JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Chia-Liang SUN

A Local-Global Criteria of Affine Varieties Admitting Points in Rank-One Subgroups of a Global Function Field

Tome 30, nº 1 (2018), p. 59-79.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_1_59_0>

Journal de Théorie des Nombres
de Bordeaux **30** (2018), 59–79

A Local-Global Criteria of Affine Varieties Admitting Points in Rank-One Subgroups of a Global Function Field

par Chia-Liang SUN

Résumé. Pour toute variété affine sur un corps fini, nous montrons qu'elle admet des points à coordonnées dans un sous-groupe multiplicatif de rang 1 d'un corps de fonctions global sur ce corps fini si et seulement si cette variété admet des points à coordonnées dans la clôture topologique de ce sous-groupe dans le produit des groupes multiplicatifs des complétions locales du corps de fonctions sur toutes les places sauf un nombre fini d'entre elles. Sous l'hypothèse de Riemann généralisée, nous montrons aussi que l'énoncé ci-dessus est vrai pour toute réunion finie de variétés affines linéaires sur tout corps global et pour beaucoup de sous-groupes multiplicatifs de rang 1. Dans le cas où cette réunion finie est irréductible et définie sur un corps fini, nous montrons de plus que les deux ensembles de points coincident.

Abstract. For every affine variety over a finite field, we show that it admits points with coordinates in an arbitrary rank-one multiplicative subgroup of a global function field over this finite field if and only if this variety admits points with coordinates in the topological closure of this subgroup in the product of the multiplicative group of those local completion of this global function field over all but finitely many places. Under the generalized Riemann hypothesis, we also show that the above statement holds for every finite union of affine linear varieties over any global field and for many rank-one multiplicative subgroup. In the case where this finite union is irreducible and defined over a finite field, we moreover show that the topological closure of the set of all such former points is exactly the set of all such latter points.

Manuscrit reçu le 7 février 2016, révisé le 13 octobre 2016, accepté le 17 octobre 2016.
2010 *Mathematics Subject Classification.* 14G05.
Mots-clefs. local-global criteria, constant subfield, topological closure.

1. Introduction

Let K be a global function field over a finite field k of positive characteristic p. We denote by k^{alg} the algebraic closure of k inside a fixed algebraic closure K^{alg} of K. The definition that K is a global function field over k in particular forces that $k^{\text{alg}} \cap K = k$. Let Σ_K be the set of all places of K. For each $v \in \Sigma_K$, denote by K_v the completion of K at v; by O_v, $\mathfrak{m}_v$, and $\mathbb{F}_v$ respectively the valuation ring, the maximal ideal, and the residue field associated to v. For each finite subset $S \subset \Sigma_K$, we denote by O_S the ring of S-integers in K. For any commutative ring R with unity, denote by R^* the group of its units. We fix a subgroup $\Gamma \subset O_S^*$ for some finite $S \subset \Sigma_K$. Let M be a natural number, and $\mathbb{A}^M$ be the affine M-space, whose coordinate is denoted by $\mathbf{X} = (X_1, \ldots, X_M)$. For each polynomial $f \in K[X_1, \ldots, X_M]$, we denote by H_f the hypersurface in $\mathbb{A}^M$ defined by f. If the total degree of f is one, we say that H_f is a hyperplane. By a linear K-variety in $\mathbb{A}^M$, we mean an intersection of K-hyperplanes. We say that a closed K-variety W in $\mathbb{A}^M$ is homogeneous if W can be defined by homogeneous polynomials.

For any closed K-variety W in $\mathbb{A}^M$ and any subset Θ of some ring containing K, let $W(\Theta)$ denote the set of points on W with each coordinate in Θ. For each subset $\widetilde{S} \subset \Sigma_K$, we endow $\prod_{v\in\widetilde{S}} K_v^*$ with the natural product topology; via the diagonal embedding, we identify $W(\Gamma)$ with its image $W(\Gamma)_{\widetilde{S}}$ in $W(\prod_{v\in\widetilde{S}} K_v^*)$ and denote by $\overline{W(\Gamma)_{\widetilde{S}}}$ its topological closure. We naturally identify Γ with $\mathbb{A}^1(\Gamma)$, and write $\overline{\Gamma_{\widetilde{S}}}$ for $\overline{\mathbb{A}^1(\Gamma)_{\widetilde{S}}}$. For each place $v \in \Sigma_K$, we write $\overline{\Gamma_v}$ for $\overline{\Gamma_{\{v\}}}$. Note that $\overline{\Gamma_{\widetilde{S}}} \subset \prod_{v\in\widetilde{S}} \overline{\Gamma_v}$. We fix a cofinite subset $\Sigma \subset \Sigma_K$, and drop the lower subscript Σ in the notation of topological closure; for example, we simply write $\overline{\Gamma}$ for $\overline{\Gamma_\Sigma}$.

For any closed K-variety W in $\mathbb{A}^M$, we let $I_W \subset K[X_1, \ldots, X_M]$ be its vanishing ideal; for each $v \in \Sigma_K$, denoting by $I_W^{(v)}$ the subset of $I_W \cap O_v[X_1, \ldots, X_M]$ which consists of polynomials with some coefficients not in $\mathfrak{m}_v$, we define

$$W\left((O_v/\mathfrak{m}_v^{n_v})^*\right) = \left\{ P \in \mathbb{A}^M(O_v/\mathfrak{m}_v^{n_v}) : \begin{array}{l} P = (x_1 + \mathfrak{m}_v^{n_v}, \ldots, x_M + \mathfrak{m}_v^{n_v}) \\ x_i \in O_v^* \text{ for all } i \\ f(x_1, \ldots, x_M) \in \mathfrak{m}_v^{n_v} \text{ for all } f \in I_W^{(v)} \end{array} \right\}$$

for each integer $n_v \geq 1$; for each finite subset $S \subset \Sigma_K$ and each tuple $(n_v)_{v\in S}$ of natural numbers indexed by S. we declare

$$W\left(\prod_{v\in S} (O_v/\mathfrak{m}_v^{n_v})^*\right) = \prod_{v\in S} W\left((O_v/\mathfrak{m}_v^{n_v})^*\right).$$

Remark 1.1. In the case where W is defined over k, the ring $O_v/\mathfrak{m}_v^{n_v}$ is a k-algebra; the set $W(O_v/\mathfrak{m}_v^{n_v})$ is defined in the usual way, and the set $W((O_v/\mathfrak{m}_v^{n_v})^*)$ we define above consists of exactly those points in $W(O_v/\mathfrak{m}_v^{n_v})$ with each coordinate being an unit.

For any closed K-variety W in $\mathbb{A}^M$, we consider the following conjectures.

Conjecture 1.2. $W(\overline{\Gamma_{\widetilde{S}}}) = \overline{W(\Gamma)_{\widetilde{S}}}$ for every cofinite subset $\widetilde{S} \subset \Sigma_K$.

Conjecture 1.3. For every cofinite subset $\widetilde{S} \subset \Sigma_K$, there exists a finite subset $S_0 \subset \widetilde{S}$ and a tuple $(n_v)_{v \in S_0}$ of natural numbers indexed by S_0 such that for every $v \in S_0$ we have that $\Gamma \subset O_v^*$, and in the following commutative diagram

$$\begin{array}{ccc} W(\Gamma) & \longrightarrow & W\left(\prod_{v\in S_0}(O_v/\mathfrak{m}_v^{n_v})^*\right) \\ \downarrow & & \downarrow \\ \mathbb{A}^M(\Gamma) & \longrightarrow & \mathbb{A}^M\left(\prod_{v\in S_0}(O_v/\mathfrak{m}_v^{n_v})^*\right) \end{array}$$

we have that $W(\Gamma) = \emptyset$ if and only if the image of the bottom map and that of the right hand downward map do not meet.

Conjecture 1.4. For every cofinite subset $\widetilde{S} \subset \Sigma_K$, we have that $W(\Gamma) = \emptyset$ if and only if $W(\overline{\Gamma_{\widetilde{S}}}) = \emptyset$.

Trivially, we have that Conjecture 1.2 implies Conjecture 1.4. Since the constant field k is finite, Conjecture 1.3 and Conjecture 1.4 are actually equivalent. (Corollary 2.2 in Section 2)

The author [5] proves Conjecture 1.2 for linear varieties W satisfying some hypothesis, which particularly rule outs the case where W has any irreducible component defined over the constant field k with dimension greater than one. When W is a hyperplane passing through $(0, \ldots, 0) \in \mathbb{A}^M$, Conjecture 1.3 reformulates the function field analog of an old conjecture raised by Skolem [4]. (cf. [1, Remark 2.4]). It is predicted by Poonen ([3, Conjecture 5.1]) that the number-field counterpart of Conjecture 1.3 always holds with a tuple $(n_v)_{v \in S_0}$ being all ones; however, we will see that the analog of this prediction in the present setting cannot holds in general.

Note that Conjecture 1.2 (hence both Conjecture 1.3 and Conjecture 1.4) holds trivially if Γ has rank zero. In this paper, we focus on the case where Γ has rank one. We investigate Conjecture 1.2, Conjecture 1.3 and Conjecture 1.4 in the case where W is defined over the constant field k. In this situation, we prove that Conjecture 1.4 always holds; more precisely, we establish the next result saying that Conjecture 1.3 always holds with some effectively determined finite subset $S_0 \subset \Sigma$ and the tuple $(n_v)_{v \in S_0}$ being all ones.

Theorem 1.5. *Let W be a closed k-variety in $\mathbb{A}^M$. Suppose that Γ has rank at most one. Then there exists an effectively determined finite subset $S_0 \subset \Sigma$ such that $\Gamma \subset O_v^*$ for every $v \in S_0$, and in the following commutative diagram*

$$\begin{array}{ccc} W(\Gamma) & \longrightarrow & W\left(\prod_{v \in S_0} \mathbb{F}_v^*\right) \\ \downarrow & & \downarrow \\ \mathbb{A}^M(\Gamma) & \longrightarrow & \mathbb{A}^M\left(\prod_{v \in S_0} \mathbb{F}_v^*\right) \end{array}$$

we have that $W(\Gamma) = \emptyset$ if and only if the image of the bottom map and that of the right hand downward map do not meet.

Remark 1.6. Theorem 1.5 would not hold if we did not assume that W is defined over k. In fact, Conjecture 1.3 cannot hold with a tuple $(n_v)_{v \in S_0}$ *bounded* over *all* closed K-varieties W in $\mathbb{A}^M$. See Example 3.7.

In the case where W is a hypersurface, Pasten and the author [2] show that Theorem 1.5 holds with some *singleton* S_0, assuming the truth of the next conjecture involving the following condition, where $m \in \mathbb{N}$ and $r \in \mathbb{N} \setminus p\mathbb{N}$.

Cond(m, r): For every $(a_1, \dots, a_m) \in \mathbb{A}^m(k)$ and every $(e_1, \dots, e_m) \in \mathbb{A}^m(\mathbb{Z})$ such that $\sum_{i=1}^m a_i \neq 0$, we have $\sum_{i=1}^m a_i \xi_r^{e_i} \neq 0$, where $\xi_r \in (k^{\mathrm{alg}})^*$ is a primitive r-th root of unity.

