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

DRAGOS GHIOCA AND YIFENG HUANG

Abstract. We advance a non-abelian variant of the classical Mordell-Lang conjecture in the context of division algebras. We also prove a first instance for our conjecture and also show through examples the relevance of the hypotheses in our question.

1. Introduction

We start by stating our notation for division algebras in Section 1.1 and also introduce Definition 1.1, which is key for our result.

1.1. **Notation.** Throughout this paper, let $\mathbb{N}$ denote the set of nonnegative integers, 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

$$|f| := \mathrm{Norm}_{K(f)/K}(f)^{[D:K(f)]} \in K. \tag{1.1}$$

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

$$P_1(x_1, \dots, x_\ell) = \cdots = P_m(x_1, \dots, x_\ell) = 0 \tag{1.2}$$

for some given polynomials $P_1, \dots, P_m \in K[t_1, \dots, t_\ell]$. A point of D, written as $\sum_{i=1}^{\ell} x_i \cdot y_i$ (for some $x_1, \dots, x_\ell \in K$), lies on V if and only if $(x_1, \dots, x_\ell)$ satisfies equation (1.2).

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 $a, b, c, d \in \overline{\mathbb{Q}} \cap \mathbb{R}$.

Definition 1.1. (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 $s_1^{n_1} \cdot \cdots \cdot s_r^{n_r} = 1$ imply $n_1 = \cdots = n_r = 0$.

(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.

[1] In this paper, a subvariety always refers to a closed subvariety.

1.2. **Our results.** Motivated by the classical S-unit equation (see [Sch90]) and also by the recent work of the second author on arithmetic questions in the noncommutative setting of division algebras [Hua20], we propose the following conjecture.

Conjecture 1.2. *Let K be a field of characteristic 0, let D be a finite dimensional division algebra over K, let Γ be a subgroup of $D^\times$ generated by finitely many elements with multiplicatively independent norms, and V be a K-subvariety of D not passing through 0. Then*

$$|V \cap \Gamma| < \infty. \tag{1.3}$$

Example 1.6 shows that in the absence of any hypothesis on the norms of the generators of Γ, the conclusion in Conjecture 1.2 may no longer be valid.

We view our Conjecture 1.2 as a non-abelian version of the classical Mordell-Lang conjecture (see Remark 1.9).

Our main result is the following weaker version of Conjecture 1.2 (see also our Theorem 4.2).

Theorem 1.3. *Let K, D be as above, V be a K-subvariety of D not passing through zero, $f_1, \dots, f_r \in D^\times$, and Γ be the set:*

$$\Gamma = \{f_1^{n_1} \cdot \dots \cdot f_r^{n_r} : n_1, \dots, n_r \in \mathbb{Z}\} \subseteq D^\times. \tag{1.4}$$

Then the following statements hold:

(i) If D is a field and V is a K-hyperplane, then $|V \cap \Gamma| < \infty$.
(ii) If $f_1, \dots, f_r$ have multiplicatively independent norms, then $|V \cap \Gamma| < \infty$.

The setting from Theorem 1.3 is also inspired by the Dynamical Mordell-Lang problem for finitely many endomorphisms (see Remark 1.10).

Using a result of the second author [Hua20, Thm. 1.2], a slight variant of our Theorem 1.3 (see Theorem 4.2) 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 1.5, we introduce the following notation.

Notation 1.4. 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 1.5. *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*

$$afa' + bgb' = 1 \tag{1.5}$$

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

1.3. **Remarks regarding our results.** We start by noting that in Conjecture 1.2, one needs to impose the condition the the variety V does not pass through the origin since otherwise there will be many examples for which the intersection (1.3) is infinite. Indeed, 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 Conjecture 1.2, as shown by the following example.

Example 1.6. 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 shows that for each positive integer n, there are some integers a_n and b_n such that:

$$f_1^n = a_n + b_n i \text{ and } f_2^n = \frac{a_n - b_n j}{5^{2n}},$$

where $a_n^2 + b_n^2 = 5^{2n}$. Then

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

and so, $f_1^n f_2^n \in V$ for all $n \in \mathbb{N}$; furthermore, these elements are all distinct. On the other hand, we also note that the hypothesis from Theorem 1.3 is not verified since $|f_1| \cdot |f_2| = 1$, i.e., f_1 and f_2 do not have multiplicatively independent norms.

