# Two Special Cases of the Dynamical Mordell-Lang Conjecture in Positive Characteristic

by

Kristina Nelson

B.Sc., The University of British Columbia, 2015

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate and Postdoctoral Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

April 2017

# Abstract

We prove the positive characteristic version of the Dynamical Mordell-Lang Conjecture in two novel cases. Let $p$ be a prime and $K$ a field of characteristic $p > 0$. Let $k \in \mathbb{N}$, $\alpha \in \mathbb{G}_m^k(K)$ and $V \subset \mathbb{G}_m^k$ be a variety. Let $\varphi : \mathbb{G}_m^k \to \mathbb{G}_m^k$ be a group endomorphism defined over $K$. We know

$$\varphi(x_1, x_2, ..., x_k) = (x_1^{a_{1,1}} x_2^{a_{1,2}} \cdots x_k^{a_{1,k}}, ..., x_1^{a_{k,1}} x_2^{a_{k,2}} \cdots x_k^{a_{k,k}})$$

for some $a_{i,j} \in \mathbb{Z}$. In the case where the matrix of exponents, $(a_{i,j})$ is similar to a single Jordan block, we show that the set $S = \{n \in \mathbb{N} : \varphi^n(\alpha) \in V\}$ is a finite union of arithmetic progressions. When the dimension $k = 3$, we show $S$ is a finite union of arithmetic progressions for any group endomorphism $\varphi$.

# Preface

The topic and general ideas behind this thesis were the suggestion of my advisor, Prof. Dragos Ghioca. Examples 1.1 was previously published in [2] and Examples 5.1 and 5.2 appeared in [3]. The remainder of this thesis is the original, unpublished work of the author.

# Table of Contents

# Acknowledgements

I would like to thank my advisor, Prof. Dragos Ghioca, not only for his guidance with regard to this thesis, but also for his wisdom and advice regarding my adventures in academia and mathematics.

Thank you also, dad, for telling me seven years ago I just *had* to go to UBC and take Science One.

# Chapter 1

# Introduction

Let $K$ be a characteristic zero field, $X$ a quasiprojective variety, $\alpha \in X$ a point, $\varphi$ an endomorphism of $X$ defined over $K$, and $V \subset X$ a subvariety. As is usual in arithmetic dynamics we write $\varphi^n(\alpha) = \varphi \circ \varphi \circ \cdots \circ \varphi(\alpha)$ to denote $n$ applications of the endomorphism. Given this, the dynamical Mordell-Lang Conjecture predicts that the set

$$S := \{n \in \mathbb{N} : \varphi^n(\alpha) \in V\} \tag{1.1}$$

is a finite union of arithmetic progressions. Here, as in the remainder of this note, a singleton set is considered an arithmetic progression with common difference zero between its terms.

The dynamical Mordell-Lang Conjecture has been shown to hold under certain conditions [1, 4, 5, 6, 9]. For a full survey of recent progress on the dynamical Mordell-Lang Conjecture readers may review [2]. A natural extension of the conjecture is to positive characteristic $K$, however in this case counterexamples immediately arise where $S$ cannot be written as any finite union of arithmetic progressions. See Example 1.1 below, and Chapter 5 for further examples. In the following, as in the rest of this note, $\mathbb{N}_0$ denotes the set of non-negative integers.

**Example 1.1.** *Let $K = \overline{\mathbb{F}_p}(t)$. Let $\alpha = (1, t, 1, 1-t) \in \mathbb{G}_m^4$, and define $\varphi : \mathbb{G}_m^4 \to \mathbb{G}_m^4$ by*

$$\varphi(x_1, x_2, x_3, x_4) = (x_1x_2, x_2, x_3x_4, x_4).$$

*Then*

$$\varphi^n(\alpha) = (t^n, t, (1-t)^n, (1-t)).$$

*Let $f(x_1, x_2, x_3, x_4) = x_1 + x_3 - 1$. We take $V = Z(f) = \{\beta \in \mathbb{G}_m^4(K) : f(\beta) = 0\}$ and show in this case the set $S$ of (1.1) is not a finite union of*

*arithmetic progressions. Let $n = mp^j$ for $m$ coprime to $p$, and $j \in \mathbb{N}_0$. Then*

$$\begin{aligned} f(\varphi^n(\alpha)) &= t^{mp^j} + (1-t)^{mp^j} - 1 \\ &= t^{mp^j} + \sum_{i=0}^{m} \binom{m}{i} (-t)^{ip^j} - 1. \end{aligned}$$

*If $m > 1$ then $f(\varphi^n(\alpha))$ contains a non-zero term of the form $m(-t)^{p^j}$, contributed by the $i = 1$ term of the sum. Given this, it is easy to see $f(\varphi^n(\alpha)) = 0$ occurs if and only if $m = 1$. Thus the set of $n \in \mathbb{N}$ such that $\varphi^n(\alpha)$ is in $Z(f)$ is $\{p^j : j \in \mathbb{N}_0\}$. Note that this is not a finite union of arithmetic progressions.*

So, the dynamical Mordell-Lang Conjecture as stated above fails in positive characteristic. However, motivated by results of Moosa and Scanlon [8], the following positive characteristic version of Dynamical Mordell-Lang conjecture was proposed [2, Conjecture 13.2.0.1]. Here, as in the remainder of this note, $[m]$ denotes the set of integers $\{1, ..., m\}$.

**Conjecture 1.2.** *(Ghioca-Scanlon). Let $K$ be a field of characteristic $p > 0$, $X$ a quasiprojective variety, $V$ a subvariety, $\alpha \in X(K)$ a point and $\varphi$ an endomorphism of $X$ defined over $K$. Then the set $S = \{n \in \mathbb{N} : \varphi^n(\alpha) \in V\}$ is a finite union of arithmetic progressions, along with finitely many sets of the form*

$$\left\{ \sum_{j=1}^{m} c_j p^{k_j n_j} : n_j \in \mathbb{N}_0 \text{ for each } j \in [m] \right\}, \tag{1.2}$$

*for some $c_j \in \mathbb{Q}$, and $k_j \in \mathbb{N}$.*

To describe the cases of this conjecture under consideration in this note, we introduce the following notation. In the case where $X = \mathbb{G}_m^k$ for some $k \in \mathbb{N}$ and $\varphi$ is a group endomorphism of $\mathbb{G}_m^k$, we have that $\varphi$ is given by

$$\varphi(x_1, x_2, ..., x_k) = (x_1^{a_{1,1}} x_2^{a_{1,2}} \cdots x_k^{a_{1,k}}, ..., x_1^{a_{k,1}} x_2^{a_{k,2}} \cdots x_k^{a_{k,k}}) \tag{1.3}$$

for some $a_{i,j} \in \mathbb{Z}$, and all $(x_1, x_2, ..., x_k) \in \mathbb{G}_m^k$. Let $A$ be a matrix with $(A)_{i,j} = a_{i,j} \in \mathbb{Z}$. Then we denote the endomorphism of (1.3) with $\varphi_A = \varphi$. Since the matrix of $\varphi_A \circ \varphi_B$ is simply $A \cdot B$, we have in general that $\varphi_A^n = \varphi_{A^n}$.

Conjecture 1.2 has been proven in [2], in the case where $X = \mathbb{G}_m^k$ and $\varphi = \varphi_A$ for a diagonalizable matrix $A$ (see Proposition 4.1). Conjecture 1.2 has also been proven by [3] when $X = \mathbb{G}_m^k$, $\varphi$ is any regular self-map, and the variety $V$ is a curve. We prove the conjecture in the following two novel cases.

