J. Eur. Math. Soc. 9, 2103–2138

DOI 10.4171/JEMS/714

Kirsten Eisenträger · Alexandra Shlapentokh

Hilbert's Tenth Problem over function fields of positive characteristic not containing the algebraic closure of a finite field

Received September 3, 2014

Abstract. We prove that the existential theory of any function field K of characteristic $p > 0$ is undecidable in the language of rings augmented by constant symbols for the elements of a suitable recursive subfield, provided that the constant field does not contain the algebraic closure of a finite field. This theorem is the natural generalization of a theorem of Kim and Roush from 1992. We also extend our previous 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.

Keywords. Undecidability, Hilbert's Tenth Problem

1. Introduction

Hilbert's Tenth Problem in its original form was to find an algorithm to decide, given a polynomial equation $f(x_1, \dots, x_n) = 0$ with coefficients in the ring $\mathbb{Z}$ of integers, whether it has a solution with $x_1, \dots, x_n \in \mathbb{Z}$. 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 equipped with a bijection onto a recursive subset S of natural numbers such that the graphs of addition and multiplication correspond to recursive subsets of S^3. 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

K. Eisenträger: Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA; e-mail: eisentra@math.psu.edu

A. Shlapentokh: Department of Mathematics, East Carolina University, Greenville, NC 27858, USA; e-mail: shlapentokha@ecu.edu

Mathematics Subject Classification (2010): Primary 11U05; Secondary 11D72, 11R58, 03D35

infinite constant fields of positive characteristic [Shl00, Shl03, Eis03, KR92]. The results of [Eis03] and [Shl00] also generalize to higher transcendence degree (see [Shl02] and [Shl03]) 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 deal with a function field in at least two variables.

Given our theorems below, the only big question that remains for function fields of positive characteristic is whether Hilbert's Tenth Problem for a one-variable function field over an algebraically closed field of constants is undecidable. Our two theorems below will shrink the window of the "unknown" almost precisely to this question. Our results enable us to finally give a complete generalization of the theorem by Kim and Roush from 1992 that Hilbert's Tenth Problem is undecidable for rational function fields $F(t)$ when F is a proper subfield of the algebraic closure of $\mathbb{F}_p$ ($p > 2$). Below we separate the recursive and uncountable or non-recursive countable cases. Before proceeding we should also note that any function field over a recursive field of constants is recursive.

Theorem 1.1. *If K is any recursive function field of positive characteristic not containing the algebraic closure of a finite field, then Hilbert's Tenth Problem is not solvable over K (under any recursive presentation of the field).*

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 recursive finitely generated subfield $K_f \subseteq K$ such that there is no algorithm to determine whether a polynomial equation with coefficients in K_f has solutions in K. (We can take K_f to be a finite extension of a rational field $\mathbb{F}_p(t)$, where $\mathbb{F}_p$ is a finite field of p elements and t is a non-constant element of K to be specified later. We assume that we are given a recursive presentation of K_f.)*

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, which yields the following theorem.

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* or *existentially definable* over R in the language of rings if there exists a polynomial $f(t_1, \ldots, t_k, x_1, \ldots, x_n)$ with coefficients in R such that for any k-tuple $\bar{a} = (a_1, \ldots, a_k) \in R^k$ we have $\bar{a} \in A \Leftrightarrow \exists b_1, \ldots, b_n \in R : f(\bar{a}, b_1, \ldots, b_n) = 0$. Then $f(t_1, \ldots, t_k, x_1, \ldots, x_n)$ is called a *diophantine definition* of A over R. In general, if the fraction field of a recursive integral domain is not alge-

braically 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,

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

This approach is due to Pheidas who used it to show that Hilbert's Tenth Problem for rational function fields over finite fields of odd characteristic is undecidable [Phe91].

In [ES09] we showed that we can existentially define one of these sets for a large class of fields: we proved that the set $P(K)$ of p-th powers is existentially definable in *any* function field K of characteristic $p > 2$ whose constant field has transcendence degree at least 1 over $\mathbb{F}_p$. In [PPV14] 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. So it took more than twenty years to achieve the complete generalization of the pioneering lemma of Pheidas.

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 $C_K(t)$ ([Shl00, Lemma 2.6] and [Eis03, Lemma 3.5]). 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 5.7, 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 a set which we call $\mathrm{INT}(K, \mathfrak{p}, t)$. Here t is a non-constant element of K with $\mathrm{ord}_{\mathfrak{p}}\, t = 1$. The set $\mathrm{INT}(K, \mathfrak{p}, t)$ will contain only elements $x \in K$ with $\mathrm{ord}_{\mathfrak{p}}\, x \geq 0$. At the same time, 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 will be 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 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

In this section we show that existential definitions of p-th powers and (almost-)integrality are enough to prove that Hilbert's Tenth Problem is undecidable. This strategy was first used by Pheidas [Phe91]. We start by defining a relation on positive integers.

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

In [Phe87] Thanases Pheidas proved that the existential theory of $(\mathbb{Z}_{>0}, 1, +, \mid_p, =)$ 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. (Here by "uniform" we mean "not dependent on the given system".) 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 the latter 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 $K \setminus \{0\} \to \mathbb{Z}$ 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 note that for positive integers n, m,

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

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 discrete valuation (or prime) of K, $t \in K \setminus k$ has order 1 at $\mathfrak{p}$, and $P(K)$ and $\mathrm{INT}(K, \mathfrak{p}, t)$ 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 a 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. It is essentially [Shl06, Lemma B.7.5 in the Number Theory Appendix] or [Shl00, Lemma 1.3].

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

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

be polynomials with coefficients in K. Assume that the degree of g in X is positive and the same for all values of $T_1, \ldots, T_n$. (In other words, the leading coefficient of g as a polynomial in X over the algebraic closure of $\mathbb{F}_p(T_1, \ldots, T_n)$ is never zero for any choice of $T_1, \ldots, T_n \in K$, and the degree of g in X is positive.) Let $A \subset K^n$ be defined as follows: $(t_1, \ldots, t_n) \in A$ if and only if there exist $x_1, \ldots, x_{n_2} \in K$, $x \in \tilde{K}$, $y_1, \ldots, y_{n_3} \in K(x)$ such that

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

Then A has a diophantine definition over K. Further, there is a diophantine definition of A with coefficients depending only on the 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 also need the theorem itself).

Corollary 3.2. *Let K be a field, let G be a finite extension of K, let $f(T_1, \ldots, T_l, X_1, \ldots, X_{n_2}, Y_1, \ldots, Y_{n_3})$ be a polynomial with coefficients in K, and let $A \subset K^l$ be defined in the following manner: $(t_1, \ldots, t_l) \in A$ if and only if there exist $x_1, \ldots, x_{n_2} \in K$, $y_1, \ldots, y_{n_3} \in G$ such that*

$$f(t_1, \ldots, t_l, x_1, \ldots, x_{n_2}, y_1, \ldots, y_{n_3}) = 0.$$

Then 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 or not recursive, then assume we are considering equations with coefficients in a finitely generated recursive 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 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 one 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 F of constants of characteristic $p > 0$.
(3) Let $q = p$, if $p > 2$, and $q = p^2$ if $p = 2$.
(4) 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.)
(5) A *prime* of M is a discrete F-valuation of M.
(6) 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 1.
(7) A *divisor* is an element of the free abelian group on the set of primes of M. We will denote the group law multiplicatively.
(8) 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).
(9) If $\mathfrak{I}$ is an integral divisor and $\mathfrak{p}$ is a prime, then $\operatorname{ord}_{\mathfrak{p}} \mathfrak{I}$ is the multiplicity of $\mathfrak{p}$ in the product.
(10) 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 $\operatorname{ord}_{\mathfrak{p}} \mathfrak{I}_1 \leq \operatorname{ord}_{\mathfrak{p}} \mathfrak{I}_2$. Similarly for any prime $\mathfrak{p}$ of M we write $\mathfrak{p} \mid \mathfrak{I}_1$ ($\mathfrak{p}$ divides $\mathfrak{I}_1$) to mean $\operatorname{ord}_{\mathfrak{p}} \mathfrak{I}_1 > 0$.
(11) Given an M-prime $\mathfrak{p}$, let $R_{\mathfrak{p}}$ be the *valuation ring* of $\mathfrak{p}$ (i.e. the set of all elements of M assigned a non-negative value by the valuation). We will also let $\mathfrak{p}$ denote the prime ideal of $R_{\mathfrak{p}}$. (The valuation ring is a local ring.) Now for any $x \in R_{\mathfrak{p}}$, there exists $n \in \mathbb{Z}_{\geq 0}$ such that $x \in \mathfrak{p}^n$ and $x \notin \mathfrak{p}^{n+1}$. We define $\operatorname{ord}_{\mathfrak{p}} x$ to be n. If $y \notin R_{\mathfrak{p}}$, then $y^{-1} \in R_{\mathfrak{p}}$ and we set $\operatorname{ord}_{\mathfrak{p}} y = -\operatorname{ord}_{\mathfrak{p}} y^{-1}$.
(12) For $x \in M$, let $\mathfrak{n}(x) = \prod_{\mathfrak{q},\, \operatorname{ord}_{\mathfrak{q}} x > 0} \mathfrak{q}^{\operatorname{ord}_{\mathfrak{q}} x}$ denote the *zero divisor* of x and let $\mathfrak{d}(x) = \mathfrak{n}(x^{-1})$ be the *pole divisor* of x. Let $(x) = \frac{\mathfrak{n}(x)}{\mathfrak{d}(x)}$ be the *divisor* of x. Let $H(x)$ denote the *height* of x, i.e. $H(x) = \deg \mathfrak{d}(x) = \deg \mathfrak{n}(x)$.
(13) 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, its 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. In particular, $\frac{dx^p}{dt} = 0$.