Furthermore, the norm condition from Conjecture 1.2 is necessary even assuming $(D^\times, \cdot)$ is abelian, i.e., D/K is a finite field extension, as shown by the following example.

Example 1.7. We can take $K = \mathbb{R}$ and $D = \mathbb{R}(i) = \mathbb{C}$; each element $z \in D$ is then uniquely represented as $x + i \cdot y$ with $x, y \in K$. Then we may consider the variety V given by the equation $x^2 + y^2 = 1$; clearly, V is a K-variety which does not pass through 0. On the other hand, for any finitely generated subgroup Γ consisting of points in D of norm 1, we have $\Gamma \subset V$, thus showing that one cannot expect the intersection $V \cap \Gamma$ be finite even when V avoids 0, unless we assume a further condition on the generators of Γ. Note that in this example, each element of Γ has norm 1, which is the exact opposite of what we ask in Definition 1.1.

A similar construction as in Example 1.7 can be made also in a noncommutative setting; for example, one could consider $K = \mathbb{R}$, $D = \mathbb{H}$, $V = S^3$ (i.e., the variety consisting of all points of norm equal to 1) and then pick any $\Gamma \subset V$. Once again, the intersection $V \cap \Gamma$ is infinite even though V does not pass through 0; however, the elements of Γ have all norm equal to 1.

Remark 1.8. Example 1.7 shows that the conclusion from Theorem 1.3 (i) does not extend to arbitrary K-varieties V (not passing through 0). Also, Example 1.7 shows that the conclusion from Theorem 1.3 (ii) does not hold when $f_1, \dots, f_r$ do not have multiplicatively independent norms.

Next, our Remarks 1.9 and 1.10 explain why we view our Conjecture 1.2 and Theorem 1.3 as non-abelian variants of the Mordell-Lang conjecture.

Remark 1.9. Our Conjecture 1.2 has its genesis in the classical Mordell-Lang conjecture (proven by Faltings [Fal91] in the case of abelian varieties, and by Vojta [Voj96] for all semiabelian varieties). We were motivated by finding the points in common for an algebraic variety and a finitely generated group in a non-abelian setting; note that the classical Mordell-Lang conjecture asks precisely this question in the commutative setting of semiabelian varieties. Finding analogue statements to this classical problem to more general algebraic groups, beyond the world of semiabelian varieties is a difficult question in general (for more details, see [GHST19]).

It is tempting to relax the hypotheses in our Conjecture 1.2 and predict that if the corresponding intersection $V \cap \Gamma$ is infinite, then this is always explained by finitely many cosets of algebraic subgroups of $D^\times$ which live inside the variety V. However, Example 1.6 is a warning that this is not always the case.

Remark 1.10. Our Conjecture 1.2 was also inspired by the Dynamical Mordell-Lang Conjecture (see [BGT16] for a comprehensive discussion of this still open question from arithmetic dynamics).

Indeed, the Dynamical Mordell-Lang Conjecture predicts the shape of the intersection between a subvariety of some given ambient algebraic variety X endowed with an endomorphism Φ with an orbit (under Φ) of a point in X; for its precise statement, see [GT09]. Furthermore, one could consider an extension of the Dynamical Mordell-Lang Conjecture considering finitely many endomorphisms $\Phi_i : X \longrightarrow X$ (for $i = 1, \dots, r$) and for a given subvariety $V \subseteq X$ and a given point $\alpha \in X$, then study the set $\mathcal{S}$ of r-tuples $(n_1, \dots, n_r) \in \mathbb{N}^r$ for which

$$\left(\Phi_1^{\circ n_1} \circ \cdots \circ \Phi_r^{\circ n_r}\right)(\alpha) \in V.$$

It is natural then to ask under which hypotheses, the above set $\mathcal{S}$ is finite, or perhaps, it is a union of a finite set with finitely many cosets of subsemigroups of $\mathbb{N}^r$. This problem turns out to be very subtle (even in the case when the ambient space X is a semiabelian variety and each Φ_i is a group endomorphism of X), as it was explained in [GTZ11].