**Theorem 1.3.** *Let $K$ be a field of characteristic $p > 0$. Let the group endomorphism $\varphi_A : \mathbb{G}_m^k \to \mathbb{G}_m^k$ be defined by*

$$\varphi(x_1, ..., x_k) = (x_1^{a_{1,1}} x_2^{a_{1,2}} \cdots x_k^{a_{1,k}}, ..., x_1^{a_{k,1}} x_2^{a_{k,2}} \cdots x_k^{a_{k,k}})$$

*for some $a_{i,j} \in \mathbb{Z}$, and assume that the matrix $A = (a_{i,j})$ is similar to a single Jordan block. Let $V \subset \mathbb{G}_m^k$ be a variety, and $\alpha \in \mathbb{G}_m^k(K)$ a point. Then the set*

$$S = \{n \in \mathbb{N} : \varphi_A^n(\alpha) \in V\}$$

*is a finite union of arithmetic progressions.*

**Theorem 1.4.** *Let $K$ be a field of characteristic $p > 0$. Let $\varphi : \mathbb{G}_m^3 \to \mathbb{G}_m^3$ be a group endomorphism, let $V \subset \mathbb{G}_m^3$ be a variety, and $\alpha \in \mathbb{G}_m^3(K)$ a point. Then the set*

$$S = \{n \in \mathbb{N} : \varphi^n(\alpha) \in V\}$$

*is a finite union of arithmetic progressions.*

As we can see, in these cases the more complicated sets of (1.2) do not even arise.

# Chapter 2

# Preliminaries

## 2.1 Notation

Throughout the remainder of this note, $K$ will be a field of characteristic $p > 0$. We set $X = \mathbb{G}_m^k$ for $k \in \mathbb{N}$ and suppose $\varphi$ is a group endomorphism of $\mathbb{G}_m^k$. A *function field* $E$ over field $F$ is a finitely generated field extension, $E/F$, of positive transcendence degree. We will often consider the case where $K$ is a function field over $\overline{\mathbb{F}_p}$.

In this note an arithmetic progression $\mathcal{N}$ is a subset of $\mathbb{N}$ of the form

$$\mathcal{N} = \{b + d \cdot i : i \in \mathbb{N}_0\},$$

for some $b \in \mathbb{N}$ and $d \in \mathbb{N}_0$. Note that $\mathcal{N}$ may be a singleton set if $d = 0$, otherwise $\mathcal{N}$ is infinite.

Given polynomials $f_1, ..., f_m \in K[x_1, ..., x_k]$ we use $Z(f_1, ..., f_m)$ to denote their zero locus in $\mathbb{G}_m^k$. That is, the points of $Z(f_1, ..., f_m)$ in $K$ are

$$\left\{\beta \in \mathbb{G}_m^k(K) : f_i(\beta) = 0,\ \forall\, i \in [m]\right\}.$$

For the sake of brevity, we invent the following notation. Given $V \subset \mathbb{G}_m^k$ a variety, $\alpha = (\alpha_1, ..., \alpha_k) \in \mathbb{G}_m^k(K)$, $A \in M_{k\times k}(\mathbb{Z})$, and $\mathcal{N}$, we let $S = S(V, \alpha, A, \mathcal{N}) = \{n \in \mathcal{N} : \varphi_A^n(\alpha) \in V\}$. Given a matrix $A \in M_{k\times k}(\mathbb{Z})$, we say '$S(A)$ is a finite union of arithmetic progressions' if

$$S = S(V, \alpha, A, \mathcal{N}) = \{n \in \mathcal{N} : \varphi_A^n(\alpha) \in V\}$$

is indeed a finite union of arithmetic progressions for any choice of variety $V \subset \mathbb{G}_m^k$, $\alpha \in \mathbb{G}_m^k(K)$ and arithmetic progression $\mathcal{N}$.

**Definition 2.1.** *We say a sequence $(a_n)_{n=0}^{\infty}$ is preperiodic if there exists $N, d \in \mathbb{N}$ such that for all $n > N$, $a_n = a_{n-d}$.*

*Given a point $\alpha$ of quasiprojective variety $X$ and an endomorphism $\varphi : X \to X$, we say $\alpha$ is a preperiodic point of $\varphi$ if the sequence $(\varphi^i(\alpha))_{i=1}^{\infty}$ is preperiodic.*

**Definition 2.2.** *An absolute value on the field $F$ is a map $|\cdot|_v : F \to \mathbb{R}$ such that:*

- *$|x|_v \geq 0$ for all $x \in F$ and $|x|_v = 0$ if and only if $x = 0$.*
- *$|xy|_v = |x|_v|y|_v$ for all $x, y \in F$.*
- *$|x + y|_v \leq |x|_v + |y|_v$ for all $x, y \in F$.*

*Furthermore, we say that an absolute value $|\cdot|_v$ on $F$ is non-archimedean if*

- *$|x + y|_v \leq \max(|x|_v, |y|_v)$ for all $x, y \in F$.*

In this paper $F$ will usually be a field of positive characteristic. Every absolute value on a field of positive characteristic is non-archimedian [7, Chapter 1, Section 1].

**Definition 2.3.** *Field $F$ is said to be a Product Formula Field if the following conditions are satisfied:*

- *There exists a set of absolute values on $F$, $M_F$.*
- *For any fixed $x \in F^{\times}$, $|x|_v \neq 1$ holds for only finitely many $|\cdot|_v \in M_F$.*
- *There exists a function $M_F \to \mathbb{N}$ with its value at $|\cdot|_v \in M_F$ denoted by $N_v$, such that the following product formula holds:*

$$\prod_{|\cdot|_v \in M_k} |x|_v^{N_v} = 1 \text{ for all } x \in F^{\times}. \tag{2.1}$$

In this note we rely on the fact that any function field $F$ is a product formula field, see [7, Chapter 2] for background and details. By replacing every $|\cdot|_v$ in the standard set of absolute values with $|\cdot|_v^{N_v}$ we may assume the set is *normalized* with $N_v = 1$ for all $|\cdot|_v$. For simplicity we make this the definition of $M_F$.

**Definition 2.4.** *Let $M_K$ be a normalized, standard set of absolute values on $K$.*

We also have the following fact from the theory of absolute values on function fields.

**Fact 2.5.** *If $K$ is a function field over the field of constants $\overline{\mathbb{F}_p}$, and $|x|_v = 1$ for all $|\cdot|_v \in M_K$, then $x \in \overline{\mathbb{F}_p}$. See [7, Chapter 2, Section 5].*

## 2.2 Lemmas

The following results will be used by Chapters 3 and 4, and will help us reduce certain instances of the problem to other already solved cases.

### On Arithmetic Progressions

**Proposition 2.6.**

1. *For all $i \in [\ell]$, let $S_i$ be a finite union of arithmetic progressions. Then $\cap_{i=1}^{\ell} S_i$ is also a finite union of arithmetic progressions.*

2. *The complement of a finite union of arithmetic progressions is another finite union of arithmetic progressions.*

Part (1) of Proposition 2.6 follows from the fact that the intersection of two arithmetic progressions is another arithmetic progression or the empty set. Part (2) follows from the fact that the complement of a single arithmetic progression is a finite (possibly empty) union of arithmetic progressions.

**Lemma 2.7.** *Let $X$ be a quasiprojective variety, $V \subset X$ a subvariety, $\varphi : X \to X$ an endomorphism and $\alpha \in X(K)$ a point. Suppose the sequence $(\varphi^n(\alpha))_{n=1}^{\infty}$ is preperiodic (in the sense of definition 2.1). Then $\{n \in \mathbb{N} : \varphi^n(\alpha) \in V\}$ is a finite union of arithmetic progressions.*

*Proof.* Because $(\varphi^n(\alpha))_{n=1}^{\infty}$ is preperiodic we can find $N, d \in \mathbb{N}$ such that $\varphi^n(\alpha) = \varphi^{n-d}(\alpha)$ for all $n > N$. For all $i \in [N]$, let $\mathcal{M}_i := \{i\}$ be a singleton arithmetic progression. For all $i \in [d]$, let $\mathcal{N}_i = \{(N+i) + d \cdot k : k \in \mathbb{N}_0\}$. Then we have defined $N \cdot d$ arithmetic progressions, and their union is $\mathbb{N}$. For $i \in [N]$, let $\beta_i = \varphi^i(\alpha)$. For $i \in [d]$, let $\gamma_i = \varphi^{N+i}(\alpha)$, and note that $\varphi^n(\alpha) = \gamma_i$ for any $n \in \mathcal{N}_i$. Thus $\{n \in \mathbb{N} : \varphi^n(\alpha) \in V\}$ is a finite union of the $\mathcal{M}_i$ for which $\beta_i \in V$, and the $\mathcal{N}_i$ for which $\gamma_i \in V$. ■

