HILBERT'S TENTH PROBLEM OVER FUNCTION FIELDS OF POSITIVE CHARACTERISTIC NOT CONTAINING THE ALGEBRAIC CLOSURE OF A FINITE FIELD

KIRSTEN EISENTRÄGER AND ALEXANDRA SHLAPENTOKH

ABSTRACT. We prove that the existential theory of any function field K of characteristic $p > 0$ is undecidable in the language of rings provided that the constant field does not contain the algebraic closure of a finite field. We also extend the undecidability proof for function fields of higher transcendence degree to characteristic 2 and show that the first-order theory of **any** function field of positive characteristic is undecidable in the language of rings without parameters.

1. Introduction

Hilbert's Tenth Problem in its original form was to find an algorithm to decide, given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in the ring $\mathbb{Z}$ of integers, whether it has a solution with $x_1, \ldots, x_n \in \mathbb{Z}$. Matiyasevich [Mat70], building on earlier work by Davis, Putnam, and Robinson [DPR61], proved that no such algorithm exists, i.e. Hilbert's Tenth Problem is undecidable.

Since then, analogues of this problem have been studied by asking the same question for polynomial equations with coefficients and solutions in other recursive commutative rings. A recursive ring is a countable ring for which there is an algorithm to determine what the elements of the ring are and such that the graphs of addition and multiplication are also recursive. Perhaps the most important unsolved question in this area is Hilbert's Tenth Problem over the field of rational numbers which, at the moment, seems out of reach.

The function field analogue of Hilbert's Tenth Problem in positive characteristic turned out to be much more tractable. Hilbert's Tenth Problem is known to be undecidable for the function field K of a curve over a finite field [Phe91, Vid94, Shl96, Eis03]. We also have undecidability of Hilbert's Tenth Problem for certain function fields over possibly infinite constant fields of positive characteristic [Shl00, Shl, Eis03, KR92]. The results of [Eis03] and [Shl00] also generalize to higher transcendence degree (see [Shl02] and [Shl]) and give undecidability of Hilbert's Tenth Problem for finite and some infinite extensions of $\mathbb{F}_q(t_1, \ldots, t_n)$ with $n \geq 2$. In [Eis12] the problem was shown to be undecidable for finite extensions of $k(t_1, \ldots, t_n)$ with $n \geq 2$ and k algebraically closed of odd characteristic.

So all known undecidability results for Hilbert's Tenth Problem in positive characteristic either require that the constant field not be algebraically closed or that we are dealing with a function field in at least 2 variables. The big open question that remains is whether Hilbert's Tenth Problem for a one-variable function field over an algebraically closed field of constants is undecidable. In this paper we will shrink the window of the "unknown" almost precisely to the question above by proving the following theorems (we separate the countable and uncountable cases).

Theorem 1.1. *If K is any countable function field not containing the algebraic closure of a finite field, then Hilbert's Tenth Problem is not solvable over K.*

Theorem 1.2. *If K is any function field of positive characteristic not containing the algebraic closure of a finite field, then there exists a finitely generated subfield $K_0 \subseteq K$ such that there is no algorithm to determine whether a polynomial equation with coefficients in K_0 has solutions in K.*

Key words and phrases. Undecidability, Hilbert's Tenth Problem.

K. Eisenträger was partially supported by National Science Foundation grant DMS-1056703. A. Shlapentokh was partially supported by National Science Foundation grant DMS-1161456.

In [ES09], the authors proved that the first-order theory of any function field not equal to a function field of transcendence degree at least 2 and characteristic 2 in the language of rings without parameters is undecidable. In this paper we prove the result in the missing case to show that the following theorem is true.

Theorem 1.3. *The first-order theory of any function field of positive characteristic in the language of rings without parameters is undecidable.*

To explain the idea of the proof we need the notion of a Diophantine (or existentially definable) set. Given a commutative integral domain R and a positive integer k, we say that a subset $A \subset R^k$ is *Diophantine* over R or is *existentially definable* over R in the language of rings if there exists a polynomial $f(t_1, \dots, t_k, x_1, \dots, x_n)$ with coefficients in R such that for any k-tuple $\bar{a} = (a_1, \dots, a_k) \in R^k$ we have that $\bar{a} \in A \iff \exists b_1, \dots, b_n \in R : f(\bar{a}, b_1, \dots, b_n) = 0$. In this case, $f(t_1, \dots, t_k, x_1, \dots, x_n)$ is called a Diophantine definition of A over R. In general, if the fraction field of a recursive integral domain is not algebraically closed, a system of polynomial equations can always be effectively replaced by a single polynomial equation without changing the relation [Shl06, Chapter 1, §2, Lemma 1.2.3].

The current methods for proving undecidability of Hilbert's Tenth Problem for function fields K of positive characteristic p usually require showing that the following sets are existentially definable in the language of rings (or, equivalently, have a Diophantine definition over K):

$$P(K) = \{(x, x^{p^s}) : x \in K, s \in \mathbb{Z}_{\geq 0}\},$$

and for some nontrivial prime $\mathfrak{p}$ of K,

$$\mathrm{INT}(K, \mathfrak{p}) = \{x \in K : \mathrm{ord}_{\mathfrak{p}} x \geq 0\}.$$

In [ES09] we showed that we can existentially define one of these sets for a large class of fields: we proved that the set of p-th powers $P(K)$ is existentially definable in *any* function field K of characteristic $p > 2$ whose constant field has transcendence degree at least one over $\mathbb{F}_p$. In [PPV11] a uniform definition of p-th powers was given for arbitrary function fields with the characteristic "large enough" compared to the genus of the field. In this paper, we show that the set $P(K)$ is existentially definable in *any* function field K of positive characteristic. In particular, we are finally able to remove the assumption in [Shl00] and [Eis03] that the algebraic closure of $\mathbb{F}_p$ in K should have an extension of degree p.

The most difficult part of our argument is defining p^s-th powers of a special element t. In [Shl00, Eis03] we needed to assume that we had suitable extensions of degree p of the constant field to conclude that a certain set of equations over K, which was satisfied by an element $x \in K$, actually forced x to be in the rational function field $C_K(t)$ (Lemma 2.6 in [Shl00] and Lemma 3.5 in [Eis03]). Here C_K denotes the constant field of K. This argument does not work in our setting because our constant field can be algebraically closed. Perhaps the most important new technical part is contained in Lemma 5.6, which is the key new argument in Section 5.1 that allows us to define p^s-th powers of t in arbitrary function fields of positive characteristic.

The second set that is required to be existentially definable to prove the undecidability of Hilbert's Tenth Problem is the set $\mathrm{INT}(K, \mathfrak{p})$ defined above. In [Shl00] the second author showed that $\mathrm{INT}(K, \mathfrak{p})$ was existentially definable for some non-trivial prime $\mathfrak{p}$ of K over any function field whose constant field was algebraic over a finite field and not algebraically closed, and some higher transcendence degree constant fields not containing the algebraic closure of a finite field. In fact to show the Diophantine undecidability of a function field K of positive characteristic, it is enough to give an existential definition of $P(K)$ and of the set which we call $\mathrm{INT}(K, \mathfrak{p}, t)$, where t is a non-constant element of K with $\mathrm{ord}_{\mathfrak{p}} t > 0$, such that for any $x \in K$ we have that $x \in \mathrm{INT}(K, \mathfrak{p}, t) \Rightarrow \mathrm{ord}_{\mathfrak{p}} x \geq 0$ and if $x \in k_0(t)$, where k_0 is the algebraic closure of a finite field in K, and $\mathrm{ord}_{\mathfrak{p}} x \geq 0$, then $x \in \mathrm{INT}(K, \mathfrak{p}, t)$.

The structure of the remainder of the paper is as follows. In Section 2 we explain how to derive the existential undecidability of a function field K of positive characteristic from existential definitions of $P(K)$ and $\mathrm{INT}(K, \mathfrak{p}, t)$ for some non-trivial prime $\mathfrak{p}$ of K and a non-constant element $t \in K$. In Section 3 we discuss some general properties of Diophantine definitions. In Section 4 we discuss some technical properties of function fields of positive characteristic we will need to define $P(K)$. In Section 5 we give an existential definition of $P(K)$, and in Section 6 we give an existential definition of $\mathrm{INT}(K, \mathfrak{p}, t)$. Finally, in Section 7 we use the existential definition of $P(K)$ to obtain the first-order results in Theorem 1.3.

2. From p-th powers and integrality at a prime to Diophantine undecidability

We start with defining a relation on positive integers.

Definition 2.1. For $m, n \in \mathbb{Z}_{>0}$ and p a rational prime number, define $n \mid_p m$ to mean $m = np^s$ for some $s \in \mathbb{Z}_{\geq 0}$.

In [Phe87] Thanases Pheidas proved that the existential theory of $(\mathbb{Z}_{>0}, +, \mid_p)$ is undecidable by showing that multiplication of positive integers is definable using "+" and "$\mid_p$". That means there is no uniform algorithm that, given a system of equations over the positive natural numbers with addition and $\mid_p$, determines whether this system has a solution or not. When $P(K)$ and $\mathrm{INT}(K, \mathfrak{p}, t)$ are existentially definable, we can reduce this problem to Hilbert's Tenth Problem over K and prove that Hilbert's Tenth Problem over K must be undecidable.

To do this we define a map f from the positive integers to subsets of K by associating to an integer n the subset $f(n) = \{x \in \mathrm{INT}(K, \mathfrak{p}, t) : \mathrm{ord}_{\mathfrak{p}} x = n\}$. Then the equation $n_3 = n_1 + n_2$ ($n_i \in \mathbb{Z}_{>0}$) is equivalent to the existence of elements $z_i \in f(n_i)$ with $z_3 = z_1 \cdot z_2$.

To ensure that we are only constructing equations over K with z_i elements of positive order (to obtain elements in $\mathbb{Z}_{>0}$ under the map $K \to \mathbb{Z}$ that maps z_i to $\mathrm{ord}_{\mathfrak{p}}(z_i)$) we add the condition that $\mathrm{ord}_{\mathfrak{p}}(z_i/t) \in \mathrm{INT}(K, \mathfrak{p}, t)$.

We also have that for positive integers n, m,

$$\begin{aligned} n \mid_p m &\iff \exists s \in \mathbb{N} m = p^s n \\ &\iff \exists x \in f(n)\ \exists y \in f(m)\ \exists s \in \mathbb{N}\ (\mathrm{ord}_{\mathfrak{p}} y = p^s \mathrm{ord}_{\mathfrak{p}} x). \end{aligned}$$

This equivalence can be seen by letting $x = t^n$ and $y = t^m$.

But the last formula is equivalent to

$$\exists x \in f(n)\ \exists y \in f(m)\ \exists w \in K\ \exists s \in \mathbb{N}\ w = x^{p^s} \text{ and } \{w/y, y/w\} \subset \mathrm{INT}(K, \mathfrak{p}, t).$$

Saying that both w/y and y/w are in $\mathrm{INT}(K, \mathfrak{p}, t)$ simply means that they have the same order at $\mathfrak{p}$.

We have now proved the following proposition.

Proposition 2.2. *If K is a function field of positive characteristic p over a field of constants k, $\mathfrak{p}$ is a non-trivial valuation (or prime) of K, $t \in K \setminus k$, has a positive order at $\mathfrak{p}$, and $P(K)$ and $INT(K, \mathfrak{p}, t)$ are existentially definable over K, then for some finitely generated subfield K_0 of K, there is no algorithm to determine whether an arbitrary polynomial equation in several variables and with coefficients in K_0 has solutions in K.*

3. Rewriting equations over finite extensions

In constructing Diophantine definitions it is often convenient to work over finite extension of the given field, sometimes in fixed extensions and sometimes in extensions of bounded degree. The theorem below and its corollaries allow us to do this. The next theorem is Lemma B.7.5 in the Number Theory Appendix of [Shl06].

Theorem 3.1. *Let K be a field, let $\tilde{K}$ be the algebraic closure of K, let*

$$g(X, Z_1, \ldots, Z_{n_1}),$$
$$f(T_1, \ldots, T_n, X_1, \ldots, X_{n_2}, Y_1, \ldots, Y_{n_3})$$

be polynomials with coefficients in K, and let $A \subset K^n$ be defined in the following manner: $(t_1, \ldots, t_n) \in A$ if and only if there exist $z_1, \ldots, z_{n_1}, x_1, \ldots, x_{n_2} \in K, x \in \tilde{K}, y_1, \ldots, y_{n_3} \in K(x)$ such that

$$g(x, z_1, \ldots, z_{n_1}) = 0 \wedge f(t_1, \ldots, t_n, x_1, \ldots, x_{n_2}, y_1, \ldots, y_{n_3}) = 0.$$

In this case A has a Diophantine definition over K. Further, there is a Diophantine definition of A with coefficients depending only on coefficients and degrees of g and f and it can be constructed effectively from those coefficients.

The most often used versions of the theorem above are the following corollaries (though we will need the theorem also).

Corollary 3.2. *Let K be a field, let G be a finite extension of K, let $f(T, X_1, \ldots, X_{n_2}, Y_1, \ldots, Y_{n_3})$ be a polynomial with coefficients in K, and let $A \subset K$ be defined in the following manner: $t \in A$ if and only if there exist $x_1, \ldots, x_{n_2} \in K, y_1, \ldots, y_{n_3} \in G$ such that*

$$f(t, x_1, \ldots, x_{n_2}, y_1, \ldots, y_{n_3}) = 0.$$

In this case A has a Diophantine definition over K.

Corollary 3.3. *Let G/K be a finite extension of fields and assume Hilbert's Tenth Problem is unsolvable over G (if G is uncountable, then assume we are considering equations with coefficients in a finitely generated subfield of G). In this case Hilbert's Tenth Problem is unsolvable over K (as above, if K is uncountable, then assume we are considering equations with coefficients in a finitely generated subfield of K).*

4. Technical preliminaries

Notation and Assumptions 4.1. In this section we go over or prove several technical facts we need to construct our existential definition of p-th powers. We will initially work under the assumption that the constant field is algebraically closed. This assumption will be removed later. Below we use the following notation and assumptions.

