lies in $\{j\} \times \mathbb{N}^m$ and contains infinitely many elements since it contains $\underline{x}_2, \underline{x}_3, \dots$. Thus letting $\pi : \mathbb{Z}^{m+1} \to \mathbb{Z}^m$ be the projection onto the last m coordinates, we can apply the inductive hypothesis to $\pi(\underline{c}_1 + H_1)$, which is a coset $\underline{c}_2 + H_2$ of a subgroup in $\mathbb{Z}^m$, and conclude that H_2 contains a nontrivial element in $\mathbb{N}^m$. In particular, H_1 contains an element $\underline{x}_0$ whose last m coordinates are nonnegative integers, not all equal to 0. But elements of H_1 all have their first coordinate equal to 0, so $\underline{x}_0 \in H_1 \subseteq H$ is as desired in the conclusion of Lemma 3.2. □

3.3. **A general result regarding an infinite system of equations.** We will use the following Lemma in the proof of Theorem 2.2.

Lemma 3.3. *Let L be a field of characteristic 0. Let $m \in \mathbb{N}$ and let $a_1, \dots, a_m, \delta_1, \dots, \delta_m \in L$ such that*

$$\sum_{i=1}^{m} a_i \delta_i^n = 1 \text{ for each } n \in \mathbb{N}. \tag{3.4}$$

Then $\delta_i = 1$ *for some* $i \in \{1, \dots, m\}$.

Proof. We employ [GS23, Lemma 2.3], which states that for any distinct $\gamma_1, \dots, \gamma_\ell \in L$ (for some $\ell \in \mathbb{N}$) and for any $a_1, \dots, a_\ell \in L$, if we have that

$$\sum_{i=1}^{\ell} a_i \gamma_i^n = 0 \text{ for each } n \in \mathbb{N},$$

then $a_1 = a_2 = \cdots = a_\ell = 0$.

Now, we let $\lambda_1, \dots, \lambda_k$ (for some $k \le m$) be the distinct elements appearing in $\delta_1, \dots, \delta_m$ (so, if the δ_i's are all distinct, then $k = m$, while if the δ_i's are all equal to each other, then $k = 1$). Next, for each $i = 1, \dots, k$, we let A_i be the sum of the a_j's for which $\delta_j = \lambda_i$. Then our hypothesis (3.4) yields that

$$(-1) \cdot 1^n + \sum_{i=1}^{k} A_i \lambda_i^n = 0 \text{ for all } n \in \mathbb{N}.$$

So, [GS23, Lemma 2.3] yields that one of the λ_i's must equal to 1 (note that the λ_i's are already distinct). Thus, there exists $j \in \{1, \dots, m\}$ such that $\delta_j = 1$, as desired in the conclusion of Lemma 3.3. □

4. Proof of Theorem 1.3

In this Section 4, we work under the hypotheses of Theorem 1.3.

The main part of our proof lies in Subsection 4.1, in which we obtain a very useful reformulation of the condition that

$$f_1^{n_1} f_2^{n_2} \cdots f_r^{n_r} \in V \tag{4.1}$$

to an exponential equation (see (4.4)). It is important to note that while the condition (4.1) lives in a non-abelian setting, the exponential equation (4.4) lives in an abelian setting, which will allow us later to apply Theorem 3.1.

4.1. Conversion to an exponential equation in the hypersurface case.

In this Subsection, we work under the additional hypothesis that V is a K-hypersurface of D. So, D is a finite-dimensional division algebra over a field K of characteristic 0, V is a hypersurface of D cut out by one equation $F(x) = 0$ with $F : D \to K$ a K-polynomial (see Subsection 1.3), while $f_1, \dots, f_r \in D^\times$.

For each $i = 1, \dots, r$, we have that $L_i := K(f_i)$ is a finite-dimensional commutative algebra over K (since $K(f_i) \subseteq D$ and D is finite-dimensional). As D is a division algebra, L_i is an integral domain with $[L_i : K] < \infty$, and hence a field by Nullstellensatz. In other words, L_i/K is a finite extension of fields, though not canonically embedded in an algebraic closure of K.