### On the Jordan Normal Form

**Fact 2.8.** *We briefly outline several definitions and results from the theory of generalized eigenvectors and the Jordan normal form of a matrix. Let $A \in M_{k \times k}(\mathbb{C})$.*

1. *Definition. A matrix $J$ is said to be in Jordan normal form if it is of the form:*

$$J = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_N \end{pmatrix},$$

$$\text{for square } J_i = \begin{pmatrix} \lambda_i & 1 & & \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{pmatrix},$$

*for some $\lambda_i \in \mathbb{C}$. The $J_i$ matrices are said to be Jordan blocks.*

2. *Definition. Let $\mathcal{B}$ be a basis and $B$ be the matrix whose columns are the vectors of $\mathcal{B}$. Then $\mathcal{B}$ is an ordered canonical basis $\mathcal{B}$ for $A$ if $B^{-1}AB$ is in Jordan normal form.*

3. *Definition. The vector $\overline{x}$ is a generalized eigenvector of $A$, with eigenvalue $\lambda$ and rank $m$, if $(A - \lambda I)^m \overline{x} = \overline{0}$ and $(A - \lambda I)^{m-1} \overline{x} \neq \overline{0}$.*

4. *A basis is canonical if and only if it is composed completely of disjoint Jordan chains, that is, sets of the form $\{(A-\lambda I)^k \overline{x} : k \in \{0, ..., m-1\}\}$ where $\overline{x}$ is a generalized eigenvector of $A$ with eigenvalue $\lambda$ and rank $m$.*

5. *There exists an ordered canonical basis of $A$. Furthermore, if $A$ has integer entries and integer eigenvalues, then it is possible to choose the canonical basis such that all basis vectors are in $\mathbb{Q}^k$.*

6. *Each Jordan chain of $A$ corresponds to a Jordan block in the Jordan normal form of $A$, and the number of vectors in a Jordan chain equals the size of the corresponding block.*

**Lemma 2.9.** *Suppose every eigenvalue of $A \in M_{k\times k}(\mathbb{Z})$ is in $\mathbb{Z}$, and let $J \in M_{k\times k}(\mathbb{Z})$ be its Jordan normal form. Then $S(A)$ is a finite union of arithmetic progressions, if $S(J)$ is.*

*Proof.* Suppose $S(J)$ is a finite union of arithmetic progressions, in other words, suppose $S(V', \alpha', J, \mathcal{N}')$ is a finite union of arithmetic progressions for any choice of variety $V' \subset \mathbb{G}_m^k, \alpha' \in \mathbb{G}_m^k(K)$ and arithmetic progression $\mathcal{N}'$. Let $V \subset \mathbb{G}_m^k$ be a variety, $\alpha \in \mathbb{G}_m^k(K)$ a point and $\mathcal{N}$ an arithmetic progression, we show $S(V, \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions as well.

By Fact 2.8 part 5 there exists invertible $B \in M_{k\times k}(\mathbb{Q})$ such that $A = B^{-1}JB$. At the cost of scaling $B$ and $B^{-1}$, we may assume $B \in M_{k\times k}(\mathbb{Z})$. Because the inverse is obtained through gaussian elimination, $B^{-1}$ is in $M_{k\times k}(\mathbb{Q})$, and there exists non-zero $c \in \mathbb{Z}$ such that $cB^{-1} \in M_{k\times k}(\mathbb{Z})$. Let $C = c \cdot I_k$ and $D = CB^{-1} \in M_{k\times k}(\mathbb{Z})$. At the cost of replacing $K$ with a finite extension, we can find $\gamma \in \mathbb{G}_m^k(K)$, such that $\varphi_C(\gamma) = \alpha$ and let $\beta = \varphi_B(\gamma)$. Then we have:

$$\begin{aligned}\varphi_A^n(\alpha) =& \varphi_{A^n}(\alpha) = \varphi_{B^{-1}J^nB}(\alpha) = \varphi_{B^{-1}J^nB}(\varphi_C(\gamma)) \\ =& \varphi_{CB^{-1}J^nB}(\gamma) = \varphi_D(\varphi_{J^nB}(\gamma)) = \varphi_{DJ^n}(\beta).\end{aligned}$$

Then $\varphi_D(\varphi_{J^n}(\beta)) \in V$ if and only if $\varphi_{J^n}(\beta) \in \varphi_D^{-1}(V)$. Because $\varphi_D$ is an endomorphism of $\mathbb{G}_m^k$ we have that the last set is again a variety, say $W = \varphi_D^{-1}(V)$. So we have shown $\varphi_A^n(\alpha) \in V$ if and only if $\varphi_J^n(\beta) \in W$ and the lemma follows easily. ■

**Lemma 2.10.** *Let $N \in \mathbb{N}$. Let $A \in M_{k\times k}(\mathbb{Z})$, let $J_N$ be the Jordan normal form of $A^N$ and assume $J_N \in M_{k\times k}(\mathbb{Z})$. Then $S(A)$ is a finite union of arithmetic progressions if $S(J_N)$ is.*

*Proof.* Assume $S(J_N)$ is a finite union of arithmetic progressions. Let $V \subset \mathbb{G}_m^k$ be a variety, $\alpha \in \mathbb{G}_m^k(K)$ a point and $\mathcal{N}$ an arithmetic progression. We show show $S(V, \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions as well.

We call the sequence of points $(\varphi_A(\alpha), \varphi_A^2(\alpha), \varphi_A^3(\alpha), ...)$ the orbit of $\varphi_A$ at $\alpha$. Note that the orbit of $\varphi_A$ at $\alpha$ can be written as the finite union of the orbits of $\varphi_{A^N}$ at $\alpha, \varphi_A(\alpha)$, ..., $\varphi_A^{N-1}(\alpha)$. Thus $S(V, \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions if $S(V, \varphi_A^i(\alpha), A^N, \mathcal{N})$ is a finite union of arithmetic progressions for all $i \in \{0, ..., N-1\}$. Since $S(V, \varphi_A^i(\alpha), A^N, \mathcal{N})$ is a finite union of arithmetic progressions by Lemma 2.9, we are done. ■

**Lemma 2.11.** *Let $N \in \mathbb{N}$ and $a \in \mathbb{Z}$. Let $J_a$ and $J_{a^N}$ be $k \times k$ single Jordan block matrices with $a$ and $a^N$ on the diagonal, respectively. That is:*

$$J_a = \begin{pmatrix} a & 1 & \cdots & 0 \\ 0 & a & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & a \end{pmatrix}, J_{a^N} = \begin{pmatrix} a^N & 1 & \cdots & 0 \\ 0 & a^N & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & a^N \end{pmatrix}.$$

*Then $S(J_a)$ is a finite union of arithmetic progressions if $S(J_{a^N})$ is.*

*Proof.* We first prove the minimal polynomial of $J_a^N$ is $(x-a^N)^k$. The matrix $J_a^N$ is triangular with $a^N$ along the diagonal; thus this is its only eigenvalue and the minimal polynomial of $J_a^N$ is $p(x) = (x - a^N)^m$ for some $m \in [k]$. Let $q(x) = (x - a)^k$ be the minimal polynomial of $J_a$. Because $p(J_a^N) = 0$ we must have that $q(x) \mid p(x^N)$. Let $\xi_0, ..., \xi_{N-1}$ be the $N^{th}$ roots of unity, so that $p(x^N) = \prod_{j=0}^{N-1}(x - a\xi_j)^m$. Then we have:

$$(x-a)^k \mid \prod_{j=0}^{N-1}(x - a\xi_j)^m,$$

and it follows that $m = k$, as desired. Because the minimal polynomial of $J_a^N$ is $(x - a^N)^k$, its Jordan form must contain a Jordan block of size $k$, corresponding to eigenvalue $a^N$. But then the Jordan form of $J_a^N$ is precisely $J_{a^N}$, and the claim follows from Lemma 2.10. ■

### Simplifying Cases

**Claim 2.12.** *To prove $S(A)$ is a finite union of arithmetic progressions, it is sufficient to show $S(Z(f), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions, for any $f \in K[x]$, $\alpha \in \mathbb{G}_m^k(K)$ and arithmetic progression $\mathcal{N}$, by Proposition 2.6.*

With the following three technical lemmas we develop tools to be used by both Chapters 3 and 4. Our setting will be as follows: let $s \in [k]$, let $A \in M_{k\times k}(\mathbb{Z})$, and define

$$\widetilde{A}^s \in M_{k-1\times k-1}(\mathbb{Z}) \tag{2.2}$$

to be the submatrix of $A$ formed by removing the $s^{th}$ row and column. Similarly, given any $\alpha = (\alpha_1, ..., \alpha_k) \in \mathbb{G}_m^k$, let $\widetilde{\alpha}^s$ be the vector with the $s^{th}$ entry removed. Using a circumflex to denote the missing element, we have $\widetilde{\alpha}^s = (\alpha_1, ..., \widehat{\alpha}_s, ..., \alpha_k)$.

