Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Liang-Chung HSIA et Joseph SILVERMAN

On a dynamical Brauer–Manin obstruction

Tome 21, nº 1 (2009), p. 235-250.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_1_235_0>

Journal de Théorie des Nombres de Bordeaux **21** (2009), 235-250

On a dynamical Brauer–Manin obstruction

par Liang-Chung HSIA et Joseph SILVERMAN

Résumé. Soient $\varphi : X \to X$ un morphisme d'une variété définie sur un corps de nombres K, $V \subset X$ une sous-variété définie sur K et $\mathcal{O}_\varphi(P) = \{\varphi^n(P) : n \geq 0\}$ l'orbite d'un point $P \in X(K)$. Nous décrivons un principe local-global pour l'intersection $V \cap \mathcal{O}_\varphi(P)$. Ce principe peut être vu comme l'analogue dynamique de l'obstruction de Brauer–Manin. Nous prouvons que les points rationnels de $V(K)$ ne sont pas soumis à l'obstruction de Brauer–Manin pour l'application puissance sur $\mathbb{P}^2$ dans deux cas : (1) V est la translatée d'un tore. (2) V est une droite and P a une coordonnée prépériodique. Un outil principal des preuves est le théorème classique de Bang–Zsigmondy sur les diviseurs primitifs dans les suites. Nous prouvons également des résultats local-globaux analogues pour les systèmes dynamiques associés aux endomorphismes de variétés abéliennes.

Abstract. Let $\varphi : X \to X$ be a morphism of a variety defined over a number field K, let $V \subset X$ be a K-subvariety, and let $\mathcal{O}_\varphi(P) = \{\varphi^n(P) : n \geq 0\}$ be the orbit of a point $P \in X(K)$. We describe a local-global principle for the intersection $V \cap \mathcal{O}_\varphi(P)$. This principle may be viewed as a dynamical analog of the Brauer–Manin obstruction. We show that the rational points of $V(K)$ are Brauer–Manin unobstructed for power maps on $\mathbb{P}^2$ in two cases: (1) V is a translate of a torus. (2) V is a line and P has a preperiodic coordinate. A key tool in the proofs is the classical Bang–Zsigmondy theorem on primitive divisors in sequences. We also prove analogous local-global results for dynamical systems associated to endomoprhisms of abelian varieties.

Introduction

An important part of the field of arithmetic dynamics is the study of the arithmetic properties of algebraic points under iteration of maps on algebraic varieties. Many of the fundamental problems in this subject are transpositions to a dynamical setting of classical results and conjectures in the theory of Diophantine equations. A key tool in the study of Diophantine

---

The first author's research supported under project NSC 95-2115-M-008-002 of the National Science Council of Taiwan. The second author's research supported by NSA H98230-04-1-0064 and NSF DMS-0650017.

Mots clefs. arithmetic dynamical systems, local-global principle, Brauer–Manin obstruction.

equations is the application of local-global principles, such as the Hasse principle and the Brauer–Manin obstruction. In this paper we begin to develop a local-global theory for arithmetic dynamics.

Our starting point is a beautiful recent result of Scharaschkin, who showed in his thesis [6] that the Brauer–Manin obstruction for rational points on curves of genus at least 2 can be reformulated in non-cohomological terms as a purely adèlic-geometric statement. (See [4] for an analysis of Scharaschkin's criterion over function fields.) A straightforward translation of Scharaschkin's ideas into the dynamical setting yields the following criterion.

Definition. [Dynamical Brauer–Manin Obstruction] Let K be a number field, let X/K be a projective variety, and let

$$\varphi : X \to X$$

be a K-morphism of infinite order. Let A_K denote the ring of adèles of K, and for any point $P \in X(K)$, write $\mathsf{C}(\mathcal{O}_\varphi(P))$ for the closure of the orbit $\mathcal{O}_\varphi(P)$ of P in $X(\mathsf{A}_K)$. Let V be a subvariety of X that contains no nontrivial φ-preperiodic subvarieties (as defined in Section 1). We say that $V(K)$ is *Brauer–Manin unobstructed* (*for* φ) if for every point $P \in X(K)$ we have

$$\mathcal{O}_\varphi(P) \cap V(K) = \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K).$$

In Section 2 (Theorem 4) we show that $V(K)$ is Brauer–Manin unobstructed for the d^{th}-power map on $\mathbb{P}^2$ and varieties V that are translates of tori in $\mathbb{G}_m^2$. We also give partial results in Section 3 (Theorem 7) in the case that V is an arbitrary line in $\mathbb{P}^2$. In Section 4 (Theorem 9) we show that $V(K)$ is Brauer–Manin unobstructed for the the multiplication-by-d map on an abelian variety when V is a translate of a codimension 1 abelian subvariety of A. (This is the analog for abelian varieties of the multiplicative group result in Section 2.) All of these results rely on the existence of primitive divisors, i.e., Bang–Zsigmondy type theorems. Finally, in Section 5 (Theorem 11) we use results of Serre [8] and Stoll [11] to study the dynamical Brauer–Manin obstruction for multiplication maps and more general subvarieties of abelian varieties.

Remark 1. Zhang [12, Remark 4.2.3] has also studied algebraic dynamics over the adèles, although the questions that he raises have a somewhat different flavor from those considered in this paper. Let $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over a number field K and let S be a finite set of places of K. For each $v \in S$ there is a canonical probability measure μ_v on $\hat{\mathbb{P}}^N(\mathbb{C}_v)$ attached to φ. (Here $\hat{\mathbb{P}}^N$ is $\mathbb{P}^N$ if v is archimedean and $\hat{\mathbb{P}}^N$ is Berkovich projective space if v is nonarchimedean. In any case, the construction of μ_v is nontrivial.) Let $P_1, P_2, \ldots \in \mathbb{P}^N(\bar{K})$ be a sequence of algebraic points such that no infinite subsequence is contained in a preperiodic subvariety of $\mathbb{P}^N$ and assume further that $\hat{h}_\varphi(P_i) \to 0$ as $i \to \infty$, where $\hat{h}_\varphi$ is the canonical height associated to φ. Then Zhang conjectures that the the set $\{P_i\}_{i\geq 1}$ is equidistributed in $\prod_{v\in S} \hat{\mathbb{P}}^N(\mathbb{C}_v)$ with respect to the product measure $\prod_{v\in S} \mu_v$.