For each $d \ge 0$, let F_d be the degree d homogeneous part of F, and we choose a d-multilinear form (over K, as always) $\Theta_d : D^{\times d} \to K$ such that $F_d(x) = \Theta_d(x, \dots, x)$. Choose $M \gg 0$ such that $F_d = 0$ for all $d > M$. By setting $\alpha = -F_0 \in K$ (the value of the constant function), the defining equation for V can be rewritten as

$$\Theta_1(z) + \Theta_2(z, z) + \cdots + \Theta_M(z, \dots, z) = \alpha. \tag{4.2}$$

For each $1 \le d \le M$, define a dr-multilinear map $\theta_d : (L_1 \times \cdots \times L_r)^{\times d} \to K$ by

$$\theta_d(z_1^{(1)}, \ldots, z_r^{(1)}, \ldots, z_1^{(d)}, \ldots, z_r^{(d)}) := \Theta_d(z_1^{(1)} \cdots z_r^{(1)}, \ldots, z_1^{(d)} \cdots z_r^{(d)}), \tag{4.3}$$

where the multiplication in the right-hand side takes place in D. Then the equation (4.1) becomes

$$\theta_1(f_1^{n_1}, \ldots, f_r^{n_r}) + \theta_2(f_1^{n_1}, \ldots, f_r^{n_r}, f_1^{n_1}, \ldots, f_r^{n_r}) + \cdots + \theta_M(f_1^{n_1}, \ldots, f_r^{n_r}, \ldots, f_1^{n_1}, \ldots, f_r^{n_r}) = \alpha. \tag{4.4}$$

To better understand the exponential equation (4.4), we rewrite the multilinear maps θ_d more explicitly. Fix an algebraic closure $\overline{K}$ of K. For $1 \le i \le r$, let G_i be the set of all K-embeddings $\sigma : L_i \to \overline{K}$; we have $|G_i| = [L_i : K]$. From basic Galois theory, G_i forms a $\overline{K}$-basis of the $\overline{K}$-vector space of K-linear maps $\mathrm{Hom}_K(L_i, \overline{K})$. In other words, we have a direct sum decomposition and canonical isomorphism $\mathrm{Hom}_K(L_i, \overline{K}) = \bigoplus_{\sigma \in G_i} \overline{K}\sigma \simeq KG_i$. On the other hand, by the tensor-hom adjunction $\mathrm{Hom}_A(V \otimes_A W, B) \simeq \mathrm{Hom}_A(V, B) \otimes_B \mathrm{Hom}_A(W, B)$ for any commutative ring homomorphism $A \to B$ and any B-modules V, W, we have a canonical isomorphism of $\overline{K}$-vector spaces

$$\mathrm{Hom}_K((L_1 \otimes_K \cdots \otimes_K L_r)^{\otimes_K d}, \overline{K}) \simeq (\mathrm{Hom}_K(L_1, \overline{K}) \otimes_{\overline{K}} \cdots \otimes_{\overline{K}} \mathrm{Hom}_K(L_r, \overline{K}))^{\otimes_{\overline{K}} d}, \tag{4.5}$$

where $(\cdot)^{\otimes_K d}$ means d-fold tensor power over K. As a result, we have canonical isomorphisms

$$\begin{aligned} \mathrm{Hom}_K((L_1 \otimes_K \cdots \otimes_K L_r)^{\otimes_K d}, \overline{K}) &\simeq (\mathrm{Hom}_K(L_1, \overline{K}) \otimes_{\overline{K}} \cdots \otimes_{\overline{K}} \mathrm{Hom}_K(L_r, \overline{K}))^{\otimes_{\overline{K}} d} \\ &\simeq (\overline{K}G_1 \otimes_{\overline{K}} \cdots \otimes_{\overline{K}} \overline{K}G_r)^{\otimes_{\overline{K}} d} \simeq \overline{K}(G_1 \times \cdots \times G_r)^{\times d}, \end{aligned}$$

where the last expression is the $\overline{K}$-vector space with basis $G^d = \underbrace{G \times \cdots \times G}_{d}$, where $G := G_1 \times \cdots \times G_r$. As a result, the dr-multilinear form $\theta_d \in \mathrm{Hom}_K((L_1 \otimes_K \cdots \otimes_K L_r)^{\otimes_K d}, \overline{K})$ can be canonically interpreted as an element of $\overline{K}G^d$. In particular, there are elements $a_{\sigma^{(1)}, \ldots, \sigma^{(d)}}$ indexed by $(\sigma^{(1)}, \ldots, \sigma^{(d)}) \in G^d$, uniquely determined by θ_d, such that we have for $z_i \in L_i$

$$\theta_d(z_1, \ldots, z_r, \ldots, z_1, \ldots, z_r) = \sum_{\sigma^{(1)}, \ldots, \sigma^{(d)} \in G} a_{\sigma^{(1)}, \ldots, \sigma^{(d)}} z^{\sigma^{(1)}} \cdots z^{\sigma^{(d)}}, \tag{4.6}$$

where for any $\sigma = (\sigma_1, \ldots, \sigma_r) \in G$, we define $z^\sigma := \sigma_1(z_1) \cdots \sigma_r(z_r)$. (The product takes place in a fixed copy of $\overline{K}$, which importantly, is commutative.) If $\underline{n} = (n_1, \ldots, n_r)$ is in $\mathbb{Z}^r$, then (4.6) gives

$$\theta_d(f_1^{n_1}, \ldots, f_r^{n_r}, \ldots, f_1^{n_1}, \ldots, f_r^{n_r}) = \sum_{\sigma^{(1)}, \ldots, \sigma^{(d)} \in G} a_{\sigma^{(1)}, \ldots, \sigma^{(d)}} f^{\underline{n}, \sigma^{(1)}} \cdots f^{\underline{n}, \sigma^{(d)}}, \tag{4.7}$$

where

$$f^{\underline{n}, \sigma} := \prod_{i=1}^{r} \sigma_i(f_i)^{n_i} \in \overline{K}. \tag{4.8}$$