(1) By a *function field (in 1 variable)* over a field k we mean a field K containing k and an element x, transcendental over k, such that $K/k(x)$ is a finite algebraic extension. The algebraic closure of k in K is called the constant field of K, and it is a finite extension of k.
(2) Let M be a function field of genus $g > 0$ over an algebraically closed field of constants F of characteristic $p > 0$.
(3) Let $t \in M$ be such that it is not a p-th power. (Since the constant field is perfect, this assumption implies $M/F(t)$ is separable.)
(4) A *prime* of M is an F-discrete valuation of M.
(5) The degree of a prime is the degree of its residue field over the field of constants. Under our assumption that the constant field is algebraically closed, the degree is always one.
(6) A divisor is an element of the free abelian group on the set of primes of M. We will denote the group law multiplicatively.
(7) If $\mathfrak{I}$ is an integral (or effective) divisor, we will denote by $\deg \mathfrak{I}$ the degree of $\mathfrak{I}$, i.e. the number of primes in the product (counting multiplicity).
(8) If $\mathfrak{I}$ is an integral divisor and $\mathfrak{p}$ is a prime, then $\mathrm{ord}_{\mathfrak{p}}\mathfrak{I}$ is the multiplicity of $\mathfrak{p}$ in the product.
(9) If $\mathfrak{I}_1$ and $\mathfrak{I}_2$ are integral divisors, we write $\mathfrak{I}_1 \mid \mathfrak{I}_2$ ($\mathfrak{I}_1$ divides $\mathfrak{I}_2$) to mean that for all primes $\mathfrak{p}$ of K we have that $\mathrm{ord}_{\mathfrak{p}}\mathfrak{I}_1 \leq \mathrm{ord}_{\mathfrak{p}}\mathfrak{I}_2$. Similarly for any prime $\mathfrak{p}$ of M we write that $\mathfrak{p} \mid \mathfrak{I}_1$ ($\mathfrak{p}$ divides $\mathfrak{I}_1$) to mean $\mathrm{ord}_{\mathfrak{p}}\mathfrak{I}_1 > 0$.
(10) For $x \in M$, let $\mathfrak{n}(x)$ denote the zero divisor of x and $\mathfrak{d}(x)$ the pole divisor of x. Let $\mathfrak{D}(x) = \frac{\mathfrak{n}(x)}{\mathfrak{d}(x)}$ be the divisor of x. Let $H(x)$ denote the height of x, i.e. $\deg \mathfrak{d}(x) = \deg \mathfrak{n}(x)$, and if $\mathfrak{p}$ is a prime, let

$$\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}\mathfrak{D}(x) = \mathrm{ord}_{\mathfrak{p}}\mathfrak{n}(x) - \mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x).$$

(11) Since the extension M over $F(t)$ is separable, we can define a global derivation with respect to t. Over $F(t)$, we use the usual definition of the derivative, and we use implicit differentiation to extend a derivation to the extension (see [Mas96, p. 9 and p. 94]). Given an element x of M, the derivative with respect to t will be denoted in the usual fashion as x' or $\frac{dx}{dt}$. Observe that usual differentiation rules apply to the global derivation with respect to t.
(12) For any prime $\mathfrak{p}$ of M, we can also define a local derivation with respect to the prime $\mathfrak{p}$. More specifically, if π is any local uniformizing parameter with respect to $\mathfrak{p}$ (any element of M which has order one at $\mathfrak{p}$), in the $\mathfrak{p}$-adic completion of M, every element x of the field can be written as an infinite power series

$$\sum_{i=m}^{\infty} a_i \pi^i$$

with $m \in \mathbb{Z}$ and $a_i \in F$. Given this representation, we denote

$$\frac{\partial x}{\partial \mathfrak{p}} = \sum_{i=m}^{\infty} i a_i \pi^{i-1}$$

(see [Mas96, p. 9 and p. 96]). Observe that $\operatorname{ord}_{\mathfrak{p}}(\frac{\partial x}{\partial \mathfrak{p}})$ is independent of the choice of the local uniformizing parameter.

(13) For all primes $\mathfrak{p}$ of M, let

$$d_t(\mathfrak{p}) = \operatorname{ord}_{\mathfrak{p}} \left(\frac{\partial t}{\partial \mathfrak{p}} \right).$$

(14) If $\mathfrak{U} = \frac{\mathfrak{A}}{\mathfrak{B}}$, where $\mathfrak{A}$ and $\mathfrak{B}$ are integral divisors, then, we will write

$$L(\mathfrak{U}) = \{f \in M \mid \operatorname{ord}_{\mathfrak{p}} f \geq \operatorname{ord}_{\mathfrak{p}} \mathfrak{A} - \operatorname{ord}_{\mathfrak{p}} \mathfrak{B} \text{ for all primes } \mathfrak{p} \text{ of } M\} \cup \{0\},$$

where $L(\mathfrak{U})$ is a vector space over F, and $\ell(\mathfrak{A})$ for the dimension of $L(\mathfrak{A})$ over F.

The following lemma gathers some general formulae we need in this section.

Lemma 4.2.

(1) *Let E be a finite degree subfield of a function field K. Let $\mathfrak{P}$ be a prime of E and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes in K above $\mathfrak{P}$. Let $e(\mathfrak{p}_i/\mathfrak{P})$ be the ramification index of $\mathfrak{p}_i$ over $\mathfrak{P}$. Let $f(\mathfrak{p}_i/\mathfrak{P})$ be the relative degree of $\mathfrak{p}_i$ over $\mathfrak{P}$ (the degree of the extension of the residue field). We have*

$$[K : E] = \sum_{i=1}^{n} e(\mathfrak{p}_i/\mathfrak{P}) f(\mathfrak{p}_i/\mathfrak{P}).$$

If the field of constants of E is algebraically closed, the relative degrees will always be equal to one.

(2) *(Riemann-Roch) Let $\mathfrak{U} = \frac{\mathfrak{A}}{\mathfrak{B}}$ be a ratio of integral divisors of K such that* $\deg \mathfrak{B} - \deg \mathfrak{A} = d \in \mathbb{Z}$.
   (a) *If $g = 0$ and $d \geq 0$ then $\ell(\mathfrak{A}) = d + 1$;*
   (b) *If $g > 0$ and $0 < d < 2g - 2$ then $\ell(\mathfrak{A}) \geq d - g + 1$;*
   (c) *If $g > 0$ and $d = 2g - 2$ then $\ell(\mathfrak{A}) \geq g - 1$;*
   (d) *If $g > 0$ and $d > 2g - 2$ then $\ell(\mathfrak{A}) = d - g + 1$;*

Proof. For (1) see [FJ05, Proposition 2.3.2, Theorem 3.6.1]. For (2) see [Koc00, Theorem 5.6.2]. □

The next lemma is an elementary result from linear algebra that we need to make use of the Riemann-Roch Theorem.

Lemma 4.3. *If V is a vector space of dimension $n > 0$ over an infinite field of scalars and $\{V_1, \ldots, V_m\}$ is a finite collection of subspaces of V, each of dimension $n - 1$, then $V \setminus (\bigcup_{i=1}^{m} V_i)$ contains infinitely many elements.*

Proof. Let A be a countable subset of the field of scalars, let $\{a_1, a_2, \ldots\}$ be an ordering of A, and let $A_j = \{a_1, \ldots, a_j\}$. It is enough to show that

$$C = \left\{ \sum_{i=1}^{n} b_i v_i, b_i \in A \right\} \setminus (V_1 \cup \ldots \cup V_m)$$

is infinite, and note further that it is enough to show that C contains finite subsets of arbitrary size. Let

$$C_r = \left\{ \sum_{i=1}^{n} b_i v_i : b_i \in A_r \right\} \setminus (V_1 \cup \ldots \cup V_m)$$

and observe that $C_r \subset C$ for all $r \in \mathbb{Z}_{>0}$. Select a basis $v_1, \ldots, v_n$ for V. If we fix $i = 1, \ldots, m$, then without loss of generality, after possibly renumbering the elements $v_1, \ldots, v_n$ (with the renumbering depending on i), we can assume that for $j = 1, \ldots, n - 1$, each V_i has a basis $\{w_{i,1}, \ldots, w_{i,n-1}\}$, where $w_{i,j} = v_j + c_{i,j} v_n$. Let

$$u \in \left\{ \sum_{i=1}^{n} b_i v_i : b_i \in A_r \right\} \cap V_i.$$

In this case $u = \sum_{j=1}^{n-1} b_j w_{i,j}$, where $b_j \in A_r$. Thus,

$$\left| \left\{ \sum_{i=1}^{n} b_i v_i : b_i \in A_r \right\} \cap V_i \right| = r^{n-1}.$$

Therefore

$$|C_r| \geq (r^n - mr^{n-1}) \to \infty \text{ as } r \to \infty.$$

□

Below is the first application of the Riemann-Roch Theorem we need.

Lemma 4.4. *If $\mathfrak{t}$ is a prime of M and $\mathfrak{A}$ and $\mathfrak{B}$ are two integral relatively prime divisors of M, both also relatively prime to $\mathfrak{t}$, then there exists $y \in M$ such that $\mathfrak{d}(y) = \mathfrak{t}^{2g+1+\deg \mathfrak{A}}$ and $\mathfrak{n}(y) = \mathfrak{A}\mathfrak{C}$, where $\mathfrak{C}$ is an integral divisor relatively prime to $\mathfrak{A}$ and $\mathfrak{B}$. Further, $\deg \mathfrak{C} = 2g+1$.*

Proof. Let $\mathfrak{U} = \dfrac{\mathfrak{A}}{\mathfrak{t}^{2g+1+\deg \mathfrak{A}}}$ and note that by Lemma 4.2(2) we have that

$$\ell(\mathfrak{U}) = g + 2 > 0.$$

Further, let $\mathfrak{U}_1 = \dfrac{\mathfrak{A}}{\mathfrak{t}^{2g+\deg \mathfrak{A}}}$ and observe that $\ell(\mathfrak{U}_1) = g+1$ while $\mathcal{L}(\mathfrak{U}_1) \subset \mathcal{L}(\mathfrak{U})$. Finally, let $\mathcal{A}$ be the set of all primes $\mathfrak{r}$ of M such that either $\mathrm{ord}_{\mathfrak{r}}\mathfrak{A} \neq 0$ or $\mathrm{ord}_{\mathfrak{r}}\mathfrak{B} \neq 0$ and let $|\mathcal{A}| = m$. Set $\mathfrak{U}_{i+1} = \dfrac{\mathfrak{A}\mathfrak{r}_i}{\mathfrak{t}^{\deg \mathfrak{A}+2g+1}}$, where $\mathfrak{r}_i$ is the i-th element of $\mathcal{A}$ under some enumeration of $\mathcal{A}$. Observe that by Lemma 4.2(2) again $\ell(\mathfrak{U}_{i+1}) = g+1$ for $i = 1, \ldots, m$ while $\mathcal{L}(\mathfrak{U}_{i+1}) \subset \mathcal{L}(\mathfrak{U})$. (We remind the reader that since the constant field of M is algebraically closed all the primes are of degree 1.) Now consider

$$y \in L(\mathfrak{U}) \setminus \left(\bigcup_{j=1}^{m+1} L(\mathfrak{U}_j) \right).$$

Such a y exists by Lemma 4.3. By construction, we have that $\mathfrak{d}(y) = \mathfrak{t}^{2g+1+\deg \mathfrak{A}}$ and $\mathfrak{n}(y) = \mathfrak{A}\mathfrak{C}$, where $\mathfrak{C}$ is relatively prime to $\mathfrak{A}\mathfrak{B}\mathfrak{t}$. Finally,

$$\deg \mathfrak{C} = \deg \mathfrak{d}(y) - \deg(\mathfrak{A}) = 2g + 1 + \deg \mathfrak{A} - \deg \mathfrak{A} = 2g + 1.$$

□

We now specialize the lemma above to a particular divisor.

Corollary 4.5. *Suppose $w \in M$ is an element whose divisor is of the form $\dfrac{\mathfrak{X}\mathfrak{A}^{p^a}}{\mathfrak{Y}\mathfrak{B}^{p^a}}$, where $\mathfrak{X}, \mathfrak{Y}, \mathfrak{A}, \mathfrak{B}$ are pairwise relatively prime integral divisors, and $\deg \mathfrak{Y} \geq \deg \mathfrak{X}$. Assume further that the prime $\mathfrak{t}$ is a factor of $\mathfrak{Y}$, and that for some positive constant C we have $\deg(\mathfrak{Y}) < C$. Then $w = \xi \dfrac{z_1^{p^a}}{z_2^{p^a}}$, where $\mathfrak{t}$ is the only pole of z_1 and z_2, ξ does not have a zero or a pole at any prime which is a zero of z_1 or z_2, and $H(\xi) < (p^a+1)(C+g+1)$.*

Proof. First of all observe that $\deg \mathfrak{Y} - \deg \mathfrak{X} = p^a \deg \mathfrak{A} - p^a \deg \mathfrak{B} < C$. Further, by Lemma 4.4, there exist $z_1, z_2 \in M$ with divisors $\dfrac{\mathfrak{A}\mathfrak{C}}{\mathfrak{t}^{\deg \mathfrak{A}+2g+1}}$, $\dfrac{\mathfrak{B}\mathfrak{D}}{\mathfrak{t}^{\deg \mathfrak{B}+2g+1}}$, respectively, such that $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \mathfrak{X}, \mathfrak{Y}$ are all pairwise relatively prime and such that

$$\deg \mathfrak{C} = \deg \mathfrak{D} = 2g + 1.$$

Let $\xi = w \dfrac{z_2^{p^a}}{z_1^{p^a}}$. In this case

$$(\xi) = \frac{\mathfrak{X}\mathfrak{A}^{p^a}}{\mathfrak{Y}\mathfrak{B}^{p^a}} \frac{\mathfrak{B}^{p^a}\mathfrak{D}^{p^a}}{\mathfrak{t}^{p^a(\deg \mathfrak{B}+2g+1)}} \frac{\mathfrak{t}^{p^a(\deg \mathfrak{A}+2g+1)}}{\mathfrak{A}^{p^a}\mathfrak{C}^{p^a}} = \frac{\mathfrak{X}}{\mathfrak{Y}} \frac{\mathfrak{D}^{p^a}\mathfrak{t}^{p^a(\deg \mathfrak{A}-\deg \mathfrak{B})}}{\mathfrak{C}^{p^a}},$$

and therefore

$$H(\xi) \leq \deg \mathfrak{X} + p^a \deg \mathfrak{D} + p^a \deg \mathfrak{A} - p^a \deg \mathfrak{B} \leq C + p^a(g+1) + p^a C < (p^a+1)(C+g+1).$$

□

The next two lemmas deal with the relationship between the derivatives (global and local) and order at a prime.