Acknowledgements. The authors would like to thank Felipe Voloch for making available a preprint of his paper [4], and Mike Rosen and the referee for a number of helpful suggestions. The second author would also like to thank Jing Yu, Yen-Mei Chen, his coauthor, and the NCTS for their hospitality during his visit when this work was initiated.

1. Definitions and notations

We set the following notation, which will remain fixed throughout this paper.

K	a number field.
M_K	the set of inequivalent places of K.
M_K^∞	the set of archimedean (infinite) places of K.
M_K^0	the set of nonarchimedean (finite) places of K.
$\mathfrak{p}_v$	the prime ideal associated to a finite place $v \in M_K$.
A_K	the ring of adèles of K.
X/K	a projective variety.
φ	a morphism $\varphi : X \to X$ defined over K.
V	a subvariety of X, defined over K.
$\mathcal{O}_\varphi(P)$	The (forward) orbit of a point $P \in X$ under iteration of φ.
$\mathsf{C}(\mathcal{O}_\varphi(P))$	The adèlic closure of $\mathcal{O}_\varphi(P)$ in $X(\mathsf{A}_K)$.

Definition. A subvariety W of X is said to be *φ-preperiodic* if there are integers $n > m$ such that $\varphi^n(W) = \varphi^m(W)$. If also $\dim(W) \geq 1$, we say that W is *nontrivial.*

It is clear that we have an inclusion

$$\mathcal{O}_\varphi(P) \cap V(K) \subseteq \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K),$$

since $\mathcal{O}_\varphi(P)$ is contained in its closure and $V(K)$ is contained in $V(\mathsf{A}_K)$. A point in the right-hand side is given by local data, and the following Brauer–Manin property asks if this local data is sufficient to characterize the set of global points.

Definition. With notation as above, let V_φ^{pp} be the union of all nontrivial φ-preperiodic subvarieties of V. Then we say that $V(K)$ is *Brauer–Manin unobstructed* (*for* φ) if for every point $P \in X(K)$ satisfying the condition $\mathcal{O}_\varphi(P) \cap V_\varphi^{\mathrm{pp}} = \emptyset$ we have

$$\mathcal{O}_\varphi(P) \cap V(K) = \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K).$$

Since we are assuming that X and V are projective, they are proper over K, so their sets of adèlic points are simply the products

$$X(\mathsf{A}_K) = \prod_{v \in M_K} X(K_v) \qquad \text{and} \qquad V(\mathsf{A}_K) = \prod_{v \in M_K} V(K_v).$$

Thus for example, a point $Q \in X(\mathsf{A}_K)$ has the form $Q = (Q_v)_{v \in M_K}$ with $Q_v \in X(K_v)$. Then by definition of the adèlic (in this case, product) topology, a point $Q \in X(\mathsf{A}_K)$ is in $\mathsf{C}(\mathcal{O}_\varphi(P))$ but not in $\mathcal{O}_\varphi(P)$ if and only if there is an infinite set of positive integers $\mathcal{N}_{P,Q} \subset \mathbb{N}$ such that for every $v \in M_K$,

$$Q_v = \mathop{v\text{-}\lim}_{\substack{n \in \mathcal{N}_{P,Q} \\ n \to \infty}} \varphi^n(P). \tag{1}$$

(We write v-lim to indicate that the limit is being taken in the v-adic topology.) N.B. The set of integers $\mathcal{N}_{P,Q}$ depends on P and Q, but it must be independent of $v \in M_K$.

Remark 2. We explain why it is necessary to assume some sort of condition on the nontrivial φ-preperiodic subvarieties of V. Suppose for example that V contains a nontrivial φ-preperiodic subvariety W and suppose further that $W(K)$ contains a point Q with infinite φ-orbit. We will construct a point $P \in X(K)$ with the property that

$$\mathcal{O}_\varphi(P) \cap V(K) \neq \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K). \tag{2}$$

Our assumptions mean that $\varphi^n(W) = \varphi^m(W)$ for some $n > m$ and that there is a non-preperiodic point $Q \in W(K)$. Replacing φ, W, and Q by φ^{n-m}, $\varphi^m(W)$, and $\varphi^m(Q)$, respectively, we have

$$\varphi(W) = W \qquad \text{and} \qquad Q \in W(K).$$

The variety W is projective, so $W(\mathsf{A}_K)$ is compact. The infinite set $\mathcal{O}_\varphi(Q)$ is contained in $W(\mathsf{A}_K)$, so its adèlic closure contains at least one accumulation point R. If R is not in $\mathcal{O}_\varphi(Q)$, then

$$R \notin \mathcal{O}_\varphi(Q) \cap V(K) \qquad \text{and} \qquad R \in \mathsf{C}(\mathcal{O}_\varphi(Q)) \cap V(\mathsf{A}_K),$$

so we are done.