So, we converted the equation (4.1) into an exponential equation

$$\sum_{d=1}^{M} \sum_{\sigma^{(d,1)}, \ldots, \sigma^{(d,d)} \in G} a_{\sigma^{(d,1)}, \ldots, \sigma^{(d,d)}} f^{\underline{n}, \sigma^{(d,1)}} \cdots f^{\underline{n}, \sigma^{(d,d)}} = \alpha \tag{4.9}$$

for some coefficients $a_{\sigma^{(d,1)}, \ldots, \sigma^{(d,d)}} \in \overline{K}$ that are determined by the equation of the hypersurface V. Of course, $a_{\sigma^{(d,1)}, \ldots, \sigma^{(d,d)}}$ cannot be arbitrary: since θ_d actually lands in K rather than $\overline{K}$, the collection $\{a_{\sigma^{(d,1)},\dots,\sigma^{(d,d)}}\}_{\sigma^{(d,j)}\in G}$ must be "Galois invariant" in a suitable sense for each d. However, we will not need it in this paper.

For future convenience, we further compactify the notation. Let $\mathbf{G} := G \sqcup G^2 \sqcup \cdots \sqcup G^M$, a formal disjoint union, so a typical element of $\mathbf{G}$ can be viewed as a pair $(d, \boldsymbol{\sigma})$, where $1 \le d \le M$ and $\boldsymbol{\sigma} = (\sigma^{(d,1)}, \dots, \sigma^{(d,d)}) \in G^d$. For $\boldsymbol{\sigma} \in G^d$, define

$$f^{\underline{n},\boldsymbol{\sigma}} := f^{\underline{n},\sigma^{(d,1)}} \cdots f^{\underline{n},\sigma^{(d,d)}}. \tag{4.10}$$

Then we may rewrite (4.9) compactly as

$$\sum_{\boldsymbol{\sigma}\in\mathbf{G}} a_{\boldsymbol{\sigma}} f^{\underline{n},\boldsymbol{\sigma}} = \alpha. \tag{4.11}$$

Remark 4.1. Also, we note that in the case D/K is a finite field extension, we have an even simpler counterpart of (4.11), by working with (4.2) directly. Let G simply be the set of K-embeddings from D to $\overline{K}$. Then $\mathrm{Hom}_K(D, \overline{K}) = \overline{K}G$ and

$$\mathrm{Hom}_K(D^{\otimes_K d}, \overline{K}) \simeq \mathrm{Hom}_K(D^{\otimes_K} d, \overline{K})^{\otimes_{\overline{K}}\, d} \simeq \overline{K}G^d,$$

so by applying the argument leading to (4.6) directly to Θ_d (instead of θ_d), we get

$$\Theta_d(z, \dots, z) = \sum_{\sigma^{(1)},\dots,\sigma^{(d)}\in G} a_{\sigma^{(1)},\dots,\sigma^{(d)}} \sigma^{(1)}(z) \cdots \sigma^{(d)}(z), \tag{4.12}$$

for some scalars $a_{\sigma^{(1)},\dots,\sigma^{(d)}} \in \overline{K}$. Therefore, the counterpart of equation (4.7) is simply the equation:

$$\Theta_d(f_1^{n_1}, \dots, f_r^{n_r}) = \sum_{\sigma^{(1)},\dots,\sigma^{(d)}\in G} a_{\sigma^{(1)},\dots,\sigma^{(d)}} f^{\underline{n},\sigma^{(1)}} \cdots f^{\underline{n},\sigma^{(d)}}, \tag{4.13}$$

where $f^{\underline{n},\sigma} := \prod_{i=1}^{r} \sigma(f_i)^{n_i}$. As a result, the equation (4.1) is equivalent to

$$\sum_{\sigma\in\mathbf{G}} a_\sigma f^{\underline{n},\sigma} = \alpha, \tag{4.14}$$

where $\mathbf{G} := G \sqcup G^2 \sqcup \cdots \sqcup G^M$ as before.

4.2. **Conclusion of our proof for Theorem 1.3.** We re-state the conclusion in Theorem 1.3 as follows.