Conjecture 1.7. For any $m \in \mathbb{N}$, the condition Cond(m, r) holds for infinitely many $r \in \mathbb{N} \setminus p\mathbb{N}$.

Remark 1.8. It is known that there is a set E of rational primes with $|E| \leq 2$ such that Conjecture 1.7 holds if $p \notin E$. Under the generalized Riemann hypothesis, we have that $E = \emptyset$, i.e. Conjecture 1.7 holds in general. If we further assume that the set of Wieferich primes to any given basis has natural density zero, then for any given $m \in \mathbb{N}$ we may find a prime $\ell \in \mathbb{N} \setminus p\mathbb{N}$ such that Cond(m, ℓ^j) holds for each $j \in \mathbb{N}$. (For details, see [2].) Having such a prime $\ell \in \mathbb{N} \setminus p\mathbb{N}$, we will show in conclusion (3) of Theorem 3.6 in Section 3 that Theorem 1.5 holds with some *effectively determined singleton* S_0.

As a corollary of Theorem 1.5 and an application of one of the key intermediate results in [5], we establish the following conditional result concerning Conjecture 1.4.

Theorem 1.9. *Let W be a union of linear K-varieties. Suppose that Γ has rank one, and that there is a non-torsion element $\gamma \in \Gamma$ such that for every $c \in k^*$ the element $c\gamma$ does not have any n-th root in K^* for any $n \in \mathbb{N} \backslash p\mathbb{N} \setminus \{1\}$. Assume that Conjecture 1.7 holds. Then we have that $W(\prod_{v \in \Sigma} \overline{\Gamma_v}) \neq \emptyset$ implies $W(\Gamma) \neq \emptyset$; in particular, Conjecture 1.4 holds.*

Theorem 1.9 is the first result showing the truth of Conjecture 1.4 for a given W of an arbitrary dimension without imposing any hypothesis on its positive-dimensional subvarieties.

Obtained from the more general Theorem 3.12, the next result shows that in the case where Γ has rank one, Conjecture 1.2 holds for a large class of k-varieties W, including any linear k-variety.

Theorem 1.10. *Suppose that $W = \bigcap_{j=1}^{J} H_{f_j}$, where J is a natural number, and for each $j \in \{1, \ldots, J\}$ we have that*

$$f_j(X_1, \ldots, X_M) = c_{j,0} + \sum_{i=1}^{M} c_{j,i} X_i^{d_j} \in k[X_1, \ldots, X_M]$$

with $d_j > 0$. Suppose that Γ has rank one. Then we have that $W(\overline{\Gamma}) = \overline{W(\Gamma)}$.

2. Preliminaries

For each subset $\widetilde{S} \subset \Sigma_K$, we let $\mathcal{C}_{\widetilde{S}}$ be the collection of those pairs $(S, (n_v)_{v \in S})$ where $S \subset \widetilde{S}$ is a finite subset, and $(n_v)_{v \in S}$ is a tuple of natural numbers indexed by S.

Lemma 2.1. *Let $\widetilde{S} \subset \Sigma_K$ be a subset such that $\Gamma \subset O_v^*$ for every $v \in \widetilde{S}$. Then we have that $W(\overline{\Gamma_{\widetilde{S}}}) \neq \emptyset$ if and only if for every $(S, (n_v)_{v \in S}) \in \mathcal{C}_{\widetilde{S}}$ the images of the following two maps meet*

$$\begin{array}{ccc} & & W\left(\prod_{v \in S} (O_v/\mathfrak{m}_v^{n_v})^*\right) \\ & & \downarrow \\ \mathbb{A}^M(\Gamma) & \longrightarrow & \mathbb{A}^M\left(\prod_{v \in S} (O_v/\mathfrak{m}_v^{n_v})^*\right). \end{array}$$

Proof. To prove the "only if" part, suppose that

$$(x_1, \ldots, x_M) \in W(\overline{\Gamma_{\widetilde{S}}}) \subset \mathbb{A}^M(\overline{\Gamma_{\widetilde{S}}}) \subset \mathbb{A}^M\left(\prod_{v \in \widetilde{S}} O_v^*\right)$$

and write $x_i = (x_{i,v})_{v \in \widetilde{S}}$ for each i. Fix an arbitrary $(S, (n_v)_{v \in S}) \in \mathcal{C}_{\widetilde{S}}$. Since the kernel of $\mathbb{A}^M(\prod_{v \in \widetilde{S}} O_v^*) \to \mathbb{A}^M(\prod_{v \in S} (O_v/\mathfrak{m}_v^{n_v})^*)$ is an open subset, there is some $(\gamma_1, \ldots, \gamma_M) \in \mathbb{A}^M(\Gamma)$ such that for each i and each $v \in S$ we have $\frac{\gamma_i}{x_{i,v}} - 1 \in \mathfrak{m}_v^{n_v}$; since $x_{i,v} \in O_v^*$, it follows that $\gamma_i - x_{i,v} \in \mathfrak{m}_v^{n_v}$. Then by definition, we have that

$$\begin{aligned} &((x_{1,v} + \mathfrak{m}_v^n, \ldots, x_{M,v} + \mathfrak{m}_v^n))_{v \in S} \\ &\qquad \in W\left(\prod_{v \in S} (O_v/\mathfrak{m}_v^{n_v})^*\right) \subset \mathbb{A}^M\left(\prod_{v \in S} (O_v/\mathfrak{m}_v^{n_v})^*\right) \end{aligned}$$

and that this point coincides with $((\gamma_1+\mathfrak{m}_v^n,\dots,\gamma_M+\mathfrak{m}_v^n))_{v\in S}$, which is the image of $(\gamma_1,\dots,\gamma_M)$ under the map $\mathbb{A}^M(\Gamma)\to\mathbb{A}^M(\prod_{v\in S}(O_v/\mathfrak{m}_v^{n_v})^*)$. This establishes the "only if" part.

Now we prove the "if" part. Choose a subcollection $\{(S_i,(n_{i,v})_{v\in S_i}) : i\in\mathbb{N}\}$ of $\mathcal{C}_{\widetilde{S}}$ such that, as i ranges over $\mathbb{N}$, the collection of kernels of

$$\mathbb{A}^M\left(\prod_{v\in\widetilde{S}}O_v^*\right)\longrightarrow\mathbb{A}^M\left(\prod_{v\in S_i}(O_v/\mathfrak{m}_v^{n_{i,v}})^*\right)$$

forms a system of neighborhood around the neutral element of topological group $\mathbb{A}^M(\prod_{v\in\widetilde{S}}O_v^*)$. For each $i\in\mathbb{N}$, we pick an element $\mathbf{x}_i\in\mathbb{A}^M(\Gamma)$ whose image in $\mathbb{A}^M(\prod_{v\in S_i}(O_v/\mathfrak{m}_v^{n_{i,v}})^*)$ lies in $W(\prod_{v\in S_i}(O_v/\mathfrak{m}_v^{n_{i,v}})^*)$. Since k is finite, $\mathbb{A}^M(\prod_{v\in\widetilde{S}}O_v^*)$ is a compact set containing $\mathbb{A}^M(\Gamma)$. Thus by taking subsequence we may assume that $(\mathbf{x}_i)_{i\geq1}\in\mathbb{A}^M(\Gamma)$ converges to some $\mathbf{x}\in\mathbb{A}^M(\prod_{v\in\widetilde{S}}O_v^*)$. By construction we have that $\mathbf{x}\in\mathbb{A}^M(\overline{\Gamma_{\widetilde{S}}})$. It remains to show that $\mathbf{x}$ lies in W. Write $\mathbf{x}=((x_{1,v})_{v\in\widetilde{S}},\dots,(x_{M,v})_{v\in\widetilde{S}})$. Fixing an arbitrary $f\in K[X_1,\dots,X_M]$ vanishing on W, and an arbitrary $v\in\widetilde{S}$, we only need to show that $f(x_{1,v},\dots,x_{M,v})=0$. Choose some $\alpha\in K^*$ such that $\alpha f\in O_v[X_1,\dots,X_M]$ has some coefficients not in $\mathfrak{m}_v$, and fix an arbitrary $n\in\mathbb{N}$. By construction and taking further subsequence, we may choose some $i_0\in\mathbb{N}$ such that for each $i\geq i_0$ we have $v\in S_i$ and $n_{i,v}\geq n$. Writing $\mathbf{x}_i=(x_{1,i},\dots,x_{M,i})\in\mathbb{A}^M(\Gamma)\subset\mathbb{A}^M(O_v^*)$, we see that the image of $\mathbf{x}_i$ in $\mathbb{A}^M((O_v/\mathfrak{m}_v^{n_{i,v}})^*)$ is $(x_{1,i}+\mathfrak{m}_v^{n_{i,v}},\dots,x_{M,i}+\mathfrak{m}_v^{n_{i,v}})$; since this image lies in $W((O_v/\mathfrak{m}_v^{n_v})^*)$, we have that $\alpha f(x_{1,i},\dots,x_{M,i})\in\mathfrak{m}_v^{n_{i,v}}\subset\mathfrak{m}_v^n$ for any $i\geq i_0$. Letting $i\to\infty$, it follows that $\alpha f(x_{1,v},\dots,x_{M,v})\in\mathfrak{m}_v^n$. Since $n\in\mathbb{N}$ is arbitrary and $\alpha\in K^*$, we conclude that $f(x_{1,v},\dots,x_{M,v})=0$ as desired. □

Corollary 2.2. *Conjecture 1.3 holds if and only if Conjecture 1.4 holds.*

Proof. Obviously, the "only if" part of this corollary follows from "only if" part of Lemma 2.1. For the "if" part, we only need to consider the case where $W(\Gamma)=\emptyset$. Choose a cofinite subset $\widetilde{S}\subset\Sigma_K$ such that $\Gamma\subset O_v^*$ for every $v\in\widetilde{S}$. By Conjecture 1.4, we have that $W(\overline{\Gamma_{\widetilde{S}}})=\emptyset$. Then Lemma 2.1 yields the desired conclusion. □

Remark 2.3. From the proofs, we see that the "only if" part of both Lemma 2.1 and Corollary 2.2 still holds even if our constant field k is infinite.

3. The proofs

For any $a, b \in \mathbb{N}$ with b not divisible by p, consider the polynomial

$$g_{a,b}(T) = \frac{T^{ab} - 1}{T^a - 1} \in k[T].$$

Remark 3.1. For any finite subset $\mathcal{S} \subset k[T]$ containing only irreducible polynomials, there is always an effectively constructed $a_0 \in \mathbb{N} \setminus p\mathbb{N}$ such that for any $a \in a_0\mathbb{N}$ and $b \in \mathbb{N} \setminus p\mathbb{N}$ the polynomial $g_{a,b}(T)$ is not divisible by any element in $\mathcal{S}$. In fact, we may take $a_0 = q^d - 1$, where $q = |k|$ and d is the least common multiple of degrees of all elements in S. Then every polynomial in $\mathcal{S}$ divides $T(T^{a_0} - 1)$, which divides $T(T^a - 1)$ for any $a \in a_0\mathbb{N}$; for any $b \in \mathbb{N} \setminus p\mathbb{N}$, we see that $g_{a,b}(T) = \sum_{i=0}^{b-1} T^{ai}$ and $T^a - 1$ are coprime; it follows that $g_{a,b}(T)$ is not divisible by any element in $\mathcal{S}$ as claimed.