Note that in Theorem 1.3, one could consider the maps $\Phi_i : D \longrightarrow D$ given by $x \mapsto f_i \cdot x$ (for $i = 1, \dots, r$) and then the conclusion in Theorem 1.3 is another instance of the above Dynamical Mordell-Lang question (for finitely many maps), but this time in a non-abelian setting.

1.4. **Plan for our paper.** In Section 2 we state a couple of useful facts that will be used in our proof of Theorem 1.3. Then we prove Theorem 1.3 in Section 3. Finally, in Section 4, we state and prove Theorem 4.2 and then derive Theorem 1.5 as an easy consequence of Theorem 4.2 coupled with [Hua20, Thm. 1.2].

2. Preliminaries

In this Section 2, we gather a couple of technical results to be employed in our proofs.

2.1. **The classical Mordell-Lang.** Our key tool is the classical Mordell-Lang theorem for tori, proven by Laurent. We state the following version of it, that can be deduced immediately from [Lau84].

Theorem 2.1 (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 $\{(n_1, \dots, n_r) : \varphi(n_1, \dots, n_r) \in V(L)\}$ is a finite union of cosets of subgroups of $\mathbb{Z}^r$.*

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

Lemma 2.2. *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 $i\ge 2$) 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 $\underline{c}_1+H_1$. Because all elements of $\underline{c}_1+H_1$ have their first entry equal to j, all elements in H_1 have their first entry equal to 0. Furthermore, H_1 is a subgroup of H.

Now $(\underline{c}_1+H_1)\cap\mathbb{N}^{m+1}$ 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 2.2. □

2.3. **Reduction to hypersurface case.** The following observation shows that in Theorem 1.3 we may assume without generality that V is a hypersurface not containing 0.

Lemma 2.3. *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 $\underline{0}=(0,\dots,0)$. Then there is a K-hypersurface of $\mathbb{A}^\ell(K)$ not passing through $\underline{0}$ that contains V.*

Proof. Say (1.2) is the equation that cuts out 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 $P_j(x_1,\dots,x_l)=0$ then does the job. □

3. Proof of Theorem 1.3

In this Section 3, we work under the hypotheses of Theorem 1.3. We start with a useful reduction for the case (i) in Theorem 1.3.

3.1. **In case (i) of Theorem 1.3, it suffices to assume $f_1,\dots,f_r$ are multiplicatively independent.** We assume in this Section 3.1 that $(D^\times,\cdot)$ is abelian and therefore, D/K is a finite field extension. Thus, Γ is actually the subgroup of $(D^\times,\cdot)$ spanned by $f_1,\dots,f_r$. So, since it is a finitely generated abelian group, we have that Γ is the direct product of a torsion-free finitely generated abelian subgroup Γ_0 with a finite torsion subgroup Γ_1. Thus

$$V\cap\Gamma=\bigcup_{\gamma\in\Gamma_1}V\cap(\gamma\cdot\Gamma_0)=\bigcup_{\gamma\in\Gamma_1}\gamma\cdot\left(\left(\gamma^{-1}\cdot V\right)\cap\Gamma_0\right), \tag{3.1}$$

where for each $\gamma\in D^\times$, the variety $V_\gamma:=\gamma^{-1}\cdot V$ is another K-hyperplane not passing through the origin.

So, equation (3.1) reduced case (i) of Theorem 1.3 to the intersection between a finitely generated torsion-free subgroup of $D^\times$ with a subvariety not passing through $0\in D$. Therefore, we may assume from now on, that in case (i) of Theorem 1.3, we have that the elements $f_1,\dots,f_r\in D^\times$ are multiplicatively independent (again, note that in this case (i), we have that D is itself a field).

3.2. **Conversion to an exponential equation.** We continue with our proof of Theorem 1.3; this argument now is common to both parts (i) and (ii) in Theorem 1.3.