(14) 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 1 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.

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

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

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

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

which is a vector space over F, and $\ell(\mathfrak{U})$ for the dimension of $\mathcal{L}(\mathfrak{U})$ 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). Then*

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

If the field of constants of E is algebraically closed, the relative degrees will always be equal to 1.

(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 $\ell(\mathfrak{U}) = d + 1$.*
(b) *If $g > 0$ and $0 < d \leq 2g - 2$ then $\ell(\mathfrak{U}) \geq d - g + 1$.*
(c) *If $g > 0$ and $d > 2g - 2$ then $\ell(\mathfrak{U}) = d - g + 1$.*

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

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

Lemma 4.3. *If $\mathfrak{t}$ is a prime of M, and $\mathfrak{A}$ and $\mathfrak{B}$ are 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 $\mathfrak{U} = \frac{\mathfrak{A}}{\mathfrak{t}^{2g+1+\deg \mathfrak{A}}}$ and note that by Lemma 4.2(2),

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

Further, let $\mathfrak{U}_1 = \frac{\mathfrak{A}}{\mathfrak{t}^{2g+\deg \mathfrak{A}}}$ 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 $\operatorname{ord}_{\mathfrak{r}} \mathfrak{A} \neq 0$ or $\operatorname{ord}_{\mathfrak{r}} \mathfrak{B} \neq 0$, and let $|\mathcal{A}| = m$. Set $\mathfrak{U}_{i+1} = \frac{\mathfrak{A}\mathfrak{r}_i}{\mathfrak{t}^{\deg \mathfrak{A}+2g+1}}$, where $\mathfrak{r}_i$ is the i-th element of $\mathcal{A}$ under some enumeration. 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

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

Such a y exists because a vector space over an infinite field is not the union of finitely many proper subspaces. By construction, $\mathfrak{d}(y) = \mathfrak{t}^{2g+1+\deg \mathfrak{A}}$ and $\mathfrak{n}(y) = \mathfrak{A}\mathfrak{C}$, where $\mathfrak{C}$ is relatively prime to $\mathfrak{A}\mathfrak{B}\mathfrak{t}$. Finally,

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

We now specialize the lemma above to a particular divisor.

Corollary 4.4. *Let $\mathfrak{t}$ be a prime of M. Suppose $w \in M$ is an element whose divisor is of the form $\frac{\mathfrak{X}\mathfrak{A}^q}{\mathfrak{Y}\mathfrak{B}^q}$, 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 $\mathfrak{t}$ is a factor of $\mathfrak{Y}$. Let C be a positive constant such that* $\deg \mathfrak{Y} < C$. *Then $w = \xi \frac{z_1^q}{z_2^q}$, 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 occurring in $\mathfrak{A}$ or $\mathfrak{B}$, and $H(\xi) < (q + 1)(C + g + 1)$.*

Proof. First of all observe that $0 \leq \deg \mathfrak{Y} - \deg \mathfrak{X} = q \deg \mathfrak{A} - q \deg \mathfrak{B} < C$. Further, by Lemma 4.3, there exist $z_1, z_2 \in M$ with divisors $\frac{\mathfrak{A}\mathfrak{C}}{\mathfrak{t}^{\deg \mathfrak{A}+2g+1}}$, $\frac{\mathfrak{B}\mathfrak{D}}{\mathfrak{t}^{\deg \mathfrak{B}+2g+1}}$, respectively, such that $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \mathfrak{X}, \mathfrak{Y}$ are pairwise relatively prime and

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

Let $\xi = w \frac{z_2^q}{z_1^q}$. Then

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

and therefore

$$\begin{aligned} H(\xi) &\leq \deg \mathfrak{X} + q \deg \mathfrak{D} + q \deg \mathfrak{A} - q \deg \mathfrak{B} \leq C + q(g + 1) + qC \\ &< (q + 1)(C + g + 1). \end{aligned} \qquad \square$$

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

Lemma 4.5. *Let $x \in M$ and $\mathfrak{t}$ be a prime of M. We have*

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

Proof. See [Mas96, p. 9]. □

Lemma 4.6. *Let $x \in M$ and let $\mathfrak{p}$ be a prime of M.*

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

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

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

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

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

If $\operatorname{ord}_{\mathfrak{p}} x < 0$, then

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

by Lemma 4.5. □

Lemma 4.7. *For any $z \in M \setminus M^p$ 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 $d_z(\mathfrak{t}) \leq 2g - 2 + 2H(z)$.*

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

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

since z has non-zero global derivative. By Lemma 4.5, if $\operatorname{ord}_{\mathfrak{t}}(\partial z/\partial \mathfrak{t}) < 0$, then $\operatorname{ord}_{\mathfrak{t}} z < 0$. Thus,

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

Further,

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

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

Lemma 4.8. *If* $\mathfrak{t}$ *is a prime of* M *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 not a pole of t, then $\operatorname{ord}_{\mathfrak{t}}(t-c) = 1$ for some $c \in F$. To see this, let $\mathfrak{T}$ be the prime below $\mathfrak{t}$ in $F(t)$. Since the constant field is algebraically closed, all the primes of $F(t)$ are of degree 1, that is, the residue field of every prime is isomorphic to the constant field, and every element of the valuation ring of the prime is equivalent to a constant modulo the prime. If $\mathfrak{t}$ is not a pole of t, then $\mathfrak{T}$ is not either, and therefore t is an element of the valuation ring of $\mathfrak{T}$. Further, in the valuation ring of $\mathfrak{T}$ we have $t \equiv c \bmod \mathfrak{T}$. Thus, $\operatorname{ord}_{\mathfrak{T}}(t-c) > 0$. At the same time, in $F(t)$, the height of t is 1, and therefore $\operatorname{ord}_{\mathfrak{T}}(t-c) = 1$. Now $\operatorname{ord}_{\mathfrak{t}}(t-c) = e(\mathfrak{t}/\mathfrak{T}) \operatorname{ord}_{\mathfrak{T}}(t-c)$, where $e(\mathfrak{t}/\mathfrak{T})$ is the ramification degree of $\mathfrak{t}$ over $\mathfrak{T}$. By assumption, $\mathfrak{t}$ is unramified over $\mathfrak{T}$, i.e. this degree is 1, and hence $\operatorname{ord}_{\mathfrak{t}}(t-c) = \operatorname{ord}_{\mathfrak{T}}(t-c) = 1$.

Consequently, 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 $\operatorname{ord}_{\mathfrak{t}}(\partial t/\partial \mathfrak{t}) = 0$. □

From this lemma we derive a corollary which will help us construct p-th powers. It follows directly from Lemmas 4.6 and 4.8

Corollary 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 for any* x *which is integral at* $\mathfrak{t}$ *we have* $\operatorname{ord}_{\mathfrak{t}}(dx/dt) \geq \max(0, \operatorname{ord}_{\mathfrak{t}} x - 1)$.

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 in 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 5.24. 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 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. We let $q = p$ if $p > 2$ and set $q = p^2$ if $p = 2$. Next we let $z \in M$ be such that the equations in Lemma 5.7 below are satisfied with $w = z + c$ for a sufficiently large number of c's. Here the requisite number depends on the genus g of M and the characteristic p

only. The equations lead us to conclude that either z has "bounded" height (with the bound ultimately depending on g and p only), or the divisor of $z + c$ is a q-th power of another divisor for all c's. In the first case we use the equations from Proposition 5.9 and Corollary 5.10 to conclude that $z \in F(t)$, and Propositions 5.11 and 5.12 to conclude that either z is a q-th power of another field element, or $z = t$.

In the second case we use Lemmas 5.13–5.15 to conclude that z is a q-th power of another element. Then we use a descent argument to obtain new equations which we re-examine. 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. We now extend the notation and assumptions from Section 4.