Lemma 4.6. *Let $x \in M$ and $\mathfrak{t}$ be a prime of M. We have*

(1) *$ord_{\mathfrak{t}}(\frac{\partial x}{\partial \mathfrak{p}}) \geq ord_{\mathfrak{t}}(x) - 1$; and*
(2) *if $ord_{\mathfrak{t}}(x) \geq 0$, then $ord_{\mathfrak{t}}(\frac{\partial x}{\partial \mathfrak{t}}) \geq 0$.*

Proof. See [Mas96, p. 9]. □

Lemma 4.7. *Let $x \in M$ and let $\mathfrak{p}$ be a prime of M.*

(1) *If $ord_{\mathfrak{p}}(x) \geq 0$, then $ord_{\mathfrak{p}}(x') \geq \max(0, ord_{\mathfrak{p}}(x) - 1) - d_t(\mathfrak{p})$.*
(2) *If $ord_{\mathfrak{p}}(x) < 0$, then $ord_{\mathfrak{p}}(x') \geq ord_{\mathfrak{p}}(x) - 1 - d_t(\mathfrak{p})$.*

Proof. By [Mas96, p. 96] we have that for any prime $\mathfrak{p}$

$$\frac{\partial x}{\partial \mathfrak{p}} = \frac{dx}{dt}\frac{\partial t}{\partial \mathfrak{p}}. \tag{4.1}$$

Hence if $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$, then

$$\mathrm{ord}_{\mathfrak{p}}(x') = \mathrm{ord}_{\mathfrak{p}}\left(\frac{dx}{dt}\right) = \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial x}{\partial \mathfrak{p}}\right) - \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial t}{\partial \mathfrak{p}}\right) \geq \max(0, \mathrm{ord}_{\mathfrak{p}}(x) - 1) - d_t(\mathfrak{p}).$$

If $\mathrm{ord}_{\mathfrak{p}}(x) < 0$, then

$$\mathrm{ord}_{\mathfrak{p}}(x') = \mathrm{ord}_{\mathfrak{p}}\left(\frac{dx}{dt}\right) = \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial x}{\partial \mathfrak{p}}\right) - \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial t}{\partial \mathfrak{p}}\right) \geq \mathrm{ord}_{\mathfrak{p}}(x) - 1 - d_t(\mathfrak{p})$$

by Lemma 4.6. □

Lemma 4.8. *For any element $z \in M \setminus M^p$ there are at most $2g - 2 + 2H(z)$ primes $\mathfrak{t}$ of M such that $d_z(\mathfrak{t}) > 0$, and for all M-primes $\mathfrak{t}$ we have that $d_z(\mathfrak{t}) \leq 2g - 2 + 2H(z)$.*

Proof. By [Mas96, Equation (5) p. 10], we have

$$\sum_{\mathfrak{t}} d_z(\mathfrak{t}) = \sum_{\mathfrak{t}} \mathrm{ord}_{\mathfrak{t}}\left(\frac{\partial z}{\partial \mathfrak{t}}\right) = 2g - 2,$$

since z has non-zero global derivative. By Lemma 4.6, if $\mathrm{ord}_{\mathfrak{t}}\partial z/\partial \mathfrak{t} < 0$, then $\mathrm{ord}_{\mathfrak{t}} z < 0$. Thus,

$$\sum_{\mathrm{ord}_{\mathfrak{t}}\partial z/\partial \mathfrak{t} < 0} |\mathrm{ord}_{\mathfrak{t}}\partial z/\partial \mathfrak{t}| \leq \sum_{\mathrm{ord}_{\mathfrak{t}} z < 0} (|\mathrm{ord}_{\mathfrak{t}} z| + 1) \leq 2H(z).$$

Further,

$$\sum_{\mathrm{ord}_{\mathfrak{t}}\partial z/\partial \mathfrak{t} > 0} \mathrm{ord}_{\mathfrak{t}}\partial z/\partial \mathfrak{t} = 2g - 2 + \sum_{\mathrm{ord}_{\mathfrak{t}}\partial z/\partial \mathfrak{t} < 0} |\mathrm{ord}_{\mathfrak{t}}\partial z/\partial \mathfrak{t}| \leq 2g - 2 + 2H(z).$$

□

The last technical lemma of this section deals with the case of $d_t(\mathfrak{t}) = 0$.

Lemma 4.9. *If $\mathfrak{t}$ is a prime of M which is unramified over $F(t)$, and $\mathfrak{t}$ is not a pole of t, then $d_t(\mathfrak{t}) = 0$.*

Proof. If $\mathfrak{t}$ is unramified over $F(t)$ and it is not a pole of t, then for some $c \in F$ we have that $\mathrm{ord}_{\mathfrak{t}}(t - c) = 1$. Thus if we set $t - c = \pi$, a $\mathfrak{t}$-adic expansion of t is of the form $c + \pi$, and the derivative of that expression with respect to π is 1, implying $\mathrm{ord}_{\mathfrak{t}}\partial t/\partial \mathfrak{t} = 0$. □

From this lemma we derive a corollary which will help us construct p-th powers. The proof of the corollary follows directly from Lemma 4.7 and Lemma 4.9

Corollary 4.10. *If $\mathfrak{t}$ is a prime of M which is unramified over $F(t)$, and $\mathfrak{t}$ is not a pole of t, then for any x which is integral at $\mathfrak{t}$ we have $ord_{\mathfrak{t}}dx/dt \geq \max(0, ord_{\mathfrak{t}}x - 1)$.*

5. Defining p-th powers

In this section we construct an existential definition of the set $P(K)$ of p^s-th powers. We start under the assumption that the field of constants is algebraically closed and remove this assumption later in Subsection 5.5. As for any construction of a Diophantine definition, the construction of the set of p^s-th powers has two main parts: one part consists of showing that the given equations have at most p^s-th powers as their solutions. For the second part we have to show that elements of $P(K)$ are in fact solutions. As it turns out, the second part is trivial in our case and we will delay it until the very end in Lemma 5.23. The bulk of the section below will be devoted to showing that the only elements that can be solutions of our equations are the elements of $P(K)$. We do this in several steps. As in earlier papers, the first part will be devoted to dealing with the p^s-th powers of a particular element, the second part will deal with p^s-th powers of elements of the field with simple zeros and poles, and finally the third part will address the case of arbitrary elements.

5.1. **Defining p-th powers of a particular element.** The most difficult part of the argument is the first one: defining p^s-th powers of a particular element. We outline this construction before proceeding with the technical details. We first fix a non-constant element t of M satisfying certain conditions described below and let $a = 1$ or $a = 2$ depending on the characteristic of the field. Next we let $z \in M$ be such that the equations in Lemma 5.6 below are satisfied with $w = z + c$ for a sufficiently large number of c's. Here the requisite number ultimately depends on the genus g of M only. The equations lead us to conclude that either z has "bounded" height (with the bound ultimately depending on g only) or that the divisor of $z + c$ is a p^a-th power of another divisor for all c's. In the first case we use the equations from Proposition 5.8 and Corollary 5.9 to conclude that $z \in F(t)$, and Propositions 5.10 and 5.11 to conclude that either z is a p^a-th power of another field element or it is equal to t. In the second case we use Lemmas 5.12, 5.13 and 5.14 to conclude that z is a p^a-th power of another element.

Once we conclude that z is a p^a-th power of another element, we "take a p^a-th root" of all the equations (or perform a form of descent) and re-examine the resulting equations. Since this descent cannot continue forever, at some point we can conclude that z was a p^s-th power of t for some $s \in \mathbb{Z}_{>0}$.

Notation and Assumptions 5.1. Below we add to the notation and assumptions above.

- Let $a = 1$, if $p > 2$ and let $a = 2$, if $p = 2$.
- Let $t \in M$ be such that no zero or pole of t is ramified in the extension $M/F(t)$ or alternatively all zeros and poles of t are simple.
- Denote the zero divisor of t by $\mathfrak{P}$ and the pole divisor by $\mathfrak{Q}$. (We will also use the same notation for the primes which are the zero and the pole of t in $F(t)$.) Let $\mathfrak{P} = \prod_i \mathfrak{p}_i, \mathfrak{Q} = \prod_i \mathfrak{q}_i$ be the factorization of $\mathfrak{P}$ and $\mathfrak{Q}$ into distinct prime divisors of M.
- Let $\mathcal{E}$ be the set of all primes ramifying in the extension $M/F(t)$ and let e be the size of the set.
- Let M^G be the Galois closure of M over $F(t)$. Let $i_G = [M^G : M]$.
- For $j = 1, \dots, k$, let $\sigma_j : M \longrightarrow M^G$ be an embedding of M into M^G over $F(t)$.
- Let $\Omega = \{\omega_1 = 1, \dots, \omega_k\}$ be a basis of M over $F(t)$.
- Let $H_\Omega = \max\{H_{M^G}(\omega_i), i = 1, \dots, k\}$, where H_{M^G} is the height in M^G.
- Let $C = H(t)$. (In Lemma 5.4 we show that we can always assume that $C \leq \max(1, 2g - 1)$.)
- Let $C_1 = 2g - 2 + (p^a + 1)(C + g + 1)$.
- Let $C_2 = \dfrac{2g - 1 + (p^a + 1)(C + g + 1)}{p^a - 1}$.
- Let $C_3 = C + p^a C_1 C_2$.
- Let $C_4 = k! k^k H_\Omega C_3$
- Let $C_5 = C_4 + 2e + 2k + 4H(t) + 2$.
- Let $C(F) = \{c_0, \dots, c_{C_5}\} \subset F_0$ – the algebraic closure of $\mathbb{F}_p$ in F, let $d_{i,j} = c_i^{p^j}$, let

$$V_i = \{c_i^{p^k}, k \in \mathbb{Z}_{\geq 0}\},$$

and let $r_i := |V_i|$. Assume for $i \neq j$, for any $n_i, n_j \in \mathbb{Z}_{\neq 0}$ we have that $c_i^{n_i} \neq c_j^{n_j}$. (The existence of $C(F)$ in a finite extension of $\mathbb{F}_p$ can be seen from the following inductive argument: let $c_0 \in \mathbb{F}_p, c_i \in F_0 \setminus \mathbb{F}_p(c_0, \dots, c_{i-1})$.)

- If $z \in M \setminus F$, let $C_z \subset C(F)$ be the such that $c \in C_z$ if and only if $c \in C(F)$ and $z - c^{p^s}$ does not have a zero at any prime which is a zero or a pole of t or at any prime ramified in $M/F(t)$ for any positive integer s.
- For a $w \in M$, let $\mathcal{V}(w)$ be a set of primes of $F(t)$ satisfying the following requirements.
  (1) Each prime of $\mathcal{V}(w)$ is unramified in the extension $M/F(t)$.
  (2) w is integral at all primes of $\mathcal{V}(w)$.
  (3) $\{\omega_1, \dots, \omega_n\}$ is a local integral basis with respect to every prime of $\mathcal{V}(w)$ or in other words every $\mathfrak{A} \in \mathcal{V}(w)$ is relatively prime to the the discriminant of the basis.
  (4) The size of $\mathcal{V}(w)$ is greater than C_4.

We start with a sequence of preliminary lemmas, some of them coming from earlier papers and included here for the convenience of the reader.

Lemma 5.2 (Essentially [Shl06], Lemma 8.2.10)**.** *For any $u, w \in M \setminus F$, we have that $|C_w|$ and $|C_w \cap C_u|$ contain more than $C_4 + 2k + 2$ elements.*

Compared to the lemma in the citation we need more constants, so we start with more constants, and in our case $C_4 + 2k$ replaces n, but otherwise the argument is the same.

The next lemma is an elementary fact concerning valuations, and we state it without proof.

Lemma 5.3. *For any non-constant element $z \in M$ and any constants $c' \neq c$ we have that the zeros of $\dfrac{z-c'}{z-c}$ are exactly the zeros of $z - c'$ and all the poles of $\dfrac{z-c'}{z-c}$ are exactly the zeros of $z - c$.*

The next lemma provides a bound on the chosen element t in terms of the genus of the field.

Lemma 5.4. *There exists an element $t \in M$ satisfying conditions of Notation and Assumptions 5.1 such that*

$$H(t) \leq \max(1, 2g - 1).$$

Proof. If $g = 0$, i.e. M is a rational function field, the assertion of the lemma is clearly true. So suppose $g > 0$ and apply Lemma 4.2, Part (2d) with $d = 2g-1$ to conclude that there is $x \in M$ whose height is $2g-1$. By an argument similar to the one in Lemma 5.2, for any constant field large enough (and certainly for an infinite constant field) there exist constants $c, \tilde{c}$ such that $t = \dfrac{x-c}{x-\tilde{c}}$ does not have zeros or poles at primes ramifying in the extension $M/F(t)$. Further, by Lemma 5.3 we have that $H(t) = H(x-c) = H(x) \leq \max(1, 2g-1)$. □

Remark 5.5. While for the purposes of our arguments the bound on the height of t is not important, since in the proofs below we only care about the fact that the height is fixed, it is useful to know that all the bounds in the paper are ultimately determined by the genus, which can serve as a measure of the Diophantine complexity of the field. Finally note that $k = [M : F(t)] = H(t)$ by Lemma 1 and $i_G \leq k!$, so that all the constants occurring in the paper can be bound in terms of the genus of the field.

The lemma below is perhaps the most important new technical part which allowed for the extension of earlier results.

Lemma 5.6. *Suppose $w, u, v \in M$ satisfy the following equations:*

$$\begin{cases} w - t = v^{p^a} - v, \\ \frac{1}{w} - \frac{1}{t} = u^{p^a} - u. \end{cases} \tag{5.1}$$

If the divisor of w is not a p^a-th power of another divisor, then $H(w) < C_3$.

Proof. We assume that the divisor of w is not a p^a-th power of another divisor in M and obtain a bound on its height. First of all note that all pole orders of $v^{p^a} - v$ and $u^{p^a} - u$ are 0 modulo p^a. Therefore, if for some prime $\mathfrak{r}$ we have that $\mathrm{ord}_{\mathfrak{r}} w \neq 0$, then either $\mathrm{ord}_{\mathfrak{r}} w = \pm 1$ or $\mathrm{ord}_{\mathfrak{r}} w \equiv 0 \mod p^a$. Further, if $\mathrm{ord}_{\mathfrak{r}} w = -1$, then $\mathrm{ord}_{\mathfrak{r}} t = -1$ and $\mathrm{ord}_{\mathfrak{r}} v \geq 0$. Similarly, if $\mathrm{ord}_{\mathfrak{r}} w = 1$, then $\mathrm{ord}_{\mathfrak{r}} t = 1$ and $\mathrm{ord}_{\mathfrak{r}} u \geq 0$. Given our assumption on the divisor of w, for at least one prime $\mathfrak{r}$ we have that $\mathrm{ord}_{\mathfrak{r}} w = 1$ (implying that for at least one other prime the order is -1). Thus

$$(w) = \frac{\mathfrak{X}\mathfrak{A}^{p^a}}{\mathfrak{Y}\mathfrak{B}^{p^a}},$$

where $\mathfrak{X}, \mathfrak{Y}, \mathfrak{A}, \mathfrak{B}$ are pairwise relatively prime integral divisors, multiplicity of all prime factors of $\mathfrak{X}$ and $\mathfrak{Y}$ is one, $\deg(\mathfrak{X}) < H(t) = C$, and $\deg(\mathfrak{Y}) < H(t) = C$. Note that neither $\mathfrak{X}$ nor $\mathfrak{Y}$ is a trivial divisor. Further, without loss of generality we can assume that $\deg(\mathfrak{X}) \leq \deg(\mathfrak{Y})$, and also note that the pole divisor of v is $\mathfrak{B}$ and of u is $\mathfrak{A}$. Now as in Corollary 4.5, using the same notation, set

$$w = \xi \frac{z_1^{p^a}}{z_2^{p^a}},$$

where

$$H(\xi) \leq (p^a + 1)(C + g + 1),$$

rewrite rewrite the first equation of (5.1) as

$$\xi \frac{z_1^{p^a}}{z_2^{p^a}} - t = v^{p^a} - v,$$

$$\xi z_1^{p^a} - t z_2^{p^a} = (v z_2)^{p^a} - (v z_2) z_2^{p^a - 1}, \tag{5.2}$$

and set $s = v z_2$. Note that if for some prime $\mathfrak{r}$ of M we have that $\mathrm{ord}_{\mathfrak{r}} \mathfrak{B} = h > 0$, then

$$\mathrm{ord}_{\mathfrak{r}} s = 0,$$

$$\mathrm{ord}_{\mathfrak{r}} z_2 = h,$$

$$\mathrm{ord}_{\mathfrak{r}} t z_2^{p^a} \geq h p^a - 1 \geq h(p^a - 1),$$

$$\mathrm{ord}_{\mathfrak{r}} \xi = 0,$$

$$\mathrm{ord}_{\mathfrak{r}} z_1 = 0.$$

We now rewrite (5.2) to get

$$\xi z_1^{p^a} - s^{p^a} = t z_2^{p^a} - s z_2^{p^a - 1}.$$

Observe that $\mathrm{ord}_{\mathfrak{r}}(t z_2^{p^a} - s z_2^{p^a - 1}) \geq h(p^a - 1) \geq 2h$, and therefore

$$\mathrm{ord}_{\mathfrak{r}}(\xi z_1^{p^a} - s^{p^a}) \geq h(p^a - 1) \geq 2h.$$