**Lemma 2.13.** *Let $K$ be a function field over $\overline{\mathbb{F}_p}$. Let $A \in M_{k\times k}(\mathbb{Z})$, $s \in [k]$, and suppose every element of the $s^{th}$ row is zero, except possibly $A_{s,s}$. Let $\widetilde{A}^s$ be as in (2.2) and assume $S(\widetilde{A}^s)$ is a finite union of arithmetic progressions. Suppose $\alpha = (\alpha_1, ..., \alpha_k) \in \mathbb{G}_m^k$ satisfies $\alpha_s \in \overline{\mathbb{F}_p}$. Then $S(V, \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions, for any variety $V \subset \mathbb{G}_m^k$ and arithmetic progression $\mathcal{N}$.*

*Proof.* Since $s \in [k]$ is fixed, we drop the superscript $s$ from our notation, writing $\widetilde{A} := \widetilde{A}^s$ and $\widetilde{\alpha} := \widetilde{\alpha}^s$.

Let $h \in K[x_1, ..., x_k]$. By Claim 2.12, it is sufficient to show $S(Z(h), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions.

Let $m$ be the order of $\alpha_s$ in $\overline{\mathbb{F}_p}^\times$, and let $\overline{(A)_{i,j}}$ denote the value of $(A)_{i,j}$ modulo $m$. Because the reduced matrix $\overline{A^n}$ ranges over a finite set and $\overline{A^n}$ is a linear function of $\overline{A^{n-1}}$, we see the sequence $(\overline{A^n} : n \in \mathbb{N})$ is preperiodic, in the sense of definition 2.1.

By $\overline{A^n}$'s preperiodicity, we can find arithmetic progressions $\{\mathcal{N}_i\}_{i=1}^{\ell}$ such that $\cup_{i=1}^{\ell}\mathcal{N}_i = \mathcal{N}$ and $\overline{A^n}$ is a fixed matrix (modulo $m$) for all $n \in \mathcal{N}_i$.

Note that:

$$\begin{aligned}\varphi_A^n(\alpha_1, ..., \alpha_s, ..., \alpha_k) = \big(&\alpha_1^{(A^n)_{1,1}} \cdots \alpha_s^{(A^n)_{1,s}} \cdots \alpha_k^{(A^n)_{1,k}},\\ &\cdots\\ &\alpha_1^0 \cdots \alpha_s^{(A^n)_{s,s}} \cdots \alpha_k^0,\\ &\cdots\\ &\alpha_k^{(A^n)_{k,1}} \cdots \alpha_s^{(A^n)_{k,s}} \cdots \alpha_k^{(A^n)_{k,k}}\big).\end{aligned}$$

Given this, for each $i \in [\ell]$ and $j \in [k]$, choose any $n \in \mathcal{N}_i$ and use it to define

$$\beta_{i,j} := \alpha_s^{(A^n)_{j,s}}.$$

This is independent to the particular $n \in \mathcal{N}_i$ chosen. For each $i$ we also define:

$$h_i(x_1, ..., \widehat{x_s}, ...x_k) := h(x_1\beta_{i,1}, ..., \beta_{i,s}, ...x_k\beta_{i,k}).$$

By our assumption that $(A)_{s,i}$ is zero for all $i \neq s$, we have $(\widetilde{A})^n = \widetilde{(A^n)}$.

It follows easily that:

$$h_i(\varphi^n_{\widetilde{A}}(\widetilde{\alpha})) = h(\varphi^n_A(\alpha)), \tag{2.3}$$

for all $n \in \mathcal{N}_i$. The set $S(Z(h_i), \widetilde{\alpha}, \widetilde{A}, \mathcal{N}_i)$ is a finite union of arithmetic progressions by assumption, and so by (2.3) $S(Z(h), \alpha, A, \mathcal{N}_i)$ is a finite union of arithmetic progressions as well. The lemma follows. ■

Let $s \in [k]$. In the following two lemmas we will express polynomials of $K[x_1, ..., x_k]$ with the following notation:

$$h(x_1, ..., x_k) = \sum_{i=0}^{d} x_s^i h_i(x_1, ..., \widehat{x_s}, ..., x_k), \tag{2.4}$$

where $d$ is the degree of $h$ in $x_s$.

**Lemma 2.14.** *Let $A \in M_{k\times k}\mathbb{Z}$, $s \in [k]$, and suppose every element of the $s^{th}$ column of $A$ is zero, except possibly $A_{s,s}$. Suppose $S(\widetilde{A}^s)$ is a finite union of arithmetic progressions (with $\widetilde{A}^s$ as in (2.2)). Let $h$ be as in (2.4) and suppose that $d = 0$. Then $S(Z(h), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions as well, for any $\alpha \in \mathbb{G}_m^k(K)$ and arithmetic progression $\mathcal{N}$.*

*Proof.* Since $s \in [k]$ is fixed, we drop the superscript $s$ from our notation, writing $\widetilde{A} := \widetilde{A}^s$ and $\widetilde{\alpha} := \widetilde{\alpha}^s$.

Let $h_i$ and $d$ be as defined in (2.4). We have $d = 0$, so let

$$\widetilde{h}(x_1, ..., \widehat{x_s}, ..., x_k) := h(x_1, ..., x_k).$$

By our assumption that $(A)_{i,s}$ is zero for all $i \neq s$, we have $(\widetilde{A})^n = \widetilde{(A^n)}$. It follows easily that

$$h(\varphi^n_A(\alpha)) = \widetilde{h}(\varphi^n_{\widetilde{A}}(\widetilde{\alpha})). \tag{2.5}$$

By assumption we have that $S(Z(\widetilde{h}), \widetilde{\alpha}, \widetilde{A}, \mathcal{N})$ is a finite union of arithmetic progressions, and so by (2.5) we get that $S(Z(h), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions as well. ■

**Lemma 2.15.** *Let $A \in M_{k\times k}(\mathbb{Z})$, $s \in [k]$, and suppose every element of the $s^{th}$ column of $A$ is zero, except possibly $A_{s,s}$. Suppose $S(\widetilde{A}^s)$ is a finite union of arithmetic progressions, and that $S(Z(h), \alpha, A, \mathcal{N})$ is as well, for any $\alpha \in \mathbb{G}_m^k(K)$, arithmetic progression $\mathcal{N}$ and polynomial $h$ (of the form (2.4)) satisfying $h_d(\varphi^n_{\widetilde{A}^s}(\widetilde{\alpha}^s)) \neq 0$ for all $n \in \mathcal{N}$. Then $S(A)$ is a finite union of arithmetic progressions as well.*

*Proof.* Since $s \in [k]$ is fixed, we drop the superscript $s$ from our notation, writing $\widetilde{A} := \widetilde{A}^s$ and $\widetilde{\alpha} := \widetilde{\alpha}^s$.

Assume $S(Z(h), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions whenever $h$'s leading term in $x_s$, $h_d$, is non-zero at $\varphi^n_{\widetilde{A}}(\widetilde{\alpha})$ for all $n \in \mathcal{N}$.