Lemma 4.2. *Let K be a field of characteristic zero, D be a finite-dimensional division algebra over K, V be a K-subvariety of D, and $\varphi : \mathbb{Z}^r \to D^\times$ be a given map of the form*

$$\varphi(n_1, \dots, n_r) = f_1^{n_1} \cdots f_r^{n_r}, \tag{4.15}$$

where $r \ge 1$ is fixed and $f_1, \dots, f_r$ are also fixed elements of $D^\times$. Then $\varphi^{-1}(V)$ is a finite union of cosets of subgroups of $\mathbb{Z}^r$.

Proof. Since V is the intersection of finitely many hypersurfaces, and the intersection of cosets of subgroups of $\mathbb{Z}^r$ is a coset of some subgroup, it suffices to prove the case where V is a hypersurface. Using the re-statement of equation (4.1) into an exponential equation (4.4) (see also equation (4.11) from the construction done in Subsection 4.1), $\varphi^{-1}(V)$ is the set of $\underline{n} = (n_1, \dots, n_r)$ that solves the equation

$$\sum_{\boldsymbol{\sigma}\in\mathbf{G}} a_{\boldsymbol{\sigma}} f^{\underline{n},\boldsymbol{\sigma}} = \alpha, \tag{4.16}$$

with the notation $\mathbf{G}$, $a_{\boldsymbol{\sigma}}$, and $f^{\underline{n},\boldsymbol{\sigma}}$ as in Subsection 4.1 (and $\alpha \in K$). Consider the torus $T := (\overline{K}^{\times})^{|\mathbf{G}|}$ with coordinates indexed by $\mathbf{G}$, and the map $\psi : \mathbb{Z}^r \to T$ defined by

$$\psi(\underline{n}) := (f^{\underline{n},\boldsymbol{\sigma}})_{\boldsymbol{\sigma}\in\mathbf{G}}. \tag{4.17}$$

Then it is clear from the definition that ψ is a group homomorphism because

$$f^{\underline{n},\boldsymbol{\sigma}} = f^{\underline{n},\sigma^{(d,1)}} \cdots f^{\underline{n},\sigma^{(d,d)}} \text{ from equation (4.10)} \tag{4.18}$$

and for each $\sigma = (\sigma_1, \ldots, \sigma_r) \in \left\{\sigma^{(d,1)}, \ldots, \sigma^{(d,d)}\right\}$, we have

$$f^{\underline{n},\sigma} = \prod_{i=1}^{r} \sigma_i(f_i)^{n_i} \text{ from equation (4.8).} \tag{4.19}$$

Since each σ_i is a homomorphism of fields, then equations (4.18) and (4.19) show that indeed, ψ is a group homomorphism. Now, consider a $\overline{K}$-subvariety of T defined by

$$W := \left\{(z_{\boldsymbol{\sigma}})_{\boldsymbol{\sigma}\in\mathbf{G}} : \sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} z_{\boldsymbol{\sigma}} = \alpha\right\} \cap T. \tag{4.20}$$

The construction implies $\varphi^{-1}(V) = \psi^{-1}(W)$, so the desired conclusion in Lemma 4.2 follows from Theorem 3.1. ☐

This concludes our proof for Theorem 1.3.

5. Our proof for Theorem 2.2

In this Section, we work under the hypotheses from Theorem 2.2. So, as before, D is a finite-dimensional division algebra over a field K of characteristic 0, and we let $f_1, \ldots, f_r \in D^{\times}$ be elements which have multiplicatively independent norms (see Definition 2.1). Also, we let V be a K-subvariety of D, which does not contain 0.

We start with a simple reduction (done in the next Subsection), in which we show that we may assume V is a hypersurface.

5.1. Reduction of Theorem 2.2 to the hypersurface case.

Lemma 5.1. *Let K be a field, $\mathbb{A}^{\ell}(K)$ be the ℓ-dimensional affine space, and V be a K-subvariety of $\mathbb{A}^{\ell}(K)$ not passing through $\underline{0} = (0, \ldots, 0)$. Then there is a K-hypersurface of $\mathbb{A}^{\ell}(K)$ not passing through $\underline{0}$ that contains V.*

Proof. Say (1.4) is the finite system of equations that cut out the K-variety V. Since $\underline{0} \notin V$, there is $1 \le j \le m$ such that $P_j(\underline{0}) \neq 0$. The hypersurface cut out by $P_j(x_1, \ldots, x_l) = 0$ then does the job. ☐

In the next Subsection we bring back the re-statement of the equation (4.1) to the exponential equation (4.4) (see also the construction from Subsection 4.1, including the notation (4.8)).