We now note that ξ is not a p-th power in M since at least one zero or pole of ξ has an order not divisible by p. Thus the global derivation with respect to ξ is defined. (We are using our assumption that the divisor of w is not a p^a-th power in this step. Otherwise, $\mathfrak{X}$ and $\mathfrak{Y}$ are trivial and ξ is a constant, and the derivation with respect to ξ would not be defined.) Taking the derivative of $(\xi z_1^{p^a} - s^{p^a})$ with respect to ξ we see that it is equal to $z_1^{p^a}$ and thus $\mathrm{ord}_{\mathfrak{r}}(\xi z_1^{p^a} - s^{p^a})' = 0$. At the same time we also have by Lemma 4.8, that $\mathrm{ord}_{\mathfrak{r}}(\xi z_1^{p^a} - s^{p^a})' \geq h(p^a - 1) - 1 - d_\xi(\mathfrak{r})$, implying that

$$d_\xi(\mathfrak{r}) \geq h(p^a - 1) - 1 > 0. \tag{5.3}$$

Thus $\mathfrak{r}$ belongs to a finite set of primes of size

$$2g - 2 + H(\xi) < 2g - 2 + (p^a + 1)(C + g + 1) = C_1.$$

Using Lemma 4.8 again and (5.3), we can also obtain a bound on h:

$$2g - 1 + (p^a + 1)(C + g + 1) \geq d_\xi(\mathfrak{r}) + 1 \geq h(p^a - 1).$$

Hence

$$h < \frac{2g - 1 + (p^a + 1)(C + g + 1)}{p^a - 1} = C_2.$$

Returning now to the structure of the divisor of w, we see that

$$H(w) \leq \deg \mathfrak{X} + p^a \deg \mathfrak{B} \leq C + p^a C_1 C_2.$$

□

The next lemma is a standard estimate of the height of the coefficients in a linear combination of basis elements in terms of the height of the linear combination itself.

Lemma 5.7. *If $w \in M$ and $w = \sum_{i=1}^{k} A_i \omega_i$, where $A_i \in F(t)$, then $H(A_i) < k! k^k H_\Omega H(w)$.*

Proof. Consider a non-singular linear system $\sum_{i=1}^{k} A_i\sigma_j(\omega_i) = \sigma_j(w), j = 1,\dots,k$, where we consider $A_1,\dots,A_k$ as the unknowns. Solving this system by Cramer's Rule, and using the fact that the height of a sum/product is less or equal to the sum of heights, we can get an estimate on $H_{M^G}(A_i)$– the height of A_i in M^G. More specifically, we get

$$H_{M^G}(A_i) \leq 2k!k^k \max(H_{M^G}(\sigma_j(h), H_\Omega) \leq k!k^k H_\Omega H_{M^G}(w).$$

Since for an element z of M we have that $H_{M^G}(z) = i_G H(z)$, we cancel i_G from both sides of the inequality and get the desired result. □

The proposition below allows us to exploit fixed bounds on height. Elsewhere, this proposition has been referred to as the Weak Vertical Method.

Proposition 5.8 (Slightly modified Theorem 10.1.1 of [Shl06])**.** *Suppose for some $w \in M$ with $H(w) < C_3$, for all primes $\mathfrak{A}$ of $\mathcal{V}(w)$ we have*

$$w \equiv b(\mathfrak{A}) \mod \mathfrak{A}, \tag{5.4}$$

where $b(\mathfrak{A}) \in F$, and we interpret the equivalence as saying that for any factor $\mathfrak{c}$ of $\mathfrak{A}$ in M we have that

$$ord_{\mathfrak{c}}(w - b(\mathfrak{A})) \geq e(\mathfrak{c}/\mathfrak{A}),$$

the ramification degree of $\mathfrak{c}$ over $\mathfrak{A}$. Then $w \in F(t)$.

Proof. First of all we note that by Part (3) of the description of $\mathcal{V}(w)$ in Notation and Assumption 5.1, any element $z \in M$ integral with respect to $\mathfrak{A} \in \mathcal{V}(w)$, i.e. integral with respect to every factor of $\mathfrak{A}$ in M, can be written as

$$z = \sum_{i=1}^{k} f_i\omega_i,$$

where for all $i = 1,\dots,n$, we have that $f_i \in F(t)$ and f_i is integral at $\mathfrak{A}$. Thus, we now write $w = \sum_{i=1}^{k} A_i\omega_i$, where $A_i \in F(t)$. Observe that for all $\mathfrak{A} \in \mathcal{V}(w)$, we have that $w - b(\mathfrak{A})$ is equivalent to zero modulo every prime $\mathfrak{A}$ of $\mathcal{V}(w)$. At the same time

$$w - b(\mathfrak{A}) = A_1 - b(\mathfrak{A}) + A_2\omega_2 + \cdots + A_k\omega_k.$$

For each prime $\mathfrak{A}$ of $\mathcal{V}(w)$, let $B(\mathfrak{A}) \in F(t)$ be such that $\mathrm{ord}_{\mathfrak{A}} B(\mathfrak{A}) = 1$. (Such a $B(\mathfrak{A})$) exists by the Weak Approximation Theorem.) Note that $z = \dfrac{w - b(\mathfrak{A})}{B(\mathfrak{A})}$ is integral at $\mathfrak{A}$ and thus $z = \sum_{i=1}^{k} f_i(\mathfrak{A})\omega_i$, where $f_i(\mathfrak{A})$ are elements of $F(t)$ integral at $\mathfrak{A}$. Furthermore,

$$A_1 - b(\mathfrak{A}) + A_2\omega_2 + \cdots + A_k\omega_k = w - b(\mathfrak{A}) = B(\mathfrak{A})z = \sum_{i=1}^{k} B(\mathfrak{A})f_i(\mathfrak{A})\omega_i.$$

Thus, for $i = 2,\dots,k$ for all $\mathfrak{A}$ in $\mathcal{V}(w)$ we have that $A_i = B(\mathfrak{A})f_i(\mathfrak{A})$, implying that for $i = 2,\dots,k$, for all $\mathfrak{A}$ in $\mathcal{V}(w)$ we have that $\mathrm{ord}_{\mathfrak{A}} A_i > 0$, implying that $H(A_i) > C_4$ or $A_i = 0$. The last inequality contradicts our assumption on $H(w)$ and Lemma 5.7. Therefore for $i = 2,\dots,k$ we have that $A_i = 0$ and thus $w \in F(t)$. □

We now apply the Weak Vertical Method to our situation.

Corollary 5.9. *Suppose that for some $w \in M$ with $H(w) < C_3$, and $C_4 + e$ quadruples $(b, c, b', c') \in F^4$ with $b \neq b'$, we have a solution u_b in M to*

$$\frac{w - c'}{w - c} - \frac{t - b'}{t - b} = u_b^{p^a} - u_b. \tag{5.5}$$

In this case, $w \in F(t)$.

Proof. Let $b \in F$ be such that it occurred as the first element in one of the quadruples above, so that the $F(t)$-prime $\mathfrak{P}_b$ corresponding $t - b$ is unramified in the extension $M/F(t)$, and let $\mathfrak{p}_b$ be any factor of $\mathfrak{P}_b$ in M. (We have at least C_4 such elements b.) Since $\mathfrak{p}_b$ is unramified, Lemma 5.3 implies that $\mathrm{ord}_{\mathfrak{p}_b}(t-b) = -\mathrm{ord}_{\mathfrak{p}_b} \dfrac{t - b'}{t - b} = 1$. At the same time, for any pole $\mathfrak{q}_b$ of u_b in M we have that $\mathrm{ord}_{\mathfrak{q}_b}(u_b^p - u_b) \equiv 0$

mod p^a as above. Thus, $c \neq c'$ and, by Lemma 5.3 again, we have that $-\mathrm{ord}_{\mathfrak{p}_b}\dfrac{w-c'}{w-c} = \mathrm{ord}_{\mathfrak{p}_b}(w-c) > 0$. In other words, for C_4 pairs $(b,c) \in F^2$ we have that $w \equiv c \mod \mathfrak{P}_b$, where $\mathfrak{P}_b$ is, as above, the zero divisor in M and $F(t)$ of $t-b$. Now the assertion of the corollary follows from Proposition 5.8. □

The next proposition gives equations that let us conclude that an element w is a p^s-th power of t provided that we know that w is in the rational function field $F(t)$.

Proposition 5.10 ([Shl06], Lemma 8.3.3, Corollary 8.3.4 and [Eis03], Lemma 3.4)**.** *Suppose for some element $w \in F(t)$, having no poles or zeros at the primes ramifying in the extension $M/F(t)$, there exist $u, v \in M$ such that the following system is satisfied:*

$$\begin{cases} \dfrac{1}{w} - \dfrac{1}{t} = u^{p^a} - u \\ w - t = v^{p^a} - v. \end{cases} \tag{5.6}$$

Then for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^{as}}$.

In general we do not know if w has all of its poles and zeros at primes not ramifying in the extension $M/F(t)$. Therefore we might have to replace w by $\dfrac{w-b}{w-b'}$, where $b, b' \in F_0$. (Recall that F_0 is the algebraic closure of $\mathbb{F}_p$ in F.) The proposition below carries out this construction.

Proposition 5.11. *Let $w \in F(t)$, assume the system (5.6) holds, and for all $i \neq j \in \{1, \ldots, C_5\}$, for some $b \in V_i, b' \in V_j$ there exist $u_{i,j,b,b'}, v_{i,j,b,b'} \in M$ such that*

$$\begin{cases} \dfrac{w-b}{w-b'} - \dfrac{t-c_i}{t-c_j} = u_{i,j,b,b'}^{p^a} - u_{i,j,b,b'} \\ \dfrac{w-b'}{w-b} - \dfrac{t-c_j}{t-c_i} = v_{i,j,b,b'}^{p^a} - v_{i,j,b,b'} \end{cases} \tag{5.7}$$

In this case for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^{as}}$.

Proof. First of all, by Lemma 5.2 we conclude that for some c_i, c_j and $b \in V_i, c \in V_j$, we have that $t-c_i, t-c_j, w-b, w-c$ do not have zeros at any prime ramifying in the $M/F(t)$ and therefore $\dfrac{t-c_i}{t-c_j}, \dfrac{w-b}{w-b'} \in F(t)$ do not have zeros or poles at any primes ramifying in the extension $M/F(t)$. It follows that all the zeros and poles of $\dfrac{t-c_i}{t-c_j}$ are simple, since they are simple in $F(t)$. Now applying Proposition 5.10 we conclude that

$$\frac{w-b}{w-b'} = \left(\frac{t-c_i}{t-c_j}\right)^{p^{as}} \tag{5.8}$$

for some $s \geq 0$. From (5.8) we deduce

$$1 + \frac{b'-b}{w-b'} = 1 + \frac{c_j^{p^{as}} - c_i^{p^{as}}}{t^{p^{as}} - c_j^{p^{as}}}. \tag{5.9}$$

Since we know from the second equation of (5.6) that t and w have a common zero, considering the equation above modulo this prime gives us

$$\frac{b'-b}{b'} = \frac{c_j^{p^{as}} - c_i^{p^{as}}}{c_j^{p^{as}}},$$

or

$$\frac{b}{b'} = \frac{c_i^{p^{as}}}{c_j^{p^{as}}}.$$

Thus, from (5.9), for some $r \in \mathbb{Z}_{\geq 0}$ we have that

$$w = b' + \frac{b'-b}{c_j^{p^{as}} - c_i^{p^{as}}}(t^{p^{as}} - c_j^{p^{as}}) = b' + \frac{b'}{c_j^{p^{as}}}(t^{p^{as}} - c_j^{p^{as}}) = \frac{b'}{c_j^{p^{as}}} t^{p^{as}} = \frac{c_j^{p^r}}{c_j^{p^{as}}} t^{p^{as}} = c_j^{p^r - p^{as}} t^{p^{as}}.$$

In a similar fashion we conclude that for some $m \in \mathbb{Z}_{\geq 0}$ we have that $w = c_i^{p^m - p^{as}} t^{p^{as}}$ and hence $c_j^{p^r - p^{as}} = c_i^{p^m - p^{as}}$. By assumption on elements of $C(F)$ we must have $p^r - p^{as} = p^m - p^{as} = 0$ and $w = t^{p^{as}}$. $\square$

We will now prepare for the case when we cannot conclude right away that w is of bounded height and use the Weak Vertical Method to see that it is in the fixed rational subfield. In this case by Lemma 5.6, the divisor of w is a p^{as}-th power of another divisor. The three lemmas below take advantage of this fact to conclude that under certain conditions w is a p^a-th power of another field element. The proofs for all three lemmas can be found in [Shl06].

Lemma 5.12 ([Shl06], Lemma 8.2.4)**.** *Let M/G be a finite separable extension of fields of positive characteristic p. Let $\alpha \in M$ be such that for some positive integer a, all the coefficients of its monic irreducible polynomial over G are p^a-th powers in G. Then α is a p^a-th power in M.*

Lemma 5.13 ([Shl06], Lemma 8.2.5)**.** *Let M/G be a finite separable extension of fields of positive characteristic p. Let $[M : G] = n$. Let r be a positive integer. Let $x \in M$ be such that $M = G(x)$ and for distinct $b_0, \ldots, b_n \in G$ we have that $\mathbf{N}_{M/G}(b_i^{p^r} - x) = y_i^{p^r}$. Then x is a p^r-th power in M.*

Lemma 5.14 ([Shl06], Lemma 8.4.1)**.** *Let M be a function field over a perfect field of constants L and let $t \in M$ be such that $M/L(t)$ is a finite and separable extension of degree n. Let m be a positive integer. Let $v \in M$ and assume that for some distinct $b_0 = 0, b_1, \ldots, b_n \in L$, the divisor of $v + b_0, \ldots, v + b_n$ is a p^m-th power of some other divisor of M. Then, assuming for all i we have that $v + b_i$ does not have any zeros or poles at any prime ramifying in the extension $M/L(t)$, it is the case that v is a p^m-th power in M.*

We are now ready to put all the parts together.