We are reduced to the case that some point $\varphi^k(Q)$ in the orbit of Q is an adèlic accumulation point of the orbit. We set $P = \varphi^{k+1}(Q)$. Note that $\varphi^k(Q) \notin \mathcal{O}_\varphi(P)$, since we are assuming that Q is not φ-preperiodic. On the other hand, the accumulation points of $\mathcal{O}_\varphi(P)$ and $\mathcal{O}_\varphi(Q)$ in $X(\mathsf{A}_K)$ are the same, since the two sets differ by only finitely many elements. Hence

$$\varphi^k(Q) \notin \mathcal{O}_\varphi(P) \cap V(K) \qquad \text{and} \qquad \varphi^k(Q) \in \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K),$$

so in all cases we have constructed an orbit satisfying (2).

Remark 3. We will make frequent use of the following elementary observation. Let f be a rational function on X and let $Z(f)$ be the support of the polar divisor of f. Then for any $v \in M_K$, the function f is continuous on $X(K_v) \smallsetminus Z(f)$ with respect to the v-adic topology. In particular, if the v-adic closure of the set $\{\varphi^n(P) : n \in \mathcal{N}_{P,Q}\}$ in $X(K_v)$ is disjoint from $Z(f)$, then (1) implies that

$$f(Q_v) = \operatorname*{v\text{-lim}}_{n \in \mathcal{N}_{P,Q}} f(\varphi^n(P)).$$

2. Power maps and translated tori

In this section we consider the case that $X = \mathbb{P}^2$ and φ is a power map and we show that the rational points on a translated torus are Brauer–Manin unobstructed.

Theorem 4. *let*

$$\varphi : \mathbb{P}^2 \longrightarrow \mathbb{P}^2, \qquad \varphi([X, Y, Z]) = [X^d, Y^d, Z^d]$$

be the d^{th}-power map for some $d \geq 2$. Let $k \geq \ell \geq 1$, let $A, B \in K$, and let $V \subset \mathbb{P}^2$ be the curve

$$V : AX^k = BY^\ell Z^{k-\ell}. \tag{3}$$

Further let $P \in \mathbb{P}^2(K)$ be a point whose φ-orbit $\mathcal{O}_\varphi(P)$ is infinite. Then one of the following two statements is true:

(i) $\mathcal{O}_\varphi(P) \cap V(K) = \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K)$.

(ii) *The variety V is preperiodic for φ, and there exists an $i \geq 0$ such that $\mathcal{O}_\varphi(P) \cap \varphi^i(V)$ is an infinite set.*

A key tool in the proof of Theorem 4 is the following classical result on the distribution of the multiplicative orders of an element of K^* when reduced modulo primes.

Theorem 5. (Bang, Zsigmondy) *Let K be a number field, let $\lambda \in K^*$ be an element that is not a root of unity, and let*

$$S_\lambda = M_K^\infty \cup \{v \in M_K : |\lambda|_v \neq 1\}.$$

For each $v \notin S_\lambda$, let $f_v(\lambda)$ denote the order of λ in $\mathbb{F}_v^*$, the multiplicative group of residue field at v. Then the set

$$\mathbb{N} \smallsetminus \{f_v(\lambda) : v \notin S_\lambda\}$$

is finite, i.e., all but finitely many positive integers occur as the order modulo $\mathfrak{p}$ of λ for some prime $\mathfrak{p}$ of K.

Proof. This was originally proven by Bang [1], Zsigmondy [13], and Birkhoff and Vandiver [2] for $K = \mathbb{Q}$. It was extended to number fields by Postnikova and Schinzel [5] and in strengthened form by Schinzel [7]. $\square$

We use the Bang–Zsigmondy theorem to prove an adèlic property of iterated power maps.

Proposition 6. *Let $d \geq 2$, let $\lambda, \xi \in K^*$, let S be a finite set of places of K, and let $\mathcal{N}$ be an infinite sequence of positive integers. Suppose that for every $v \notin S$ we have*

$$\xi = v\text{-}\lim_{\substack{n \in \mathcal{N} \\ n \to \infty}} \lambda^{d^n}. \tag{4}$$

Then both ξ and λ are roots of unity, and there is an integer $r > 0$ such that $\xi = \lambda^{d^r}$.

Proof. If λ is a root of unity, then the set $\{\lambda^{d^n}\}_{n \geq 1}$ is finite and consists entirely of roots of unity. Hence the set $\{\lambda^{d^n}\}_{n \in \mathcal{N}}$ is a discrete subset of K_v (for any v), so the existence of the limit (4) implies that ξ is one of the roots of unity in this set.

We assume henceforth that λ is not a root of unity and derive a contradiction. Without loss of generality, we may adjoin finitely many places to S, so we may assume that S contains all archimedean places and that

$$|\lambda|_v = |\xi|_v = 1 \quad \text{for all } v \notin S.$$

Theorem 5 tells us that all but finitely many integers appear as the order of λ modulo $\mathfrak{p}_v$ for some place $v \notin S$. Hence after discarding finitely many elements from the set $\mathcal{N}$, we find for every $n \in \mathcal{N}$ there is a distinct place $v_n \notin S$ such that

$$f_{v_n}(\lambda) = d^n. \tag{5}$$

For notational convenience, we write $\mathfrak{p}_n$ for the prime ideal associated to v_n. Then (5) implies that

$$\lambda^{d^n} = \lambda^{f_{v_n}(\lambda)} \equiv 1 \pmod{\mathfrak{p}_n}.$$

We also observe that if $N \geq n$, then

$$\lambda^{d^N} = \left(\lambda^{d^n}\right)^{d^{N-n}} \equiv 1 \pmod{\mathfrak{p}_n}.$$

Hence if we choose any list of distinct elements $n_1, n_2, \ldots, n_t \in \mathcal{N}$, then

$$\lambda^{d^N} \equiv 1 \pmod{\mathfrak{p}_{n_1}\mathfrak{p}_{n_2}\cdots\mathfrak{p}_{n_t}} \qquad \text{for all } N \geq \max\{n_1, n_2, \ldots, n_t\}. \tag{6}$$

We now use the assumption (4) that

$$\xi = v\text{-}\lim_{n \in \mathcal{N}} \lambda^{d^n} \qquad \text{for all } v \notin S.$$

This says that λ^{d^n} is v-adically close to ξ for all large $n \in \mathcal{N}$, so in particular

$$\lambda^{d^n} \equiv \xi \pmod{\mathfrak{p}_i} \qquad \text{for all sufficiently large } n \in \mathcal{N} \text{ and all } 1 \le i \le t. \tag{7}$$

Combining (6) and (7) yields

$$\xi \equiv 1 \pmod{\mathfrak{p}_{n_1}\mathfrak{p}_{n_2}\cdots\mathfrak{p}_{n_t}}.$$

But t is arbitrary and the primes $\mathfrak{p}_{n_i}$ are distinct, so $\xi = 1$.