(1) Assume that t has no zero or pole which is ramified in the extension $M/F(t)$, or equivalently, all zeros and poles of t are simple.
(2) 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 $\mathfrak{P} = \prod_i \mathfrak{p}_i$ and $\mathfrak{Q} = \prod_i \mathfrak{q}_i$ be the factorizations of $\mathfrak{P}$ and $\mathfrak{Q}$ into distinct prime divisors of M.
(3) Let $\mathcal{E}$ be the set of all primes ramifying in the extension $M/F(t)$ and let $e = |\mathcal{E}|$.
(4) Let M^G be the Galois closure of M over $F(t)$. Let $k = [M : F(t)]$. Let $i_G = [M^G : M]$.
(5) For $j = 1, \ldots, k$, let $\sigma_j : M \to M^G$ be an embedding over $F(t)$.
(6) Let $\Omega = \{\omega_1 = 1, \ldots, \omega_k\}$ be a basis of M over $F(t)$.
(7) Let $H_\Omega = \max\{H_{M^G}(\omega_i) : i = 1, \ldots, k\}$, where H_{M^G} is the height in M^G.
(8) Let $C = H(t)$. (In Lemma 5.5 we show that we can always assume that $C \leq \max(1, 2g - 1)$.)
(9) Let $C_1 = 2g - 2 + 2(q + 1)(C + g + 1)$.
(10) Let $C_2 = \dfrac{2g - 1 + 2(q + 1)(C + g + 1)}{q - 1}$.
(11) Let $C_3 = C + qC_1C_2$.
(12) Let $C_4 = k!k^k H_\Omega C_3$.
(13) Let $C_5 = C_4 + 2e + 2k + 4H(t) + 2$.
(14) Let F_0 be the algebraic closure of $\mathbb{F}_p$ in F. Let $C(F) = \{c_0, \ldots, c_{C_5}\} \subset F_0$ be a set of pairwise distinct elements of F_0 satisfying the following requirements:

(a) $c_1 \notin \mathbb{F}_p$, and for $i > 1$, $c_i \in F_0$ is such that $\mathbb{F}_p(c_i)$ is linearly disjoint from each $\mathbb{F}_p(c_1), \ldots, \mathbb{F}_p(c_{i-1})$ over $\mathbb{F}_p$.
(b) $[\mathbb{F}_p(c_i) : \mathbb{F}_p]$ is relatively prime to $p - 1$.

Let

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

let $d_{i,j} = c_j^{q^j}$, and let $r_i = |V_i|$.

(15) If $z \in M \setminus F$, let $C_z \subset C(F)$ be the set of all $c \in C(F)$ such that for any positive integer s, $z - c^{q^s}$ does not have a zero at any prime which is a zero or a pole of t, or at any prime ramified in $M/F(t)$.
(16) For $w \in M$, let $\mathcal{V}(w)$ be a set of primes of $F(t)$ satisfying the following requirements:

(a) Each prime in $\mathcal{V}(w)$ is unramified in the extension $M/F(t)$.
(b) w is integral at all primes of $\mathcal{V}(w)$.
(c) The discriminant of $\{\omega_1, \dots, \omega_k\}$ is relatively prime to every $\mathfrak{A} \in \mathcal{V}(w)$ so that $\{\omega_1, \dots, \omega_k\}$ is a local integral basis with respect to every prime in $\mathcal{V}(w)$.
(d) The size of $\mathcal{V}(w)$ is greater than C_4.

Remark 5.2. Observe that since $\mathbb{F}_p(c_i)$ is linearly disjoint from $\mathbb{F}_p(c_j)$ for $i \neq j$, the equality $c_i^{n_i} = c_j^{n_j}$ for some positive integers n_i and n_j implies that both powers are in $\mathbb{F}_p$. Further, if $c, c' \in V_i$, then c and c' are images of c_i under some (possibly different) powers of Frobenius, and therefore if $\frac{c}{c'} \in \mathbb{F}_p$, then $c = c'$. Indeed, since c and c' are conjugate over $\mathbb{F}_p$, we have $\mathbf{N}_{\mathbb{F}_p(c_i)/\mathbb{F}_p}\left(\frac{c}{c'}\right) = 1$. If $\frac{c}{c'} \in \mathbb{F}_p$, then $\mathbf{N}_{\mathbb{F}_p(c_i)/\mathbb{F}_p}\left(\frac{c}{c'}\right) = \left(\frac{c}{c'}\right)^{[\mathbb{F}_p(c_i):\mathbb{F}_p]}$. Since $([\mathbb{F}_p(c_i) : \mathbb{F}_p], p-1) = 1$, it follows that $\frac{c}{c'} = 1$. Thus, if for some $c \in V_i$ we have $c^{q^r - q^s} \in \mathbb{F}_p$, then $c^{q^r - q^s} = 1$.

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 5.3 (essentially [Shl06, Lemma 8.2.10]). *For any $u, w \in M \setminus F$, the set $C_w \cap C_u$ contains 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 5.4. *For any non-constant $z \in M$ and any constants $c' \neq c$ the zeros of $\frac{z-c'}{z-c}$ are exactly the zeros of $z - c'$, and the poles of $\frac{z-c'}{z-c}$ 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 5.5. *There exists $t \in M$ satisfying condition (1) 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 is clearly true. So suppose $g > 0$ and apply Lemma 4.2(2c) 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 5.3, for any constant field large enough (and certainly for an infinite constant field) there exist constants $c, \tilde{c}$ such that $t = \frac{x-c}{x-\tilde{c}}$ does not have zeros or poles at primes ramifying in the extension $M/F(t)$. Further, by Lemma 5.4 we have $H(t) = H(x - c) = H(x) \leq \max(1, 2g - 1)$. □

Remark 5.6. 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 determined by the genus (and of course the characteristic), so the genus can serve as a measure of the diophantine complexity of the field. Finally, note that $k = [M : F(t)] = H(t)$ and $i_G \leq k!$, so that all the constants occurring in the paper can be bounded in terms of the genus.

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

Lemma 5.7. *Suppose $w, u, v \in M$ satisfy the following equations:*

$$\begin{cases} w - t = v^q - v, \\ \dfrac{1}{w} - \dfrac{1}{t} = u^q - u. \end{cases} \tag{5.1}$$

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

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

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

where $\mathfrak{X}, \mathfrak{Y}, \mathfrak{A}, \mathfrak{B}$ are pairwise relatively prime integral divisors, the multiplicity of all prime factors of $\mathfrak{X}$ and $\mathfrak{Y}$ is 1, $\deg \mathfrak{X} < H(t) = C$, and $\deg \mathfrak{Y} < H(t) = C$. Note that neither $\mathfrak{X}$ nor $\mathfrak{Y}$ is the trivial divisor. Further, without loss of generality we can assume that $\deg \mathfrak{X} \leq \deg \mathfrak{Y}$; also note that the pole divisor of v is $\mathfrak{B}$, and that of u is $\mathfrak{A}$. Now as in Corollary 4.4, using the same notation, set

$$w = \xi \frac{z_1^q}{z_2^q}, \quad \text{where} \quad H(\xi) \leq (q+1)(C+g+1),$$

no prime factor of $\mathfrak{B}$ occurs in the divisor of ξ, the zero divisor of z_1 is of the form $\mathfrak{A}\mathfrak{C}$, the zero divisor of z_2 is of the form $\mathfrak{B}\mathfrak{D}$, the pole divisors of z_1 and z_2 are powers of a prime factor of $\mathfrak{Y}$, and $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \mathfrak{X}, \mathfrak{Y}$ are pairwise relatively prime. Next rewrite the first equation of (5.1) as

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

so

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

and set $s = vz_2$. Note that if for some prime $\mathfrak{r}$ of M we have $\operatorname{ord}_{\mathfrak{r}} \mathfrak{B} = h > 0$, then

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

since the pole divisor of v is exactly $\mathfrak{B}$, and for any prime divisor $\mathfrak{r}$ of $\mathfrak{B}$ we have

$$\operatorname{ord}_{\mathfrak{r}} z_2 = \operatorname{ord}_{\mathfrak{r}} \mathfrak{B} = h. \tag{5.3}$$

In addition,

$$\operatorname{ord}_{\mathfrak{r}} t z_2^q \geq hq - 1 \geq h(q-1),$$

because all poles and zeros of t are simple by assumption. We have

$$\operatorname{ord}_{\mathfrak{r}} \xi = 0$$

because no prime factor of $\mathfrak{B}$ occurs in the divisor of ξ. We also have

$$\operatorname{ord}_{\mathfrak{r}} z_1 = 0$$

since $\mathfrak{B}$ is relatively prime to the zero divisor of z_1 and, by construction, the pole divisor of z_1 is a factor of $\mathfrak{Y}$, relatively prime to $\mathfrak{B}$. We now rewrite (5.2) to get

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

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

$$\operatorname{ord}_{\mathfrak{r}}(\xi z_1^q - s^q) \geq 2h.$$

Also, since at least one zero or pole of ξ has order not divisible by p, ξ is not a p-th power in M. Thus the global derivation with respect to ξ is defined, and we denote it by x'. (We are using our assumption that the divisor of w is not a q-th power in this step. Otherwise, $\mathfrak{X}$ and $\mathfrak{Y}$ are trivial, making ξ a constant, so that the derivation with respect to ξ would not be defined.) Taking the derivative of $\xi z_1^q - s^q$ with respect to ξ we see that it is equal to z_1^q, and thus $\operatorname{ord}_{\mathfrak{r}} (\xi z_1^q - s^q)' = 0$. At the same time, by Lemma 4.6, we also have $\operatorname{ord}_{\mathfrak{r}} (\xi z_1^q - s^q)' \geq h(q-1) - 1 - d_\xi(\mathfrak{r})$, implying that

$$d_\xi(\mathfrak{r}) \geq h(q-1) - 1 > 0. \tag{5.4}$$

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

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

Using Lemma 4.7 again and (5.4), we can also obtain a bound on h:

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

Hence

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

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

$$H(w) \leq \deg \mathfrak{X} + q \deg \mathfrak{B} \leq C + qC_1C_2. \qquad \square$$

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

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

Since $H_{M^G}(z) = i_G H(z)$ for $z \in M$, we cancel i_G on both sides to 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 5.9 (slightly modified [Shl06, Theorem 10.1.1]). *Suppose for some $w \in M$ with $H(w) < C_3$, for all primes $\mathfrak{A} \in \mathcal{V}(w)$ there are $b(\mathfrak{A}) \in F$ such that for any factor $\mathfrak{c}$ of $\mathfrak{A}$ in M we have*

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

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

Proof. First of all we note that by the description of $\mathcal{V}(w)$ in Notation and Assumption 5.1 (16c), 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 $i = 1, \ldots, n$, we have $f_i \in F(t)$ and f_i is integral at $\mathfrak{A}$. We now write $w = \sum_{i=1}^{k} A_i \omega_i$, where $A_i \in F(t)$. Observe that for all $\mathfrak{A} \in \mathcal{V}(w)$, the element $w - b(\mathfrak{A})$ is equivalent to zero modulo $\mathfrak{A}$ for every prime $\mathfrak{A} \in \mathcal{V}(w)$. 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 $\mathfrak{A} \in \mathcal{V}(w)$, 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 $z = \frac{w - b(\mathfrak{A})}{B(\mathfrak{A})}$ 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 $i = 2, \ldots, k$ and all $\mathfrak{A} \in \mathcal{V}(w)$, we have $A_i = B(\mathfrak{A}) f_i(\mathfrak{A})$, implying $\mathrm{ord}_{\mathfrak{A}} A_i > 0$, implying $H(A_i) > C_4$ or $A_i = 0$. The last inequality contradicts our assumption on $H(w)$ and Lemma 5.8. Therefore $A_i = 0$ for $i = 2, \ldots, k$, and thus $w \in F(t)$. □

We now apply the Weak Vertical Method to our situation.

Corollary 5.10. *Suppose that for some $w \in M$ with $H(w) < C_3$, and $C_4 + e$ quadruples $(c, b, c', b') \in F^4$ with $b \neq b'$ and each c occurring in one quadruple only, we have a solution u_c in M to*

$$\frac{w-b'}{w-b} - \frac{t-c'}{t-c} = u_c^q - u_c. \tag{5.5}$$

Then $w \in F(t)$.

Proof. Suppose that $c \in F$ occurs as the first element in one of the quadruples above, so that the $F(t)$-prime $\mathfrak{P}_c$ corresponding to the zero divisor of $t - c$ is unramified in the extension $M/F(t)$, and let $\mathfrak{p}_c$ be any factor of $\mathfrak{P}_c$ in M. (There are at least C_4 such elements c, since only e primes ramify in $M/F(t)$.) Since $\mathfrak{p}_c$ is unramified, Lemma 5.4 implies that $\operatorname{ord}_{\mathfrak{p}_c}(t-c) = -\operatorname{ord}_{\mathfrak{p}_c}\frac{t-c'}{t-c} = 1$. At the same time, for any pole $\mathfrak{q}_c$ of u_c in M we have $\operatorname{ord}_{\mathfrak{q}_c}(u_c^q - u_c) \equiv 0 \bmod q$ as above. Thus, $b \neq b'$, and by Lemma 5.4 again, $-\operatorname{ord}_{\mathfrak{p}_c}\frac{w-b'}{w-b} = \operatorname{ord}_{\mathfrak{p}_c}(w-b) > 0$. In other words, for C_4 pairs $(c, b) \in F^2$ we have $w \equiv b \bmod \mathfrak{P}_c$, where $\mathfrak{P}_c$ is, as above, the zero divisor of $t-c$ in M and $F(t)$. Now the assertion of the corollary follows from Proposition 5.9. □

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

Proposition 5.11 ([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 primes ramifying in the extension $M/F(t)$, there exist $u, v \in M$ such that the following system is satisfied:*

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

Then $w = t^{q^s}$ for some $s \in \mathbb{Z}_{\geq 0}$.

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

Proposition 5.12. *Let $w \in F(t)$, assume that the system (5.6) holds, and for all $r \in \{0, \ldots, C_5\}$, there exist $b_r \in V_r$ such that for all pairs (i, j) with $j \neq i$ there exist $u_{i,j,b_i,b_j}, v_{i,j,b_i,b_j} \in M$ such that*

$$\begin{cases} \dfrac{w-b_i}{w-b_j} - \dfrac{t-c_i}{t-c_j} = u_{i,j,b_i,b_j}^q - u_{i,j,b_i,b_j}, \\ \dfrac{w-b_j}{w-b_i} - \dfrac{t-c_j}{t-c_i} = v_{i,j,b_i,b_j}^q - v_{i,j,b_i,b_j}. \end{cases} \tag{5.7}$$

Then $w = t^{q^s}$ for some $s \in \mathbb{Z}_{\geq 0}$.

Proof. First of all, by Lemma 5.3, for some $c_i, c_j \notin \mathbb{F}_p$ and $b_i \in V_i$, $b_j \in V_j$, the elements $t - c_i, t - c_j, w - b_i, w - b_j$ do not have zeros at any prime ramifying in $M/F(t)$. Therefore $\frac{t-c_i}{t-c_j}, \frac{w-b_i}{w-b_j} \in F(t)$ do not have zeros or poles at any prime ramifying in $M/F(t)$. It follows that all the zeros and poles of $\frac{t-c_i}{t-c_j}$ are simple, since they are simple in $F(t)$. Now Proposition 5.11 yields

$$\frac{w-b_i}{w-b_j} = \left(\frac{t-c_i}{t-c_j}\right)^{q^s} \tag{5.8}$$

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

$$1 + \frac{b_j - b_i}{w - b_j} = 1 + \frac{c_j^{q^s} - c_i^{q^s}}{t^{q^s} - c_j^{q^s}}. \tag{5.9}$$

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

$$\frac{b_j - b_i}{b_j} = \frac{c_j^{q^s} - c_i^{q^s}}{c_j^{q^s}},$$

or

$$\frac{b_i}{b_j} = \frac{c_i^{q^s}}{c_j^{q^s}}.$$

Thus, from (5.9), for some $r \in \mathbb{Z}_{\geq 0}$, since $b_j \in V_j = \{c_j^{q^k} : k \in \mathbb{Z}_{\geq 0}\}$, we have

$$w = b_j + \frac{b_j - b_i}{c_j^{q^s} - c_i^{q^s}}(t^{q^s} - c_j^{q^s}) = b_j + \frac{b_j}{c_j^{q^s}}(t^{q^s} - c_j^{q^s}) = \frac{b_j}{c_j^{q^s}} t^{q^s} = \frac{c_j^{q^r}}{c_j^{q^s}} t^{q^s} = c_j^{q^r - q^s} t^{q^s}.$$

In a similar fashion we deduce that for some $m \in \mathbb{Z}_{\geq 0}$ we have $w = c_i^{q^m - q^s} t^{q^s}$, and hence $c_j^{q^r - q^s} = c_i^{q^m - q^s}$. Thus, by Remark 5.2 we conclude that $c_j^{q^r - q^s} = 1$ and $w = t^{q^s}$. □

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 5.7, the divisor of w is a q-th power of another divisor. In the three lemmas below we take advantage of this fact to conclude that under certain conditions w is a q-th power of another field element. The proofs for all three lemmas can be found in [Shl06].

Lemma 5.13 ([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 5.14 ([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 some distinct $b_0, \dots, b_n \in G$ we have $\mathbf{N}_{M/G}(b_i^{p^r} - x) = y_i^{p^r}$ for $y_0, \dots, y_n \in G$. Then x is a p^r-th power in M.*

Lemma 5.15 ([Shl06, Lemma 8.4.1]). *Let M be a function field over a perfect field L of constants, and let $t \in M$ be such that $M/L(t)$ is a finite separable extension of degree n. Let m be a positive integer. Let $v \in M$ and assume that for some distinct $b_0 = 0, b_1, \dots, b_n \in L$, the divisor of each $v + b_0, \dots, v + b_n$ is a p^m-th power of some other divisor of M. If for all i, $v + b_i$ does not have any zeros or poles at any prime ramifying in $M/L(t)$, then v is a p^m-th power in M.*

We are now ready to put all the parts together.