Claim 2.16. Consider $S(Z(h), \alpha, A, \mathcal{N})$. If $h$'s leading term $h_d(\varphi^n_{\widetilde{A}}(\widetilde{\alpha}))$ is *identically* zero for all $n \in \mathcal{N}$, then proving $S(Z(h), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions reduces to proving the same for $S(Z(h'), \alpha, A, \mathcal{N})$, for a polynomial $h'$ whose degree in $x_s$ is strictly less than $d$. To see this, define

$$h'(x_1, ..., x_k) = \sum_{i=0}^{d-1} x_s^i h_i(x_1, ..., \widehat{x_s}, ..., x_k),$$

and note $h'(\varphi^n_A(\alpha)) = h(\varphi^n_A(\alpha))$ for all $n \in \mathcal{N}$.

Claim 2.17. Proving $S(Z(h), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions reduces to proving the same for $S(Z(h), \alpha, A, \mathcal{N}')$ where $h_d(\varphi^n_{\widetilde{A}}(\widetilde{\alpha}))$ is identically zero for all $n \in \mathcal{N}'$. To see this, note that by assumption,

$$\{n \in \mathcal{N} : h_d(\varphi^n_{\widetilde{A}}(\widetilde{\alpha})) = 0\}$$

is a finite union of arithmetic progressions. Thus by Proposition 2.6, we can find a collection of arithmetic progressions such that their union is $\mathcal{N}$, and $h_d(\varphi^n_{\widetilde{A}}(\widetilde{\alpha}))$ is either identically zero or non-zero on each. If it is non-zero we are done by the assumption. The claim follows.

Finally, let $g \in K[x_1, ..., x_k]$, $\alpha \in \mathbb{G}^k_m(K)$ and arithmetic progression $\mathcal{N}$ be arbitrary. That $S(Z(g), \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions now follows easily by alternatively applying Claims 2.16 and 2.17, and by Lemma 2.14. ■

## Asymptotic Bound

**Definition 2.18.** *Given functions $f, g : \mathbb{N} \to \mathbb{R}$, we say that $f = o(g)$ if for every $\epsilon > 0$, there exists an $N \in \mathbb{N}$ such that $n > N$ implies $|f(n)| < \epsilon |g(n)|$.*

**Lemma 2.19.** *Let $K$ be a function field over $\overline{\mathbb{F}_p}$. Let $\mathcal{N}$ be an arithmetic progression. Let $g_1, ..., g_k$ be functions $\mathbb{N} \to K^\times$, and $|\cdot|_w \in M_K$. Let $h \in K[x_1, ..., x_k]$, and write $h(x_1, ..., x_k) = \sum_{i=0}^d x_1^i h_i(x_2, ..., x_k)$ where $d$ is the degree of $h$ in $x_1$. Suppose the following conditions hold:*

*(a) $|g_1|_w$ is monotonically increasing to infinity, and $\log(|g_i|_u) =$*

$o(\log(|g_1|_w))$ *for all* $i > 1$ *and any* $|\cdot|_u \in M_K$.

*(b)* $d > 0$, *and* $h_d(g_2(n), ..., g_k(n))$ *is non-zero for all* $n \in \mathcal{N}$.

*(c) There exist only finitely many* $|\cdot|_u \in M_K$ *such that* $|h_d(g_2(n), ..., g_k(n))|_u > 1$ *for some* $n \in \mathcal{N}$.

*Given this, the set*

$$S = \{n \in \mathcal{N} : h(g_1(n), ..., g_k(n)) = 0\}$$

*is finite.*

*Proof.* Let $y_{n,i} = g_i(n)$. We begin with a remark on assumption $(a)$. For any $|\cdot|_u \in M_K$, $\ell_2, ..., \ell_k \in \mathbb{N}$, $\alpha \in K^\times$ and $b > 0$ we have:

$$\begin{aligned}\log(|\alpha|_u) + \ell_2 \log(|g_2(n)|_u) + ... + \ell_k \log(|g_k(n)|_u) \\ < b \log(|g_1(n)|_w)\end{aligned}$$

for sufficiently large $n \in \mathcal{N}$. Thus:

$$|\alpha \cdot y_{n,2}^{\ell_2} \cdots y_{n,k}^{\ell_k}|_u < |y_{n,1}|_w^b,$$

and in particular for any $i \in [d]$, there exists an $N_i \in \mathbb{N}$ such that:

$$|h_i(y_{n,2}, ..., y_{n,k})|_u < |y_{n,1}|_w^b \tag{2.6}$$

for all $n > N_i$.

Suppose for contradiction that there exists infinite set $I \subset \mathcal{N}$ such that $h(y_{n,1}, ..., y_{n,k}) = 0$ for all $n \in I$. Note first that at any point $(y_1, ..., y_k) \in \mathbb{G}_m^k$ we have:

$$|h(y_1, ..., y_k)|_w \geq \left|y_1^d\right|_w \cdot \left||h_d(y_2, ..., y_k)|_w - \left|\sum_{i=1}^{d-1} y_1^{i-d} h_i(y_2, ..., y_k)\right|_w\right|.$$

Thus we must have:

$$|h_d(y_{n,2}, ..., y_{n,k})|_w = \left|\sum_{i=1}^{d-1} y_{n,1}^{i-d} h_i(y_{n,2}, ..., y_{n,k})\right|_w$$

for all $n \in I$. By (2.6) there exists $N$ such that for all $n > N$ in $I$:

$$|h_d(y_{n,2}, ..., y_{n,k})|_w = \left|\sum_{i=1}^{d-1} y_{n,1}^{i-d} h_i(y_{n,2}, ..., y_{n,k})\right|_w < |y_{n,1}|_w^{-1/2}. \tag{2.7}$$

By throwing out at most finitely many elements from $I$, we may assume (2.7) and $|y_{n,1}|_w^{1/2} > 1$ hold for all $n \in I$. Let $\mathcal{W}$ be the set of places $|\cdot|_u \in M_K$ where $|h_d(g_2(n), ..., g_k(n))|_u > 1$ for some $n$. Let $s = |\mathcal{W}|$, which is finite by assumption (c).

By $(b)$ $h_d(y_{n,2}, ..., y_{n,k})$ is non-zero and so the product formula, (2.1), holds:

$$\prod_{u \in M_K} |h_d(y_{n,2}, ..., y_{n,k})|_u = 1. \tag{2.8}$$

From (2.7) and (2.8), we know $s > 0$ and moreover that for each $n \in I$ there must exist place $|\cdot|_{w_n} \in \mathcal{W}$ such that:

$$1 < |y_{n,1}|_w^{\frac{1}{2s}} < |h_d(y_{n,2}, ..., y_{n,k})|_{w_n}.$$

But $\mathcal{W}$ is finite, so a single place, $|\cdot|_{w'}$, must appear infinitely many times. We can find an infinite subset $I' \subset I$ such that

$$|y_{n,1}|_w^{\frac{1}{2s}} < |h_d(y_{n,2}, ..., y_{n,k})|_{w'},$$

for all $n \in I'$. This contradicts (2.6), and so the original set $I$ cannot exist. ■

**Remark 2.20.** *In Lemma 2.19, we singled out $x_1$ and $g_1$, but by relabelling, the results apply for $x_s$ and $g_s$, for any $s \in [k]$.*

# Chapter 3

# Single Jordan Block

We prove Theorem 1.3. In this case $X = \mathbb{G}_m^k$, $\varphi$ is a group endomorphism of $X$, and the matrix $A \in M_{k\times k}(\mathbb{Z})$, corresponding to $\varphi$, is similar to a single Jordan block.

**Proposition 3.1.** *Let $K$ be a field of characteristic $p > 0$. Let $a \in \mathbb{Z}$ and let $J_a \in M_{k\times k}(\mathbb{Z})$ be a single Jordan block, that is:*

$$J_a = \begin{pmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & a & 1 \\ 0 & 0 & 0 & 0 & a \end{pmatrix}.$$

*Then $S(J_a)$ is a finite union of arithmetic progressions.*

## 3.1 Proof of Proposition 3.1

We show $S = S(V, \alpha, J_a, \mathcal{N})$ is a finite union of arithmetic progressions, where $V \subset \mathbb{G}_m^k$ is a variety, $\alpha \in \mathbb{G}_m^k(K)$ a point and $\mathcal{N}$ an arithmetic progression. As usual we write $\alpha$ as $\alpha = (\alpha_1, ..., \alpha_k)$. Since $V, \alpha$, and $\varphi_{J_a}$ are defined over a finitely generated subfield of $K$, we may assume, without loss of generality, that $K$ is a function field over $\overline{\mathbb{F}_p}$.