Proposition 5.15. *Suppose for some $w \in M$ we have that* (5.6) *and* (5.7) *hold with all the variables taking values in M. In this case $w = t^{p^{as}}$ for some positive integer s.*

Proof. Suppose (5.6) and (5.7) hold. We need to consider two cases:

Case 1: For one pair c_i, c_j with $t - c_i$ and $t - c_j$ corresponding to primes that are not ramified (over $F(t)$), we have that the divisor of $\dfrac{w-b}{w-b'}$ is not a p^a-th power of another divisor in M. In this case applying Lemma 5.6 we conclude that $H\left(\dfrac{w-b}{w-b'}\right) = H(w) < C_3$. (The equality of heights follows from Lemma 5.3.) Now by Corollary 5.9 we conclude that $w \in F(t)$. Applying Proposition 5.11, we finally conclude that $w = t^{p^{as}}$ for some $s \in \mathbb{Z}_{\geq 0}$.

Case 2: For all values of $c_i \neq c_j$ such that the $F(t)$-primes corresponding to $t - c_i$ and to $t - c_j$ are not ramified, we have that that the divisors of $\dfrac{w-b'}{w-b}$ are p^a-th powers of other divisors. (We remind the reader that $b \in V_i, b' \in V_j$.) In this case, the divisor of $1 + \dfrac{b-b'}{w-b}$ is a p^a-th power of another divisor and therefore the divisor of

$$\frac{1}{b-b'} + \frac{1}{w-b'} := d_{i,j} + \frac{1}{w_j}$$

is a p^a-th power of another divisor for all such $i \neq j$. This follows since $\dfrac{w-b'}{w-b}$ and $d_{i,j} + \frac{1}{w_j}$ differ by a constant factor only, and therefore have the same divisor in M. By Lemma 5.2 we have that $|C_t \cap C_w| > 2k$. Thus, to summarize the discussion above, for a fixed value of j with $c_j \in C_t \cap C_w$ and at least $k+1$ values of $i \neq j$ with $c_i \in C_t \cap C_w$, we have that $d_{i,j} + \dfrac{1}{w_j}$ does not have a pole or a zero at a prime ramified over $F(t)$. Also, for any pair $i_1 \neq i_2$ we have $d_{i_1,j} \neq d_{i_2,j}$, and the divisor of each $d_{i,j} + \dfrac{1}{w_j}$ is a p^a-th power of another divisor. Hence by Lemma 5.14 we conclude that w_j for this j is a p^a-th power in M, and thus w is a p^a-th power in M.

At this point we can take the "p^a-th root'' of our equations as was done in Proposition 5.11 and again ask, this time for the "new" w, whether the divisor of $\dfrac{w-b'}{w-b}$ is not a p^a-th power of another divisor for some i, j with $c_i, c_j \in C_t \cap C_w$.

Since our "p^a-th root descent'' cannot go on indefinitely, at some step we will conclude that the divisor of $\dfrac{w-b'}{w-b}$ is not a p^a-th power of another divisor for some i, j with $c_i, c_j \in C_t$. When this happens, we will follow the *Case 1* argument to reach the desired conclusion.

□

The results in Sections 5.2, 5.3 and 5.4 are only slight modifications of known results going back in some form to [Phe87]. We include these results and some of the proofs for the convenience of the reader.

5.2. **Defining p-th powers of elements with simple zeros and poles.** In this section we need additional notation listed below.

Notation and Assumptions 5.16.

- For $s \in \mathbb{Z}_{\geq 0}, i, l \in \{1, \ldots, C_5\}, j_i \in \{1, \ldots, r_i\}, j_l \in \{1, \ldots, r_l\}$, $z = -1, 1$, $m = 0, 1$, $u, v, \mu_{i,j_i,l,j_l,z,m}$, $\lambda_1, \lambda_{-1}, \sigma_{i,j_i,l,j_l} \in M$, let
$$D(s, i, j_i, l, z, m, j_l, u, v, \mu_{i,j_i,l,j_l,z,m}, \sigma_{i,j_i,l,j_l}, \lambda_1, \lambda_{-1})$$
be the following system of equations:

$$u_{i,k} = \frac{u + c_i}{u + c_l}, \tag{5.10}$$

$$v_{i,j_i,l,j_l} = \frac{v + d_{i,j_i}}{v + d_{l,j_l}}, \tag{5.11}$$

$$v_{i,j_i,l,j_l}^{2z} t^{mp^{as}} - u_{i,l}^{2z} t^m = \mu_{i,j_i,l,j_l,z,m}^{p^{as}} - \mu_{i,j_i,l,j_l,z,m}, \tag{5.12}$$

$$v_{i,j_i,l,j_l} - u_{i,k} = \sigma_{i,j_i,l,j_l}^{p^a} - \sigma_{i,j_i,l,j_l}, \tag{5.13}$$

$$v - u = \lambda_1^{p^a} - \lambda_1 \tag{5.14}$$

$$v^{-1} - u^{-1} = \lambda_{-1}^{p^a} - \lambda_{-1} \tag{5.15}$$

- Let $j, r, s \in \mathbb{Z}_{\geq 0}$, $u, \tilde{u}, v, \tilde{v}, x, y \in M$. Let $E(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s)$ denote the following system of equations

$$v = u^{p^r} \tag{5.16}$$

$$\tilde{v} = \tilde{u}^{p^j} \tag{5.17}$$

$$u = \frac{x^p + t}{x^p - t} \tag{5.18}$$

$$\tilde{u} = \frac{x^p + t^{-1}}{x^p - t^{-1}} \tag{5.19}$$

$$v = \frac{y^p + t^{p^s}}{y^p - t^{p^s}} \tag{5.20}$$

$$\tilde{v} = \frac{y^p + t^{-p^s}}{y^p - t^{-p^s}} \tag{5.21}$$

- Let $j, r, s \in \mathbb{Z}_{\geq 0}$, $u, \tilde{u}, v, \tilde{v}, x, y \in M$, and let $E2(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s)$ denote the following system of equations

$$v = u^{2^r} \tag{5.22}$$

$$\tilde{v} = \tilde{u}^{2^j} \tag{5.23}$$

$$u = \frac{x^2 + t^2 + t}{x^2 + t} \tag{5.24}$$

$$\tilde{u} = \frac{x^2 + t^{-2} + t^{-1}}{x^2 + t^{-1}} \tag{5.25}$$

$$v = \frac{y^2 + t^{2^{s+1}} + t^{2^s}}{y^2 + t^{2^s}} \tag{5.26}$$

$$\tilde{v} = \frac{y^2 + t^{-2^{s+1}} + t^{-2^s}}{y^2 + t^{-2^s}} \tag{5.27}$$

We start with a way to produce elements with simple zeros and poles.

Lemma 5.17 ([Shl96], Lemma 4.5 or [Shl06], Lemma 8.4.2)**.** *Let $p > 2$. Let $x \in M$. Let $u = \frac{x^p + t}{x^p - t}$. Let $b \in F, b \neq \pm 1$. Then all zeros and poles of $u^{\pm 1} + b$ are simple except possibly for zeros or poles of t or at primes ramifying in the extension $M/F(t)$.*

Proof. It is enough to show that the proposition holds for u. The argument for u^{-1} follows by symmetry. First of all we remind the reader that the global derivation with respect to t is defined over M, and the derivative follows the usual rules. So consider

$$\frac{d(u+b)}{dt} = \frac{2x^p}{(x^p - t)^2}.$$

If $\mathfrak{t}$ is a prime of M such that $\mathfrak{t}$ does not ramify in the extension $M/F(t)$ and is not a pole or zero of t, then Corollary 4.10 implies that

$$\mathrm{ord}_{\mathfrak{t}}(u+b) = \mathrm{ord}_{\mathfrak{t}} \frac{(1+b)x^p + (1-b)t}{x^p - t} > 1$$

if and only if $\mathfrak{t}$ is a common zero of $u + b$ and $\frac{d(u+b)}{dt}$. If $\mathrm{ord}_{\mathfrak{t}} \frac{2x^p}{(x^p - t)^2} > 0$, then $\mathfrak{t}$ is either a zero of x or a pole of $x^p - t$. Any zero of x, which is not a zero of t, is not a zero of $u + b$ for $b \neq 1$. Furthermore, any pole of x is also not a zero of $u + b$. Thus all zeros of $u + b$ at primes not ramifying in the extension $M/F(t)$ and different from poles and zeros of t are simple. Next we note that poles of $u + b$ are zeros of u^{-1}. Further

$$\frac{du^{-1}}{dt} = \frac{-2x^p}{(x^p + t)^2},$$

and by a similar argument, u^{-1} and $\frac{du^{-1}}{dt}$ do not have any common zeros at any primes not ramifying in the extension $M/F(t)$ and not being poles or zeros of t. □

The following lemma (which we state without a proof) deals with the case of $p = 2$.

Lemma 5.18 ([Eis03], Lemma 3.8)**.** *Let $p = 2$ and $x \in M$. Let $u = \frac{x^2 + t^2 + t}{x^2 + t}$. Let $b \in F, b \neq 1$. In this case all zeros and poles of $u + b$ are simple except possibly for zeros or poles of t or at primes ramifying in the extension $M/F(t)$.*

The lemma below is a technical result we need to define the p^a-th powers of elements with simple zeros and poles.

Lemma 5.19 (This lemma is slightly modified from [Shl06], Lemma 8.2.11)**.** *Let $\sigma, \mu \in M$. Assume that all the primes that are poles of σ or μ do not ramify in the extension $M/F(t)$. Further, assume the following equality holds.*

$$t(\sigma^{p^a} - \sigma) = \mu^{p^a} - \mu. \tag{5.28}$$

In this case $\sigma^{p^a} - \sigma = \mu^{p^a} - \mu = 0$. (Here we remind the reader that by assumption, the primes occurring in the divisor of t do not ramify in $M/F(t)$.)

Proof. Let $\mathfrak{A}, \mathfrak{B}$ be integral divisors of M, relatively prime to each other and to $\mathfrak{P} = \prod_i \mathfrak{p}_i$ and $\mathfrak{Q} = \prod_i \mathfrak{q}_i$ (in other words, no prime occurring in $\mathfrak{A}$ or $\mathfrak{B}$ occurs in the divisor of t), and such that the divisor of σ is of the form $\frac{\mathfrak{A}}{\mathfrak{B}} \prod_i \mathfrak{p}_i^{n_i} \prod_i \mathfrak{q}_i^{k_i}$, where n_i, k_i are integers for all i. It is not hard to see that for some integral divisor $\mathfrak{C}$, relatively prime to $\mathfrak{B}, \mathfrak{P}$, and $\mathfrak{Q}$, some integers a_i, b_i, the divisor of μ is of the form $\frac{\mathfrak{C}}{\mathfrak{B}} \prod_i \mathfrak{p}_i^{a_i} \prod_i \mathfrak{q}_i^{b_i}$. Indeed, if $\mathfrak{t}$ is a pole of μ such that $\mathfrak{t}$ does not divide $\mathfrak{P}$ or $\mathfrak{Q}$, then

$$0 > p^a \mathrm{ord}_{\mathfrak{t}} \mu = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a} - \mu) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^{p^a} - \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\sigma^{p^a} - \sigma) = p^a \mathrm{ord}_{\mathfrak{t}} \sigma.$$

Conversely, if $\mathfrak{t}$ is a pole of σ such that $\mathfrak{t}$ does not divide $\mathfrak{P}$ or $\mathfrak{Q}$, then

$$0 > p^a \mathrm{ord}_{\mathfrak{t}} \sigma = \mathrm{ord}_{\mathfrak{t}}(\sigma^{p^a} - \sigma) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^{p^a} - \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a} - \mu) = p^a \mathrm{ord}_{\mathfrak{t}} \mu.$$

Further we can also deduce that for each $\mathfrak{p}_i$ we have that $\mathrm{ord}_{\mathfrak{p}_i} \sigma \geq 0$ and $\mathrm{ord}_{\mathfrak{p}_i} \mu \geq 0$. To see that this is the case suppose $\mathrm{ord}_{\mathfrak{p}_i} \sigma < 0$ and conclude that

$$\mathrm{ord}_{\mathfrak{p}_i} t(\sigma^{p^a} - \sigma) < 0, \text{ and} \tag{5.29}$$

$$\mathrm{ord}_{\mathfrak{p}_i} t(\sigma^{p^a} - \sigma) \not\equiv 0 \mod p. \tag{5.30}$$

At the same time (5.29) implies that

$$\mathrm{ord}_{\mathfrak{p}_i} (\mu^{p^a} - \mu) < 0, \text{ and} \tag{5.31}$$

$$\mathrm{ord}_{\mathfrak{p}_i} (\mu^{p^a} - \mu) \equiv 0 \mod p. \tag{5.32}$$

Therefore assuming $\mathrm{ord}_{\mathfrak{p}_i} \sigma < 0$ leads to a contradiction. Similarly, if $\mathrm{ord}_{\mathfrak{p}_i} \mu < 0$ then (5.31) and (5.29) hold and we again obtain a contradiction. Assuming that $\mathrm{ord}_{\mathfrak{q}_i} \sigma < 0$, $\mathrm{ord}_{\mathfrak{q}_i} \mu < 0$ results in a contradiction of a similar type. Thus, we can assume that $a_i, b_i, n_i, k_i \geq 0$ for all i.

By the Strong Approximation Theorem there exists $b \in M^\times$ such that the divisor of b is of the form $\mathfrak{B}\mathfrak{D}/\mathfrak{q}_1^c$, where $\mathfrak{D}$ is an integral divisor relatively prime to $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{P}, \mathfrak{Q}$, and c is a positive integer. Then $b\sigma = s_1, b\mu = s_2$, where s_1, s_2 are integral over $F[t]$ and have zero divisors relatively prime to $\mathfrak{B}$. Indeed, consider the divisors of $s_1 = b\sigma$:

$$\frac{\mathfrak{B}\mathfrak{D}}{\mathfrak{q}_1^c} \frac{\mathfrak{A}}{\mathfrak{B}} \prod_i \mathfrak{p}_i^{n_i} \prod_j \mathfrak{q}_j^{k_j} = \mathfrak{D}\mathfrak{A} \prod_i \mathfrak{p}_i^{n_i} \mathfrak{q}_1^{k_1 - c} \prod_{j>1} \mathfrak{q}_j^{k_j}$$

The pole of s_1 is a factor of $\mathfrak{Q}$ and therefore s_1 is integral over $F[t]$. Further, by construction $\mathfrak{A}$ and $\mathfrak{D}$ are integral divisors relatively prime to $\mathfrak{P}$ and $\mathfrak{B}$. A similar argument applies to s_2.