5.2. **Back to the conversion of our question to an exponential equation.** Recall from Subsection 4.1 that the equation $f_1^{n_1}\dots f_r^{n_r}\in V$ can be rewritten as

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} f^{\underline{n},\boldsymbol{\sigma}} = 1. \tag{5.1}$$

Note that we can safely assume the right-hand side of equation (5.1) equals 1 since the assumption we have that the hypersurface V does not pass through 0 yields that the right-hand side of (5.1) is a nonzero element $\alpha\in K$; then dividing by α yields the above form of equation (5.1). Moreover, the conclusion of Lemma 4.2 states that the set of $\underline{n}\in\mathbb{Z}^r$ that solve (5.1) is a finite union of cosets of $\mathbb{Z}^r$.

Assume the contrary of the conclusion of Theorem 2.2, i.e., $|V\cap\Gamma|=\infty$. Then (5.1) is solved by infinitely many $\underline{n}\in\mathbb{Z}^r$, so one of the aforementioned cosets, say $\underline{c}+H$, must be infinite. Hence, H contains a nonzero element $\underline{x}\in\mathbb{Z}^r$. Thus (5.1) restricted to $\underline{c}+\mathbb{Z}\underline{x}$ yields

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} f^{\underline{c}+n\underline{x},\boldsymbol{\sigma}} = 1 \text{ for all } n\in\mathbb{Z}, \tag{5.2}$$

or (restricting only to $n\in\mathbb{N}$)

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} f^{\underline{c},\boldsymbol{\sigma}} (f^{\underline{x},\boldsymbol{\sigma}})^n = 1 \text{ for all } n\in\mathbb{N}. \tag{5.3}$$

So, combining equation (5.3) with Lemma 3.3 yields that there exists $\boldsymbol{\sigma}\in\mathbf{G}$ such that

$$f^{\underline{x},\boldsymbol{\sigma}} = 1. \tag{5.4}$$

Now, we know that

$$f^{\underline{x},\boldsymbol{\sigma}} = f^{\underline{x},\sigma^{(d,1)}}\cdots f^{\underline{x},\sigma^{(d,d)}} \text{ from equation (4.10)}, \tag{5.5}$$

for some $d\in\{1,\dots,M\}$ and some $\sigma^{(d,1)},\dots,\sigma^{(d,d)}\in G$. Also, for each $\sigma\in\left\{\sigma^{(d,1)},\dots,\sigma^{(d,d)}\right\}$, we have that

$$f^{\underline{x},\sigma} = \prod_{i=1}^r \sigma_i(f_i)^{x_i} \text{ from equation (4.8)}. \tag{5.6}$$

Combining equations (5.4), (5.5) and (5.6), we obtain

$$\prod_{j=1}^d \prod_{i=1}^r \sigma_i^{(d,j)}(f_i)^{x_i} = 1. \tag{5.7}$$

The next lemma provides the desired contradiction; we will state and prove the key Lemma 5.2 in Subsection 5.3.

5.3. **Conclusion of our proof for Theorem 2.2.** This next result will also be used in our proof of Theorem 6.4.

Lemma 5.2. *With the above notation, assume equation (5.7) holds for some $x_1,\dots,x_r\in\mathbb{Z}$. Then there exists a positive integer b such that*

$$\prod_{i=1}^r \|f_i\|^{bx_i} = 1. \tag{5.8}$$

Proof of Lemma 5.2. We identify $L_i = K(f_i)$ with its image under a choice of K-embedding $L_i \to \overline{K}$, and fix a large enough finite extension L/K in $\overline{K}$ such that $L \supseteq L_i$ and $[L : K]$ is divisible by $[D : K]$; say that $[L : K] = m \cdot [D : K]$ for some positive integer m. Taking the norm $\mathrm{Norm}_{L/K}$ on both sides of (5.7) yields

$$1 = \prod_{i=1}^{r} \mathrm{Norm}_{L/K}(f_i)^{dx_i} = \prod_{i=1}^{r} \mathrm{Norm}_{L_i/K}(f_i)^{[D:L_i]dmx_i}. \tag{5.9}$$

Using Definition 1.3 and setting $b = dm$ (note that $\|f_i\| = \mathrm{Norm}_{L_i/K}(f_i)^{[D:L_i]}$), we obtain the desired equation (5.8). □

Now, we finish our proof of Theorem 2.2. Since not all integers x_i from equation (5.8) (see Lemma 5.2) are equal to 0 (while b is a positive integer), we see that equation (5.8) contradicts the assumption that $f_1, \dots, f_r$ have multiplicatively independent norms.

This concludes our proof for Theorem 2.2.