We make the following convention. For a polynomial $Q(T) \in k[T]$ and a rational function $P(T) \in k(T)$, we say that $Q(T)$ divides $P(T)$ if any zero of $Q(T)$ in k^{alg} is not a pole of $\frac{P(T)}{Q(T)}$.

Lemma 3.2. *Let $f(T) = \sum_{i \in I} c_i T^{e_i} \in k(T)$ with each $c_i \in k$ and $e_i \in \mathbb{Z}$, where I is a finite index set. Let $a \in \mathbb{N}$ and $b \in \mathbb{N} \setminus p\mathbb{N}$ with b greater than the cardinality of I. Denote by $\mathscr{C}$ the collection of those partitions $\mathscr{P}$ on the set I such that for each set $\Omega \in \mathscr{P}$ we have $\sum_{i \in \Omega} c_i = 0$ and for each nonempty proper subset $\Omega' \subset \Omega$ we have $\sum_{i \in \Omega'} c_i \neq 0$. Suppose that $g_{a,b}(T)$ divides $f(T)$. Then there is some $\mathscr{P} \in \mathscr{C}$ such that for each set $\Omega \in \mathscr{P}$ and each $i_1, i_2 \in \Omega$ we have that ab divides $e_{i_1} - e_{i_2}$.*

Proof. By our convention, the condition that $g_{a,b}(T)$ divides $f(T)$ implies the existence of some $e \in \mathbb{N}$ such that $f(T)T^e$ is in $k[T]$ and is divisible by $g_{a,b}(T)$. Observe that for any nonnegative integer e and positive integer m, the remainder obtained while performing the long division of T^e by $T^m - 1$ is T^r, where r is the remainder of e divided by m. Thus, the remainder obtained while performing the long division of $f(T)T^e = \sum_{i \in I} c_i T^{e_i + e}$ by $T^{ab} - 1$ is $\sum_{i \in I} c_i T^{r_i}$, where r_i denotes the remainder of $e_i + e$ divided by ab. Since $g_{a,b}(T)$ divides both $f(T)$ and $T^{ab} - 1$, it also divides $\sum_{i \in I} c_i T^{r_i}$. Hence there is a polynomial $\sum_{i=0}^{a-1} \alpha_i T^i \in k[T]$ with degree at most $a - 1 = (ab - 1) - a(b - 1)$ such that

$$\sum_{i \in I} c_i T^{r_i} = \left(\sum_{i=0}^{b-1} T^{ai} \right) \left(\sum_{i=0}^{a-1} \alpha_i T^i \right).$$

Observe that no cancellation occurs during expanding the right hand side. Thus, if $\alpha_i \neq 0$ for some i, then there are at least b nonzero terms in the polynomial $\sum_{i \in I} c_i T^{r_i}$. From the assumption that b greater than the cardinality of I, this shows that $\sum_{i\in I} c_i T^{r_i}$ is a zero polynomial. Then by definition of $\mathscr{C}$, there is some $\mathscr{P} \in \mathscr{C}$ such that for each set $\Omega \in \mathscr{P}$ and each $i_1, i_2 \in \Omega$ we have that $r_{i_1} = r_{i_2}$, i.e. ab divides $e_{i_1} - e_{i_2}$. $\square$

Lemma 3.3. *Let $f(X_1, \dots, X_M) \in k[X_1, \dots, X_M]$ be a polynomial over the finite field k of characteristic p. Let $\mathcal{S}$ be a finite set of irreducible polynomials in $k[T]$. Then there are effectively constructed $a, b \in \mathbb{N}$, neither divisible by p, such that the following two properties holds:*

(1) *$g_{a,b}(T)$ is not divisible by any element in $\mathcal{S}$;*
(2) *if $f(1, \dots, 1) \neq 0$, then $g_{a,b}(T)$ does not divide $f(T^{e_1}, \dots, T^{e_M})$ for any tuple $(e_1, \dots, e_M)$ of nonnegative integers.*

Proof. Write $f(X_1, \dots, X_M) = \sum_{i\in I} c_i X_1^{e_{1,i}} \cdots X_M^{e_{M,i}}$ with each $c_i \in k$ and *each tuple* $(e_{1,i}, \cdots, e_{M,i})$ of nonnegative integers, where I is a finite index set. Fix some $b \in \mathbb{N} \setminus p\mathbb{N}$ greater than the number of nonzero terms in $f(X_1, \dots, X_M)$. By Remark 3.1, there is a effectively constructed $a \in \mathbb{N} \setminus p\mathbb{N}$ such that the polynomial $g_{a,b}(T)$ is not divisible by any element in $\mathcal{S}$. Suppose that $g_{a,b}(T)$ divides $f(T^{e_1}, \dots, T^{e_M})$ for some tuple $(e_1, \dots, e_M)$ of nonnegative integers. Because the number of nonzero terms in $f(T^{e_1}, \dots, T^{e_M})$ is not greater than that in $f(X_1, \dots, X_M)$, this number is less than b. Thus, Lemma 3.2 shows that there is some partitions $\mathscr{P}$ on the set I such that for each set $\Omega \in \mathscr{P}$ we have $\sum_{i\in\Omega} c_i = 0$; this means that

$$f(1, \dots, 1) = \sum_{\Omega\in\mathscr{P}} \sum_{i\in\Omega} c_i = 0,$$

which is a contradiction finishing the proof. $\square$

Proposition 3.4. *Let $f \in k[X_1, \dots, X_M]$. Suppose that Γ is infinitely cyclic. Then there exists an effectively determined finite subset $S_0 \subset \Sigma$ such that $\Gamma \subset O_v^*$ for every $v \in S_0$, and in the following commutative diagram*

$$\begin{array}{ccc} H_f(\Gamma) & \longrightarrow & H_f\left(\prod_{v\in S_0} \mathbb{F}_v^*\right) \\ \downarrow & & \downarrow \\ \mathbb{A}^M(\Gamma) & \longrightarrow & \mathbb{A}^M\left(\prod_{v\in S_0} \mathbb{F}_v^*\right) \end{array}$$

we have that $H_f(\Gamma) = \emptyset$ if and only if the image of the bottom map and that of the right hand downward map do not meet.

Proof. Let $\gamma \in \Gamma$ generate Γ. Choose a finite subset $S \subset \Sigma_K$ containing the set $\Sigma_K \setminus \Sigma$ such that $\gamma \in O_S^*$. Consider the field isomorphism $k(T) \to k(\gamma)$ given by $T \mapsto \gamma$. Through this isomorphism, let $\mathcal{S}$ be a finite set of those irreducible polynomials in $k[T]$ corresponding any place of $k(\gamma)$ lying below some place in S. By Lemma 3.3, there are effectively computable $a, b \in \mathbb{N}$, neither divisible by p, such that $g_{a,b}(T)$ is not divisible by any element in

$\mathcal{S}$ and that if $f(1,\ldots,1)\neq 0$, then $g_{a,b}(T)$ does not divide $f(T^{e_1},\ldots,T^{e_M})$ for any tuple $(e_1,\ldots,e_M)$ of nonnegative integers. Since neither a nor b is divisible by p, it follows that $g_{a,b}(T)$ is equal to a product of distinct irreducible polynomials; let $\mathcal{S}_0$ be the set of these irreducible polynomials. Note that the polynomial T does not belong to $\mathcal{S}_0$. Let $S_0\subset\Sigma_K$ be a finite subset such that for each irreducible polynomials in $\mathcal{S}_0$ there is exactly one place in S_0 lying above the place of $k(\gamma)$ corresponding to this polynomial. Now we show that S_0 has the desired property. To prove the nontrivial implication, suppose that $H_f(\Gamma)=\emptyset$, which follows that $f(1,\ldots,1)\neq 0$. We need to show that the image of the map $\mathbb{A}^M(\Gamma)\to\mathbb{A}^M(\prod_{v\in S_0}\mathbb{F}_v^*)$ do not intersect with H_f. Assuming for the contradiction that H_f contains the image of some element $\mathbb{A}^M(\Gamma)$ in $\mathbb{A}^M(\prod_{v\in S_0}\mathbb{F}_v^*)$; since Γ is generated by γ, this element is equal to $(\gamma^{e_1},\ldots,\gamma^{e_M})$ for some tuple $(e_1,\ldots,e_M)\in\mathbb{A}^M(\mathbb{Z})$. This says that for each $v\in S_0$ we have that $f(\gamma^{e_1},\ldots,\gamma^{e_M})\in\mathfrak{m}_v$. Note that $f(\gamma^{e_1},\ldots,\gamma^{e_M})\in k[\gamma,\gamma^{-1}]$; for each $v\in S_0$, since $\gamma\in O_v^*$, the intersection $\mathfrak{m}_v\cap k[\gamma,\gamma^{-1}]$ is still a maximal ideal of $k[\gamma,\gamma^{-1}]$. Now we have that $f(\gamma^{e_1},\ldots,\gamma^{e_M})\in\bigcap_{v\in S_0}(\mathfrak{m}_v\cap k[\gamma,\gamma^{-1}])=\prod_{v\in S_0}(\mathfrak{m}_v\cap k[\gamma,\gamma^{-1}])$. Through the k-isomorphism $k[T,T^{-1}]\to k[\gamma,\gamma^{-1}]$ of rings given by $T\mapsto\gamma$, it follows that $f(T^{e_1},\ldots,T^{e_M})\in k[T,T^{-1}]$ is divisible by the product of all irreducible polynomials in $\mathcal{S}_0$. By construction, this product is exactly $g_{a,b}(T)$. This contradiction finishes our proof. □

Proposition 3.5. *Let $f\in k[X_1,\ldots,X_M]$. Assume that Conjecture 1.7 holds. Suppose that Γ is infinitely cyclic. Then there exists $v_0\in\Sigma$ such that $\Gamma\subset O_{v_0}^*$ and in the following commutative diagram*

$$\begin{array}{ccc} H_f(\Gamma) & \longrightarrow & H_f(\mathbb{F}_{v_0}^*) \\ \downarrow & & \downarrow \\ \mathbb{A}^M(\Gamma) & \longrightarrow & \mathbb{A}^M(\mathbb{F}_{v_0}^*) \end{array}$$

we have that $H_f(\Gamma)=\emptyset$ if and only if the image of the bottom map and that of the right hand downward map do not meet. If we assume further that Conjecture 1.7 holds in a constructive way that for any given $m\in\mathbb{N}$ and $R\in\mathbb{N}$ we may explicitly find an $r>R$ such that the condition $\mathrm{Cond}(m,r)$ *holds, then the place $v_0\in\Sigma$ may be effectively constructed.*

Proof. It suffices to consider only the case where $H_f(\Gamma)=\emptyset$, which follows that $f(1,\ldots,1)\neq 0$. By Proposition 5.2 in [2], it follows from Conjecture 1.7 that there exists $v_0\in\Sigma$ such that $\Gamma\subset O_{v_0}^*$ and for every $(\gamma_1,\ldots,\gamma_M)\in\mathbb{A}^M(\Gamma)$ we have that $f(\gamma_1,\ldots,\gamma_M)\notin\mathfrak{m}_{v_0}$. Since the coefficients of f lie in k^*, which is mapped injectively to $\mathbb{F}_{v_0}^*$, it implies that the image of $\mathbb{A}^M(\Gamma)$ in $\mathbb{A}^M(\mathbb{F}_{v_0}^*)$ does not meet with H_f as desired. In fact, the statement of Proposition 5.2 in [2] specifies an $m\in\mathbb{N}$ (in terms of f) and an $R\in\mathbb{N}$

(in terms of k and Γ) such that the truth of $\mathrm{Cond}(m,r)$ for some $r > R$ ensures the existence of such a place $v_0 \in \Sigma$; the proof of that proposition shows how to construct such $v_0 \in \Sigma$ in terms of r, k, Γ and K. $\square$

Theorem 1.5 follows from conclusion (1) of the following result.