Proposition 5.16. *Suppose for some $w \in M$, (5.6) and (5.7) hold with all the variables taking values in M. Then $w = t^{q^s}$ for some non-negative integer s.*

Proof. 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 do not ramify (over $F(t)$), the divisor of $\frac{w-b_i}{w-b_j}$ is not a q-th power of another divisor in M. In this case applying Lemma 5.7 we conclude that $H\left(\frac{w-b_i}{w-b_j}\right) = H(w) < C_3$. (The equality of heights follows from Lemma 5.4.) Now by Corollary 5.10, using C_5 quadruples (c_i, b_i, c_j, b_j) from (5.7) we conclude that $w \in F(t)$. (Recall that $C_5 > C_4 + e$ by definition of C_5 in Notation and Assumptions 5.1(13).) Applying Proposition 5.12, we conclude that $w = t^{q^s}$ 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 $t - c_j$ do not ramify, the divisors of $\frac{w-b_i}{w-b_j}$ are q-th powers of other divisors. (Recall that $b_i \in V_i$ and $b_j \in V_j$.) In this case, the divisor of $1 + \frac{b_j-b_i}{w-b_j}$ is a q-th power of another divisor. Let $w_j = \frac{1}{w-b_j}$ and $a_{i,j} = \frac{1}{b_j-b_i}$, so that

$$\frac{1}{b_j - b_i} + \frac{1}{w - b_j} = a_{i,j} + \frac{1}{w_j}.$$

Then the divisor of $a_{i,j} + \frac{1}{w_j}$ is a q-th power of another divisor for all $i \neq j$ such that the $F(t)$-primes corresponding to $t - c_i$ and to $t - c_j$ do not ramify. This follows since $\frac{w-b_i}{w-b_j}$ and $a_{i,j} + \frac{1}{w_j}$ differ by a constant factor only, and therefore have the same divisor in M.

By Lemma 5.3 we know that $|C_t \cap C_w| > 2k$, or, in other words, we have at least $2k + 1$ values of r such that $t - c_r$ and $w - b_r$ for any $b_r \in V_r$ have no zeros at any prime ramifying in $M/F(t)$. Thus for a fixed $r = j$ with $c_j \in C_t \cap C_w$ and at least $k + 1$ values of $i \neq j$ with $c_i \in C_t \cap C_w$, the element $a_{i,j} + \frac{1}{w_j}$ does not have a pole or a zero at a prime ramifying over $F(t)$. Also, for any pair $i_1 \neq i_2$ we have $a_{i_1,j} \neq a_{i_2,j}$, and the divisor of

each $a_{i,j} + \frac{1}{w_j}$ is a q-th power of another divisor. (If $a_{i_1,j} = a_{i_2,j}$, then $b_j - b_{i_1} = b_j - b_{i_2}$, $b_{i_2} = b_{i_1}$, and therefore some conjugate of c_{i_1} over $\mathbb{F}_p$ is equal to some conjugate of c_{i_2} over $\mathbb{F}_p$. The last equality is impossible by construction of c_{i_1} and c_{i_2}.) Hence Lemma 5.15 shows that w_j for this j is a q-th power in M, and thus w is a q-th power in M.

At this point we can, so to speak, take the "q-th root'' of our equations as in the proof of Proposition 5.11 and again ask, this time for the "new" w (a q-th root of the old w), whether the divisor of $\frac{w-b_i}{w-b_j}$ is not a q-th power of another divisor for some i, j with $c_i, c_j \in C_t \cap C_w$.

Since our "q-th root descent'' cannot go on indefinitely, at some step we conclude that the divisor of $\frac{w-b_i}{w-b_j}$ is not a q-th power of another divisor for any i, j with $c_i, c_j \in C_t$, $b_i \in V_i, b_j \in V_j$. When this happens, we follow the argument of Case 1 to reach the desired conclusion. □

The results in Sections 5.2–5.4 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 5.17.

- 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:

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

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

$$v_{i,j_i,l,j_l}^{2z} t^{mq^s} - u_{i,l}^{2z} t^m = \mu_{i,j_i,l,j_l,z,m}^{q^s} - \mu_{i,j_i,l,j_l,z,m}, \tag{5.12}$$

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

$$v - u = \lambda_1^q - \lambda_1, \tag{5.14}$$

$$v^{-1} - u^{-1} = \lambda_{-1}^q - \lambda_{-1}. \tag{5.15}$$

- Let $j, r, s \in \mathbb{Z}_{\geq 0}$ and $u, \tilde{u}, v, \tilde{v}, x, y \in M$. 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 $j, r, s \in \mathbb{Z}_{\geq 0}$ and $u, \tilde{u}, v, \tilde{v}, x, y \in M$, 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 5.18 ([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 4.9 implies that

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

if and only if $\mathfrak{t}$ is a common zero of $u + b$ and $\frac{d(u+b)}{dt}$. If $\operatorname{ord}_{\mathfrak{t}} \frac{2x^p}{(x^p-t)^2} > 0$, 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, no pole of x is a zero of $u+b$. Thus all zeros of $u+b$ at primes not ramifying in $M/F(t)$ 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 $M/F(t)$ and not being poles or zeros of t. □

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

Lemma 5.19 ([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 result we need to define the q-th powers of elements with simple zeros and poles.

Lemma 5.20 (slightly modified [Shl06, Lemma 8.2.11]). *Let $\sigma, \mu \in M$. Assume that no primes that are poles of σ or μ ramify in the extension $M/F(t)$. Further, assume that*

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

Then $\sigma^q - \sigma = \mu^q - \mu = 0$. (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 $\mathfrak{B}, \mathfrak{P}, \mathfrak{Q}$, and for 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 that does not divide $\mathfrak{P}$ or $\mathfrak{Q}$, then

$$0 > q \operatorname{ord}_{\mathfrak{t}} \mu = \operatorname{ord}_{\mathfrak{t}}(\mu^q - \mu) = \operatorname{ord}_{\mathfrak{t}}(t(\sigma^q - \sigma)) = \operatorname{ord}_{\mathfrak{t}}(\sigma^q - \sigma) = q \operatorname{ord}_{\mathfrak{t}} \sigma.$$

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

$$0 > q \operatorname{ord}_{\mathfrak{t}} \sigma = \operatorname{ord}_{\mathfrak{t}}(\sigma^q - \sigma) = \operatorname{ord}_{\mathfrak{t}}(t(\sigma^q - \sigma)) = \operatorname{ord}_{\mathfrak{t}}(\mu^q - \mu) = q \operatorname{ord}_{\mathfrak{t}} \mu.$$

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

$$\operatorname{ord}_{\mathfrak{p}_i}(t(\sigma^q - \sigma)) < 0, \tag{5.29}$$

$$\operatorname{ord}_{\mathfrak{p}_i}(t(\sigma^q - \sigma)) \not\equiv 0 \bmod p. \tag{5.30}$$

At the same time (5.29) implies that

$$\operatorname{ord}_{\mathfrak{p}_i}(\mu^q - \mu) < 0, \tag{5.31}$$

$$\operatorname{ord}_{\mathfrak{p}_i}(\mu^q - \mu) \equiv 0 \bmod p. \tag{5.32}$$

Therefore assuming $\operatorname{ord}_{\mathfrak{p}_i}\sigma < 0$ leads to a contradiction. Similarly, if $\operatorname{ord}_{\mathfrak{p}_i}\mu < 0$ then (5.31) and (5.29) hold and we again obtain a contradiction. Assuming that $\operatorname{ord}_{\mathfrak{q}_i}\sigma < 0$ and $\operatorname{ord}_{\mathfrak{q}_i}\mu < 0$ 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 $\frac{\mathfrak{B}\mathfrak{D}}{\mathfrak{q}_1^c}$, 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^q we obtain

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

We can rewrite this in the form

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

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 $q > 2$, we know that $\operatorname{ord}_{\mathfrak{t}}(s_1^q t - s_2^q) \geq 2$. Further, by Corollary 4.9 we also have

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

Finally,

$$\operatorname{ord}_{\mathfrak{t}}\frac{d(s_1^q t - s_2^q)}{dt} = \operatorname{ord}_{\mathfrak{t}}(s_1^q).$$

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) implies that t times a constant is equal to a constant. This can happen only if both constants are zero. □

Lemma 5.21 ([Shl06, Lemma 8.4.4]). *Let $s \in \mathbb{Z}_{>0}$. Let $x, v \in M \setminus \{0\}$ and assume that $\tilde{v}^q = v$ for some $\tilde{v} \in M$. Let*

$$u = \begin{cases} \dfrac{x^p + t}{x^p - t} & \text{if } p > 2, \\ \dfrac{x^2 + t^2 + t}{x^2 + t} & \text{if } p = 2. \end{cases}$$

Further, assume that

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

Then

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

Lemma 5.22 ([Shl06, Lemma 8.4.5, Corollary 8.4.6] and [Eis03, Lemma 3.9]). *Let* $s \in \mathbb{Z}_{\geq 0}$ *and* $x, v \in M \setminus \{0\}$. *Let*

$$u = \begin{cases} \dfrac{x^p + t}{x^p - t} & \text{if } p > 2, \\ \dfrac{x^2 + t^2 + t}{x^2 + t} & \text{if } p = 2. \end{cases}$$

Further, assume that (5.35) *holds. Then* $v = u^{q^s}$.