6. Proofs of two other results related to Theorem 2.2

Using a result of the second author [Hua20, Thm. 1.2], a slight variant of our Theorem 2.2 (see Theorem 6.4) yields the following result on a unit equation, which also proves another special case of [Hua20, Conj. 1.4]. In order to state our Theorem 6.2, we introduce the following notation.

Notation 6.1. For a division algebra D over a field K of characteristic 0, given $f_1, \dots, f_r \in D^\times$, we let $\langle f_1, \dots, f_r \rangle$ denote the subsemigroup of $D^\times$ generated by $f_1, \dots, f_r$, and let $\Gamma_{f_1,\dots,f_r}$ be the subset:

$$\{f_1^{n_1} \cdot \dots \cdot f_r^{n_r} : n_1, \dots, n_r \in \mathbb{N}\} \subseteq \langle f_1, \dots, f_r \rangle.$$

Theorem 6.2. *Let $\mathbb{H}_a$ be the ring of algebraic quaternions, let a, a', b, b' be fixed nonzero algebraic quaternions, let $f_1, \dots, f_k \in D^\times$ and $g_1, \dots, g_\ell \in D^\times$ be elements of norm greater than 1. Then the unit equation*

$$afa' + bgb' = 1 \tag{6.1}$$

has only finitely many solutions with $f \in \Gamma_{f_1,\dots,f_k}$ and $g \in \langle g_1, \dots, g_\ell \rangle$.

In Section 6.1, we state and prove Theorem 6.4; then in Section 6.2, we derive Theorem 6.2 as a consequence of Theorem 6.4.

6.1. A variant of Theorem 2.2.

In order to state Theorem 6.4, we need the following definition.

Definition 6.3. We say a collection of elements $f_1, \dots, f_r \in D^\times$ has **semimultiplicatively independent norms** if whenever $\|f_1\|^{n_1} \cdots \|f_r\|^{n_r} = 1$ for some $n_1, \dots, n_r \in \mathbb{N}_0$, then we must have $n_1 = \cdots = n_r = 0$.

Note that Definition 6.3 asks for a weaker condition than Definition 2.1 (ii). Furthermore, the condition from Definition 6.3 that the elements f_i have semimultiplicatively independent norms generalizes the following setting. Let $K = \mathbb{R}$, and $D = \mathbb{H}$ be the usual Hamilton quaternions. Then $\|\cdot\|$ is the fourth power of the Euclidean norm on $\mathbb{H}$ (see (2.2)). A collection $f_1, \dots, f_r \in \mathbb{H}^\times$ then automatically has semimultiplicatively independent norms as long as their Euclidean norms are all > 1. This condition already shows up in [Hua20].

Theorem 6.4. *Let D be a finite-dimensional division algebra over the field K of characteristic 0, let V be a K-subvariety of D not passing through the origin, let $f_1, \dots, f_r \in D^\times$ have semimultiplicatively independent norms, and let $\Gamma := \Gamma_{f_1,\dots,f_r}$ be the set:*

$$\Gamma = \{f_1^{n_1} \dots f_r^{n_r} : n_1, \dots, n_r \in \mathbb{N}\} \subseteq D^\times. \tag{6.2}$$

Then $|V \cap \Gamma| < \infty$.

Since both the hypothesis but also the conclusion in Theorem 6.4 are weaker than their counterparts from Theorem 2.2, neither theorem implies the other one.

Proof of Theorem 6.4. Our proof follows the exact same steps as the proof of Theorem 2.2 from Section 4. In particular, we re-state the condition that $\prod_{i=1}^r f_i^{n_i} \in V$ for some $(n_1, \dots, n_r) \in \mathbb{N}^r$ as the equation:

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} f^{\underline{n}, \boldsymbol{\sigma}} = 1, \tag{6.3}$$

for some suitable $a_{\boldsymbol{\sigma}} \in \overline{K}$, where $f^{\underline{n}, \boldsymbol{\sigma}}$ is defined as in equation (4.10) (see Section 4.1). Then assuming there exist infinitely many $\underline{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$ such that equation (6.3) holds, once again using Lemma 4.2 (as in Section 5) we derive the existence of a coset $\underline{c} + H$ of a subgroup $H \subseteq \mathbb{Z}^r$ with the property that for each of the infinitely many $\underline{n} \in (\underline{c} + H) \cap \mathbb{N}^r$, we have that equation (6.3) holds. An application of Lemma 3.2 yields then the existence of some nontrivial $\underline{x} := (x_1, \dots, x_r) \in \mathbb{N}_0^r$ with the property that for each $n \in \mathbb{N}$, we have that

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} f^{\underline{c}, \boldsymbol{\sigma}} (f^{\underline{x}, \boldsymbol{\sigma}})^n = 1. \tag{6.4}$$