Multiplying (5.28) through by b^{p^a} we will obtain the following equation.

$$t(s_1^{p^a} - b^{p^a - 1} s_1) = s_2^{p^a} - b^{p^a - 1} s_2. \tag{5.33}$$

We can now rewrite (5.33) in the form

$$(s_1^{p^a} t - s_2^{p^a}) = b^{p^a - 1}(s_1 t - s_2). \tag{5.34}$$

If $\mathfrak{t}$ is any prime factor of $\mathfrak{B}$ in M, then $\mathfrak{t}$ does not ramify in the extension $M/F(t)$, and since $p^a > 2$, we know that $\mathrm{ord}_{\mathfrak{t}}(s_1^{p^a} t - s_2^{p^a}) \geq 2$. Further, we also have by Corollary 4.10

$$\mathrm{ord}_{\mathfrak{t}} \frac{d(s_1^{p^a} t - s_2^{p^a})}{dt} > 0.$$

Finally,

$$\mathrm{ord}_{\mathfrak{t}}\frac{d(s_1^{p^a}t - s_2^{p^a})}{dt} = \mathrm{ord}_{\mathfrak{t}}(s_1^{p^a}).$$

Therefore, s_1 has a zero at $\mathfrak{t}$. This, however, is impossible by construction of s_1 as described above. Consequently, $\mathfrak{B}$ is a trivial divisor and μ and σ are constants since their pole divisor is trivial. Now (5.28) is implying that t times a constant is equal to a constant. This can happen only if both constants are zero. □

Lemma 5.20 ([Shl06], Lemma 8.4.4)**.** *Let $s \in \mathbb{Z}_{>0}$. Let $x, v \in M \setminus \{0\}$ and assume that for some $\tilde{v} \in M$ we have that $\tilde{v}^{p^a} = v$. Let $u = \dfrac{x^p + t}{x^p - t}$ if $p > 2$ and let $u = \dfrac{x^2 + t^2 + t}{x^2 + t}$, if $p = 2$. Further, assume that*

$$\begin{gathered}\exists \mu_{i,j_i,l,j_l,z,m}, \sigma_{i,j_i,l,j_l}, \lambda_1, \lambda_{-1} \in M \\ \forall i \exists j_i \forall (l \neq i) \exists j_l \forall m \forall z : \\ D(s, i, j_i, l, j_l, m, z, u, v, \mu_{i,j_i,l,j_l,z,m}, \sigma_{i,j_i,l,j_l}, \lambda_1, \lambda_{-1})\end{gathered} \tag{5.35}$$

holds. Then

$$\begin{gathered}\exists \tilde{\mu}_{i,j_i,l,j_l,z,m}, \tilde{\sigma}_{i,j_i,l,j_l}, \tilde{\lambda}_1, \tilde{\lambda}_{-1} \in M \\ \forall i \exists j_i \forall (l \neq i) \exists j_l \forall m \forall z : \\ D(s-1, i, j_i, l, j_l, m, z, u, \tilde{v}, \tilde{\mu}_{i,j_i,l,j_l,z,m}, \tilde{\sigma}_{i,j_i,l,j_l}, \tilde{\nu}_{i,j_i,z}, \tilde{\lambda}_1, \tilde{\lambda}_{-1})\end{gathered} \tag{5.36}$$

holds.

Lemma 5.21 ([Shl06], Lemma 8.4.5, Corollary 8.4.6 and [Eis03], Lemma 3.9)**.** *Let $s \in \mathbb{Z}_{\geq 0}, x, v \in M \setminus \{0\}$. Let $u = \dfrac{x^p + t}{x^p - t}$, if $p > 2$, and let $u = \dfrac{x^2 + t^2 + t}{x^2 + t}$, if $p = 2$. Further, assume that (5.35) holds. Then $v = u^{p^{as}}$.*

Proof. First of all, we claim that for all i, l, it is the case that $u_{i,l}$ has no multiple zeros or poles except possibly at the primes with factors ramifying in $M/F(t)$, or poles or zeros of t. Indeed, all the poles of $u_{i,l}$ are zeros of $u + c_l$ and all the zeros of $u_{i,l}$ are zeros $u + c_i$. However, by Lemma 5.17 and by assumption on c_i and c_l, all the zeros of $u + c_l$ and $u + c_i$ are simple, except possibly for zeros at the primes which are zeros or poles of t or have factors ramifying in the extension $M/F(t)$.

We will show that if $s > 0$ then v is a p^a-th power in M, and if $s = 0$ then $u = v$. This assertion together with Lemma 5.20 will produce the desired conclusion.

Note that by Corollary 5.2, we can choose distinct natural numbers

$$i, l_1, \ldots, l_{k+1} \in \{0, \ldots, C_5\}$$

such that

$$\{c_i, c_{l_1}, \ldots, c_{l_{k+1}}\} \subset C_v \cap C_u$$

and for all $1 \leq j_i \leq r_i, 1 \leq j_{l_f} \leq r_{l_f}$, with $f = 1, \ldots, k+1$, we have that u_{i,l_f} and $v_{i,j_i,l_f,j_{l_f}}$ have no zeros or poles at the primes of M with factors ramifying in the extension $M/F(t)$, or primes occurring in the M-divisor of t. Note also that for thus selected indices, all the poles and zeros of u_{i,l_f} are simple. We now proceed to pick natural numbers $i, l_1, \ldots, l_{k+1}, j_i, j_{l_1}, \ldots, j_{l_{k+1}}$ such that the equations in (5.10) - (5.13) are satisfied for these values of indices, and u_{i,l_1}, $v_{i,j_i,l_1,j_{l_1}}, \ldots$, $u_{i,l_{k+1}}$, $v_{i,j_i,l_{k+1},j_{l_{k+1}}}$ have no poles or zeros at primes with factors ramifying in the extension $M/F(t)$, or at primes occurring in the M-divisor of t.

Now assume $s > 0$, and let f range over the set $\{1, \ldots, k+1\}$. First let $z = \pm 1$, while $m = 0$, and consider the two versions of the equation in (5.12) with these values of z and m.

$$v^2_{i,j_i,l_f,j_{l_f}} - u^2_{i,l_f} = \mu^{p^a}_{i,j_i,l_f,j_{l_f},1,0} - \mu_{i,j_i,l_f,j_{l_f},1,0}, \tag{5.37}$$

$$v^{-2}_{i,j_i,l_f,j_{l_f}} - u^{-2}_{i,l_f} = \mu^{p^a}_{i,j_i,l_f,j_{l_f},-1,0} - \mu_{i,j_i,l_f,j_{l_f},-1,0}, \tag{5.38}$$

Here either for all $f = 1, \ldots, k+1$, the divisor of $v_{i,j_i,l_f,j_{l_f}}$ in M is a p^a-th power of another divisor, or for some f and some prime $\mathfrak{t}$ without factors ramifying in the extension $M/F(t)$ and not occurring in the M-divisor of t we have that $\mathrm{ord}_{\mathfrak{t}} v_{i,j_i,l_f,j_{l_f}} = \pm 1$.

In the first case, given the assumption that $v_{i,j_i,l_f,j_{l_f}}$'s do not have poles or zeros at ramifying primes and Lemma 5.14, we have that v is a p^a-th power in M.

So suppose the second alternative holds. In this case, without loss of generality, assume $\mathfrak{t}$ is a pole of $v_{i,j_i,l_f,j_{l_f}}$ for some f. Next consider the following equations

$$v^2_{i,j_i,l_f,j_{l_f}} t^{p^{as}} - u^2_{i,l_f} t = \mu^{p^a}_{i,j_i,l_f,j_{l_f},1,1} - \mu_{i,j_i,l_f,j_{l_f},1,1}, \tag{5.39}$$

$$v^2_{i,j_i,l_f,j_{k_f}} - u^2_{i,l_f} = \mu^{p^a}_{i,j_i,l_f,j_{l_f},0,1} - \mu_{i,j_i,l_f,j_{l_f},0,1}, \tag{5.40}$$

obtained from (5.12) by first making $z = 1, m = 1$ and then $z = 1, m = 0$. (If $\mathfrak{t}$ were a zero of $v_{i,j_i,l_f,j_{l_f}}$, then we would set z equal to -1 in both equations.) Since t does not have a pole or zero at $\mathfrak{t}$ and $p^a > 2$, we must conclude that

$$\mathrm{ord}_{\mathfrak{t}}(v^2_{i,j_i,l_f,j_{l_f}} t^{p^{as}} - u^2_{i,l_f} t) = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a}_{i,j_i,l_f,j_{l_f},1,1} - \mu_{i,j_i,l_f,j_{l_f},1,1}) \geq 0$$

and

$$\mathrm{ord}\ _{\mathfrak{t}}(v^2_{i,j_i,l_f,j_{l_f}} - u^2_{i,l_f}) = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a}_{i,j_i,l_f,j_{l_f},0,1} - \mu_{i,j_i,l_f,j_{l_f},0,1}) \geq 0$$

Thus,

$$\mathrm{ord}_{\mathfrak{t}} v^2_{i,j_i,l_f,j_{l_f}} (t^{p^{as}} - t)$$

$$= \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a}_{i,j_i,l_f,j_{l_f},1,1} - \mu_{i,j_i,l_f,j_{l_f},1,1} - t\mu^{p^a}_{i,j_i,l_f,j_{l_f},0,1} + t\mu_{i,j_i,l_f,j_{l_f},0,1}) \geq 0.$$

Finally, we must deduce that $\mathrm{ord}_{\mathfrak{t}}(t^{p^{as}} - t) \geq 2|\mathrm{ord}_{\mathfrak{t}} v|$. But in $F(t)$ all the zeros of $(t^{p^{as}} - t)$ are simple. Thus, this function can have multiple zeros only at primes ramifying in the extension $M/F(t)$. By assumption $\mathfrak{t}$ is not one of these primes and thus we have a contradiction, unless v is a p^a-th power.

Suppose now that $s = 0$. Set $e = 1$ again and let $i, l_1, \ldots, l_{k+1}$ be selected as above. Then from (5.39) and (5.40) we obtain for $l_f \in \{l_1, \ldots, l_{k+1}\}$,

$$\mu^{p^a}_{i,j_i,l_f,j_{l_f},1,1} - \mu_{i,j_i,l_f,j_{l_f},1,1} = t(\mu^{p^a}_{i,j_i,l_f,j_{l_f},0,1} - \mu_{i,j_i,l_f,j_{l_f},0,1}).$$

Note here that all the poles of $\mu_{i,j_i,l_f,j_{l_f},1,1}$ and $\mu_{i,j_i,l_f,j_{l_f},0,1}$ are poles of u_{i,l_f}, $v_{i,j_i,l_f,j_{l_f}}$ or t, and thus are not at any valuation ramifying in the extension $M/F(t)$. From Lemma 5.19 and equation (5.40) we can then conclude that for all $l_f \in \{l_1, \ldots, l_{k+1}\}$

$$v^2_{i,j_i,l_f,j_{l_f}} - u^2_{i,l_f} = 0.$$

Thus, $v_{i,j_i,l_f,j_{l_f}} = \pm u_{i,l_f}$. Since all the poles of u_{i,l_f} are simple, (5.13) rules out "-". Therefore,

$$v_{i,j_i,l_f,j_{l_f}} = u_{i,l_f}. \tag{5.41}$$

Rewriting (5.41) we obtain

$$\frac{d_{i,j_i} - d_{l_f,j_{l_f}}}{v + d_{l_f,j_{l_f}}} = \frac{c_i - c_{l_f}}{u + c_{l_f}},$$

or

$$v = au + b, \tag{5.42}$$

where a, b are constants. However, unless $b = 0$, we have a contradiction with (5.15) because, unless $b = 0$, we have that v^{-1} and u^{-1} have different, and in the case of u, always simple poles. Finally, if $a \neq 1$, then we have a contradiction with (5.14) because the difference, unless it is 0 (and therefore $a = 1$), will have simple poles.

□

5.3. **Satisfying equations.** We now address address the issue we have avoided so far: satisfying the equations constituting our Diophantine definitions. Before we proceed we introduce one more notation.

Notation 5.22. Let $F_1 = \mathbb{F}_p(C(F))$.

Lemma 5.23. *If $w = t^{p^{as}}, s \in \mathbb{Z}_{\geq 0}$ then Equations* (5.6) *can be satisfied over $\mathbb{F}_p(t)$ and Equations* (5.7) *can be satisfied over $F_1(t)$. Further, if $v = u^{p^{as}}$ then Equations* (5.35) *can be satisfied over $F_1(t)$.*

Proof. We start with an elementary equality which constitute the basis of all the constructions in this section.

$$x^{p^{as}} - x = (x^{p^{a(s-1)}} + x^{p^{a(s-2)}} + \cdots + x)^{p^a} - (x^{p^{a(s-1)}} + x^{p^{a(s-2)}} + \cdots + x) \tag{5.43}$$

To satisfy Equations (5.6), it is enough to note that (5.43) holds over $\mathbb{F}_p(x)$. To satisfy Equations (5.7), it is enough to make sure that if $w = t^{p^{as}}, s \in \mathbb{Z}_{\geq 0}$, then for all i, j there exist $b \in V_i, b' \in V_j$ such that $\dfrac{w+b}{w+b'} = \left(\dfrac{t+c_i}{t+c_j}\right)^{p^{as}}$. This fact, however, follows immediately from the definition of V_i and V_j which contain all the p-th powers of c_i and c_j respectively.

Assuming $v = u^{p^{as}}$, for some $1 \leq j_i \leq r_i, 1 \leq j_k \leq r_k$, we have $v_{i,j_i,k,j_k} = (u_{i,k})^{p^{as}}$ for the same reason, since $|V_i| = r_i$ and $|V_j| = r_j$. □

5.4. **Defining p-th powers of arbitrary elements.** We are now ready for the last sequence of propositions concluding the proof. We will have to separate the case of $p = 2$ again. We start with the case of $p > 2$.

Proposition 5.24 ([Shl06], Proposition 8.4.8)**.** *Let $p > 2$. Let $x, y \in M$. Then there exist $v, \tilde{v}, u, \tilde{u}, v_1, \tilde{v}_1, u_1, \tilde{u}_1 \in M$, $s, i, j, r_1, j_1 \in \mathbb{Z}_{\geq 0}$ such that*

$$\begin{cases} E(u, \tilde{u}, v, \tilde{v}, x, y, j, i, s) \\ E(u_1, \tilde{u}_1, v_1, \tilde{v}_1, x+1, y+1, j_1, r_1, s) \end{cases} \tag{5.44}$$

hold if and only if $y = x^{p^s}$.

The following propositions treat the characteristic 2 case.

Lemma 5.25 ([Shl06], Proposition 8.4.9)**.** *Let $p = 2$. Then for $x, y = \tilde{y}^2 \in M, j, r, s \in \mathbb{Z}_{\geq 0} \setminus \{0\}, u, \tilde{u} \in M$ there exist $v, \tilde{v} \in M$ such that*

$$E2(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s) \tag{5.45}$$

holds if and only if there exist $v_1, \tilde{v}_1 \in M$ such that

$$E2(u_1, \tilde{u}_1, v_1, \tilde{v}_1, x, \tilde{y}, j-1, r-1, s-1) \tag{5.46}$$

holds.