**Claim 3.2.** *It is sufficient to prove the proposition in the case where $a > 0$.*

*Proof.* If $a = 0$, then $(J_a)^n = 0$ for all $n \geq k$, so the image $\varphi_{J_a}^n(\alpha) = (1, ..., 1)$ for all $n \geq k$. It follows easily that $S(V, \alpha, J_a, \mathcal{N}) = \{n \in \mathbb{N} : \varphi_{J_a}^n(\alpha) \in V\}$ is a finite union of arithmetic progressions.

If $a < 0$, then by Lemma 2.11 it is sufficient to show $S(J_{a^2})$ is a finite union of arithmetic progressions, where $J_{a^2}$ is the matrix consisting of a single Jordan block with $a^2 > 0$ on the diagonal. ■

**Remark 3.3.** *For $n \geq k$ we have:*

$$J_a^n = \begin{pmatrix} a^n & na^{n-1} & \binom{n}{2}a^{n-2} & \cdots & \binom{n}{k-1}a^{n-(k-1)} \\ 0 & a^n & na^{n-1} & \cdots & \binom{n}{k-2}a^{n-(k-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & a^n & na^{n-1} \\ 0 & 0 & 0 & 0 & a^n \end{pmatrix},$$

*and so:*

$$\varphi_{J_a}^n(\alpha_1, ..., \alpha_k) = (\alpha_1^{a^n} \alpha_2^{na^{n-1}} \cdots \alpha_k^{\binom{n}{k-1}a^{n-(k-1)}}, \alpha_2^{a^n} \cdots \alpha_k^{\binom{n}{k-2}a^{n-(k-2)}}, ..., \alpha_k^{a^n}).$$

We now proceed to prove Proposition 3.1 via induction on the dimension $k$. By Claim 2.12, we may assume $V = Z(f)$ for $f \in K[x_1, ..., x_k]$, and by Claim 3.2 that $a > 0$.

### Base Case

Let $k = 1$. The set $Z(f)$ is either empty, all of $\mathbb{G}_m^k$, or a finite set of points, and in the first two cases the claim trivially holds – so consider only the last. Let $\beta \in Z(f)$ be arbitrary, it is sufficient to show $\{n \in \mathbb{N} : \varphi_{J_a}^n(\alpha) = \beta\}$ is a finite union of arithmetic progressions. If $\varphi_{J_a}^n(\alpha) = \beta$ for only one $n \in \mathbb{N}$ then we are done, otherwise $\alpha$ is a preperiodic point of $\varphi_{J_a}$ and we are done by lemma 2.7.

Thus the set of $n \in \mathbb{N}$ such that $\varphi_{J_a}^n(\alpha) \in Z(f)$ is a finite union of arithmetic progressions, as desired.

### Inductive Step

Now assume the inductive hypothesis for dimension $k - 1$, that is, assume $S(V', \alpha', J_a', \mathcal{N}')$ is a finite union of arithmetic progressions for any $J_a' \in M_{k-1 \times k-1}(\mathbb{Z})$, $\alpha' \in \mathbb{G}_m^k(K)$, variety $V' \subset \mathbb{G}_m^k$ and arithmetic progression $\mathcal{N}'$.

If $|\alpha_k|_v \leq 1$ for all $|\cdot|_v \in M_K$, then $\alpha_k \in \overline{\mathbb{F}_p}$ by Fact 2.5, and so by Lemma 2.13 (with $s = k$) and the induction hypothesis we are done. Instead, assume we can find $|\cdot|_v \in M_K$ such that $|\alpha_k|_v > 1$.

Let the maximum power of $x_1$ found in $f(x_1, ..., x_k)$ be $d$. Then for some polynomials $f_i \in K[x_2, ..., x_k]$ we have:

$$f(x_1, ..., x_k) = \sum_{i=0}^{d} x_1^i f_i(x_2, ...x_k).$$

We now invoke Lemma 2.19. Recall we have:

$$\varphi^n_{J_a}(\alpha_1,...,\alpha_k) = (\alpha_1^{a^n}\alpha_2^{na^{n-1}}\cdots\alpha_k^{\binom{n}{k-1}a^{n-(k-1)}}, \alpha_2^{a^n}\cdots\alpha_k^{\binom{n}{k-2}a^{n-(k-2)}}, ..., \alpha_k^{a^n}).$$

Given this, define the $g_i$ from Lemma 2.19 so that $\varphi^n_{J_a}(\alpha) = (g_1(n),...,g_k(n))$. In particular we have (for example) that:

$$g_1(n) = \alpha_1^{a^n}\alpha_2^{na^{n-1}}\cdots\alpha_k^{\binom{n}{k-1}a^{n-(k-1)}}.$$

Let $|\cdot|_v$ be the place $|\cdot|_w$ of the lemma. Then because $|\alpha_k|_v > 1$ we have

$$\binom{n}{k-i}a^{n-(k-i)}\log(|\alpha_j|_u) = o\left(\binom{n}{k-1}a^{n-(k-1)}\log(|\alpha_k|_v)\right),$$

for any place $|\cdot|_u \in M_K$, all $j \in [k]$ and $1 \in [k]$ with $i > 1$. Assumption $(a)$ of the lemma follows easily. We let $f$ be the polynomial $h$ of the lemma. By Lemma 2.14 we may assume $d > 0$, while by Lemma 2.15 (with $s = 1$), we may assume $f_d(\varphi^n_{A_{k-1}}(\alpha_2,...,\alpha_k))$ is non-zero for all $n \in \mathcal{N}$. Together these give us assumption $(b)$. Finally, assumption $(c)$ follows by noting there are only finitely many places where either a coefficient of $h_d$, or an $\alpha_i$ has norm greater than 1.

Thus Lemma 2.19 completes the proof. ■

## 3.2 Theorem 1.3

We now prove Theorem 1.3. For convenience, the theorem is reproduced below.

**Theorem 1.3.** *Let $K$ be a field of characteristic $p > 0$. Let the group endomorphism $\varphi_A : \mathbb{G}_m^k \to \mathbb{G}_m^k$ be defined by*

$$\varphi(x_1,...,x_k) = (x_1^{a_{1,1}}x_2^{a_{1,2}}\cdots x_k^{a_{1,k}}, ..., x_1^{a_{k,1}}x_2^{a_{k,2}}\cdots x_k^{a_{k,k}})$$

*for some $a_{i,j} \in \mathbb{Z}$, and assume that the matrix $A = (a_{i,j})$ is similar to a single Jordan block. Let $V \subset \mathbb{G}_m^k$ be a variety, and $\alpha \in \mathbb{G}_m^k(K)$ a point. Then the set*

$$S = \{n \in \mathbb{N} : \varphi_A^n(\alpha) \in V\}$$

*is a finite union of arithmetic progressions.*

*Proof.* Let $A \in M_{k\times k}(\mathbb{Z})$, and suppose $A$ has Jordan form:

$$J_a = \begin{pmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & a & 1 \\ 0 & 0 & 0 & 0 & a \end{pmatrix},$$

for some $a \in \mathbb{C}$. By Proposition 3.1 and Lemma 2.9, in order to prove Theorem 1.3, it is sufficient to show that $a$ must be in $\mathbb{Z}$. Note that $Tr(A) = Tr(J_a) = ka$ and $Det(A) = Det(J_a) = a^k$. Thus both $ka$ and $a^k$ are in $\mathbb{Z}$. We see that $a$ is both a rational number and an algebraic integer, and so we must have $a \in \mathbb{Z}$. ■

# Chapter 4

# Dimension 3

The goal of this section is to prove Theorem 1.4. We will need the following result, which appears in [2, Proposition 13.3.0.2].

**Proposition 4.1.** *Let $K$ be a field of characteristic $p > 0$, $\alpha \in \mathbb{G}_m^k(K)$, $V \subset \mathbb{G}_m^k$ be a variety and $\mathcal{N}$ be an arithmetic progression. Let $A \in M_{k\times k}(\mathbb{Z})$ be diagonalizable. Then*

$$S(V, \alpha, A, \mathcal{N}) = \{n \in \mathcal{N} : \varphi_A^n(\alpha) \in V\}$$

*is a finite union of arithmetic progressions.* ■

Our proof of Theorem 1.4 will rely on the following lemma.