Once again applying Lemma 3.3 (similar to its use in Subsection 5.2), we obtain that

$$\prod_{i=1}^r \prod_{j=1}^d \sigma_i^{(d,j)}(f_i)^{x_i} = 1, \tag{6.5}$$

for some $1 \le d \le M$ and suitable maps $\sigma_i^{(d,j)}$ as in Section 4.1. Finally, using Lemma 5.2, we conclude that there exists a positive integer b such that

$$\prod_{i=1}^r \|f_i\|^{bx_i} = 1. \tag{6.6}$$

Since each $x_i \in \mathbb{N}_0$, but not all of them are equal to 0, equation (6.6) yields a contradiction to our hypothesis that $f_1, \dots, f_r$ have semimultiplicatively independent norms. This contradiction shows that we must have finitely many r-tuples $(n_1, \dots, n_r) \in \mathbb{N}^r$ with the property that $f_1^{n_1} \cdots f_r^{n_r} \in V$, thus concluding our proof of Theorem 6.4. $\square$

6.2. **Proof of Theorem 6.2.** Finally, we can prove Theorem 6.2 as a consequence of Theorem 6.4. We need to use:

Theorem 6.5 ([Hua20, Theorem 1.2])**.** *Let Γ_1, Γ_2 be semigroups of $\mathbb{H}_a^\times$ generated by finitely many elements of norms greater than 1, and fix $a, a', b, b' \in \mathbb{H}_a^\times$. Then the equation*

$$afa' + bgb' = 1$$

has only finitely many solutions with $f \in \Gamma_1$ and $g \in \Gamma_2$ such that $|1 - afa'| \neq |afa'|$.

Proof of Theorem 6.2. We work under the hypotheses of Theorem 6.2. We claim that $|afa'| = |1-afa'|$ has only finitely many solutions with $f \in \Gamma_{f_1,\ldots,f_k}$. But we have seen in [Hua20, §5] that $|afa'| = |1-afa'|$ is equivalent to $f \in V$ for a certain $(\mathbb{R} \cap \bar{\mathbb{Q}})$-hyperplane V of $\mathbb{H}_a$ not passing through 0. Indeed, we may take

$$V = a^{-1} \cdot \{1/2 + \beta i + \gamma j + \delta k : \beta, \gamma, \delta \in \mathbb{R} \cap \bar{\mathbb{Q}}\} \cdot a'^{-1}.$$

Now by Theorem 6.4 and the fact that $f_1, \ldots, f_k$ have norms > 1 (and thus have semimultiplicatively independent norms), the claim follows.

Now let $\Gamma_1 = \langle f_1, \ldots, f_k \rangle$ and $\Gamma_2 = \langle g_1, \ldots, g_\ell \rangle$, and note that $\Gamma_{f_1,\ldots,f_k} \subseteq \Gamma_1$ as sets. By [Hua20, Theorem 1.2] above, $afa' + bgb' = 1$ has only finitely many solutions with $f \in \Gamma_{f_1,\ldots,f_k}$, $g \in \Gamma_2$, and $|1-afa'| \neq |afa'|$. On the other hand, the claim above implies that $afa' + bgb' = 1$ has only finitely many solutions with $f \in \Gamma_{f_1,\ldots,f_k}$, $g \in \Gamma_2$, and $|1-afa'| = |afa'|$. (Indeed, $f \in \Gamma_{f_1,\ldots,f_k}$, $|1-afa'| = |afa'|$ have only finitely many solutions, and the equation $afa' + bgb' = 1$ determines g uniquely once f is given.) Combining the above, the desired finiteness follows. □

References

[BGT10] J. P. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell-Lang problem for étale maps.* Amer. J. Math. **132** (2010), no. 6, 1655–1675.

[BGT16] J. P. Bell, D. Ghioca, and T. J. Tucker, *The Dynamical Mordell-Lang Conjecture.* Mathematical Surveys and Monographs **210** (2016), American Mathematical Society, Providence, RI, xiv+280 pp.

[BL15] J. P. Bell and J. C. Lagarias, *A Skolem-Mahler-Lech theorem for iterated automorphisms of K-algebras.* Canad. J. Math. **67** (2015), no. 2, 286–314.

[BSS17] J. P. Bell, M. Satriano, and S. J. Sierra, *On a dynamical Mordell-Lang conjecture for coherent sheaves.* J. Lond. Math. Soc. (2) **96** (2017), no. 1, 28–46.

[BGKT10] R. L. Benedetto, D. Ghioca, P. Kurlberg, and T. J. Tucker, *A gap principle for dynamics.* Compos. Math. **146** (2010), no. 4, 1056–1072.

[BGKT12] R. L. Benedetto, D. Ghioca, P. Kurlberg, and T. J. Tucker, *A case of the dynamical Mordell-Lang conjecture.* With an appendix by Umberto Zannier. Math. Ann. **352** (2012), no. 1, 1–26.