Proposition 5.26 ([Shl06], Proposition 8.4.10 and [Eis03], Theorem 3.1)**.** *Let $p = 2$. Then for $x, y \in M, s \in \mathbb{Z}_{\geq 0}$ there exist $j, r \in \mathbb{Z}_{\geq 0}$, $u, \tilde{u}, v, \tilde{v} \in M$ such that (5.45) holds if and only if $y = x^{2^s}$.*

5.5. **Adjusting for arbitrary constant fields.** We will now describe how to adjust the arguments above to take care of the case where the field of constants is not necessarily algebraically closed. So let K be an arbitrary function field of positive characteristic. Let M be the field obtained from K by adjoining the algebraic closure of the constant field of K and as above denote the constant field of M by F. Let $t \in M$ be a non-constant element such that all of its poles and zeros are simple. (As we have seen above, such an element always exists.) The element t and all other elements of M are algebraic over K. Given such an element t, compute C_5 and construct $C(F)$. Let $\hat{K} = K(t, C(F))$. Then $\hat{K}/K$ is a finite extension. Now all the equations discussed above have their coefficients in $\hat{K}$ and can be satisfied over $\hat{K}$. As far as solutions to these equation go, we can always consider solutions in M to make sure we have only the solutions we want. E.g., if we know that (5.6) and (5.7) imply that $w = t^{p^{as}}$ when we are looking at all possible solutions in M, then this is certainly true of $\hat{K}$. Thus $P(\hat{K})$ is existentially definable over $\hat{K}$. Finally, we appeal to Corollary 3.2, to conclude that $P(K)$ is existentially definable over K.

6. Subsets of a field integral at a prime

In this section we construct a Diophantine definition of the set $\mathrm{INT}(K, \mathfrak{t}, t)$ for some prime $\mathfrak{t}$ and some non-constant element t of our function field. Unfortunately, we have to somewhat modify the assumptions and notation for this section. The new notation and assumptions can be found below. Also, as in the section on p-th powers, our initial assumptions will include some conditions on the field, which might not be true of the given field. We will show however, that they can be made true in a finite extension of the given field.

Notation and Assumptions 6.1.

- p, q will denote two not necessarily distinct rational primes.
- $\mathbb{F}_p$ will denote a finite field of p elements.
- K will denote a function field over a field of constants C of characteristic $p > 0$.
- $t \in K$ will denote an element of the field such that $K/C(t)$ is finite and separable.
- C_0 will denote the algebraic closure of $\mathbb{F}_p$ in C, and K_0 will denote the algebraic closure of $C_0(t)$ in K. If $q \neq p$, then assume that C_0 contains the primitive q-th root of unity.
- Let $\gamma \in K$ generate K over $C(t)$ and let γ_0 generate K_0 over $C_0(t)$.
- For some $a \in C$ algebraic over $\mathbb{F}_p$, K and C will not contain any root of a polynomial

$$T^q - a, \tag{6.1}$$

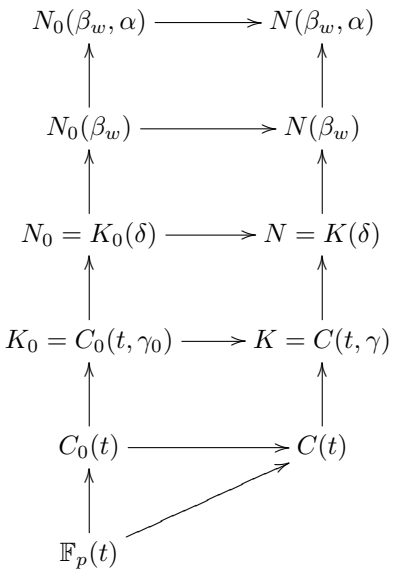
in the case $q \neq p$, and any root of

$$T^p - T + a, \tag{6.2}$$

in the case $q = p$. Let α be a root of (6.1), if $q \neq p$ and let α be the root of (6.2) otherwise.

- Assume all the poles and zeros of t in K and K_0 are simple. In particular, $\mathfrak{P}$, the zero of t in $C(t)$ or $C_0(t)$ is not ramified in $K/C(t)$ or $K_0/C_0(t)$. Note also that if $\mathfrak{p}$ (or $\mathfrak{p}_0$) is a prime of K (K_0 respectively) lying above $\mathfrak{P}$, then $\mathrm{ord}_{\mathfrak{p}} t = 1$ ($\mathrm{ord}_{\mathfrak{p}_0} t = 1$ respectively).
- Denote by $\mathfrak{Q}$ the pole divisor of t in K or K_0.
- If $q \neq p$, let $b \in C_0 \setminus \{0\}$ be such that for some $c \in C_0$ we have that $c^q = b$.
- For $w \in K$, let $h_w = t^{-1} w^q + t^{-q}$.
- If $p = q$, let β_w be the root in $\tilde{K}$, the algebraic closure of K, of $T^p - T - \dfrac{1}{h_w}$. If $p \neq q$, set β_w to be the root of $T^q - (\dfrac{1}{h_w} + 1)$.
- Let $\delta \in \tilde{K}$ be a root of the polynomial $T^p - T + t$, if $q = p$ and let α be a root of the polynomial $T^q - (t + 1)$, if $q \neq p$.
- Let $N = K(\delta)$ and let $N_0 = K_0(\delta)$.

The diagram below shows the field extensions we will consider in this section:



We start with some basic lemmas concerning function fields and local fields. The proofs of the facts in the first lemma can be found in [Lan02, Ch. V, §5, and Theorem 6.4].

Lemma 6.2. *The following statements are true.*

- *If L is algebraic over a finite field of characteristic $p > 0$ and is not algebraically closed, then it has an extension of prime degree q. Further, if $q \neq p$, then for some $a \in L$, the polynomial $X^q - a$ is irreducible and if $q = p$, then for some $a \in L$, the polynomial $X^p - X - a$ is irreducible.*
- *All the solutions to $X^p - X - a = 0$ in the algebraic closure of L can be written in the form $\alpha + i, i = 0, \ldots, p-1$, where α is any root of the equation.*
- *If L is algebraic over a finite field of characteristic $p > 0$ and is not algebraically closed, then any finite extension of L is also not algebraically closed.*

Lemma 6.3. *Let G be a field of positive characteristic p and let q be a prime number. If $q \neq p$, assume G contains a primitive q-th root of unity. Let α be an element of the algebraic closure of G, either in G or of degree q over G. Let $\alpha_j = \alpha + j, j = 0, \ldots, p-1$, if $p = q$, and let $\alpha_j = \xi_q^j \alpha, j = 0, \ldots, q-1$, if $q \neq p$. Let*

$$P(a_0, \ldots, a_{q-1}) = \prod_{j=0}^{q-1} (a_0 + a_1\alpha_j + \ldots + a_{q-1}\alpha_j^{q-1}). \tag{6.3}$$

In this case, if $[G(\alpha) : G] = q$, then $P(a_0, \ldots, a_{q-1}) = \mathbf{N}_{G(\alpha)/G}(a_0 + a_1\alpha + \ldots + a_{q-1}\alpha^{q-1})$. At the same time, if $\alpha \in G$, then for any $y \in G$ the equation $P(X_0, \ldots, X_{q-1}) = y$ has solutions $x_0, \ldots, x_{q-1} \in G$.

Proof. The only assertion of the lemma which requires an argument is the assertion that for any $y \in G$ the equation $P(X_0, \ldots, X_{q-1}) = y$ has solutions $x_0, \ldots, x_{q-1} \in G$ assuming $\alpha \in G$. To see that consider the following linear system of equations in $a_0, \ldots, a_{q-1}$:

$$\sum_{i=0}^{q-1} a_i \alpha_j^i = y_j, j = 1, \ldots, q, \tag{6.4}$$

where $y_1 = y$ and $y_j = 1, j = 2, \ldots, q$. Observe that the determinant of the system is a Vandermonde determinant and thus is non-zero. Hence the system has solutions. By Cramer's rule, all the solutions will be in G. □

Lemma 6.4. *Let G/H be a Galois extension of algebraic function fields of degree n. Let $\mathfrak{p}$ be a prime of H which does not split in G. Let $x \in H$ be such that $ord_{\mathfrak{t}} x \not\equiv 0 \pmod{n}$. Then x is not a norm of an element of G.*

Proof. Let $y = y_1, \ldots, y_n \in G$ be all the conjugates of a G-element y over H. Let $\mathfrak{T}$ be the prime above $\mathfrak{t}$ in G. In this case, $\mathrm{ord}_{\mathfrak{T}} y_i = \mathrm{ord}_{\mathfrak{T}} y_j$ for all $i, j = 1, \ldots, n$. Therefore, $\mathrm{ord}_{\mathfrak{T}} \mathbf{N}_{G/H}(y) = \sum_{i=1}^{n} \mathrm{ord}_{\mathfrak{T}} y_i = n \mathrm{ord}_{\mathfrak{T}} y \equiv 0 \mod n$. At the same time we have that $\mathrm{ord}_{\mathfrak{T}} \mathbf{N}_{G/H}(y) = \mathrm{ord}_{\mathfrak{t}} \mathbf{N}_{G/H}(y)$ and the conclusion of the lemma follows. □

Lemma 6.5. *Let H/F be an unramified extension of local fields of degree n. Let $\mathfrak{t}$ be the prime of F. Let $x \in F$ be such that $ord_{\mathfrak{t}} x \equiv 0 \pmod{n}$. Then x is a norm of some element of H.*

Proof. Let π be a local uniformizing parameter for $\mathfrak{t}$. Then $x = \pi^n \varepsilon$, where ε is a unit. Since π^n is an F-norm, x is an F-norm if and only if ε is an F norm. The last statement is true by [Wei74, Corollary, page 226]. □

We now consider the ramification behavior of a given set of primes in an extension.

Lemma 6.6. *Let L be a function field of characteristic p, let $v \in L$ and let δ be a root of the equation*

$$x^p - x - v = 0. \tag{6.5}$$

In this case either $\delta \in L$ or δ is of degree p over L. In the second case the extension $L(\delta)/L$ is cyclic of degree p and the only primes possibly ramified in this extension are the poles of v. More precisely, if for some L-prime $\mathfrak{a}$, $ord_{\mathfrak{a}} v \not\equiv 0$ modulo p and $ord_{\mathfrak{a}} v < 0$, then a factor of $\mathfrak{a}$ in $L(\delta)$ will be ramified completely. At the same time all zeros of v will split completely, i.e. into factors of relative degree 1, in $L(\delta)$.

Proof. Let $\delta = \delta_1, \ldots, \delta_p$ be all the roots of (6.5) in the algebraic closure of L. Then we can number the roots so that $\delta_i = \delta + i - 1$. Thus, either the left side of (6.5) factors completely or it is irreducible. In the second case δ is of degree p over L and $L(\delta)$ contains all the conjugates of δ over L. Thus, the extension $L(\delta)/L$ is Galois of degree p, and therefore cyclic. Next consider the different of δ. This different is a constant. By [Che51, Lemma 2, page 71], this implies that no prime of L at which δ is integral has any ramified factors in the extension $L(\delta)/L$. Suppose now $\mathfrak{a}$ is a prime of L described in the statement of the lemma. Let $\tilde{\mathfrak{a}}$ be an $L(\delta)$-prime above $\mathfrak{a}$. Then $\mathrm{ord}_{\tilde{\mathfrak{a}}} v \equiv 0$ modulo p. Thus, $\tilde{\mathfrak{a}}$ must be totally ramified over $\mathfrak{a}$. Finally, let $\mathfrak{b}$ be zero of v. Since the power basis of δ has a constant discriminant, the power basis of δ is an integral basis with respect to $\mathfrak{b}$ and therefore, if the irreducible polynomial of v factors completely modulo $\mathfrak{b}$, then $\mathfrak{b}$ factors completely in the extension. □

In a similar manner one can show that the following lemma is true.

Lemma 6.7. *Let L be a function field of characteristic $p > 0$ possessing a q-th primitive root of unity, when $q \neq p$, $z \in L$, γ a root of $T^q - z$, $\mathfrak{a}$ a prime of L. In this case, if $ord_{\mathfrak{a}} z \not\equiv 0 \mod q$, then $\mathfrak{a}$ is completely ramified in the extension $L(\gamma)/L$. If z is integral at $\mathfrak{a}$ and $z \equiv c^q \neq 0 \mod \mathfrak{a}$, then $\mathfrak{a}$ splits completely, i.e. into factors of relative degree 1, in the extension $L(\gamma)/L$.*

We now specialize the lemmas above to our situation.

Corollary 6.8. *The following statements are true about the extensions N/K and N_0/K_0.*

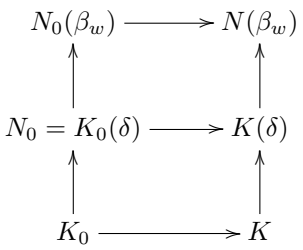
1. *There is no constant field extension.*
2. *The factors of $\mathfrak{P}$ split completely, i.e into factors of relative degree 1.*
3. *The factors of $\mathfrak{Q}$ are ramified completely, i.e. into factors of relative degree 1.*

Next we need take a look at zeros and poles of h_w and zeros and poles of w in $N, N_0, N(\beta_w)$, and $N(\beta_w)$. (We remind the reader that $h_w = t^{-1} w^q + t^{-q}$, β_w is a root of $T^p - T - \frac{1}{h_w}$ if $p = q$, and β_w is a root of $T^q - (\frac{1}{h_w} + 1)$ if $p \neq q$.)

Lemma 6.9. *The following statements are true in $N(\beta_w)$ and, assuming w is algebraic over $C_0(t)$, in $N_0(\beta_w)$:*

1. *If $\hat{\mathfrak{p}}$ is a prime of $N(\beta_w)$ (or $N_0(\beta_w)$) and $\hat{\mathfrak{p}} | \mathfrak{P}$, while $ord_{\hat{\mathfrak{p}}} w < 0$, then the relative degree of $\hat{\mathfrak{p}}$ over $\bar{\mathfrak{p}}$, the prime below it in N (respectively N_0) is 1, and therefore the relative degree of $\hat{\mathfrak{p}}$ over $\mathfrak{p}$, the prime below it in K (respectively K_0) is 1.*
2. *If $\hat{\mathfrak{p}}$ is a prime of $N(\beta_w)$ (or $N_0(\beta_w)$) and $\hat{\mathfrak{p}} | \mathfrak{P}$ in $N(\beta_w)$ (respectively $N_0(\beta_w)$) while $ord_{\hat{\mathfrak{p}}} w < 0$ then $ord_{\hat{\mathfrak{p}}} h_w < 0$ and $ord_{\hat{\mathfrak{p}}} h_w \not\equiv 0 \mod q$.*

(3) *If* $\mathfrak{t}$ *is a prime of* $N(\beta_w)$ *(or* $N_0(\beta_w)$*) and* $\mathfrak{t} \not| \mathfrak{P}$*, then* $ord_{\mathfrak{t}} h_w \equiv 0 \mod q$.
(4) *If* $\mathfrak{p}$ *is a prime of* K *(or* K_0*) such that* $\mathfrak{p}|\mathfrak{P}$ *and* $ord_{\mathfrak{p}} w \geq 0$ *then* $ord_{\mathfrak{p}} h_w \equiv 0 \mod q$.