**Lemma 4.2.** *Let $K$ be a function field over $\overline{\mathbb{F}_p}$. Let $J \in M_{3\times 3}(\mathbb{Z})$ be a matrix in Jordan form, let $V \subset \mathbb{G}_m^3$ be a variety, $\alpha \in \mathbb{G}_m^3(K)$ a point and $\mathcal{N}$ an arithmetic progression. Then the set*

$$S = \{n \in \mathcal{N} : \varphi_J^n(\alpha) \in V\}$$

*is a finite union of arithmetic progressions.*

*Proof.* We show $S(V, \alpha, J, \mathcal{N})$ is a finite union of arithmetic progressions, where $\alpha$ is written $\alpha = (\alpha_1, \alpha_2, \alpha_3)$. By Proposition 3.1 and Proposition 4.1, it is sufficient to consider the case where matrix $J$ is composed of two Jordan blocks. Without loss of generality we write:

$$J = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix},$$

for $a, b \in \mathbb{Z}$. If $a = 0$ then

$$J^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b^2 \end{pmatrix},$$

Thus $J^2$ is already diagonal and we are done by Lemma 2.10 and Theorem 4.1. Thus we may assume $a \neq 0$. In this case we claim $J^2$ has Jordan form:

$$J' = \begin{pmatrix} a^2 & 1 & 0 \\ 0 & a^2 & 0 \\ 0 & 0 & b^2 \end{pmatrix}.$$

This follows as $J^2$ has eigenvalues $b^2$ and $a^2$ with algebraic multiplicity 1 and 2 respectively, and is not diagonalizable

By the previous paragraph, and Lemma 2.10, it is enough to show $S(J')$ is a finite union of arithmetic progressions. Thus we may now assume $a > 0$ and $b \geq 0$.

By Claim 2.12 it is sufficient to consider $V = Z(f)$ for polynomial $f = f(x_1, x_2, x_3)$. If $b = 0$, then let $g(x_1, x_2) = f(x_1, x_2, 1)$ and note $f(\varphi_J^n(\alpha)) = g(\varphi_{J_a}^n((\alpha_1, \alpha_2)))$, where $J_a = \left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$, so we are done by Proposition 3.1.

By the above, we may assume $a > 0$ and $b > 0$. We split into two cases depending on the relative size of $a$ and $b$.

**Case 1:** $0 < a < b$**.** Note $\varphi_J^n(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1^{a^n} \alpha_2^{na^{n-1}}, \alpha_2^{a^n}, \alpha_3^{b^n})$. In this case, the factor of $|\alpha_3^{b^n}|_v$ dominates the value of $|f(\varphi_A^n(\alpha))|_v$. However we must first eliminate the cases where $\alpha_3$ has small norm, or $x_3$ does not appear in $f$.

Let $J_a = \left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$; $S(J_a)$ is a finite union of arithmetic progressions by Proposition 3.1. If $|\alpha_3|_v \leq 1$ for all $|\cdot|_v \in M_K$, then by Fact 2.5 and Lemma 2.13 (with $s = 3$) we are done. Therefore we now assume $|\alpha_3|_v > 1$ for some $|\cdot|_v \in M_K$.

Let $f(x_1, x_2, x_3) = \sum_{i=0}^{d} x_3^i f_i(x_1, x_2)$. By Lemma 2.14 (with $s = 3$), we may assume $d > 0$. By Lemma 2.15 (with $s = 3$), we may assume $f_d(\varphi_{J_a}^n(\alpha_1, \alpha_2))$ is non-zero for all $n \in \mathcal{N}$.

Finally, we apply Lemma 2.19 with $s = 3$ (using Remark 2.20). We let $g_1(n) = \alpha_1^{a^n} \alpha_2^{na^{n-1}}$, $g_2(n) = \alpha_2^{a^n}$ and $g_3(n) = \alpha_3^{b^n}$. Condition $(a)$ of the lemma follows from the fact that

$$\binom{n}{i} a^{n-i} \log(|\alpha_j|_u) = o\left(b^n \log(|\alpha_3|_v)\right),$$

for any place $|\cdot|_u \in M_K$, $i \in \{0,1\}$ and $j \in \{1,2\}$ (here we use that $0 < a < b$ implies in particular that $1 < b$). Letting $f$ be polynomial $h$ from the lemma, $(b)$ follows from the previous paragraph, and $(c)$ can be seen by noting there are only finitely many places where either a coefficient of $f_d$ or an $\alpha_i$ has norm greater than 1. This concludes Case 1 of the proof.

**Case 2:** $0 < b \leq a$**.** In this case the factor of $|\alpha_2^{na^{n-1}}|_v$ dominates.

Let $D = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$; $S(D)$ is a finite union of arithmetic progressions by Proposition 4.1. Thus if $|\alpha_2|_v \leq 1$ for all $|\cdot|_v \in M_K$, then by Fact 2.5 and Lemma 2.13 (with $s = 2$) we are done. So suppose $|\alpha_2|_v > 1$ for some $|\cdot|_v \in M_K$.

Let $f(x_1, x_2, x_3) = \sum_{i=0}^{d} x_1^i f_i(x_2, x_3)$. By lemma 2.14 (with $s = 1$) we may assume $d > 0$, and by Lemma 2.15 (with $s = 1$) we may assume $f_d(\varphi_D^n((\alpha_1, \alpha_3)))$ is non-zero for all $n \in \mathcal{N}$.

We apply Lemma 2.19 with $s = 1$. We let the $g_i$ and polynomial $h$ be as in Case 1. It is easy to check, by analogous arguments to those of Case 1, that conditions $(a)$, $(b)$ and$(c)$ still hold. Thus by Lemma 2.19 $S(V, \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions. ■

Theorem 1.4 (reproduced below for the reader's convenience) is now an easy corollary of Lemma 4.2.

**Theorem 1.4.** *Let $K$ be a field of characteristic $p > 0$. Let $\varphi : \mathbb{G}_m^3 \to \mathbb{G}_m^3$ be a group endomorphism, let $V \subset \mathbb{G}_m^3$ be a variety, and $\alpha \in \mathbb{G}_m^3(K)$ a point. Then the set*

$$S = \{n \in \mathbb{N} : \varphi^n(\alpha) \in V\}$$

*is a finite union of arithmetic progressions.*

*Proof.* Let $V, \alpha$ and $\varphi$ be as in the lemma statement. Let $A \in M_{3\times 3}(\mathbb{Z})$ be the matrix associated with $\varphi$, so that $\varphi = \varphi_A$. Since $V, \alpha$, and $\varphi_A$ are defined over a finitely generated subfield of $K$, we may assume, without loss of generality, that $K$ is a function field over $\overline{\mathbb{F}_p}$.

We prove $S(V, \alpha, A, \mathcal{N})$ is a finite union of arithmetic progressions. Recall that $\mathbb{Q}$ is a perfect field, that is, any polynomial irreducible over $\mathbb{Q}$

is separable. Let $p_A \in \mathbb{Z}[x]$ be the degree three characteristic polynomial of $A$. If $p_A$ were irreducible over $\mathbb{Q}$ then it would have three distinct roots and we would be done by Proposition 4.1.

Suppose instead $p_A$ were reducible over $\mathbb{Q}$, then we can write $p_A(x) = q(x)(x - r)$, for some $r \in \mathbb{Q}$ and $q \in \mathbb{Q}[x]$. If $q$ were irreducible over $\mathbb{Q}$ then it would have two distinct non-rational roots, and so $p_A$ would have three distinct roots. Thus we may assume $q$ is reducible over $\mathbb{Q}$. Then both of $q$'s roots must be in $\mathbb{Q}$. Since $p_A$ is monic, all three of its roots – that we have just seen are in $\mathbb{Q}$ – are in fact in $\mathbb{Z}$. Then by Lemma 2.9 and Lemma 4.2 we have the claim. ■

# Chapter 5

# Examples

Conjecture 1.2 has been proven by [3] when $X = \mathbb{G}_m^k$, $\varphi$ is any regular self-map, and the variety $V$ is a curve. Combining this with Theorem 1.4, Conjecture 1.2 has now been shown for the case where $X = \mathbb{G}_m^k(K)$ for $k \in \{1, 2, 3\}$ and $\varphi$ is a group endomorphism. These cases are in a sense easier because, as we saw in the three dimensional case, the set $S$ contains none of the more complicated sets of equation (1.2). As we saw in Example 1.1, and will see in the following two examples, this property no longer holds in dimension $\geq 4$.