Now (4) becomes

$$\mathop{v\text{-}\lim}_{n\in\mathcal{N}} \lambda^{d^n} = 1 \qquad \text{for all } v \notin S, \tag{8}$$

and we want to derive a contradiction to the assumption that λ is not a root of unity.

Applying Theorem 5 again, we find an infinite set of positive integers $\mathcal{M}$ such that for

$$\gcd(m,d) = 1 \quad \text{for every } m \in \mathcal{M},$$

and such that for every $m \in \mathcal{M}$ there is a place $w_m \notin S$ satisfying

$$f_{w_m}(\lambda) = m.$$

Thus

$$\lambda^m = \lambda^{f_{w_m}(\lambda)} \equiv 1 \pmod{\mathfrak{p}_m}. \tag{9}$$

On the other hand, the limit (8) tells us that for any $m \in \mathcal{M}$ there is some $n(m)$ such that

$$\lambda^{d^{n(m)}} \equiv 1 \pmod{\mathfrak{p}_m}. \tag{10}$$

Combining (9) and (10) and using the assumption that $\gcd(m,d) = 1$ for all $m \in \mathcal{M}$, we conclude

$$\lambda \equiv 1 \pmod{\mathfrak{p}_m} \qquad \text{for all } m \in \mathcal{M}.$$

Since $\mathcal{M}$ is an infinite set and the $\mathfrak{p}_m$ are distinct prime ideals, this implies that $\lambda = 1$, contradicting the assumption that λ is not a root of unity. $\square$

We now have the tools needed to prove the main theorem of this section.

Proof of Theorem 4. We suppose that there is a point

$$Q \in \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K) \quad \text{with} \quad Q \notin \mathcal{O}_\varphi(P) \tag{11}$$

and will prove under this assumption that V is preperiodic for φ and that $\mathcal{O}_\varphi(P) \cap V$ is an infinite set. As noted earlier, the point Q has the form $Q = (Q_v)_{v\in M_K}$, and the assumption that $Q \in \mathsf{C}(\mathcal{O}_\varphi(P)) \smallsetminus \mathcal{O}_\varphi(P)$ means that there is an infinite set of positive integers $\mathcal{N}_{P,Q} \subset \mathbb{N}$ such that for every $v \in M_K$,

$$Q_v = \mathop{v\text{-}\lim}_{\substack{n\in\mathcal{N}_{P,Q}\\ n\to\infty}} \varphi^n(P).$$

To ease notation, we will leave off the $n \to \infty$ and the dependence on P and Q and write simply $v\text{-}\lim_{n\in\mathcal{N}}$ to mean the v-adic limit as $n \to \infty$ with $n \in \mathcal{N}_{P,Q}$.

Let $P = [\alpha, \beta, \gamma]$. We consider first the case that $\alpha\beta\gamma \neq 0$, so we may dehomogenize by setting $\gamma = 1$. Let S be the set

$$S = M_K^\infty \cup \{v \in M_K : |\alpha|_v \neq 1\} \cup \{v \in M_K : |\beta|_v \neq 1\},$$

so in particular, α and β are both S-units. (In the notation of Theorem 5, we have $S = S_\alpha \cup S_\beta$.)

The fact that

$$Q_v = \mathop{v\text{-}\lim}_{n\in\mathcal{N}} \varphi^n(P) = \mathop{v\text{-}\lim}_{n\in\mathcal{N}} [\alpha^{d^n}, \beta^{d^n}, 1]$$

implies that for all $v \notin S$, the point Q_v has the form

$$Q_v = [x_v, y_v, 1] \quad \text{with} \quad |x_v|_v = |y_v|_v = 1,$$

and further the sequences $\{\alpha^{d^n}\}_{n\in\mathcal{N}}$ and $\{\beta^{d^n}\}_{n\in\mathcal{N}}$ converge v-adically in K_v with

$$x_v = \mathop{v\text{-}\lim}_{n\in\mathcal{N}} \alpha^{d^n} \quad \text{and} \quad y_v = \mathop{v\text{-}\lim}_{n\in\mathcal{N}} \beta^{d^n}.$$

Let $f(x, y) = Ax^k - By^\ell$. We view f as a rational function on $\mathbb{P}^2$ and observe that $f(x, y) = 0$ is an affine equation for V. Since the quantities α, β, x_v, and y_v are all v-adic units (remember that are assuming that $v \notin S$), it follows that the v-adic closure of the set

$$\{\varphi^n(P) : n \in \mathcal{N}\}$$

is disjoint from the polar divisor of f. Also by assumption we have $Q_v \in V(K_v)$, so $f(Q_v) = 0$. Hence applying Remark 3, we find that

$$\begin{aligned} 0 &= \mathop{v\text{-}\lim}_{n\in\mathcal{N}} f\bigl(\varphi^n(P)\bigr) \\ &= A \cdot \bigl(\mathop{v\text{-}\lim}_{n\in\mathcal{N}} \alpha^{d^n}\bigr)^k - B \cdot \bigl(\mathop{v\text{-}\lim}_{n\in\mathcal{N}} \beta^{d^n}\bigr)^\ell. \end{aligned}$$