Theorem 3.6. *Let W be a closed k-variety in $\mathbb{A}^M$. Suppose that Γ has rank at most one. For every finite subset $S_0 \subset \Sigma$, consider the following property*

(P) $\Gamma \subset O_v^*$ *for every $v \in S_0$, and in the following commutative diagram*

$$\begin{array}{ccc} W(\Gamma) & \longrightarrow & W\left(\prod_{v\in S_0} \mathbb{F}_v^*\right) \\ \downarrow & & \downarrow \\ \mathbb{A}^M(\Gamma) & \longrightarrow & \mathbb{A}^M\left(\prod_{v\in S_0} \mathbb{F}_v^*\right) \end{array}$$

we have that $W(\Gamma) = \emptyset$ if and only if the image of the bottom map and that of the right hand downward map do not meet.

Then we have the following conclusions.

(1) *There is an effectively determined finite subset $S_0 \subset \Sigma$ such that* (P) *holds.*
(2) *If we assume that Conjecture 1.7 holds, then there exists an one-element subset $S_0 \subset \Sigma$ such that* (P) *holds.*
(3) *If we assume further that Conjecture 1.7 holds in a constructive way that for any given $m \in \mathbb{N}$ and $R \in \mathbb{N}$ we may explicitly find some $r > R$ such that the condition* $\mathrm{Cond}(m,r)$ *holds, then there exists an effectively determined one-element subset $S_0 \subset \Sigma$ such that* (P) *holds.*

Proof. To prove the desired result, it suffices to consider the case where $W(\Gamma) = \emptyset$. Choose a free subgroup $\Phi \subset \Gamma$ such that $\Gamma = \bigcup_{\tau\in\mathrm{Tor}(\Gamma)} \tau\Phi$. Write $W = \bigcap_{i\in I} H_{f_i}$, where I is some finite index set and $f_i \in k[X_1,\ldots,X_M]$ for each $i \in I$. Since $W(\Gamma) = \emptyset$, it implies that for each $\mathbf{t} = (\tau_1,\ldots,\tau_M) \in \mathbb{A}^M(\mathrm{Tor}(\Gamma)) \subset \mathbb{A}^M(k^*)$ there exists $i_{\mathbf{t}} \in I$ such that $\mathbf{t} \notin H_{f_{i_{\mathbf{t}}}}(k^*)$, i.e. $f_{i_{\mathbf{t}}}(\mathbf{t}) = f_{i_{\mathbf{t}}}(\tau_1,\ldots,\tau_M) \neq 0$. Writing $\mathbf{tX} = (\tau_1X_1,\ldots,\tau_MX_M)$, we define

$$g(\mathbf{X}) = g(X_1,\ldots,X_M) = \prod_{\mathbf{t}\in\mathbb{A}^M(\mathrm{Tor}(\Gamma))} f_{i_{\mathbf{t}}}(\mathbf{tX}).$$

Since each $f_{i_{\mathbf{t}}}(\mathbf{tX})$ is in $k[X_1,\ldots,X_M]$, so is the product $g(\mathbf{X})$. We note that $g(1,\ldots,1) \neq 0$. Since $g(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$ and each non-trivialelement of Φ is not algebraic over k, we have that $H_g(\Phi) = \emptyset$. For conclusion (1), Proposition 3.4 shows that there exists a effectively determined finite subset $S_0 \subset \Sigma$ satisfying the following property

(P′) $\Phi \subset O_v^*$ for every $v \in S_0$, and in the following diagram

$$\begin{array}{ccc} & & H_g\left(\prod_{v\in S_0}\mathbb{F}_v^*\right) \\ & & \downarrow \\ \mathbb{A}^M(\Phi) & \longrightarrow & \mathbb{A}^M\left(\prod_{v\in S_0}\mathbb{F}_v^*\right) \end{array}$$

the image of the bottom map and that of the right hand downward map do not meet.

For conclusion (2), we apply the first part of Proposition 3.5 and obtain an one-element subset $S_0 \subset \Sigma$ satisfying the property (P′). For conclusion (3), the second part of Proposition 3.5 offers an effectively constructed one-element subset $S_0 \subset \Sigma$ satisfying the property (P′).

Now it lefts to show that the property (P′) implies the property (P). Recall that we are treating the case where $W(\Gamma) = \emptyset$. Assume for contradiction that there exists some $\mathbf{r} \in \mathbb{A}^M(\Gamma)$ whose image in $\mathbb{A}^M(\prod_{v\in S_0}\mathbb{F}_v^*)$ lies on W. Since $\Gamma = \bigcup_{\tau\in \mathrm{Tor}(\Gamma)} \tau\Phi$, there exists some $\mathbf{t} \in \mathbb{A}^M(\mathrm{Tor}(\Gamma))$ such that $\mathbf{rt}^{-1} \in \mathbb{A}^M(\Phi)$. Note that the image of $\mathbf{r}$ in $\mathbb{A}^M(\prod_{v\in S_0}\mathbb{F}_v^*)$ lies on $H_{f_{i_\mathbf{t}}}$. As $\mathrm{Tor}(\Gamma)$ is contained in k^*, which maps injectively to $\mathbb{F}_v^*$ for any $v \in S_0$, we have that the image of $\mathbf{rt}^{-1}$ in $\mathbb{A}^M(\prod_{v\in S_0}\mathbb{F}_v^*)$ lies on the translation $\mathbf{t}^{-1}H_{f_{i_\mathbf{t}}}$ of $H_{f_{i_\mathbf{t}}}$ by $\mathbf{t}^{-1} \in \mathbb{A}^M(\mathrm{Tor}(\Gamma))$. This translation is defined by the polynomial $f_{i_\mathbf{t}}(\mathbf{tX}) \in k[X_1,\dots,X_M]$. Since $\mathbf{rt}^{-1} \in \mathbb{A}^M(\Phi)$ and the polynomial $f_{i_\mathbf{t}}(\mathbf{tX})$ divides $g(\mathbf{X})$, it follows that the image of $\mathbb{A}^M(\Phi)$ in $\mathbb{A}^M(\prod_{v\in S_0}\mathbb{F}_v^*)$ meets the hypersurface H_g. This contradicts the construction of g and S_0 as desired. □

Example 3.7. Conjecture 1.3 cannot hold with a tuple $(n_v)_{v\in S_0}$ bounded over all closed K-varieties W in $\mathbb{A}^M$. To see this, consider the case where $K = k(T)$ and Γ is generated by T. Let $n \in \mathbb{N}$ and take the simple example where $W_1 = H_{f_1} \subset \mathbb{A}^1$ with

$$f_1(X_1) = X_1^{p^n} - T^{p^{n-1}} \in K[X_1].$$

To show that there is no obvious condition (other than that W is defined over k) under which this stronger version of Conjecture 1.3 holds, consider a more elaborate example where $W_2 = H_{f_2} \subset \mathbb{A}^2$ with

$$f_2(X_1, X_2) = X_1X_2 - 1 + cX_1^2X_2^{p^n+1} - cT^{p^{n-1}}X_1 \in K[X_1, X_2],$$

where $c \in k^* \setminus \{1\}$. For every $e_1 \in \mathbb{Z}$, we have

$$f_1(T^{e_1}) = T^{p^{n-1}}\left(T^{p^{n-1}(e_1p-1)} - 1\right),$$

from which we see that if $f_1(T^{e_1})=0$, then $e_1p-1=0$, which is impossible. Similarly, for every $(e_1,e_2)\in\mathbb{A}^2(\mathbb{Z})$ we have

$$\begin{aligned} f_2(T^{e_1},T^{e_2}) &= T^{e_1+e_2}+cT^{2e_1+e_2p^n+e_2}-cT^{e_1+p^{n-1}}-1\\ &= \left(T^{e_1+e_2}-1\right)+cT^{e_1+p^{n-1}}\left(T^{e_1+e_2(p^n+1)-p^{n-1}}-1\right)\\ &= T^{e_1+e_2}\left(1+cT^{e_1+e_2p^n}\right)-\left(cT^{e_1+p^{n-1}}+1\right), \end{aligned}$$

thus the condition $c\in k^*\setminus\{1\}$ implies that if $f_2(T^{e_1},T^{e_2})=0$ then it implies either that $\begin{cases} e_1+e_2=0\\ e_1+e_2(p^n+1)=p^{n-1}\end{cases}$ or that $\begin{cases} e_1+e_2p^n=0\\ e_1=-p^{n-1}\end{cases}$; however, there is no $(e_1,e_2)\in\mathbb{A}^2(\mathbb{Z})$ for which either system of equalities holds. Thus we have $W_1(\Gamma)=\emptyset=W_2(\Gamma)$. On the other hand, for any finite subset $S_0\subset\Sigma_K$ and any tuple $(n_v)_{v\in S_0}$ of natural numbers indexed by S_0 such that $\Gamma\subset O_v^*$ and $n_v\le p^{n-1}$ for each $v\in S_0$, we claim that in the case where $(W,M)\in\{(W_1,1),(W_2,2)\}$ the image of the bottom map and that of the right hand downward map in the following commutative diagram *always* meet

$$\begin{array}{ccc} W(\Gamma) & \longrightarrow & W\left(\prod_{v\in S_0}(O_v/\mathfrak{m}_v^{n_v})^*\right)\\ \downarrow & & \downarrow\\ \mathbb{A}^M(\Gamma) & \longrightarrow & \mathbb{A}^M\left(\prod_{v\in S_0}(O_v/\mathfrak{m}_v^{n_v})^*\right). \end{array}$$

To see this, first note that there is some $a\in\mathbb{N}\setminus p\mathbb{N}$ such that $T^a-1\in\bigcap_{v\in S_0}(\mathfrak{m}_v\cap K)$. Thus we have $T^{ap^{n-1}}-1\in\bigcap_{v\in S_0}(\mathfrak{m}_v^{n_v}\cap K)$. Because $a\in\mathbb{N}\setminus p\mathbb{N}$, we may choose some $b\in\mathbb{N}\setminus a\mathbb{N}$ such that $bp\in 1+a\mathbb{N}$. We have

$$f_1(T^b)=T^{p^{n-1}}\left(T^{p^{n-1}(bp-1)}-1\right)\in\left(T^{ap^{n-1}}-1\right)k[T]\subset\bigcap_{v\in S_0}\left(\mathfrak{m}_v^{n_v}\cap K\right)$$

and

$$\begin{aligned} f_2(T^{-b},T^b)&=cT^{-b+p^{n-1}}\left(T^{bp-1}-1\right)^{p^{n-1}}\\ &\in\left(T^{ap^{n-1}}-1\right)k[T]\subset\bigcap_{v\in S_0}\left(\mathfrak{m}_v^{n_v}\cap K\right). \end{aligned}$$

This proves our claim.