In both of the following examples, let the ambient field $K$ be $\overline{\mathbb{F}_p}(t)$.

**Example 5.1.** *Let $p > 2$. Let $\alpha = (1, t, 1, 1+t, 1, 1-t) \in \mathbb{G}_m^6(K)$, and define*

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

*Then*

$$\varphi_A^n(\alpha) = (t^n, t, (1+t)^n, (1+t), (1-t)^n, (1-t)).$$

*Let $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_3 + x_5 - 2x_1 - 2$. We claim the set $S = \{n \in \mathbb{N} : \varphi_A^n(\alpha) \in Z(f)\}$, equals*

$$\{p^{n_1} + p^{n_2} : n_1, n_2 \in \mathbb{N}_0\}. \tag{5.1}$$

*It is easy to check (5.1) is contained in $S$, so we prove the reverse containment. Suppose $f(\varphi_A^n(\alpha)) = 0$ and let $n = \ell p^a$ for $\ell$ coprime to $p$. Then:*

$$\begin{aligned} f(\varphi_A^n(\alpha)) &= (1 + t^{p^a})^\ell + (1 - t^{p^a})^\ell - 2t^{p^a \ell} - 2 \\ &= \sum_{i=1}^{\ell-1} \binom{\ell}{i} \left( (t^{p^a})^i + (-t^{p^a})^i \right) - t^{p^a \ell} + (-t^{p^a})^\ell. \end{aligned}$$

*It follows immediately that $\ell$ must be even, and so we have:*

$$f(\varphi_A^n(\alpha)) = \sum_{i=1}^{\ell-1} \binom{\ell}{i} \left( (t^{p^a})^i + (-t^{p^a})^i \right). \tag{5.2}$$

*If $\ell = 2$ we are done, so suppose $\ell > 2$. Then from the $i = 2$ term of (5.2) we see that $\ell \equiv 1 \pmod{p}$. Since $\ell - 1 \neq 0$ we can write $\ell - 1 = p^b m$ for some $m$ coprime to $p$. Then $\ell \equiv 1 \pmod{p}$ implies $b \in \mathbb{N}$ $(\star)$. Given this, we have $n = p^a(p^b m + 1)$ and:*

$$\begin{aligned} f(\varphi_A^n(\alpha)) &= (1 + t^{p^a})^{p^b m+1} + (1 - t^{p^a})^{p^b m+1} - 2t^{p^a(p^b m+1)} - 2 \\ &= \sum_{i=0}^{m} \binom{m}{i} \left( (t^{p^{a+b}})^i + (-t^{p^{a+b}})^i \right) - 2 \\ &\quad + t^{p^a} \sum_{i=0}^{m} \binom{m}{i} \left( (t^{p^{a+b}})^i - (-t^{p^{a+b}})^i \right) - 2t^{p^a(p^b m+1)}. \end{aligned}$$

*If $m = 1$ we are done, and $m = 0$ is impossible, so suppose $m > 1$. Then it is easy to see the $i = 1$ term of the second sum, $2mt^{p^a} t^{p^{a+b}}$, must cancel with some term of the first sum. We have:*

$$2mt^{p^{a+b}+p^a} = -2\binom{m}{i} t^{ip^{a+b}},$$

*and so $p^{a+b} + p^a = ip^{a+b}$. From this we can deduce $b = 0$, contradicting $(\star)$.*

Recall Conjecture 1.2 allowed $S$ to contain finitely many arithmetic progressions, as well as finitely many sets of the form

$$\left\{ \sum_{j=1}^{m} c_j p^{k_j n_j} : n_j \in \mathbb{N}_0 \text{ for each } j \in [m] \right\}, \tag{5.3}$$

for some $c_j \in \mathbb{Q}$, and $k_j \in \mathbb{N}$. Since $\{p^{n_1} + p^{n_2} : n_1, n_2 \in \mathbb{N}_0\}$ cannot be written as a simple geometric series (or an arithmetic progression), Example 5.1 shows that the sum to $m$ in (5.3) is necessary. With our next example we show that the $c_j$ are indeed sometimes necessarily in $\mathbb{Q}$.

**Example 5.2.** *Let $p > 2$. Let $\alpha = (1, t^{p-1}, 1, (1-t)^{p-1}) \in \mathbb{G}_m^4(K)$, and define*

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

*Then* $\varphi_A^n(\alpha) = (t^{n(p-1)}, t^{p-1}, (1-t)^{n(p-1)}, (1-t)^{p-1})$. *Let* $f(x_1, x_2, x_3, x_4) = tx_1 + (1-t)x_3 - 1$. *We claim* $S = \{n \in \mathbb{N} : \varphi_A^n(\alpha) \in Z(f)\}$ *is equal to*

$$\left\{ \frac{p^j}{p-1} - \frac{1}{p-1} : j \in \mathbb{N}_0 \right\}. \tag{5.4}$$

*It is easy to check (5.4) is contained in* $S$, *so we prove the reverse containment. As we saw in Example 1.1,* $m \in \mathbb{N}$ *satisfies*

$$t^m + (1-t)^m - 1 = 0$$

*if and only if* $m = p^j$ *for some* $j \in \mathbb{N}_0$. *So suppose* $f(\varphi_A^n(\alpha)) = 0$ *and then, defining* $m = (p-1)n + 1$, *we have:*

$$\begin{aligned} f(\varphi_A^n(\alpha)) &= (t^{n(p-1)})t + ((1-t)^{n(p-1)}))(1-t) - 1 \\ &= t^m + (1-t)^m - 1. \end{aligned}$$

*Thus* $n = \frac{p^j - 1}{p-1}$ *for some* $j \in \mathbb{N}_0$.

# Chapter 6

# Conclusion

The approach used in Chapters 3 and 4 to show Conjecture 1.2 for the similar to a Jordan block case and dimension 3 case will always yield a set $S$ that is a finite union of arithmetic progressions. However, as the examples have shown, more complicated sets (as in equation (1.2)) already begin to appear in dimension 4. Thus new ideas will be required as we press on to higher dimensions.

# Bibliography


[1] Jason P. Bell, Dragos Ghioca, and Thomas J. Tucker. The Dynamical Mordell-Lang problem for étale maps. *American Journal of Mathematics*, 132(6):1655–1675, 2010.

[2] Jason P. Bell, Dragos Ghioca, and Thomas J. Tucker. *The Dynamical Mordell–Lang Conjecture*, volume 210 of *Mathematical Surveys and Monographs*. American Mathematical Soc., 2016.

[3] Dragos Ghioca. The Dynamical Mordell-Lang Conjecture in positive characteristic. arXiv:1610.00367, 2016.

[4] Dragos Ghioca and Thomas J. Tucker. Periodic points, linearizing maps, and the Dynamical Mordell–Lang problem. *Journal of Number Theory*, 129(6):1392–1403, 2009.

[5] Dragos Ghioca, Thomas J. Tucker, and Michael E. Zieve. Intersections of polynomial orbits, and a Dynamical Mordell–Lang Conjecture. *Inventiones mathematicae*, 171(2):463–483, 2008.

[6] Dragos Ghioca, Thomas J. Tucker, Michael E. Zieve, et al. Linear relations between polynomial orbits. *Duke Mathematical Journal*, 161(7):1379–1410, 2012.

[7] Serge Lang. *Fundamentals of Diophantine Geometry*. Springer Science & Business Media, 2013.

[8] Rahim Moosa and Thomas Scanlon. F-structures and integral points on semiabelian varieties over finite fields. *American Journal of Mathematics*, pages 473–522, 2004.

[9] Junyi Xie. Dynamical Mordell–Lang Conjecture for birational polynomial morphisms on $\mathbb{A}^2$. *Mathematische Annalen*, 360(1-2):457–480, 2014.