It follows that A and B are nonzero, since α and β are v-units, so a little bit of algebra yields

$$\mathop{v\text{-}\lim}_{n\in\mathcal{N}} \left(\frac{\alpha^k}{\beta^\ell}\right)^{d^n} = \frac{B}{A}. \tag{12}$$

Now Proposition 6 tells us that B/A and α^k/β^ℓ are roots of unity and that there is an integer $r \geq 1$ such that

$$\left(\frac{\alpha^k}{\beta^\ell}\right)^{d^r} = \frac{B}{A}. \tag{13}$$

The fact that B/A is a root of unity implies that V is preperiodic for φ. To see this, we write $V_{[A,B]}$ in order to indicate the dependence of V on the parameter $[A,B]\in\mathbb{P}^1$. It is clear from the definition of φ and V that $\varphi(V_{[A,B]})=V_{[A^d,B^d]}$, and hence

$$\varphi^n(V_{[A,B]})=V_{[A^{d^n},B^{d^n}]}.$$

It thus suffices to find $n>m$ satisfying $[A^{d^n},B^{d^n}]=[A^{d^m},B^{d^m}]$, which can be done since B/A is a root of unity. Hence V is preperiodic for φ.

Let $i\ge 0$ be an integer so that $\varphi^i(V)$ is periodic for φ, say with period q. The formula (13) says that $\varphi^r(P)\in V$, so we find that $\varphi^{i+r+qj}(P)\in\varphi^i(V)$ for all $j\ge 0$. This proves that $\mathcal{O}_\varphi(P)\cap\varphi^i(V)$ is an infinite set, which completes the proof of Theorem 4 under the assumption that $\alpha\beta\gamma\ne 0$.

It remains to deal with the case $\alpha\beta\gamma=0$, where we recall that P is the point $P=[\alpha,\beta,\gamma]\in\mathbb{P}^2$. Suppose first that $\gamma=0$. The assumption that $\mathcal{O}_\varphi(P)$ is infinite implies that $\alpha\beta\ne 0$, so we can dehomogenize and write $P=[\alpha,1,0]$ with $\alpha\ne 0$. Then just as in the case $\gamma=1$, we find that

$$Q_v=v\text{-}\lim_{n\in\mathcal{N}}[\alpha^{d^n},1,0]\qquad\text{for all } v\notin S,$$

and the fact that $Q_v\in V$ tells us that

$$v\text{-}\lim_{n\in\mathcal{N}}\alpha^{d^n}=B/A.$$

Applying Proposition 6 again, we conclude that α and B/A are roots of unity. But this implies the point $P=[\alpha,1,0]$ is preperiodic for φ, contradicting to our assumption that P has infinite orbit.

Next suppose that $\gamma\ne 0$ and $\beta=0$. We dehomogenize P in the form $P=[\alpha,0,1]$, and then

$$Q_v=v\text{-}\lim_{n\in\mathcal{N}}[\alpha^{d^n},0,1].$$

Taking any v with $|\alpha|_v=1$, the fact that $Q_v=[x_v,0,1]\in V$ implies that $Ax_v^k=B\cdot 0^\ell=0$, so $A=0$. (Note that $x_v\ne 0$ since $|x_v|_v=1$.) Thus V is the line $Y=0$, i.e., it is given by the equation $BY^\ell=0$, so it is fixed by φ and the entire orbit $\mathcal{O}_\varphi(P)$ lies on V.

Finally, if $\alpha=0$, the same argument shows that $B=0$, so V is the line $X=0$, hence is fixed by φ and $\mathcal{O}_\varphi(P)\subset V$. □

3. Power maps and linear varieties

In this section we again take φ to be the a power map

$$\varphi:\mathbb{P}^2\longrightarrow\mathbb{P}^2,\qquad \varphi([X,Y,Z])=[X^d,Y^d,Z^d]$$

and consider a line $V\subset\mathbb{P}^2$ given by an equation

$$V: AX+BY+CZ=0. \tag{14}$$

Let

$$P=[\alpha,\beta,\gamma] \tag{15}$$

be the given point with infinite φ-orbit.

Note that if $ABC = 0$, then Theorem 4 says that $V(K)$ is Brauer–Manin unobstructed. We now prove analogous results for $ABC \neq 0$ when P has various special forms.

Theorem 7. *Let V and P be as given in* (14) *and* (15) *and assume that $ABC \neq 0$. Further assume that one of the following is true*:

(a) *One of the ratios α/β, β/γ, or α/γ is a root of unity.*
(b) *One of the coordinates α, β, or γ is zero.*

Then

$$\mathcal{O}_\varphi(P) \cap V(K) = \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K).$$

(*It is easy to check that the assumption that $ABC \neq 0$ implies that V cannot be preperiodic for φ.*)

Proof. (a) It suffices to consider the case that β/γ is a root of unity. Dividing the equation of V by $-CZ$ and the coordinates of P by $-\gamma$, without loss of generality we can use affine coordinates of the form

$$V : Ax + By = 1 \qquad \text{and} \qquad P = (\alpha, \beta).$$

Our assumptions are that $AB \neq 0$ and β is a root of unity. Further, since P has infinite φ-orbit, it follows that $\alpha \neq 0$ and α is not a root of unity.