Let $\rho(\Gamma)=\bigcap_{m\ge 0}(K^{p^m})^*\Gamma$, which is still a subgroup of K^*.

Lemma 3.8. *We have that*

$$\begin{aligned} &\{x\in K^*: x^n\in\Gamma \text{ for some } n\in\mathbb{N}\setminus p\mathbb{N}\}\\ &\qquad\subset\rho(\Gamma)\subset\{x\in K^*: x^n\in\Gamma \text{ for some } n\in\mathbb{N}\}. \end{aligned}$$

Moreover, if Γ *has rank one, then*

$$\rho(\Gamma) = \{x \in K^* : x^n \in \Gamma \text{ for some } n \in \mathbb{N} \setminus p\mathbb{N}\}.$$

Proof. For any $x \in K^*$ with $x^n \in \Gamma$ for some $n \in \mathbb{N} \setminus p\mathbb{N}$, we have that for every $m \geq 0$ there are $a, b \in \mathbb{Z}$ with $an + bp^m = 1$, thus $x = (x^{p^m})^b (x^n)^a \in (K^{p^m})^* \Gamma$. This shows that $\{x \in K^* : x^n \in \Gamma \text{ for some } n \in \mathbb{N} \setminus p\mathbb{N}\} \subset \rho(\Gamma)$. Lemma 3 of [6] (which uses the fact that k is finite and Γ is finitely generated) shows that $\rho(\Gamma) \subset \{x \in K^* : x^n \in \Gamma \text{ for some } n \in \mathbb{N}\}$. Now suppose that Γ has rank one and let $\gamma \in \Gamma$ generate a maximal free subgroup of Γ. To show that

$$\rho(\Gamma) \subset \{x \in K^* : x^n \in \Gamma \text{ for some } n \in \mathbb{N} \setminus p\mathbb{N}\},$$

we first choose a largest $m_0 \in \mathbb{N}$ such that $\Gamma \subset (K^{p^{m_0}})^*$. Let $x \in \rho(\Gamma)$. Since $\rho(\Gamma) \subset \{x \in K^* : x^n \in \Gamma \text{ for some } n \in \mathbb{N}\}$, we may choose a smallest $n_0 \in \mathbb{N}$ such that $x^{n_0} \in \Gamma$. Then there exists some $s \in \mathbb{Z}$ and $\tau \in \mathrm{Tor}(\Gamma)$ such that $x^{n_0} = \tau\gamma^s$. We shall show that n_0 is not divisible by p as desired. Assume that n_0 is divisible by p. Then since $\tau \in k^* \subset (K^{p^{m_0+1}})^*$, we have $\gamma^s \in (K^{p^{m_0+1}})^*$, which implies that s is divisible by p, for otherwise it would follows that $\gamma \in (K^{p^{m_0+1}})^*$ and then $\Gamma \subset (K^{p^{m_0+1}})^*$, contradicting the choice of m_0. Having that both n_0 and s are divisible by p, we see that $x^{\frac{n_0}{p}} \gamma^{-\frac{s}{p}}$ is the p-th root of τ, thus is some power of τ, hence lies in $\mathrm{Tor}(\Gamma)$. It follows that $x^{\frac{n_0}{p}} \in \Gamma$, contradicting the choice of n_0. □

Lemma 3.9. *Suppose that* Γ *has rank one. Then we have that* $\rho(\Gamma) = k^*\Gamma$ *if and only if there is a non-torsion element* $\gamma \in \Gamma$ *such that for every* $c \in k^*$ *the element* $c\gamma$ *does not have any* n*-th root in* K^* *for any* $n \in \mathbb{N} \backslash p\mathbb{N} \setminus \{1\}$.

Proof. To prove the "only if" part, suppose that $\rho(\Gamma) = k^*\Gamma$ and let $\gamma \in \Gamma$ generate a maximal free subgroup of Γ. If for some $c \in k^*$ and some $n \in \mathbb{N} \backslash p\mathbb{N} \setminus \{1\}$ the element $c\gamma$ has some n-th root x in K^*, then by Lemma 3.8, we have that $x \in \rho(k^*\Gamma) = \rho(\Gamma) = k^*\Gamma$ and thus that $x = c_1\gamma$ for some $c_1 \in k^*$; hence we obtain $c_1^n \gamma^n = x^n = c\gamma$, which implies a contradiction that $\gamma \in k^{\mathrm{alg}}$ since $n \neq 1$.

It remains to prove the "if" part. Suppose that there is a non-torsion element $\gamma \in \Gamma$ such that for every $c \in k^*$ the element $c\gamma$ does not have any n-th root in K^* for any $n \in \mathbb{N} \backslash p\mathbb{N} \setminus \{1\}$. Note that γ is contained in some maximal free subgroup of Γ, and that if $\gamma = \gamma_0^m$ for some $\gamma_0 \in \Gamma$ and $m \in \mathbb{Z}$, then for every $c \in k^*$ the element $c\gamma_0$ does not have any n-th root in K^* for any $n \in \mathbb{N} \backslash p\mathbb{N} \setminus \{1\}$ either. Hence we may assume that γ generates a maximal free subgroup of Γ. To prove that $\rho(\Gamma) = k^*\Gamma$, since we have $\rho(\Gamma) = \rho(k^*\Gamma) = \{x \in K^* : x^n \in k^*\Gamma \text{ for some } n \in \mathbb{N} \setminus p\mathbb{N}\}$ by Lemma 3.8, it suffices to consider a non-torsion $x \in K^*$ such that $x^n \in k^*\Gamma$ with a minimal $n \in \mathbb{N} \setminus p\mathbb{N}$, and show that $n = 1$. Let $c \in k^*$ satisfy that $x^n = c\gamma^s$. If $d = \gcd(n,s)$, then $(x^{\frac{n}{d}}\gamma^{-\frac{s}{d}})^d = c$ and thus $x^{\frac{n}{d}}\gamma^{-\frac{s}{d}} \in (k^{\mathrm{alg}})^* \cap K^* = k^*$; noting that $x^{\frac{n}{d}} = (x^{\frac{n}{d}}\gamma^{-\frac{s}{d}})\gamma^{\frac{s}{d}} \in k^*\Gamma$, the minimality of n shows that $d = 1$. Since $1 = \gcd(n,s) = an + bs$ for some $a, b \in \mathbb{Z}$, we see that $c^b\gamma = (c\gamma^s)^b\gamma^{an} = (x^b\gamma^a)^n$. As $x^b\gamma^a \in K^*$ and $n \in \mathbb{N} \setminus p\mathbb{N}$, the hypothesis on $c^b\gamma$ implies $n = 1$ as desired. □

Proposition 3.10. *Let W be a union of homogeneous linear K-varieties. Suppose that Γ has rank one, and that there is a non-torsion element $\gamma \in \Gamma$ such that for every $c \in k^*$ the element $c\gamma$ does not have any n-th root in K^* for any natural number $n \notin p\mathbb{N} \cup \{1\}$. Assume that Conjecture 1.7 holds. Then $W(\prod_{v\in\Sigma}\overline{\Gamma_v}) \neq \emptyset$ implies $W(\Gamma) \neq \emptyset$.*

Proof. By Proposition 6 in [5], there exists a finite union V of homogeneous linear K-subvarieties of W such that each irreducible component of V is $\rho(\Gamma)$-isotrivial and that $W(\overline{\Gamma_v}) = V(\overline{\Gamma_v})$ for every $v \in \Sigma$. Since $\Gamma \subset \overline{\Gamma_v}$ for any $v \in \Sigma$, we also have that $W(\Gamma) = V(\Gamma)$. Writing $V = \bigcup_{i\in I} V_i$ as a finite union of its irreducible components, since we have that $\rho(\Gamma) = k^*\Gamma$ by Lemma 3.9, the definition of $k^*\Gamma$-isotriviality means that for each $i \in I$ there exists some $\mathbf{c}_i\mathbf{r}_i \in \mathbb{A}^M(k^*\Gamma)$, with $\mathbf{c}_i \in \mathbb{A}^M(k^*)$ and $\mathbf{r}_i \in \mathbb{A}^M(\Gamma)$, such that the translate $\mathbf{c}_i\mathbf{r}_iV_i$ is a closed k-variety in $\mathbb{A}^M$. Since $\mathbf{c}_i \in \mathbb{A}^M(k^*)$, we see that $\mathbf{r}_iV_i$ is still a closed k-variety in $\mathbb{A}^M$. For every $v \in \Sigma$, since $\overline{\Gamma_v}$ is contained in a field and $\mathbf{r}_i \in \mathbb{A}^M(\Gamma) \subset \mathbb{A}^M(\overline{\Gamma_v})$, we have $V(\overline{\Gamma_v}) = \bigcup_{i\in I} V_i(\overline{\Gamma_v}) = \bigcup_{i\in I}(\mathbf{r}_iV_i)(\overline{\Gamma_v}) = (\bigcup_{i\in I}\mathbf{r}_iV_i)(\overline{\Gamma_v})$. Similarly we have $V(\Gamma) = (\bigcup_{i\in I}\mathbf{r}_iV_i)(\Gamma)$.