Proof. First of all, we claim that for all i, l, $u_{i,l}$ has no multiple zeros or poles except possibly at 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 5.18 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 primes which are zeros or poles of t or have factors ramifying in $M/F(t)$.

We will show that if $s > 0$ then v is a q-th power in M, and if $s = 0$ then $u = v$. This together with Lemma 5.21 will produce the desired conclusion.

Note that by Corollary 5.3, we can choose distinct natural numbers

$$i, l_1, \ldots, l_{k+1} \in \{0, \ldots, C_5\} \quad \text{such that} \quad \{c_i, c_{l_1}, \ldots, c_{l_{k+1}}\} \subset C_v \cap C_u$$

and for all $1 \leq j_i \leq r_i$ and $1 \leq j_{l_f} \leq r_{l_f}$ with $f = 1, \ldots, k+1$, the elements u_{i,l_f} and $v_{i,j_i,l_f,j_{l_f}}$ have no zeros or poles at primes of M with factors ramifying in $M/F(t)$, or primes occurring in the M-divisor of t. Note also that for the indices thus selected, all the poles and zeros of u_{i,l_f} are simple. We now 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 $M/F(t)$, or at primes occurring in the M-divisor of t.

Now assume $s > 0$, and let f range over $\{1, \ldots, k+1\}$. 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:

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

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

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

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 5.15, we find that v is a q-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 equations

$$v^2_{i,j_i,l_f,j_{l_f}} t^{q^s} - u^2_{i,l_f} t = \mu^q_{i,j_i,l_f,j_{l_f},1,1} - \mu_{i,j_i,l_f,j_{l_f},1,1}, \tag{5.39}$$

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

obtained from (5.12) by first taking $z = 1, m = 1$ 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 $q > 2$, we conclude that

$$\operatorname{ord}_{\mathfrak{t}}(v^2_{i,j_i,l_f,j_{l_f}} t^{q^s} - u^2_{i,l_f} t) = \operatorname{ord}_{\mathfrak{t}}(\mu^q_{i,j_i,l_f,j_{l_f},1,1} - \mu_{i,j_i,l_f,j_{l_f},1,1}) \geq 0,$$

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

Thus,

$$\begin{aligned}&\operatorname{ord}_{\mathfrak{t}} v^2_{i,j_i,l_f,j_{l_f}}(t^{q^s} - t)\\ &\quad = \operatorname{ord}_{(t)}(\mu^q_{i,j_i,l_f,j_{l_f},1,1} - \mu_{i,j_i,l_f,j_{l_f},1,1} - t\mu^q_{i,j_i,l_f,j_{l_f},0,1} + t\mu_{i,j_i,l_f,j_{l_f},0,1}) \geq 0.\end{aligned}$$

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

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

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

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 there are no poles at any primes that ramify in $M/F(t)$. From Lemma 5.20 and (5.40) we then conclude that for all $l_f \in \{l_1, \dots, l_{k+1}\}$,

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

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 $b = 0$, this contradicts (5.15) because, unless $b = 0$, the elements 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 the issue we have avoided so far: satisfying the equations constituting our diophantine definitions. Before we proceed, we introduce one more notation.

Notation 5.23. Let $F_1 = \mathbb{F}_p(C(F))$.

Lemma 5.24. *If $w = t^{q^s}$, $s \in \mathbb{Z}_{\geq 0}$ 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 $v = u^{q^s}$ then equations (5.35) can be satisfied over $F_1(t)$.*

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

$$x^{q^s} - x = (x^{q^{(s-1)}} + x^{q^{(s-2)}} + \cdots + x)^q - (x^{q^{(s-1)}} + x^{q^{(s-2)}} + \cdots + x). \tag{5.43}$$

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

Assuming $v = u^{q^s}$, for some $1 \leq j_i \leq r_i$ and $1 \leq j_k \leq r_k$ we have $v_{i,j_i,k,j_k} = (u_{i,k})^{q^s}$ 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 that the set of p-th powers is diophantine over K. We will have to separate the case of $p = 2$ again. We start with the case of $p > 2$.

Proposition 5.25 ([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 5.26 ([Shl06, Proposition 8.4.9]). *Let $p = 2$. Then for $x, y = \tilde{y}^2 \in M$, $j, r, s \in \mathbb{Z}_{\geq 0} \setminus \{0\}$ and $u, \tilde{u} \in M$ 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 5.27 ([Shl06, Proposition 8.4.10] and [Eis03, Theorem 3.1]). *Let $p = 2$. Then for $x, y \in M$ and $s \in \mathbb{Z}_{\geq 0}$ there exist $j, r \in \mathbb{Z}_{\geq 0}$ and $u, \tilde{u}, v, \tilde{v} \in M$ such that (5.45) holds if and only if $y = x^{2^s}$.*

We now have the following theorem for function fields over algebraically closed fields of positive characteristic:

Theorem 5.28. *Let M be a function field over an algebraically closed field of constants of characteristic $p > 0$. Then*

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

is diophantine over M.

Proof. This follows from Propositions 5.25 and 5.27. □

5.5. Adjusting for arbitrary constant fields

We can now prove that the set of p-th powers is existentially definable in arbitrary function fields of positive characteristic.

Theorem 5.29. *Let K be a function field of characteristic $p > 0$. Then*

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

is diophantine over K.

Proof. We have 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 equations are concerned, 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 $w = t^{q^s}$ 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. More specifically, to apply the corollary we set $G = \hat{K}$, $l = 2$ and $n_2 = 0$. Further, we let f be the diophantine definition $P(\hat{K})$ over $\hat{K}$ and n_3 the total number of variables required by that definition. □

6. Subsets of a field that are integral at a prime

In this section we construct a diophantine definition of a set to be called $\mathrm{INT}(K, \mathfrak{p}, t)$. Membership in this set will depend on the choice of a prime $\mathfrak{p}$ and a non-constant element t of our function field. Thus, $\mathfrak{p}$ and t appear in the name of the set. To be more specific, we show that a set with the following properties is diophantine over K: the set $\mathrm{INT}(K, \mathfrak{p}, t)$ will contain only elements $x \in K$ with $\mathrm{ord}_{\mathfrak{p}}\, x \geq 0$; at the same time, 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 will be in $\mathrm{INT}(K, \mathfrak{p}, t)$. Below, the set $\mathrm{INT}(K, \mathfrak{p}, t)$ can be taken to be the set of all elements satisfying the norm equation (6.6).

Unfortunately, we have to modify somewhat 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, ℓ are two not necessarily distinct rational primes.
- $\mathbb{F}_p$ is a finite field of p elements.
- K is a function field over a field of constants C of characteristic $p > 0$ not containing the algebraic closure of $\mathbb{F}_p$.
- $t \in K$ is such that $K/C(t)$ is finite and separable.
- C_0 is the algebraic closure of $\mathbb{F}_p$ in C, and K_0 is the algebraic closure of $C_0(t)$ in K. If $\ell \neq p$, then C_0 contains a primitive ℓ-th root of unity ξ_ℓ.
- Let $\gamma \in K$ generate K over $C(t)$ and let γ_0 generate K_0 over $C_0(t)$.
- For some $a \in C_0$, the fields K and C contain no root of the polynomial

$$T^\ell - a \tag{6.1}$$

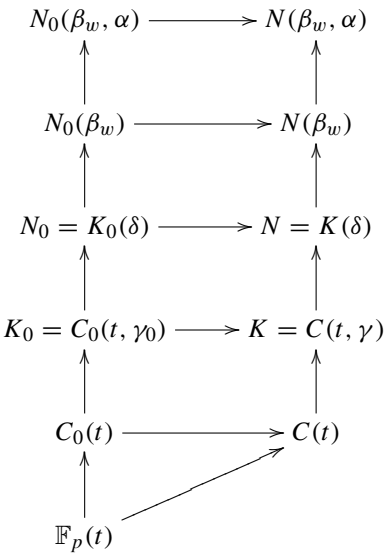
in the case $\ell \neq p$, and no root of

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

in the case $\ell = p$. Let α be a root of (6.1) if $\ell \neq p$, and of (6.2) otherwise.
- 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 $C_0(t)$, does not ramify 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 $\ell \neq p$, let $b \in C_0 \setminus \{0\}$ be such that $c^\ell = b$ for some $c \in C_0$.

- For $w \in K$, let $h_w = t^{-1}w^\ell + t^{-\ell}$.
- If $p = \ell$, let β_w be the root in $\tilde{K}$, the algebraic closure of K, of $T^p - T - \frac{1}{h_w}$. If $p \neq \ell$, set β_w to be the root of $T^\ell - \left(\frac{1}{h_w} + 1\right)$.
- Let $\delta \in \tilde{K}$ be a root of $T^p - T + t$ if $\ell = p$, and let δ be a root of $T^\ell - (t+1)$ if $\ell \neq p$.
- Let $N = K(\delta)$ and $N_0 = K_0(\delta)$.