We assume that there is a point

$$Q \in \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K) \quad \text{with} \quad Q \notin \mathcal{O}_\varphi(P)$$

and derive a contradiction. (We will show that this forces α to be a root of unity.) As in the proof of Theorem 4, we let $\mathcal{N} = \mathcal{N}_{P,Q}$ be an infinite set of integers so that

$$Q_v = (x_v, y_v) = \mathop{v\text{-lim}}_{n\in\mathcal{N}} \varphi^n(P) = \mathop{v\text{-lim}}_{n\in\mathcal{N}} (\alpha^{d^n}, \beta^{d^n}) \quad \text{for all } v \in M_K \smallsetminus S_\alpha.$$

The assumption that β is a root of unity implies that β^{d^n} takes on only finitely many distinct values, so replacing $\mathcal{N}$ with a subsequence, we may assume that $\beta^{d^n} = \beta_0$ is constant for all $n \in \mathcal{N}$. Thus

$$x_v = \mathop{v\text{-lim}}_{n\in\mathcal{N}} \alpha^{d^n} \quad \text{and} \quad y_v = \beta_0 \quad \text{for all } v \in M_K \smallsetminus S_\alpha.$$

Note that β_0 is a root of unity.

The fact that $Q_v \in V$ tells us that for all v with $|\alpha|_v = 1$.

$$\mathop{v\text{-lim}}_{n\in\mathcal{N}} \alpha^{d^n} = x_v = \frac{1 - B\beta_0}{A} \quad \text{for all } v \in M_K \smallsetminus S_\alpha.$$

It follows from Proposition 6 that α is a root of unity, contradicting our assumption that P has infinite φ-orbit.

(b) By symmetry, we may assume that $\gamma = 0$. Then the fact that P is not preperiodic implies that $\alpha\beta \neq 0$ and α/β is not a root of unity. Dehomogenizing P with respect to the Y-coordinate, we can write P in the form $P = [\alpha, 1, 0]$ with α not a root of unity. Suppose now that

$$\mathcal{O}_\varphi(P) \cap V(K) \neq \mathsf{C}(\mathcal{O}_\varphi(P)) \cap V(\mathsf{A}_K).$$

Then as in the proofs of Theorem 4 and part (a) of this theorem, there is a finite set of places S so that

$$A\, v\text{-}\lim_{n\in\mathcal{N}} \alpha^{d^n} + B \cdot 1 = C \cdot 0 \qquad \text{for all } v \notin S.$$

We have $AB \neq 0$ by assumption, so Proposition 6 tells us that α is a root of unity, contradicting our assumption that P has infinite φ-orbit. $\square$

4. Abelian varieties and translated abelian subvarieties

In this section we prove an analog of Theorem 4 for abelian varieties. The key tool will be the following elliptic analog of the Bang–Zsigmondy theorem (Theorem 5).

Theorem 8. *Let E/K be an elliptic curve defined over a number field K, let $P \in E(K)$ be a nontorsion point, and let $S \subset M_K$ be a finite set of places including M_K^∞ and all places of bad reduction for E. For each place $v \notin S$, let $f_v(P)$ be the order of $P \pmod{\mathfrak{p}_v}$ in $E(\mathbb{F}_{\mathfrak{p}_v})$. Then the set*

$$\mathbb{N} \smallsetminus \{f_v(P) : v \notin S\}$$

is finite.

Proof. See [9] for the case $K = \mathbb{Q}$ and [3] for general number fields. We note that the assertion of Theorem 8 is not an elementary fact, since its proof requires a strong form of Siegel's theorem [10, IX.3.1] on integral points on elliptic curves. $\square$

Theorem 9. *Let $K/\mathbb{Q}$ be a number field, let A/K be an abelian variety, and let B/K be an abelian subvariety of A of codimension 1. We fix a point $T \in A(K)$ and let $V = B + T$ be the translation of B by T.*

Let $d \geq 2$ be an integer and consider the multiplication-by-d map

$$[d] : A \to A.$$

Let $P \in A(K)$ be a nontorsion point. Then one of the following two statements is true:

(i) $\mathcal{O}_d(P) \cap V(K) = \mathsf{C}(\mathcal{O}_d(P)) \cap V(\mathsf{A}_K)$.

(ii) *The variety V is $[d]$-preperiodic.*

(*Here $\mathcal{O}_d$ denotes the orbit under the multiplication-by-d map on A.*) *Further, in case* (ii), *the point T has finite order in the quotient variety A/B.*

Proof. Suppose that (i) is false, and let

$$(Q_v)_{v\in M_K} \in \mathsf{C}(\mathcal{O}_d(P)) \cap V(\mathsf{A}_K) \quad \text{with} \quad (Q_v)_{v\in M_K} \notin \mathcal{O}_d(P) \cap V(K).$$

As in the proof of Theorem 4, this means that there is an infinite set of positive integers $\mathcal{N} \subset \mathbb{N}$ such that for every $v \in M_K$,

$$Q_v = v\text{-}\lim_{\substack{n\in\mathcal{N}\\ n\to\infty}} [d^n](P) \in V(K_v).$$

We now pass to the quotient abelian variety $E = A/B$. Since B has codimension 1 in A, it follows that E is an abelian variety of dimension 1, i.e., E is an elliptic curve. For convenience, we use bars to denote the image of points of A in E. Note that $Q_v \in V = B + T$, so on the quotient variety we see that

$$\bar{Q}_v = \bar{T} \in E$$

is independent of v. Hence for every $v \in M_K$ we have

$$v\text{-}\lim_{\substack{n\in\mathcal{N}\\ n\to\infty}} [d^n](\bar{P}) = \bar{T} \quad \text{in the } v\text{-adic topology,} \tag{16}$$

so in particular, for every $v \in M_K$ there is an N_v so that

$$[d^n](\bar{P}) \equiv \bar{T} \pmod{\mathfrak{p}_v} \qquad \text{for all } n \in \mathcal{N} \text{ with } n \geq N_v. \tag{17}$$