Now suppose that $W(\Gamma) = \emptyset$. Then $(\bigcup_{i\in I}\mathbf{r}_iV_i)(\Gamma) = V(\Gamma) = \emptyset$. Since we are assuming that Conjecture 1.7 holds, by the facts that $\bigcup_{i\in I}\mathbf{r}_iV_i$ is a closed k-variety in $\mathbb{A}^M$ and that Γ has rank one, it follows from conclusion (2) of Theorem 3.6 that there exists a place $v_0 \in \Sigma$ such that $\Gamma \subset O^*_{v_0}$ and that the image of $\mathbb{A}^M(\Gamma)$ in $\mathbb{A}^M(\mathbb{F}^*_{v_0})$ does not meet $\bigcup_{i\in I}\mathbf{r}_iV_i$. Applying Lemma 2.1 with $\widetilde{S} = \{v_0\}$, we see that $(\bigcup_{i\in I}\mathbf{r}_iV_i)(\overline{\Gamma_{v_0}}) = \emptyset$ and hence that $W(\overline{\Gamma_{v_0}}) = V(\overline{\Gamma_{v_0}}) = \emptyset$. It follows that $W(\prod_{v\in\Sigma}\overline{\Gamma_v}) = \emptyset$ as desired. □

Consider the rational map $\phi : \mathbb{A}^{M+1} \to \mathbb{A}^M$ given by

$$(X_1, \ldots, X_{M+1}) \mapsto \left(\frac{X_1}{X_{M+1}}, \ldots, \frac{X_M}{X_{M+1}}\right).$$

For any closed K-variety $W \subset \mathbb{A}^M$ and any subgroup $\Delta \subset K^*$, we have that the K-variety $\phi^{-1}(W)$ is homogeneous, that $W(\Delta) \neq \emptyset$ if and only if $\phi^{-1}(W)(\Delta) \neq \emptyset$; for any $v \in \Sigma$, since $\overline{\Delta_v} \subset K^*_v$ is also subgroup, we have also that $W(\overline{\Delta_v}) \neq \emptyset$ if and only if $\phi^{-1}(W)(\overline{\Delta_v}) \neq \emptyset$.

Proof of Theorem 1.9. Replacing W by $\phi^{-1}(W)$, the preceding remark shows that we may assume that W is homogeneous. Then the desired result follows from Proposition 3.10. □

Proposition 3.11. *Let J be a natural number; for each $j \in \{1, \dots, J\}$, let*

$$f_j(X_1, \dots, X_M) = c_{j,0} + \sum_{i=1}^{M} c_{j,i} X_i^{d_{j,i}} \in k[X_1, \dots, X_M]$$

with $d_{j,i} > 0$ for each i; denote by $\mathscr{C}_j$ the collection of those partitions $\mathscr{P}$ of the set $\{0, 1, \dots, M\}$ such that for each $I \in \mathscr{P}$ we have $\sum_{i \in I} c_{j,i} = 0$ and for each nonempty proper $I' \subset I$ we have $\sum_{i \in I'} c_{j,i} \neq 0$. Suppose that for every $j \in \{1, \dots, J\}$ and every $\mathscr{P} \in \mathscr{C}_j$ we have $d_{j,i} = d_{j,i'}$ for any $i, i' \in I$ and any $I \in \mathscr{P}$ such that $0 \notin I$.

Assume that there exists a sequence $\{(e_{1,n}, \dots, e_{M,n})\}_{n \geq 1}$ in $\mathbb{A}^M(\mathbb{Z})$ satisfying the following: for every $Q(T) \in k[T]$ not divisible by any element in $\mathcal{S}$, there is an $N_Q \in \mathbb{N}$ such that for any $n' \geq n \geq N_Q$ we have that $Q(T)$ divides both $f_j(T^{e_{1,n}}, \dots, T^{e_{M,n}})$ and $T^{e_{i,n}} - T^{e_{i,n'}}$ for all $j \in \{1, \dots, J\}$ and all $i \in \{1, \dots, M\}$.

Then there exists a sequence $\{(e'_{1,n}, \dots, e'_{M,n})\}_{n \in \mathcal{N}}$ in $\mathbb{A}^M(\mathbb{Z})$ indexed by an infinite subset $\mathcal{N} \subset \mathbb{N}$ satisfying the following conditions: for each $n \in \mathcal{N}$ we have $f_j(T^{e'_{1,n}}, \dots, T^{e'_{M,n}}) = 0$ for all $j \in \{1, \dots, J\}$, and for every $\widetilde{Q}(T) \in k[T]$ not divisible by any element in $\mathcal{S} \cap \{T\}$, there is some $\widetilde{N}_{\widetilde{Q}} \in \mathbb{N}$ such that for any $n \in \mathcal{N}$ with $n \geq \widetilde{N}_{\widetilde{Q}}$ we have that $\widetilde{Q}(T)$ divides $T^{e_{i,n}} - T^{e'_{i,n}}$ for all i.

Proof. Fix $D \in \mathbb{N}$ be divisible by $d_{j,i}$ for each $i \in \{1, \dots, M\}$ and $j \in \{1, \dots, J\}$. We have the following observation for each fixed $j \in \{1, \dots, J\}$, where we put $d_{j,0} = e_0 = 0$ for convenience. Suppose that $g_{aD,b}(T)$ divides

$$f_j(T^{e_1}, \dots, T^{e_M}) = \sum_{i=0}^{M} c_{j,i} T^{d_{j,i} e_i}$$

for some $a \in \mathbb{N}$, $b \in \mathbb{N} \setminus p\mathbb{N}$ with $b > M + 1$, and for some $(e_1, \dots, e_M) \in \mathbb{A}^M(\mathbb{Z})$. Then Lemma 3.2 shows that there is some $\mathscr{P} \in \mathscr{C}_j$ such that for any $i, i' \in I$ and any $I \in \mathscr{P}$ we have that abD divides $d_{j,i} e_i - d_{j,i'} e_{i'}$. In case where $0 \notin I$, it follows that that ab divides $e_i - e_{i'}$ since $d_{j,i} = d_{j,i'}$ divides D; in the other case, i.e. where $0 \in I$, because abD divides both $d_{j,i} e_i = d_{j,i} e_i - d_{j,0} e_0$ and $d_{j,i'} e_{i'} = d_{j,i'} e_{i'} - d_{j,0} e_0$, we still have that ab divides $e_i - e_{i'}$. We conclude for any $i, i' \in I$ and any $I \in \mathscr{P}$ that $T^{ab} - 1$ divides $T^{e_i} - T^{e_{i'}}$.

We construct the sequence $\{(e'_{1,n}, \dots, e'_{M,n})\}_{n \geq 1}$ as follows. Fix $a \in \mathbb{N} \setminus p\mathbb{N}$ and $b \in \mathbb{N} \setminus p\mathbb{N}$ such that every polynomial in $\mathcal{S}$ divides $T(T^a - 1)$, and that $b > M + 1$. For each $m \in \mathbb{N}$, consider the polynomial $g_{aDp^m, b(p^m - 1)}(T)$, which is not divisible by any polynomial in S. By assumption, there is an $N_m \in \mathbb{N}$ such that the following two conditions holds:

1. $g_{aDp^m, b(p^m-1)}(T)$ divides $f_j(T^{e_{1,n}}, \dots, T^{e_{M,n}}) = \sum_{i=0}^{M} c_{j,i} T^{d_{j,i} e_i}$ for any $n \geq N_m$ and any $j \in \{1, \dots, J\}$;

(2) $g_{aDp^m,b(p^m-1)}(T)$ divides that $T^{e_{i,n}} - T^{e_{i,n'}}$ for any $n' \geq n \geq N_m$ and all $i \in \{1,\dots,M\}$.

We may assume that the sequence $\{N_m\}_{m\geq 1}$ is strictly increasing. Since we have $b(p^m-1) > M+1 \geq 2$, the observation in the last paragraph shows that Condition (1) implies that for any $n \geq N_m$ there is some $\mathscr{P}_{j,m,n} \in \mathscr{C}_j$ such that $T^{abp^m(p^m-1)}-1$ divides $T^{e_{i,n}}-T^{e_{i',n}}$ for any $i,i' \in I$ and any $I \in \mathscr{P}_{j,m,n}$, while Condition (2) implies that $T^{abp^m(p^m-1)} - 1$ divides $T^{e_{i,n}} - T^{e_{i,n'}}$ for any $n' \geq n \geq N_m$ and all $i \in \{1,\dots,M\}$. Thus, for any $n \geq n' \geq N_m$, any $i,i' \in I$ and any $I \in \mathscr{P}_{j,m,n}$, the polynomial $T^{abp^m(p^m-1)} - 1$ divides $T^{e_{i,n'}} - T^{e_{i',n}}$. Taking $n' = N_m$, we obtain that for any $n \geq N_m$, any $i,i' \in I$ and any $I \in \mathscr{P}_{j,m}$, the polynomial $T^{abp^m(p^m-1)} - 1$ divides $T^{e_{i,n}} - T^{e_{i',N_m}}$, where we put $\mathscr{P}_{j,m} = \mathscr{P}_{j,m,N_m}$.

For each $j \in \{1,\dots,J\}$ the collection $\mathscr{C}_j$ is finite while $\{m! : m \in \mathbb{N}\}$ is infinite, where $m! = \prod_{\ell=1}^{m} \ell$. Thus there is an infinite subset $\mathcal{M} \subset \mathbb{N}$ such that for each $j \in \{1,\dots,J\}$ the collection $\{\mathscr{P}_{j,m!} : m \in \mathcal{M}\}$ consists of only one partition, denoted by $\mathscr{P}_j$; let $R_j \subset \{0,1,\dots,M\} \times \{0,1,\dots,M\}$ be the subset representing the equivalence relation on $\{0,1,\dots,M\}$ corresponding to the partition $\mathscr{P}_j$. Let $\mathscr{P}$ be the partition of $\{0,1,\dots,M\}$ corresponding to the minimal equivalence relation $R \subset \{0,1,\dots,M\} \times \{0,1,\dots,M\}$ containing $\bigcup_{j\in\{1,\dots,J\}} R_j$. For each $i \in \{1,\dots,M\}$, we denote by $\widehat{i}$ the smallest element in $\{0,\dots,M\}$ such that i and $\widehat{i}$ lie in the same element of $\mathscr{P}$, or equivalently $(\widehat{i}, i) \in R$. Let $\mathcal{N} = \{N_{m!} : m \in \mathcal{M}\} \subset \mathbb{N}$, which is an infinite subset. For each $i \in \{1,\dots,M\}$ and each $n = N_{m!} \in \mathcal{N}$ with $m \in \mathcal{M}$, we put $e'_{i,n} = e_{\widehat{i},n}$, where again we define $e_{0,n} = 0$ for convenience.

Now we show that the sequence $\{(e'_{1,n},\dots,e'_{M,n})\}_{n\in\mathcal{N}}$ indeed satisfies the desired properties. To verify the first property, we fix some $j \in \{1,\dots,J\}$ and some $n = N_m \in \mathcal{N}$ with $m \in \mathcal{M}$. From construction, we have

$$\begin{aligned} f_j(T^{e'_{1,n}},\dots,T^{e'_{M,n}}) &= c_{j,0} + \sum_{i=1}^{M} c_{j,i} T^{e'_{i,n} d_{j,i}} \\ &= \sum_{i=0}^{M} c_{j,i} T^{e_{\widehat{i},N_m} d_{j,i}} \\ &= \sum_{I\in\mathscr{P}_j} \sum_{i\in I} c_{j,i} T^{e_{\widehat{i},N_m} d_{j,i}}. \end{aligned}$$

Since $R_j \subset R$, each element $I \in \mathscr{P}_j$, viewed as a subset of $\{0,1,\dots,M\}$, is contained in some element of $\mathscr{P}$; thus for any $i,i' \in I$ we have $\widehat{i} = \widehat{i'}$. For each $I \in \mathscr{P}_j$, choose some fixed $i_I \in I$. Then from the definition $e_{0,N_m} = 0$ and the assumption that $d_{j,i} = d_{j,i_I}$ for any $i \in I$ and any $I \in \mathscr{P}_j$ such that $0 \notin I$. we see that $e_{\widehat{i},N_m} d_{j,i} = e_{\widehat{i_I},N_m} d_{j,i_I}$ for any $i \in I$ and any $I \in \mathscr{P}_j$.