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. • *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 ℓ. Further, if $\ell \neq p$, then for some $a \in L$, the polynomial $X^\ell - a$ is irreducible, and if $\ell = p$, 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 no finite extension of L is algebraically closed.*

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

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

If $[G(\alpha) : G] = \ell$, *then* $P(a_0, \ldots, a_{\ell-1}) = \mathbf{N}_{G(\alpha)/G}(a_0 + a_1\alpha + \cdots + a_{\ell-1}\alpha^{\ell-1})$. *If* $\alpha \in G$, *then for any* $y \in G$ *the equation* $P(X_0, \ldots, X_{\ell-1}) = y$ *has solutions* $x_0, \ldots, x_{\ell-1} \in G$.

Proof. Only the last assertion requires an argument. Consider the following linear system of equations in $a_0, \ldots, a_{\ell-1}$:

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

where $y_1 = y$ and $y_j = 1$ for $j = 2, \ldots, \ell$. 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 are 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 *with only one unramified factor in* G. *Let* $x \in H$ *be such that* $\operatorname{ord}_{\mathfrak{p}} x \not\equiv 0 \bmod n$. *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 $\mathfrak{P}$ be the prime above $\mathfrak{p}$ in G. Then $\operatorname{ord}_{\mathfrak{P}} y_i = \operatorname{ord}_{\mathfrak{P}} y_j$ for all $i, j = 1, \ldots, n$. Therefore, $\operatorname{ord}_{\mathfrak{P}} \mathbf{N}_{G/H}(y) = \sum_{i=1}^{n} \operatorname{ord}_{\mathfrak{P}} y_i = n \operatorname{ord}_{\mathfrak{P}} y \equiv 0 \bmod n$. Moreover, $\operatorname{ord}_{\mathfrak{P}} \mathbf{N}_{G/H}(y) = \operatorname{ord}_{\mathfrak{p}} \mathbf{N}_{G/H}(y)$, and the conclusion follows. □

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

Proof. Let π be a local uniformizing parameter for $\mathfrak{p}$. 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 latter is true by [Wei74, Corollary, p. 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*

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

Then either $\delta \in L$ *or* δ *is of degree* p *over* L. *In the latter case the extension* $L(\delta)/L$ *is cyclic of degree* p *and the only primes possibly ramifying in this extension are the poles of* v. *More precisely, if for some* L*-prime* $\mathfrak{a}$, $\operatorname{ord}_{\mathfrak{a}} v \not\equiv 0 \bmod p$ *and* $\operatorname{ord}_{\mathfrak{a}} v < 0$, *then a factor of* $\mathfrak{a}$ *in* $L(\delta)$ *will be completely ramified. 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 latter 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. It is a constant. By [Che51, Lemma 2,

p. 71], this implies that no prime of L at which δ is integral has any ramified factors in $L(\delta)/L$. 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 $\operatorname{ord}_{\tilde{\mathfrak{a}}} v \equiv 0 \bmod p$. Thus, $\tilde{\mathfrak{a}}$ must be totally ramified over $\mathfrak{a}$. Finally, let $\mathfrak{b}$ be a 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 the following.

Lemma 6.7. *Let L be a function field of characteristic $p > 0$ possessing an ℓ-th primitive root of unity with $\ell \neq p$. Let $z \in L$, let γ be a root of $T^\ell - z$, and let $\mathfrak{a}$ be a prime of L. If $\operatorname{ord}_{\mathfrak{a}} z \not\equiv 0 \bmod \ell$, then $\mathfrak{a}$ is completely ramified in the extension $L(\gamma)/L$. Also, if z is integral at $\mathfrak{a}$ and $z \equiv c^\ell \neq 0 \bmod \mathfrak{a}$, then $\mathfrak{a}$ splits completely, i.e. into factors of relative degree 1, in $L(\gamma)/L$.*

We now specialize the lemmas above to our situation.

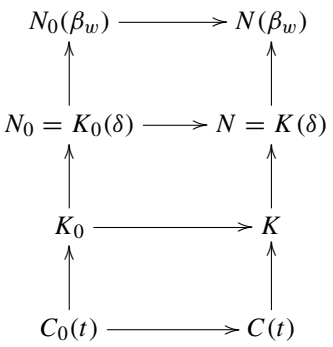
Corollary 6.8. *The following statements are true about the extensions N/K and N_0/K_0.*

(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 completely ramified, i.e. into factors of relative degree 1.*

Next we need to 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 $h_w = t^{-1}w^\ell + t^{-\ell}$, β_w is a root of $T^p - T - \frac{1}{h_w}$ if $p = \ell$, and a root of $T^\ell - \left(\frac{1}{h_w} + 1\right)$ if $p \neq \ell$.)

Lemma 6.9. *The following statements are true:*

(1) *If $\hat{\mathfrak{p}}$ is a prime of $N(\beta_w)$ and $\hat{\mathfrak{p}} \mid \mathfrak{P}$, while $\operatorname{ord}_{\hat{\mathfrak{p}}} w < 0$, then the relative degree of $\hat{\mathfrak{p}}$ over $\bar{\mathfrak{p}}$, the prime below it in N, is 1, and therefore the relative degree of $\hat{\mathfrak{p}}$ over $\mathfrak{p}$, the prime below it in K, is 1.*
(2) *If $\hat{\mathfrak{p}}$ is a prime of $N(\beta_w)$ and $\hat{\mathfrak{p}} \mid \mathfrak{P}$ in $N(\beta_w)$ while $\operatorname{ord}_{\hat{\mathfrak{p}}} w < 0$, then $\operatorname{ord}_{\hat{\mathfrak{p}}} h_w < 0$ and $\operatorname{ord}_{\hat{\mathfrak{p}}} h_w \not\equiv 0 \bmod \ell$.*
(3) *If $\mathfrak{t}$ is a prime of $N(\beta_w)$ and $\mathfrak{t} \nmid \mathfrak{P}$, then $\operatorname{ord}_{\mathfrak{t}} h_w \equiv 0 \bmod \ell$.*
(4) *If $\mathfrak{p}$ is a prime of K such that $\mathfrak{p} \mid \mathfrak{P}$ and $\operatorname{ord}_{\mathfrak{p}} w \geq 0$, then $\operatorname{ord}_{\mathfrak{p}} h_w \equiv 0 \bmod \ell$.*



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

Again by Corollary 6.8, we have $\operatorname{ord}_{\hat{\mathfrak{q}}} h_w \equiv 0 \bmod \ell$ for any N-prime $\hat{\mathfrak{q}}$ lying above a K-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 and $\mathfrak{t}$ does not occur in the divisor of t, then it is a pole of w, and h_w has order at $\mathfrak{t}$ divisible by ℓ. Hence, if $\hat{\mathfrak{t}}$ is a prime of $N(\beta_w)$ above $\bar{\mathfrak{t}}$, we also see that h_w has order at $\hat{\mathfrak{t}}$ divisible by ℓ.

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

In an analogous fashion we can also prove the following.

Lemma 6.10. *If w is algebraic over $C_0(t)$ then the following assertions are true:*

(1) *If $\hat{\mathfrak{p}}$ is a prime of $N_0(\beta_w)$ and $\hat{\mathfrak{p}} \mid \mathfrak{P}$, while $\operatorname{ord}_{\hat{\mathfrak{p}}} w < 0$, then the relative degree of $\hat{\mathfrak{p}}$ over $\bar{\mathfrak{p}}$, the prime below it in N_0, is 1, and therefore the relative degree of $\hat{\mathfrak{p}}$ over $\mathfrak{p}$, the prime below it in K_0, is 1.*
(2) *If $\hat{\mathfrak{p}}$ is a prime of $N_0(\beta_w)$ and $\hat{\mathfrak{p}} \mid \mathfrak{P}$ in $N_0(\beta_w)$ while $\operatorname{ord}_{\hat{\mathfrak{p}}} w < 0$, then $\operatorname{ord}_{\hat{\mathfrak{p}}} h_w < 0$ and $\operatorname{ord}_{\hat{\mathfrak{p}}} h_w \not\equiv 0 \bmod \ell$.*
(3) *If $\mathfrak{t}$ is a prime of $N_0(\beta_w)$ and $\mathfrak{t} \nmid \mathfrak{P}$, then $\operatorname{ord}_{\mathfrak{t}} h_w \equiv 0 \bmod \ell$.*
(4) *If $\mathfrak{p}$ is a prime of K_0 such that $\mathfrak{p} \mid \mathfrak{P}$ and $\operatorname{ord}_{\mathfrak{p}} w \geq 0$, then $\operatorname{ord}_{\mathfrak{p}} h_w \equiv 0 \bmod \ell$.*

We now look at the solvability of some norm equations.