We consider two cases. First, suppose that $\bar{P} \in E(K)$ is a nontorsion point. Then we can apply the elliptic Zsgmondy theorem (Theorem 8) to $\bar{P} \in E(K)$. This tells us that for all but finitely many $n \in \mathcal{N}$ there is a place $v_n \in M_K$ such that

$$f_{v_n}(\bar{P}) = d^n, \tag{18}$$

i.e., the point $\bar{P}$ mod $\mathfrak{p}_{v_n}$ has order d^n in $E(\mathbb{F}_{\mathfrak{p}_{v_n}})$. Hence if $m \geq n$, then

$$[d^m](\bar{P}) = [d^{m-n}][d^n](\bar{P}) = [d^{m-n}][f_{v_n}](\bar{P}) \equiv \bar{O} \pmod{\mathfrak{p}_{v_n}}. \tag{19}$$

Now choose distinct integers $n_1, n_2, \ldots, n_t \in \mathcal{N}$ so that (18) is true and, to ease notation, let $v_1, v_2, \ldots, v_t$ be the associated valuations. Then for any integer $m \in \mathcal{N}$ satisfying

$$m \geq \max\{N_{v_1}, N_{v_2}, \ldots, N_{v_t}, n_1, n_2, \ldots, n_t\}$$

we have for every $1 \leq i \leq t$,

$$\begin{aligned} [d^m](\bar{P}) &\equiv \bar{T} \pmod{\mathfrak{p}_{v_i}} &\qquad& \text{from (17),} \\ [d^m](\bar{P}) &\equiv \bar{O} \pmod{\mathfrak{p}_{v_i}} && \text{from (19).} \end{aligned}$$

Hence

$$\bar{T} \equiv \bar{O} \pmod{\mathfrak{p}_{v_i}} \qquad \text{for all } 1 \leq i \leq t.$$

Since t is arbitrary, we conclude that $\bar{T} = \bar{O}$. Thus $T \in B$, which implies that $V = B + T = B$, since B is an abelian subvariety of A. In particular, V is preperiodic for $[d]$, since in fact $[d](V) = V$.

Next we suppose that $\bar{P}$ is a torsion point of $E(K)$. Then the set of points $\{[d^n](\bar{P}) : n \in \mathcal{N}\}$ is finite, so the existence of the limit (16) implies that $\bar{T}$ is one of the torsion points appearing in this set. Hence

$$[d^n](V) = [d^n](B+T) = B + [d^n](T)$$

takes on only finitely many values, so V is preperiodic for $[d]$. □

Remark 10. We thank the referee for noting that Theorems 4 and 9 might be combined and generalized to the case that A is a semiabelian variety and V is a translate of a semiabelian subvariety B of codimension one. The proof would use the Bang–Zsigmondy theorem for the multiplicative group or for elliptic curves depending on the nature of the one-dimensional quotient group A/B.

5. Abelian varieties and general subvarieties

In this section we prove a local-global result for dynamical systems on abelian varieties that is related to the Brauer–Manin obstruction. Roughly speaking, we assume that $V(K)$ is Brauer–Manin unobstructed in $A(K)$ (as described in Theorem 11 (ii) below) and we prove that orbits of multiplication maps are Brauer–Manin unobstructed. We set the following notation:

$K/\mathbb{Q}$	a number field.
A/K	an abelian variety.
V/K	a subvariety of A/K.
$A(K_v)^0$	identity component of $A(K_v)$ for $v \in M_K^\infty$, 0 for $v \in M_K^0$.
$A(\mathsf{A}_K)_\bullet$	$= \prod_{v \in M_K} A(K_v)/A(K_v)^0$.
$V(\mathsf{A}_K)_\bullet$	the image of $V(\mathsf{A}_K)$ under the projection $A(\mathsf{A}_K) \to A(\mathsf{A}_K)_\bullet$.

Theorem 11. *We make the following assumptions*:

(i) *V does not contain a translate of a positive-dimensional abelian subvariety of A.*

(ii) *Let $\mathsf{C}(A(K))$ denote the closure of $A(K)$ in $A(\mathsf{A}_K)_\bullet$, and embed $V(K)$ and $V(\mathsf{A}_K)_\bullet$ into $A(\mathsf{A}_K)_\bullet$ in the natural way. Then*

$$V(K) = V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(A(K)).$$

Then for all integers $d \geq 2$ and all nontorsion points $P \in A(K)$ we have

$$V(K) \cap \mathcal{O}_d(P) = V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(\mathcal{O}_d(P)).$$

The proof of Theorem 11 uses the following results of Serre and Stoll.

Theorem 12. *Let*

$$\hat{A}(K) = A(K) \otimes \hat{\mathbb{Z}}$$

be the profinite completion of $A(K)$, and let S be a set of places of K of density 1, i.e., the primes corresponding to the finite places in S have density 1 in the usual sense.

(a) *The map*

$$\hat{A}(K) \longrightarrow \prod_{v\in S} A(K_v)/A(K_v)^0$$

is injective.

(b) *The natural map* $\hat{A}(K) \to A(\mathsf{A}_K)_\bullet$ *induces an isomorphism between* $\hat{A}(K)$ *and* $\mathsf{C}(A(K))$*, the topological closure of* $A(K)$ *in* $A(\mathsf{A}_K)_\bullet$.

(c) *Assume further that* $S \subset M_K^0$ *and that* A *has good reduction at every place in* S*. Then the composition of the natural maps*

$$\hat{A}(K) \longrightarrow \prod_{v\in S} A(K_v) \longrightarrow \prod_{v\in S} A(\mathbb{F}_v)$$

is injective.