This shows that $f_j(T^{e'_{1,n}}, \ldots, T^{e'_{M,n}}) = \sum_{I \in \mathscr{P}_j} {T^{e_{\widehat{i_I}, N_m}}}^{d_{j,i_I}} \sum_{i \in I} c_{j,i} = 0$ as desired.

To verify the second property, we fix some $\widetilde{Q}(T) = \widetilde{Q_+}(T)\widetilde{Q_0}(T) \in k[T]$ not divisible by any element in $\mathcal{S} \cap \{T\}$, with $\widetilde{Q_+}(T) = T^r$ for some $r \geq 0$ such that $\widetilde{Q_0}(T)$ is not divisible by T. If $r > 0$, then we must have $T \notin \mathcal{S}$, and hence by assumption, there is an $N_{\widetilde{Q_+}} \in \mathbb{N}$ such that for any $n \geq N_{\widetilde{Q_+}}$ we have that T^{Dr} divides $f_j(T^{e_{1,n}}, \ldots, T^{e_{M,n}}) = \sum_{i=0}^{M} c_{j,i} T^{d_{j,i} e_{i,n}}$ for all $j \in \{1, \ldots, J\}$; if $r = 0$, then we put $N_{\widetilde{Q_+}} = 1$. By our convention, this means that

$$\min\{d_{j,i} e_{i,n} : \ i \in \{1, \ldots, M\} \text{ and } j \in \{1, \ldots, J\} \text{ and } n \geq N_{\widetilde{Q_+}}\} \geq Dr.$$

Since D is divisible by $d_{j,i}$ for each $i \in \{1, \ldots, M\}$ and $j \in \{1, \ldots, J\}$, it follows that

$$\min\{e_{i,n} : \ i \in \{1, \ldots, M\} \text{ and } n \geq N_{\widetilde{Q_+}}\} \geq r.$$

Choosing some $m_0 \in \mathbb{N}$ with $\widetilde{Q_0}(T)$ dividing $T^{abp^{m_0}(p^{m_0}-1)} - 1$ as well as some natural number $m \in \mathcal{M}$ with $m \geq m_0$, we have that $T^{abp^{m!}(p^{m!}-1)} - 1$ is divisible by $T^{abp^{m_0}(p^{m_0}-1)} - 1$, and thus is divisible by $\widetilde{Q_0}(T)$. Let $\widetilde{N}_{\widetilde{Q}} = \max\{N_{\widetilde{Q_+}}, N_{m!}\}$.

Fix an arbitrary $i \in \{1, \ldots, M\}$ and $n \in \mathcal{N}$ with $n \geq \widetilde{N}_{\widetilde{Q}}$. We need to show that $\widetilde{Q}(T)$ divides $T^{e_{i,n}} - T^{e'_{i,n}}$. By the definition that $e'_{i,n} = e_{\widehat{i},n}$ and the fact that $\widetilde{Q_0}(T)$ divides $T^{abp^{m!}(p^{m!}-1)} - 1$, it suffices to show that $T^r(T^{abp^{m!}(p^{m!}-1)} - 1)$ divides $T^{e_{i,n}} - T^{e_{\widehat{i},n}}$. First, since $n \geq N_{\widetilde{Q_+}}$, we have that $\min\{e_{i,n}, e_{\widehat{i},n}\} \geq r$, i.e., T^r divides $T^{e_{i,n}} - T^{e_{\widehat{i},n}}$. Furthermore, by the fact that $(\widehat{i}, i) \in R$ and that $R \subset \{0, 1, \ldots, M\} \times \{0, 1, \ldots, M\}$ is the minimal equivalence relation containing $\bigcup_{j \in \{1, \ldots, J\}} R_j$ with each $R_j \subset \{0, 1, \ldots, M\} \times \{0, 1, \ldots, M\}$ being an equivalence relation, there exists $(i_0, \ldots, i_L) \in \{0, 1, \ldots, M\}^{L+1}$ and $(j_1, \ldots, j_L) \in \{1, \ldots, J\}^L$ with $L \in \mathbb{N}$ such that $(i_0, i_L) = (\widehat{i}, i)$ and $(i_{\ell-1}, i_\ell) \in R_{j_\ell}$ for each $\ell \in \{1, \ldots, L\}$. Equivalently, for each $\ell \in \{1, \ldots, L\}$ we have an $I_\ell \in \mathscr{P}_{j_\ell}$ with $i_{\ell-1}, i_\ell \in I_\ell$. Since $n \geq N_{m!}$ with $m \in \mathcal{M}$, we have for each $\ell \in \{1, \ldots, L\}$ that $\mathscr{P}_{j_\ell} = \mathscr{P}_{j_\ell, m!}$ and thus the polynomial $T^{abp^{m!}(p^{m!}-1)} - 1$ divides $T^{e_{i_{\ell-1}, N_m}} - T^{e_{i_\ell, N_m}}$; also, we have that $T^{abp^{m!}(p^{m!}-1)} - 1$ divides both $T^{e_{i_0,n}} - T^{e_{i_0, N_m}}$ and

$T^{e_{i_L,n}} - T^{e_{i_L,N_m}}$. Hence, we see that

$$\begin{aligned} &T^{\widehat{e_{i,n}}} - T^{e_{i,n}} \\ &= T^{e_{i_0,n}} - T^{e_{i_L,n}} \\ &= (T^{e_{i_0,n}} - T^{e_{i_0,N_m}}) - (T^{e_{i_L,n}} - T^{e_{i_L,N_m}}) + \sum_{\ell=1}^{L}(T^{e_{i_{\ell-1},N_m}} - T^{e_{i_\ell,N_m}}) \end{aligned}$$

is divisible by $T^{abp^{m!}(p^{m!}-1)} - 1$. Since T^r and $T^{abp^{m!}(p^{m!}-1)} - 1$ are relatively prime, it follows that $T^r(T^{abp^{m!}(p^{m!}-1)} - 1)$ divides $T^{e_{i,n}} - T^{\widehat{e_{i,n}}}$. This completes the proof. $\square$

Theorem 3.12. *Suppose that $W = \bigcap_{j=1}^{J} H_{f_i}$, where J is a natural number, and for each $j \in \{1, \dots, J\}$ we have that*

$$f_j(X_1, \dots, X_M) = c_{j,0} + \sum_{i=1}^{M} c_{j,i} X_i^{d_{j,i}} \in k[X_1, \dots, X_M]$$

with $d_{j,i} > 0$ for each i. For each $j \in \{1, \dots, J\}$, denote by $\mathscr{C}_j$ the collection of those partitions $\mathscr{P}$ of the set $\{0, 1, \dots, M\}$ such that for each $I \in \mathscr{P}$ we have $\sum_{i \in I} c_{j,i} = 0$ and for each nonempty proper $I' \subset I$ we have $\sum_{i \in I'} c_{j,i} \neq 0$. Suppose that for every $j \in \{1, \dots, J\}$ and every $\mathscr{P} \in \mathscr{C}_j$ we have $d_{j,i} = d_{j,i'}$ for any $i, i' \in I$ and any $I \in \mathscr{P}$ such that $0 \notin I$. Suppose that Γ is cyclic. Then we have that $W(\overline{\Gamma}) = \overline{W(\Gamma)}$.

Proof. To avoid trivial cases, we assume that Γ is infinite cyclic, say, generated by $\gamma \in \Gamma$. Let $\{(\gamma^{e_{1,n}}, \dots, \gamma^{e_{M,n}})\}_{n \geq 1}$ be a sequence in $\mathbb{A}^M(\Gamma)$ which converges to a point $(x_1, \dots, x_M) \in W(\overline{\Gamma}) \subset W(\prod_{v \in \Sigma} K_v^*)$, where $e_{i,n} \in \mathbb{Z}$. In particular, for each $i \in \{1, \dots, M\}$ and each $v \in \Sigma$, the sequence $\{|\gamma^{e_{i,n}}|_v\}_{n \geq 1} = \{|\gamma|_v^{e_{i,n}}\}_{n \geq 1}$ must converge in $\mathbb{R}^*$. If $|\gamma|_v \neq 1$ for some $v \in \Sigma$, then the sequence $\{(\gamma^{e_{1,n}}, \dots, \gamma^{e_{M,n}})\}_{n \geq 1}$ must be eventually stationary, and it follows that $(x_1, \dots, x_M) \in W(\Gamma)$. Therefore it suffices to treat only the case where $|\gamma|_v = 1$, i.e. $\gamma \in O_v^*$, for every $v \in \Sigma$.

Let $\Sigma|_{k(\gamma)} \subset \Sigma$ be the subset satisfying the following property that for each $v \in \Sigma$ there exists a unique $w \in \Sigma|_{k(\gamma)}$ such that both v and w restrict to the same place of $k(\gamma)$. Consider the k-isomorphism between fields

$$k(T) \to k(\gamma),\ T \mapsto \gamma. \tag{3.1}$$

Through the isomorphism (3.1), the set $\Sigma|_{k(\gamma)}$ is, by construction, injectively mapped onto a subset of the set of places of $k(T)$. For each $v \in \Sigma|_{k(\gamma)}$, we have that $\gamma \in O_v^*$; let $P_v(T) \in k[T]$ be the irreducible polynomial corresponding the image of v under this map. Let $\mathcal{S}$ be the complement of the subset $\{P_v(T) : v \in \Sigma|_{k(\gamma)}\}$ of the set of all irreducible polynomials in $k[T]$. Note that $\mathcal{S}$ is a finite set containing the polynomial T, and that $k[\Gamma] \subset O_v$ for each $v \in \Sigma$, where $k[\Gamma]$ is the smallest subring of K containing both k and Γ.