As the first new ingredient in our argument, we convert the equation

$$f_1^{n_1}\cdot\dots\cdot f_r^{n_r}\in V \tag{3.2}$$

into an exponential equation in a commutative setting, to be detailed in this section. Fix an algebraic closure $\overline{K}$ of K. By looking at the subfields $K(f_i)$ of D, there are subfields L_i of $\overline{K}$ that are finite extensions of K, embeddings $\kappa_i : L_i \to D$ as K-algebras, and elements $g_i \in L_i$ such that $\kappa_i(g_i) = f_i$.

By Lemma 2.3, we may assume from now on that V is a K-hypersurface of D not passing through 0. Thus, there is $M \geq 1$ and for each $1 \leq d \leq M$ a d-fold K-multilinear form $\Theta_d : D \times \cdots \times D \to K$ such that V is cut out by the equation

$$\Theta_1(z) + \Theta_2(z, z) + \cdots + \Theta_M(z, \dots, z) = 1. \tag{3.3}$$

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

$$\theta_d(z_1^{(1)},\dots,z_r^{(1)},\dots,z_1^{(d)},\dots,z_r^{(d)}) := \Theta_d(\kappa_1(z_1^{(1)})\dots\kappa_r(z_r^{(1)}),\dots,\kappa_1(z_1^{(d)})\dots\kappa_r(z_r^{(d)})). \tag{3.4}$$

Then the equation (3.2) becomes

$$\theta_1(g_1^{n_1},\dots,g_r^{n_r}) + \theta_2(g_1^{n_1},\dots,g_r^{n_r},g_1^{n_1},\dots,g_r^{n_r}) + \cdots + \theta_M(g_1^{n_1},\dots,g_r^{n_r},\dots,g_1^{n_1},\dots,g_r^{n_r}) = 1. \tag{3.5}$$

To better understand the exponential equation (3.5), we rewrite the multilinear maps θ_d more explicitly. For $1 \leq i \leq r$, let $G_i = \{\sigma_i : L_i \to \overline{K}\}$ be the set of K-embeddings from 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 $\mathrm{Hom}_K(L_i, \overline{K})$. Therefore, the $\overline{K}$-vector space

$$\mathrm{Hom}_K((L_1 \otimes_K \cdots \otimes_K L_r)^{\otimes_K d}, \overline{K}) = (\mathrm{Hom}_K(L_1, \overline{K}) \otimes_{\overline{K}} \cdots \otimes_{\overline{K}} \mathrm{Hom}_K(L_r, \overline{K}))^{\otimes_{\overline{K}} d} \tag{3.6}$$

has a basis given by $G^d = G \times \dots G$ (d-fold), where $G := G_1 \times \cdots \times G_r$. Here, $(\cdot)^{\otimes_K d}$ denotes the d-fold tensor product over K. As a result, there are elements $a_{\sigma^{(1)},\dots,\sigma^{(d)}}$ indexed by $(\sigma^{(1)},\dots,\sigma^{(d)}) \in G^d$, uniquely determined by θ_d, such that we have for $z_i \in L_i$

$$\theta_d(z_1,\dots,z_r,\dots,z_1,\dots,z_r) = \sum_{\sigma^{(1)},\dots,\sigma^{(d)}\in G} a_{\sigma^{(1)},\dots,\sigma^{(d)}}\, z^{\sigma^{(1)}}\dots z^{\sigma^{(d)}}, \tag{3.7}$$

where for any $\sigma = (\sigma_1,\dots,\sigma_r) \in G$, we define $z^\sigma := \sigma_1(z_1)\dots\sigma_r(z_r)$. (The product takes place in $\overline{K}$, which we have fixed.) If $\underline{n} = (n_1,\dots,n_r)$ is in $\mathbb{Z}^r$, then (3.7) gives

$$\theta_d(g_1^{n_1},\dots,g_r^{n_r},\dots,g_1^{n_1},\dots,g_r^{n_r}) = \sum_{\sigma^{(1)},\dots,\sigma^{(d)}\in G} a_{\sigma^{(1)},\dots,\sigma^{(d)}}\, g^{\underline{n},\sigma^{(1)}}\dots g^{\underline{n},\sigma^{(d)}}, \tag{3.8}$$

where

$$g^{\underline{n},\sigma} := \prod_{i=1}^r \sigma_i(g_i)^{n_i}. \tag{3.9}$$

Also, we note that in the case D/K is a finite field extension (which is the part (i) in Theorem 1.3), the equation (3.8) can be written even more explicit since we can take $g_i = f_i$