[CZ23] P. Corvaja and U. Zannier, *Finiteness theorems on elliptical billiards and a variant of the dynamical Mordell-Lang conjecture.* Proc. Lond. Math. Soc. (3) **127** (2023), no. 5, 1268–1337.

[Fak14] N. Fakhruddin, *The algebraic dynamics of generic endomorphisms of* $\mathbb{P}^n$. Algebra Number Theory **8** (2014), no. 3, 587–608.

[Fal91] G. Faltings, *The general case of S. Lang's conjecture.* Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), 175–182, Perspect. Math., **15**, Academic Press, San Diego, CA, 1994.

[GHSZ19] D. Ghioca, F. Hu, T. Scanlon, and U. Zannier, *A variant of the Mordell-Lang conjecture.* Math. Res. Lett. **26** (2019), no. 5, 1383–1392.

[GN17] D. Ghioca and K. D. Nguyen, *The orbit intersection problem for linear spaces and semiabelian varieties.* Math. Res. Lett. **24** (2017), no. 5, 1263–1283.

[GS23] D. Ghioca and S. Saleh, *Zariski dense orbits for endomorphisms of a power of the additive group scheme defined over finite fields.* J. Number Theory **244** (2023), 1–23.

[GT09] D. Ghioca and T. J. Tucker, *Periodic points, linearizing maps, and the dynamical Mordell-Lang problem.* J. Number Theory **129** (2009), no. 6, 1392–1403.

[GTZ08] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Intersections of polynomials orbits, and a dynamical Mordell-Lang conjecture.* Invent. Math. **171** (2008), no. 2, 463–483.

[GTZ11] D. Ghioca, T. J. Tucker, and M. E. Zieve, *The Mordell-Lang question for endomorphisms of semiabelian varieties.* J. Théor. Nombres Bordeaux **23** (2011), no. 3, 645–666.

[GTZ12] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Linear relations between polynomial orbits.* Duke Math. J. **161** (2012), no. 7, 1379–1410.

[Hua20] Y. Huang, *Unit equations on quaternions.* Q. J. Math. **71** (2020), no. 4, 1521–1534.

[Lau84] M. Laurent, *Équations diophantiennes exponentielles.* Invent. Math. **78** (1984), 299–327.

[LL19] J. Lesieutre and D. Litt, *Dynamical Mordell-Lang and automorphisms of blow-ups*. Algebr. Geom. **6** (2019), no. 1, 1–25.

[Mel21] J. Mello, *On intersections of polynomial semigroups orbits with plane lines*. Canad. Math. Bull. **64** (2021), no. 2, 442–451.

[Mel22] J. Mello, *On semigroup orbits of polynomials in multiplicative subgroups*. Monatsh. Math. **197** (2022), no. 1, 177–191.

[OS15] A. Ostafe and M. Sha, *On the quantitative dynamical Mordell-Lang conjecture*. J. Number Theory **156** (2015), 161–182.

[Pio19] D. Piontkovski, *Algebras of linear growth and the dynamical Mordell-Lang conjecture*. Adv. Math. **343** (2019), 141–156.

[Rou20] S. S. Rout, *The dynamical Mordell-Lang problem for intersection of two orbits*. J. Number Theory **207** (2020), 122–137.

[Sca11] T. Scanlon, *A Euclidean Skolem-Mahler-Lech-Chabauty method*. Math. Res. Lett. **18** (2011), no. 5, 833–842.

[SY14] T. Scanlon and Yu Yasufuku, *Exponential-polynomial equations and dynamical return sets*. Int. Math. Res. Not. **IMRN 2014**, no. 16, 4357–4367.

[Sch90] H. P. Schlickewei, *S-unit equations over number fields*. Invent. Math. **102** (1990), no. 1, 95–107.

[SV13] J. H. Silverman and B. Viray, *On a uniform bound for the number of exceptional linear subvarieties in the dynamical Mordell-Lang conjecture*. Math. Res. Lett. **20** (2013), no. 3, 547–566.

[Voj96] P. Vojta, *Integral points on subvarieties of semiabelian varieties, I*. Invent. Math. **126** (1996), no. 1, 133–181.

[Wan17] M.-X. Wang, *A dynamical Mordell-Lang property on the disk*. Trans. Amer. Math. Soc. **369** (2017), no. 3, 2183–2204.

[Xie17] J. Xie, *The dynamical Mordell-Lang conjecture for polynomial endomorphisms of the affine plane*. Astérisque No. **394** (2017), vi+110 pp.

Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Canada V6T 1Z2

Email address: dghioca@math.ubc.ca

Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Canada V6T 1Z2

Email address: huangyf@math.ubc.ca