Proof. First let $\mathfrak{p}|\mathfrak{P}$ in K (or K_0) and note that by Corollary 6.8, we have that $\mathfrak{p}$ will split completely into factors of relative degree 1 in N (respectively N_0). Next, if $\text{ord}_{\mathfrak{p}} w < 0$, then $\text{ord}_{\mathfrak{p}} h_w < 0$ and $\text{ord}_{\mathfrak{p}} h_w \not\equiv 0 \mod q$. Further, for any $\bar{\mathfrak{p}}|\mathfrak{p}$ (in N or N_0) we have $\text{ord}_{\bar{\mathfrak{p}}} h_w = \text{ord}_{\mathfrak{p}} h_w$, since $\bar{\mathfrak{p}}$ splits completely in the extension N/K (or N_0/K_0). Lemmas 6.6 and 6.7 imply that $\bar{\mathfrak{p}}$ will split completely in the extension $N(\beta_w)/N$ (respectively $N_0(\beta_w)/N_0$). So if $\hat{\mathfrak{p}}|\bar{\mathfrak{p}}$ we also have that $\text{ord}_{\hat{\mathfrak{p}}} h_w = \text{ord}_{\bar{\mathfrak{p}}} h_w = \text{ord}_{\mathfrak{p}} h_w$. At the same time, by the same argument, the relative degree of $\hat{\mathfrak{p}}$ over $\mathfrak{p}$ is one.

Again by Corollary 6.8, we have that $\text{ord}_{\hat{\mathfrak{q}}} h_w \equiv 0 \mod q$ for any N-prime (or N_0-prime) $\hat{\mathfrak{q}}$ lying above a K-prime (or K_0-prime) $\mathfrak{q}$ dividing $\mathfrak{Q}$. Finally consider the primes occurring in the divisor of h_w.

If $\mathfrak{t}$ is a pole of h_w in K (or K_0) and $\mathfrak{t}$ does not occur in the divisor of t, then it is a pole of w and h_w has order divisible by q at $\mathfrak{t}$. Hence, if $\hat{\mathfrak{t}}$ is a prime of $N(\beta_w)$ (or $N_0(\beta_w)$) above $\bar{\mathfrak{t}}$, we also have that h_w has order divisible by q at $\hat{\mathfrak{t}}$.

Now let $\bar{\mathfrak{t}}$ be a zero of h_w in N (or N_0) with order not divisible by q. Lemmas 6.6 and 6.7 imply that $\bar{\mathfrak{t}}$ ramifies completely in the extension $N(\beta_w)/N$ (or $N_0(\beta_w)/N_0$). Finally, the last assertion of the lemma follows from the formula defining h_w.

□

Lemma 6.10. *If* w *has a pole at any factor of* $\mathfrak{P}$ *in* K*, then there is no* $x \in N(\alpha, \beta_w)$ *such that*

$$\mathbf{N}_{N(\alpha,\beta_w)/N(\beta_w)}(x) = h_w \tag{6.6}$$

Proof. Let $\hat{\mathfrak{p}}$ be a factor of $\mathfrak{P}$ in $N(\beta_w)$ such that w has a negative order at $\hat{\mathfrak{p}}$. In this case, w has a negative order at $\mathfrak{p}$, the prime below $\hat{\mathfrak{p}}$ in K. By Lemma 6.9, $\mathfrak{p}$ splits completely into distinct unramified factors of relative degree 1 and $\mathfrak{p}$ is of degree 1 in K, so we conclude that there is no constant field extension in the extension $N(\beta_w)/N$ and either (6.1) or (6.2), depending on whether $p = q$ or $p \neq q$, do not have a root in the residue field of $\hat{\mathfrak{p}}$ in $N(\beta_w)$. Thus, $\hat{\mathfrak{p}}$ does not split in the extension $N(\beta_w, \alpha)/N(\beta_w)$. If h_w is a norm in this extension it must have order divisible by q at $\hat{\mathfrak{p}}$. However, by Lemma 6.9 again, we have that $\text{ord}_{\hat{\mathfrak{p}}} h_w = \text{ord}_{\mathfrak{p}} h_w \not\equiv 0 \mod q$. □

Lemma 6.11. *If* w *is algebraic over* $\mathbb{F}_p(t)$ *and has no poles at any factor of* $\mathfrak{P}$*, then there exists* $x \in N(\alpha, \beta_w)$ *satisfying* (6.6)*.*

Proof. First we observe that it is enough to find $x \in N_0(\alpha, \beta_w)$ with

$$\mathbf{N}_{N_0(\alpha,\beta_w)/N_0(\beta_w)}(x) = h_w. \tag{6.7}$$

Indeed, since α is of degree q over both $N(\beta_w)$ and $N_0(\beta_w)$ or is of degree 1 over both fields, any element $x \in N_0(\alpha, \beta_w)$ has the same coordinates with respect to the power basis of α (which is either $\{1\}$, if the degree of α over the fields in question is 1, or $\{1, \alpha, \ldots, q-1\}$, if the degree of α over both fields is q). Thus x has the same conjugates over $N(\beta_w)$ and $N_0(\beta_w)$ and therefore the same norm. Next, by Lemmas 6.7 and 6.6, and by construction of h_w, the divisor of h_w is a q-th power of another divisor. Now, if $\alpha \in N_0(\beta_w)$, we are done. Otherwise, we observe that there is a finite extension $\hat{N}_0$ of $\mathbb{F}_p(t)$ such that

- α is of degree q over $\hat{N}_0$,
- $w, h_w \in \hat{N}_0$,
- the divisor of h_w is a q-th power of another divisor.

By an argument similar to the one above, it is enough to solve

$$\mathbf{N}_{\hat{N}_0(\alpha,\beta_w)/\hat{N}_0(\beta_w)}(x) = h_w. \tag{6.8}$$

Since the extension $\hat{N}_0(\alpha,\beta_w)/\hat{N}_0(\beta_w)$ is unramified and thus locally every unit is a norm (see [Wei74, Corollary, page 226]), we conclude by the Strong Hasse Norm principle (see [Rei03, Theorem 32.9]), that h_w is a norm and therefore x as required exists. □

We now have the following theorem.

Theorem 6.12. *Let $\alpha_j = \alpha + j, j = 0, \ldots, p-1$, if $p = q$ and let $\alpha_j = \xi_q^j \alpha, j = 0, \ldots, q-1$, if $q \neq p$. Let*

$$P(a_0, \ldots, a_{q-1}) = \prod_{j=0}^{q-1} (a_0 + a_1\alpha_j + \ldots + a_{q-1}\alpha_j^{q-1}) = h_w. \tag{6.9}$$

In this case there exist $a_0, \ldots, a_{q-1} \in N(\beta_w)$ such that (6.9) holds only if w has no poles at any factor $\mathfrak{P}$, and if w is algebraic over $\mathbb{F}_p(t)$ and has no poles at any factor of $\mathfrak{P}$, then $a_0, \ldots, a_{q-1} \in N(\beta_w)$ such that (6.9) holds exist.

Now combining Theorem 6.12 with Theorem 3.1 we have the following result:

Proposition 6.13. *The set INT$(K, \mathfrak{p}, t)$ is Diophantine over K.*

We now add our result on definability of p-th powers to the proposition above to conclude that the following assertion is true:

Proposition 6.14. *Hilbert's Tenth Problem is unsolvable over K. (As above, if K is uncountable we consider polynomials with coefficients in a finitely generated ring, more specifically the algebraic closure of $\mathbb{F}_p(t)$.)*

6.1. **Removing the assumptions on K.** Finally, we need to remove the assumptions we imposed on K. We show that given an arbitrary function field G of positive characteristic and not containing the algebraic closure of a finite field, we can a find a finite extension K of G where all the assumptions above are satisfied. We proceed in several steps.

(1) Let M be the field obtained by adjoining to G the algebraic closure F of the constant field of G. Since the constant field of M is perfect, as in the section on p-th powers, we can find a non-constant element z of M such that $M/F(z)$ is separable, implying z is not a p-th power in M.
(2) Let M_0 be the algebraic closure in M of $F_0(z)$, where F_0 is the algebraic closure of $\mathbb{F}_p$. Observe that z is not a p-th power in M_0 and hence the extension $M_0/F_0(z)$ is also separable.
(3) Consider now the extensions $M/F(z)$ and $M_0/F_0(z)$. Let $\gamma \in M, \gamma_0 \in M_0$ be such that $M = F(\gamma, z), M_0 = F_0(\gamma_0, z)$. Let $\Gamma \subset F$ be a finite set containing all the coefficients of the monic irreducible polynomials of γ and γ_0 over $F(z)$ and $F_0(z)$, respectively.
(4) Since both extensions $M/F(z)$ and $M_0/F_0(z)$ are finite and there are only finitely many ramified primes, we can find $c_1, c_2 \in F_0$ such that $t = \dfrac{w - c_1}{w - c_2}$ has only simple zeros in both M and M_0. We can also select c_1, c_2, so that t does not have zeros or poles at the zeros of the discriminant of the power basis of γ or γ_0 and γ and γ_0 are both integral with respect to the zero and pole divisors of t. Observe that $F_0(t) = F_0(z)$ and $F(t) = F(z)$.
(5) Consider the monic irreducible polynomial of γ (or γ_0) over $F(z)$ (or $F_0(z)$) modulo the zero divisor of t and also modulo the pole divisor of t. Let $\Delta \subset F$ be a finite set containing all the roots of the reduced polynomials.
(6) Set $K = G(t, \gamma, \gamma_0, \Gamma, \Delta)$ and add, if necessary, the primitive q-th roots of unity.

As above, let C and C_0 be the constant fields of K_0 and K, respectively, and consider the extensions $K/C(t)$ and $K_0/C_0(t)$. By construction, γ has the same monic irreducible polynomial over $C(t)$ and $F(t)$, and γ_0 has the same monic irreducible polynomial over $C_0(t)$ and $F_0(t)$. Since extensions $M/F(t)$ and $M_0/F_0(t)$ are separable, all the roots of these polynomials are distinct. Hence the extensions $K/C(t)$ and $K_0/C_0(t)$ are also separable. Also by construction, the pole divisor and the zero divisor of t are prime to the divisor of the discriminant of the power bases of γ and γ_0 and both γ and γ_0 are integral with respect to the zero and the pole divisor of t. Consequently, the power bases of γ and γ_0 are both integral bases with respect to

the primes which are the pole and the zero of t in $F(t)$ and $F_0(t)$ respectively, and the pole and the zero of t do not ramify in the either extension.

Further, by [Lan70, Chapter 1, §8, Proposition 25], the factorization of the monic irreducible polynomials of γ and γ_0 corresponds to the factorization of the zero and the pole of t in K and K_0, respectively. However, by construction again, these polynomials factor completely (into distinct factors) modulo the zero and modulo the pole divisor of t. So both primes will factor into (unramified) factors of relative degree 1. Since the pole divisor and the zero divisor of t are are also of degree 1, we must conclude that their factors in M and M_0 are also of degree 1. Finally, we note that C does not contain the algebraic closure of $\mathbb{F}_p$ as was noted in Lemma 6.2.

Now by Corollary 3.3, we can conclude that Hilbert's Tenth Problem is unsolvable over G (with the usual clarification in the case G is uncountable). This concludes the proof of Theorems 1.1 and 1.2.

7. First-order undecidability of function fields of positive characteristic

Let K be any function field of positive characteristic and $t \in K$ an element with simple zeros and poles. In Theorem 2.9 of [ES09] we showed that if $P(K,t) = \{x \in K : \exists s \in \mathbb{Z}_{\geq 0}, x = t^{p^s}\}$ is first-order definable over K, then $(\mathbb{Z}, |, +)$ has a model over K in a first-order ring language with finitely many parameters, and thus the first-order theory of K in a ring language with finitely many parameters is undecidable. The transition to the ring language without parameters is in Section 5 of [ES09] and is not dependent on the nature of the field. Since we have now defined $P(K,t)$ existentially over any function field of positive characteristic, the conclusion of Theorem 2.9 applies to any such field and so does the strengthening of the result to the the first-order language without parameters.

References

[Che51] Claude Chevalley. *Introduction to the theory of Algebraic Functions of One Variable*, volume 6 of *Mathematical Surveys*. AMS, Providence, RI, 1951.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Ann. of Math. (2)*, 74:425–436, 1961.

[Eis03] Kirsten Eisenträger. Hilbert's tenth problem for algebraic function fields of characteristic 2. *Pacific J. Math.*, 210(2):261–281, 2003.

[Eis12] Kirsten Eisenträger. Hilbert's Tenth Problem for function fields of varieties over algebraically closed fields of positive characteristic. *Monatsh. Math.*, 168(1):1–16, 2012.

[ES09] Kirsten Eisenträger and Alexandra Shlapentokh. Undecidability in function fields of positive characteristic. *Int. Math. Res. Not. IMRN*, (21):4051–4086, 2009.

[FJ05] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.

[Koc00] Helmut Koch. *Number Theory. Algebraic Numbers and Functions*. American Mathematical Society, Providence, Rhode Island, 2000.

[KR92] H. K. Kim and F. W. Roush. Diophantine unsolvability for function fields over certain infinite fields of characteristic p. *Journal of Algebra*, 152(1):230–239, 1992.

[Lan70] Serge Lang. *Algebraic Number Theory*. Addison Wesley, Reading, MA, 1970.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Mas96] R. C. Mason. *Diophantine Equations over Function Fields*, volume 96 of *London Mathematical Society Lecture Notes*. Cambridge University Press, Cambridge, UK, 1996.

[Mat70] Yu. V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[Phe87] Thanases Pheidas. An undecidability result for power series rings of positive characteristic. II. *Proc. Amer. Math. Soc.*, 100(3):526–530, 1987.

[Phe91] Thanases Pheidas. Hilbert's tenth problem for fields of rational functions over finite fields. *Inventiones Mathematicae*, 103:1–8, 1991.

[PPV11] Hector Pasten, Thanases Pheidas, and Xavier Vidaux. Uniform definability and undecidability in classes of structures. 2011. Preprint.

[Rei03] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[Shl] Alexandra Shlapentokh. Diophantine undecidability for some function fields of infinite transcendence degree and positive characteristic. *Zapiski Seminarov POMI*, 304:141–167.

[Shl96] Alexandra Shlapentokh. Diophantine undecidability of algebraic function fields over finite fields of constants. *Journal of Number Theory*, 58(2):317–342, June 1996.

[Shl00] Alexandra Shlapentokh. Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic. *Pacific Journal of Mathematics*, 193(2):463–500, 2000.

[Shl02] Alexandra Shlapentokh. Diophantine undecidability of function fields of characteristic greater than 2 finitely generated over a field algebraic over a finite field. *Compositio Mathematica*, 132(1):99–120, May 2002.

[Shl06] Alexandra Shlapentokh. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press, 2006.

[Vid94] Carlos Videla. Hilbert's tenth problem for rational function fields in characteristic 2. *Proceedings of the American Mathematical Society*, 120(1):249–253, January 1994.

[Wei74] André Weil. *Basic Number Theory*. Springer Verlag, 1974.

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA.

Department of Mathematics, East Carolina University, Greenville, NC 27858, USA.