for each $i = 1, \dots, r$ (since already D/K is a finite field extension), and we may apply the argument leading to (3.7) directly to Θ_d, yielding its $r = 1$ analog:

$$\Theta_d(z, \dots, z) = \sum_{\sigma^{(1)}, \dots, \sigma^{(d)} \in G} a_{\sigma^{(1)}, \dots, \sigma^{(d)}} \sigma^{(1)}(z) \dots \sigma^{(d)}(z), \tag{3.10}$$

where G is now simply the set of K-embeddings from D to $\overline{K}$. Therefore, the counterpart of equation (3.8) is simply the equation:

$$\theta_d(f_1^{n_1}, \dots, f_r^{n_r}) = \sum_{\sigma^{(1)}, \dots, \sigma^{(d)} \in G} a_{\sigma^{(1)}, \dots, \sigma^{(d)}} f^{\underline{n}, \sigma^{(1)}} \dots f^{\underline{n}, \sigma^{(d)}}, \tag{3.11}$$

where $f^{\underline{n}, \sigma} := \prod_{i=1}^r \sigma(f_i)^{n_i}$.

In conclusion, the equation (3.2) (in both parts (i) and (ii)) is converted to an exponential equation

$$\sum_{d=1}^{M} \sum_{\sigma^{(d,1)}, \dots, \sigma^{(d,d)} \in G} a_{\sigma^{(d,1)}, \dots, \sigma^{(d,d)}} g^{\underline{n}, \sigma^{(d,1)}} \dots g^{\underline{n}, \sigma^{(d,d)}} = 1 \tag{3.12}$$

for some coefficients $a_{\sigma^{(d,1)}, \dots, \sigma^{(d,d)}} \in \overline{K}$ that are determined by the equation of the hypersurface V. Of course, $a_{\sigma^{(d,1)}, \dots, \sigma^{(d,d)}}$ 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 $\mathbf{G} := G \sqcup G^2 \sqcup \dots \sqcup G^M$, so a typical element of $\mathbf{G}$ is of the form $\boldsymbol{\sigma} = (\sigma^{(d,1)}, \dots, \sigma^{(d,d)})$ for some $1 \leq d \leq M$ that is part of the data in $\boldsymbol{\sigma}$. For this $\boldsymbol{\sigma}$, define

$$g^{\underline{n}, \boldsymbol{\sigma}} := g^{\underline{n}, \sigma^{(d,1)}} \dots g^{\underline{n}, \sigma^{(d,d)}}. \tag{3.13}$$

Then we may rewrite (3.12) compactly as

$$\sum_{\boldsymbol{\sigma} \in \mathbf{G}} a_{\boldsymbol{\sigma}} g^{\underline{n}, \boldsymbol{\sigma}} = 1. \tag{3.14}$$

3.3. **Reduction of our question to a classical Mordell-Lang type problem.** The following lemma is instrumental for our proof of Theorem 1.3.

Lemma 3.1. *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*

$$\varphi(n_1, \dots, n_r) = f_1^{n_1} \dots f_r^{n_r}, \tag{3.15}$$

where $r \geq 1$ 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 §3.2 but without the assumption that V does not pass through 0, $\varphi^{-1}(V)$ is the set of $\underline{n} = (n_1, \dots, n_r)$ that solves the equation

$$\sum_{\boldsymbol{\sigma} \in \mathbf{G}} a_{\boldsymbol{\sigma}} g^{\underline{n}, \boldsymbol{\sigma}} = \epsilon, \tag{3.16}$$

with the notation $\mathbf{G}$, $a_{\boldsymbol{\sigma}}$, and $g^{\underline{n},\boldsymbol{\sigma}}$ as in §3.2, and where $\epsilon = 0$ or 1 depending on whether V passes through 0 or not. 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

$$\psi(\underline{n}) := (g^{\underline{n},\boldsymbol{\sigma}})_{\boldsymbol{\sigma}\in\mathbf{G}}. \tag{3.17}$$