The sequence $\{(\gamma^{e_{1,n}}, \dots, \gamma^{e_{M,n}})\}_{n\geq 1}$ lies in the image of

$$\mathbb{A}^M\left(\prod_{v\in\Sigma|_{k(\gamma)}} k(\gamma)_v^*\right) \to \mathbb{A}^M\left(\prod_{v\in\Sigma} K_v^*\right)$$

under the natural map, where $k(\gamma)_v$ denotes the topological closure of the subfield $k(\gamma)$ in K_v. Note that this image is a closed subset. The topology on $\overline{\Gamma}$ is induced from the usual product topology on $\prod_{v\in\Sigma} k(\gamma)_v^*$, and the latter topology is the same as the subspace topology restricted from the usual product topology on $\prod_{v\in\Sigma} k(\gamma)_v$. Thus for each $i \in \{1, \dots, M\}$ the sequence $(\gamma^{e_{i,n}})_{n\geq 1}$ converges to x_i in $\prod_{v\in\Sigma} k(\gamma)_v$ Therefore, from the continuity of each f_j at $(x_1, \dots, x_M) \in \mathbb{A}^M(\prod_{v\in\Sigma} k(\gamma)_v)$, we see that for each $j \in \{1, \dots, J\}$ the sequence $(f_j(\gamma^{e_{1,n}}, \dots, \gamma^{e_{M,n}}))_{n\geq 1}$ converges to $f_j(x_1, \dots, x_M) = 0$ in $\prod_{v\in\Sigma} k(\gamma)_v$. Consider the sequence $\{(e_{1,n}, \dots, e_{M,n})\}_{n\geq 1}$ in $\mathbb{A}^M(\mathbb{Z})$. Fix an arbitrary polynomial $Q(T) \in k[T]$ not divisible by any element in $\mathcal{S}$. Thus we have the prime decomposition $Q(T) = \prod_{v\in\Sigma|_{k(\gamma)}} P_v(T)^{n_v}$ in $k[T]$, where there are only finitely many $v \in \Sigma|_{k(\gamma)}$ with $n_v > 0$. In particular,

$$U_Q = \prod_{\substack{v\in\Sigma|_{k(\gamma)}\\ n_v=0}} k(\gamma)_v \times \prod_{\substack{v\in\Sigma|_{k(\gamma)}\\ n_v>0}} (\mathfrak{m}_v \cap k(\gamma)_v)^{n_v}$$

is an open subset in $\prod_{v\in\Sigma|_{k(\gamma)}} k(\gamma)_v$ endowed with the the product topology. Note that $f_j(\gamma^{e_{1,n}}, \dots, \gamma^{e_{M,n}}) \in k[\gamma, \gamma^{-1}]$ for each $j \in \{1, \dots, J\}$ and $n \in \mathbb{N}$. The intersection of U_Q with the image of $k[\gamma, \gamma^{-1}]$ in $\prod_{v\in\Sigma|_{k(\gamma)}} k(\gamma)_v$ is the image of $Q(\gamma)k[\gamma, \gamma^{-1}]$, which is thus an open subset of $k[\gamma, \gamma^{-1}]$ containing zero with respect to the subspace topology restricted from $\prod_{v\in\Sigma|_{k(\gamma)}} k(\gamma)_v$. Therefore, from the fact each sequence $(f_j(\gamma^{e_{1,n}}, \dots, \gamma^{e_{M,n}}))_{n\geq 1}$ converges to zero in $\prod_{v\in\Sigma} k(\gamma)_v$, it follows that there is an $N_Q \in \mathbb{N}$ such that for any $n \geq N_Q$ we have that $f_j(\gamma^{e_{1,n}}, \dots, \gamma^{e_{M,n}}) \in Q(\gamma)k[\gamma, \gamma^{-1}]$ for each $j \in \{1, \dots, J\}$; thus by the isomorphism (3.1) we have that $Q(T)$ divides $f_j(T^{e_{1,n}}, \dots, T^{e_{M,n}})$, because 0 is not a zero of $Q(T)$. Therefore the assumption of Proposition 3.11 is verified. Applying the isomorphism (3.1) to the conclusion of Proposition 3.11, we see that there exists a sequence $\{(e'_{1,n}, \dots, e'_{M,n})\}_{n\in\mathcal{N}}$ in $\mathbb{A}^M(\mathbb{Z})$ indexed by an infinite subset $\mathcal{N} \subset \mathbb{N}$ satisfying the following properties: for each $n \in \mathcal{N}$ we have $f_j(\gamma^{e'_{1,n}}, \dots, \gamma^{e'_{M,n}}) = 0$ for all $j \in \{1, \dots, J\}$, and for every $\widetilde{Q}(T) \in k[T]$ not divisible by T, there is an $\widetilde{N}_{\widetilde{Q}} \in \mathbb{N}$ such that for any $n \in \mathcal{N}$ with $n \geq \widetilde{N}_{\widetilde{Q}}$ we have that $\gamma^{e_{i,n}} - \gamma^{e'_{i,n}} \in \widetilde{Q}(\gamma)k[\gamma, \gamma^{-1}]$ for all $i \in \{1, \dots, M\}$. The first property says that $(\gamma^{e'_{1,n}}, \dots, \gamma^{e'_{M,n}}) \in W(\Gamma)$ for each $n \in \mathcal{N}$. On the other hand, because the image of $k[\gamma, \gamma^{-1}]$ in $\prod_{v\in\Sigma|_{k(\gamma)}} k(\gamma)_v$ lies in $\prod_{v\in\Sigma|_{k(\gamma)}} (O_v \cap k(\gamma)_v)$, one may argue similarly as above that the topology on $k[\gamma,\gamma^{-1}]$, which is induced from the usual product topology on $\prod_{v\in\Sigma} k(\gamma)_v$, is generated by those subset $\widetilde{Q}(\gamma)k[\gamma,\gamma^{-1}]$ with $\widetilde{Q}(T)\in k[T]$ not divisible by any element in the set $\mathcal{S}$. Since $\mathcal{S}$ contains the polynomial T, the second property implies that for each $i\in\{1,\ldots,M\}$ the sequence $(\gamma^{e_{i,n}}-\gamma^{e'_{i,n}})_{n\in\mathcal{N}}$ converges to zero in $\prod_{v\in\Sigma} k(\gamma)_v$; this shows that the two sequences $(\gamma^{e_{i,n}})_{n\in\mathcal{N}}$ and $(\gamma^{e'_{i,n}})_{n\in\mathcal{N}}$ converge to the same element in $\prod_{v\in\Sigma} k(\gamma)_v$. Hence, for each $i\in\{1,\ldots,M\}$, the sequence $(\gamma^{e'_{i,n}})_{n\in\mathcal{N}}$ converges to x_i in $\prod_{v\in\Sigma} k(\gamma)_v$; since $x_i\in\prod_{v\in\Sigma} k(\gamma)_v^*$, it follows from what is explained above that the same convergence also happens in $\prod_{v\in\Sigma} k(\gamma)_v^*$. This shows that $(x_1,\ldots,x_M)\in\overline{\{(\gamma^{e'_{1,n}},\ldots,\gamma^{e'_{M,n}})\}_{n\in\mathcal{N}}}\subset\overline{W(\Gamma)}$, which completes the proof. □

Proof of Theorem 1.10. Choose a free subgroup $\Phi\subset\Gamma$ such that $\Gamma=\bigcup_{\tau\in\mathrm{Tor}(\Gamma)}\tau\Phi$. Let $\{(\gamma_{1,n},\ldots,\gamma_{M,n})\}_{n\geq 1}$ be a sequence in $\mathbb{A}^M(\Gamma)$ which converges to a point $(x_1,\ldots,x_M)\in W(\overline{\Gamma})$. For each i and n, choose $\tau_{i,n}\in\mathrm{Tor}(\Gamma)$ such that $\gamma_{i,n}\in\tau_{i,n}\Phi$. Since $\mathrm{Tor}(\Gamma)$ is finite, by taking subsequence we may assume that there is some $(\tau_1,\ldots,\tau_M)\in\mathbb{A}^M(\mathrm{Tor}(\Gamma))$ such that the sequence $\{(\frac{\gamma_{1,n}}{\tau_1},\ldots,\frac{\gamma_{M,n}}{\tau_M})\}_{n\geq 1}$ lies in $\mathbb{A}^M(\Phi)$ and converges to $(\frac{x_1}{\tau_1},\ldots,\frac{x_M}{\tau_M})$, which lies in the set

$$(\tau_1^{-1},\ldots,\tau_M^{-1})\left(W(\overline{\Phi})\right)=\left((\tau_1^{-1},\ldots,\tau_M^{-1})W\right)(\overline{\Phi}),$$

where the translation $(\tau_1^{-1},\ldots,\tau_M^{-1})W$ of $W=\bigcap_{j=1}^{J}H_{f_j}$ by the tuple

$$(\tau_1^{-1},\ldots,\tau_M^{-1})\in\mathbb{A}^M(\mathrm{Tor}(\Gamma))\subset\mathbb{A}^M(k^*)$$

is equal to the intersection

$$\bigcap_{j=1}^{J}\left((\tau_1^{-1},\ldots,\tau_M^{-1})H_{f_j}\right)=\bigcap_{j=1}^{J}H_{g_j},$$

where for each $j\in\{1,\ldots,J\}$ we have that

$$\begin{aligned}g_j(X_1,\ldots,X_M)&=f_j(\tau_1X_1,\ldots,\tau_MX_M)\\&=c_{j,0}+\sum_{i=1}^{M}c_{j,i}(\tau_iX_i)^{d_j}\in k[X_1,\ldots,X_M]\end{aligned}$$

with $d_j>0$. By Theorem 3.12, we have that

$$\left((\tau_1^{-1},\ldots,\tau_M^{-1})W\right)(\overline{\Phi})=\overline{\left((\tau_1^{-1},\ldots,\tau_M^{-1})W\right)(\Phi)},$$

which shows that

$$(\frac{x_1}{\tau_1},\ldots,\frac{x_M}{\tau_M})\in\overline{\left((\tau_1^{-1},\ldots,\tau_M^{-1})W\right)(\Phi)}=\overline{(\tau_1^{-1},\ldots,\tau_M^{-1})\left(W(\Phi)\right)}.$$

It follows that $(x_1, \ldots, x_M) = (\tau_1 \cdot \frac{x_1}{\tau_1}, \ldots, \tau_M \cdot \frac{x_M}{\tau_M}) \in \overline{W(\Phi)} \subset \overline{W(\Gamma)}$ as desired. $\square$

Acknowledgement

This research is supported by Ministry of Science and Technology. The plan number is 104-2115-M-001-012-MY3. The proof of Lemma 3.3 and that of Proposition 3.11 are motivated by an answer of Fedor Petrov on the following page of MathOverflow: `http://mathoverflow.net/q/226417`

References

[1] D. Harari & J. F. Voloch, "The Brauer-Manin obstruction for integral points on curves", *Math. Proc. Camb. Philos. Soc.* **149** (2010), no. 3, p. 413-421.

[2] H. Pasten & C.-L. Sun, "Multiplicative subgroups avoiding linear relations in finite fields and a local-global principle", *Proc. Am. Math. Soc.* **144** (2016), no. 6, p. 2361-2373.

[3] B. Poonen, "Heuristics for the Brauer-Manin obstruction for curves", *Exp. Math.* **15** (2006), no. 4, p. 415-420.

[4] T. A. Skolem, "Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen", *Avh. Norske Vid. Akad. Oslo* **1937** (1937), no. 12, p. 1-16.

[5] C.-L. Sun, "Local-global principle of affine varieties over a subgroup of units in a function field", *Int. Math. Res. Not.* **2014** (2014), no. 11, p. 3075-3095.

[6] J. F. Voloch, "The equation $ax + by = 1$ in characteristic p", *J. Number Theory* **73** (1998), no. 2, p. 195-200.

Chia-Liang Sun
Institute of Mathematics
Academia Sinica
Room 626, 6F, Astronomy-Mathematics Building,
No. 1, Sec. 4, Roosevelt Road,
Taipei 10617, Taiwan
E-mail: `csun@math.sinica.edu.tw`