Proof. (a) and (b) are part of [8, Theorem 3], and we refer to [11, Proposition 3.7] for the proof. The statement in (c) is part of [11, Theorem 3.10]. □

Corollary 13. *Let* H *be a subgroup of* $A(K)$ *and let* $\mathsf{C}(H)$ *be the closure of* H *inside* $A(\mathsf{A}_K)_\bullet$*. Then under the assumption*

$$V(K) = V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(A(K)) \tag{20}$$

from Theorem 11*, we have*

$$V(K) \cap H = V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(H).$$

Proof. Using the assumption (20), we have

$$V(K) \cap H \subset V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(H) \subset V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(A(K)) = V(K), \tag{21}$$

Now let $Q \in V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(H) \subset V(K)$ and suppose that $Q \notin H$. Then by definition there is a sequence of points

$$P_1, P_2, P_3, \dots \in H \quad \text{such that} \quad \lim_{n\to\infty} P_n = Q \quad \text{in the adèlic topology.}$$

In particular, if A has good reduction at $v \in M_K^0$, then

$$Q \equiv P_n \pmod{\mathfrak{p}_v} \quad \text{for all sufficiently large } n.$$

But every P_n is in H, so we conclude that for all but finitely many $v \in M_K$ we have

$$Q \bmod \mathfrak{p}_v \in H \bmod \mathfrak{p}_v.$$

The group $A(K)$ has no non-trivial divisible elements, so the natural map $A(K) \to \hat{A}(K)$ is an injection. It follows from Theorem 12(c) that $Q \in H$. This contradiction proves the inclusion

$$V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(H) \subset H,$$

which completes the proof of Corollary 13. □

We now have the tools needed to prove the main result of this section.

Proof of Theorem 11. Let $H = \mathbb{Z}P$ be the (free) subgroup of $A(K)$ generated by P, so in particular $\mathcal{O}_d(P) \subset H$. Then

$$V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(\mathcal{O}_d(P)) \subset V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(H) = V(K) \cap H. \tag{22}$$

where the equality is from Corollary 13. Now let

$$Q \in V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(\mathcal{O}_d(P)).$$

It follows from (22) that $Q \in V(K)$ is a K-rational point of V and further that $Q \in H$, so $Q = mP$ for some integer m.

Suppose now that $Q \notin \mathcal{O}_d(P)$. Then we can find an infinite sequence of positive integers $\{r_1, r_2, r_3, \ldots\}$ so that

$$\lim_{i\to\infty} d^{r_i} P = Q = mP \quad \text{in the adèlic topology.}$$

Theorem 12(a,b) tells us that

$$\mathsf{C}(H) = H \otimes \hat{\mathbb{Z}},$$

which implies that $d^{r_i} \to m$ in $\hat{\mathbb{Z}}$ as $i \to \infty$. Hence for every prime p we have

$$m = p\text{-}\lim_{i\to\infty} d^{r_i}.$$

Taking p to be any prime dividing d (this is where we use the assumption that $d \geq 2$), we find that $m = 0$. On the other hand, if p is a prime not dividing d, then $|d|_p = 1$, so $|m|_p = 1$. This contradiction shows that

$$V(\mathsf{A}_K)_\bullet \cap \mathsf{C}(\mathcal{O}_d(P)) \subset \mathcal{O}_d(P),$$

which completes the proof of Theorem 11. □

Remark 14. More generally, let $\varphi : A \to A$ be a K-endomorphism of A with the property that the subring $\mathbb{Z}[\varphi] \subset \mathrm{End}(A)$ is an integral domain. (If A is geometrically simple, this will be true for any endomorphism φ of infinite order.) Then we can repeat the proof of Theorem 11, *mutatis mutandis*, using the subgroup $H = \mathbb{Z}[\varphi]P$ and the fact that the fraction field of $\mathbb{Z}[\varphi]$ is a number field. Note that if A is not simple, then it is possible for $\mathbb{Z}[\varphi]$ to have zero-divisors.

References

[1] A. S. Bang, *Taltheoretiske Undersogelser*. Tidsskrift Mat. **4**(5) (1886), 70–80, 130–137.

[2] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*. Ann. of Math. (2) **5**(4) (1904), 173–180.

[3] J. Cheon and S. Hahn, *The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve*. Acta Arith. **88**(3) (1999), 219–222.

[4] B. Poonen and J. F. Voloch, *The Brauer–Manin obstruction for subvarieties of abelian varieties over function fields*. Annals of Math., to appear.

[5] L. P. Postnikova and A. Schinzel, *Primitive divisors of the expression $a^n - b^n$ in algebraic number fields*. Mat. Sb. (N.S.) **75**(117) (1968), 171–177.

[6] V. Scharaschkin, *Local-global problems and the Brauer–Manin obstruction*. PhD thesis, University of Michigan, 1999.

[7] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields.* J. Reine Angew. Math. **268/269** (1974), 27–33.
[8] J.-P. Serre, *Sur les groupes de congruence des variétés abéliennes. II.* Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), 731–737.
[9] J. H. Silverman, *Wieferich's criterion and the abc-conjecture.* J. Number Theory **30**(2) (1988), 226–237.
[10] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Volume **106** of Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.
[11] M. Stoll, *Finite descent obstructions and rational points on curves.* Algebra & Number Theory **1** (2007), 349–391.
[12] S.-W. Zhang, *Distributions in algebraic dynamics.* In Differential Geometry: A Tribute to Professor S.-S. Chern, Surv. Differ. Geom., Vol. X, pages 381–430. Int. Press, Boston, MA, 2006.
[13] K. Zsigmondy, *Zur Theorie der Potenzreste.* Monatsh. Math. Phys. **3**(1) (1892), 265–284.

Liang-Chung Hsia
Department of Mathematics
National Central University
Chung-Li, 32054 Taiwan, R. O. C.
E-mail: hsia@math.ncu.edu.tw

Joseph Silverman
Mathematics Department
Box 1917
Brown University
Providence, RI 02912 USA
E-mail: jhs@math.brown.edu