Then it is clear from the definition that ψ is a group homomorphism. Consider a $\overline{K}$-subvariety of T defined by

$$W := \left\{ (z_{\boldsymbol{\sigma}})_{\boldsymbol{\sigma}\in\mathbf{G}} : \sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} z_{\boldsymbol{\sigma}} = \epsilon \right\} \cap T. \tag{3.18}$$

The construction implies $\varphi^{-1}(V) = \psi^{-1}(W)$, so the desired conclusion follows from Theorem 2.1. $\square$

3.4. **Conclusion of our proof for Theorem 1.3.** We bring back the assumption that V is a hypersurface not passing through 0. Recall from §3.2 that the equation $f_1^{n_1} \dots f_r^{n_r} \in V$ can be rewritten as

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} g^{\underline{n},\boldsymbol{\sigma}} = 1; \tag{3.19}$$

furthermore, in part (i) of Theorem 1.3, the above equation (3.19) becomes even more explicit:

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} f^{\underline{n},\boldsymbol{\sigma}} = 1. \tag{3.20}$$

Moreover, the conclusion of Lemma 3.1 states that the set of $\underline{n} \in \mathbb{Z}^r$ that solve (3.19) is a finite union of cosets of $\mathbb{Z}^r$.

Assume the contrary of the conclusion of Theorem 1.3, i.e., $|V \cap \Gamma| = \infty$. Then (3.19) 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 (3.19) restricted to $\underline{c} + \mathbb{Z}\underline{x}$ yields

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} g^{\underline{c}+n\underline{x},\boldsymbol{\sigma}} = 1, \tag{3.21}$$

or

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} g^{\underline{c},\boldsymbol{\sigma}} (g^{\underline{x},\boldsymbol{\sigma}})^n = 1, \tag{3.22}$$

for all $n \in \mathbb{Z}$. By elementary facts about the Vandermonde matrix (see also [GS23, Lemma 2.3]), sequences α^n for distinct $\alpha \in \overline{K}$ are $\overline{K}$-linearly independent. It follows that there exists $\boldsymbol{\sigma} \in \mathbf{G}$ such that $g^{\underline{x},\boldsymbol{\sigma}} = 1$, or

$$\prod_{j=1}^{d} \prod_{i=1}^{r} \sigma_i^{(d,j)} (g_i)^{x_i} = 1 \tag{3.23}$$

for some $1 \le d \le M$ and $\sigma^{(d,1)}, \dots, \sigma^{(d,d)} \in G$.

Furthermore, assuming we are in part (i) of Theorem 1.3, since we know $M = 1$, that we could take $g_i = f_i$ for each $i = 1, \dots, r$ (see also equation (3.20)), and that we can take G to be the set of K-embeddings $\sigma : D \longrightarrow \overline{K}$, the equation (3.23) reads:

$$\prod_{i=1}^{r} \sigma(f_i)^{x_i} = 1, \tag{3.24}$$

for some suitable K-embedding $\sigma : D \longrightarrow \overline{K}$. In particular, equation (3.24) yields

$$\prod_{i=1}^{r} f_i^{x_i} = 1. \tag{3.25}$$

Equation (3.25) already provides the desired contradiction in case (i) of Theorem 1.3 because the fact that not all integers x_i are equal to 0 in equation (3.25) contradicts the fact that $f_1, \dots, f_r$ are multiplicatively independent (see our reduction from Section 3.1).

Next, we work towards obtaining the conclusion in part (ii) of Theorem 1.3. The following lemma provides the desired contradiction; furthermore, this next result will also be used in our proof of Theorem 4.2.

Lemma 3.2. *With the above notation, assume equation* (3.23) *holds for some* $x_1, \dots, x_r \in \mathbb{Z}$. *Then there exists a positive integer* b *such that*

$$\prod_{i=1}^{r} |f_i|^{bx_i} = 1. \tag{3.26}$$

Proof of Lemma 3.2. We take a large enough finite extension L/K in $\overline{K}$ such that $L \supseteq L_i$ (see also our notation from Section 3.2) 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 (3.23) yields

$$1 = \prod_{i=1}^{r} \mathrm{Norm}_{L/K}(g_i)^{dx_i} = \prod_{i=1}^{r} \mathrm{Norm}_{L_i/K}(g_i)^{[D:L_i]dmx_i}. \tag{3.27}$$

Using Definition 1.1 and setting $b = dm$, we obtain precisely the content of the desired equation (3.26). □

Since not all integers x_i from equation (3.26) (see Lemma 3.2) are equal to 0 (while b is a positive integer), we see that equation (3.26) contradicts the assumption that $f_1, \dots, f_r$ have multiplicatively independent norms. This contradiction finishes our proof of part (ii) and therefore, concludes our proof for Theorem 1.3.

4. Proofs of two other results related to Theorem 1.3

In Section 4.1, we state and prove Theorem 4.2; then in Section 4.2, we prove Theorem 1.5.

4.1. A variant of Theorem 1.3.

In order to state Theorem 4.2, we need the following definition.

Definition 4.1. 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 $n_1, \dots, n_r \in \mathbb{N}$, then we must have $n_1 = \cdots = n_r = 0$.

Note that Definition 4.1 asks for a weaker condition than Definition 1.1 (ii). Furthermore, the condition from Definition 4.1 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 length on $\mathbb{H}$. A collection $f_1, \dots, f_r \in \mathbb{H}^\times$ then automatically has semimultiplicatively independent norms as long as their Euclidean lengths are all > 1. This condition already shows up in [Hua20].

Theorem 4.2. *Let, as before, 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:*

$$\Gamma = \{f_1^{n_1} \dots f_r^{n_r} : n_1, \dots, n_r \in \mathbb{N}\} \subseteq D^\times. \tag{4.1}$$

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

Since both the hypothesis but also the conclusion in Theorem 4.2 are weaker than their counterparts from Theorem 1.3, neither theorem implies the other one.

Proof of Theorem 4.2. Our proof follows the exact same steps as the proof of Theorem 1.3 from Section 3. 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:

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} g^{\underline{n},\boldsymbol{\sigma}} = 1, \tag{4.2}$$

for some suitable $a_{\boldsymbol{\sigma}} \in \overline{K}$, where $g^{\underline{n},\boldsymbol{\sigma}}$ is defined as in equation (3.13) (see Section 3.2). Then assuming there exist infinitely many $\underline{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$ such that equation (4.2) holds, once again using Lemma 3.1 (as in Section 3.4) 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 (4.2) holds. An application of Lemma 2.2 yields then the existence of some nontrivial $\underline{x} := (x_1, \dots, x_r) \in \mathbb{N}^r$ with the property that for each $n \in \mathbb{N}$, we have that

$$\sum_{\boldsymbol{\sigma}} a_{\boldsymbol{\sigma}} g^{\underline{c},\boldsymbol{\sigma}} (g^{\underline{x},\boldsymbol{\sigma}})^n = 1. \tag{4.3}$$

Once again applying [GS23, Lemma 2.3] (which is a basic application of the classical Vandermonde determinants), we obtain that

$$\prod_{i=1}^r \prod_{j=1}^d \sigma_i^{(d,j)}(g_i)^{x_i} = 1, \tag{4.4}$$

for some $1 \le d \le M$ and suitable maps $\sigma_i^{(d,j)}$ as in Section 3.2. Finally, using Lemma 3.2, we conclude that there exists a positive integer b such that

$$\prod_{i=1}^r |f_i|^{bx_i} = 1. \tag{4.5}$$

Since each $x_i \in \mathbb{N}$, but not all of them are equal to 0, equation (4.5) 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 4.2. ☐

4.2. **Proof of Theorem 1.5.** Finally, we can prove Theorem 1.5 as a consequence of Theorem 4.2.

So, we work under the hypotheses of Theorem 1.5. Then, by [Hua20, Thm. 1.2], it suffices to show that $|afa'| = |1 - afa'|$ has only finitely many solutions with $f \in \Gamma_{f_1,\dots,f_k}$. 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. By Theorem 4.2 and the fact that $f_1, \dots, f_k$ have norms > 1 (and thus have semimultiplicatively independent norms), the desired finiteness follows.

References

[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.

[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.

[GHST19] 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.

[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.

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

[Hru96] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), no. 3, 667–690.

[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.

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

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

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