Lemma 6.11. *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 6.10, $\mathfrak{p}$ splits completely into distinct unramified factors of relative degree 1, and $\mathfrak{p}$ is of degree 1 in K, so there is no constant field extension in $N(\beta_w)/N$ and either (6.1) or (6.2), depending on whether $p = \ell$ or $p \neq \ell$, has no root in the residue field of $\hat{\mathfrak{p}}$ in $N(\beta_w)$. Thus, $\hat{\mathfrak{p}}$ does not split in $N(\beta_w, \alpha)/N(\beta_w)$. If h_w is a norm in this extension, it must have order at $\hat{\mathfrak{p}}$ divisible by ℓ. However, by Lemma 6.10 again, $\operatorname{ord}_{\hat{\mathfrak{p}}} h_w = \operatorname{ord}_{\mathfrak{p}} h_w \not\equiv 0 \bmod \ell$. □

Lemma 6.12. *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 ℓ over both $N(\beta_w)$ and $N_0(\beta_w)$ or 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 $\{1, \alpha, \ldots, \ell - 1\}$, if the degree is ℓ). 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 an ℓ-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 ℓ over $\hat{N}_0$,
- $w, h_w \in \hat{N}_0$,
- the divisor of h_w is an ℓ-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, p. 226]), we conclude by the Strong Hasse Norm Principle (see [Rei03, Theorem 32.9]) that h_w is a norm, and therefore an x as required exists. □

We now have the following theorem.

Theorem 6.13. *Let $\alpha_j = \alpha + j$, $j = 0, \ldots, p - 1$, if $p = \ell$, and let $\alpha_j = \xi_\ell^j \alpha$, $j = 0, \ldots, \ell - 1$, if $\ell \neq p$. Let*

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

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

Now combining Theorem 6.13 with Theorem 3.1 we have the following result:

Theorem 6.14. *The set* $\mathrm{INT}(K, \mathfrak{p}, t)$ *is diophantine over K.*

Proof. The only remaining task is rewriting (6.9) as a polynomial equation over K so that the variables range over K. It is enough to consider the case of $\ell \neq p$. The case of $\ell = p$ is similar. First of all, it is not hard to see that the coefficients of $P(a_0, \ldots, a_{\ell-1})$ are in fact in $\mathbb{F}_p(a) \subset K$. However, the variables $a_0, \ldots, a_{\ell-1}$ can take values in $N(\beta_w)$. So to reach the conclusion that

$$\{w : \exists a_0, \ldots, a_{\ell-1} \in N(\beta_w) : P(a_0, \ldots, a_{\ell-1}) = h_w = t^{-1}w^\ell + t^{-\ell}\}$$

is diophantine over N we need Theorem 3.1. In our application of the theorem, we set $n = 1$, $n_2 = 0$, $n_3 = \ell$, $t_1 = w$, $x = \beta_w$, $g(X, w) = h_w X^\ell - (h_w + 1)$, $f(w, \bar{a}) = P(\bar{a}) - h_w$. Observe that h_w is never zero. □

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

Theorem 6.15. *Let K be a function field satisfying the assumptions of 6.1. Then there exists a finitely generated recursive subfield K_f of the algebraic closure of $\mathbb{F}_p(t)$ such that Hilbert's Tenth Problem for K with coefficients in K_f is undecidable. That is, there is no algorithm to determine whether a polynomial equation with coefficients in K_f has solutions in K.*

Remark 6.16. We observe that the only symbols we needed to write down an existential definition of a model of the integers are contained in some finite extension of the rational field over a finite field of constants. So as indicated in the introduction in the statement of Theorem 1.2, we can take K_f to be a finite extension of $\mathbb{F}_p(t)$.

6.1. Proof of Theorems 1.1 and 1.2: removing the assumptions on K

To prove Theorems 1.1 and 1.2 we need to remove the assumptions we imposed on K at the beginning of Section 6. 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 of $F_0(z)$ in M. Here 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 $\gamma \in M$ and $\gamma_0 \in M_0$ be such that $M = F(\gamma, z)$ and $M_0 = F_0(\gamma_0, z)$. 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 $t = \frac{w-c_1}{w-c_2}$ 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 ℓ-th roots of unity.

Now we can give the proofs of the main theorems.

Proof of Theorems 1.1 and 1.2. 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 the 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 divisor 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 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 divisor 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 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 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 [ES09, Theorem 2.9] 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 $(\mathbb{Z}, 1, |, +, =)$ has a model over K in a first-order ring language with finitely many parameters. Since the first-order theory of $(\mathbb{Z}, 1, |, +, =)$ is undecidable (see [Rob49]), this implies that the first-order theory of K in a ring language with finitely many parameters is undecidable whenever $P(K,t)$ is first-order definable over K. The transition to the ring language without parameters uses a result of R. Robinson [Tar53]. It is in [ES09, Section 5] and does not depend 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.

Acknowledgments. The authors would like to thank the referees for numerous helpful comments.

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

References

[Che51] Chevalley, C.: Introduction to the Theory of Algebraic Functions of One Variable. Math. Surveys 6, Amer. Math. Soc., Providence, RI (1951) Zbl 0045.32301 MR 0042164

[DPR61] Davis, M., Putnam, H., Robinson, J.: The decision problem for exponential diophantine equations. Ann. of Math. (2) **74**, 425–436 (1961) Zbl 0111.01003 MR 0133227

[Eis03] Eisenträger, K.: Hilbert's tenth problem for algebraic function fields of characteristic 2. Pacific J. Math. **210**, 261–281 (2003) Zbl 1057.11067 MR 1988534

[Eis12] Eisenträger, K.: Hilbert's Tenth Problem for function fields of varieties over algebraically closed fields of positive characteristic. Monatsh. Math. **168**, 1–16 (2012) Zbl 1270.11126 MR 2971736

[ES09] Eisenträger, K., Shlapentokh, A.: Undecidability in function fields of positive characteristic. Int. Math. Res. Notices **2009**, 4051–4086 Zbl 1242.11100

[FJ05] Fried, M., Jarden, M.: Field Arithmetic. 2nd ed., Ergeb. Math. Grenzgeb. 11, Springer, Berlin (2005) Zbl 1145.12001 MR 2102046

[KR92] Kim, H. K., Roush, F. W.: Diophantine unsolvability for function fields over certain infinite fields of characteristic p. J. Algebra **152**, 230–239 (1992) Zbl 0768.12008 MR 1190413

[Koc00] Koch, H.: Number Theory. Algebraic Numbers and Functions. Amer. Math. Soc., Providence, RI (2000) Zbl 0953.11001 MR 1760632

[Lan70] Lang, S.: Algebraic Number Theory. Addison-Wesley, Reading, MA (1970) Zbl 0211.38404 MR 0282947

[Lan02] Lang, S.: Algebra. 3rd ed., Grad. Texts in Math. 211, Springer, New York (2002) Zbl 0984.00001 MR 1878556

[Mas96] Mason, R. C.: Diophantine Equations over Function Fields. London Math. Soc. Lecture Notes 96, Cambridge Univ. Press, Cambridge (1984) Zbl 0533.10012 MR 0754559

[Mat70] Matiyasevich, Y.: The Diophantineness of enumerable sets. Dokl. Akad. Nauk SSSR **191**, 279–282 (1970) (in Russian) Zbl 0212.33401 MR 0258744

[PPV14] Pasten, H., Pheidas, T., Vidaux, X.: Uniform existential interpretation of arithmetic in rings of functions of positive characteristic. Invent. Math. **196**, 453–484 (2014) Zbl 1327.03009 MR 3193753

[Phe87] Pheidas, T.: An undecidability result for power series rings of positive characteristic. II. Proc. Amer. Math. Soc. **100**, 526–530 (1987) Zbl 0664.03008 MR 0891158

[Phe91] Pheidas, T.: Hilbert's tenth problem for fields of rational functions over finite fields. Invent. Math. **103**, 1–8 (1991) Zbl 0696.12022 MR 1079837

[Rei03] Reiner, I.: Maximal Orders. London Math. Soc. Monogr. 28, Clarendon Press, Oxford (2003) Zbl 1024.16008 MR 1972204

[Rob49] Robinson, J.: Definability and decision problems in arithmetic. J. Symbolic Logic **14**, 98–114 (1949) Zbl 0034.00801 MR 0031446

[Shl96] Shlapentokh, A.: Diophantine undecidability of algebraic function fields over finite fields of constants. J. Number Theory **58**, 317–342 (1996) Zbl 0856.11058 MR 1393619

[Shl00] Shlapentokh, A.: Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic. Pacific J. Math. **193**, 463–500 (2000) Zbl 1010.12008 MR 1755826

[Shl02] Shlapentokh, A.: Diophantine undecidability of function fields of characteristic greater than 2 finitely generated over a field algebraic over a finite field. Compos. Math. **132**, 99–120 (2002) Zbl 1011.03026 MR 1914257

[Shl03] Shlapentokh, A.: Diophantine undecidability for some function fields of infinite transcendence degree and positive characteristic. Zap. Nauchn. Sem. POMI **304**, 141–167 (2003) (in Russian) Zbl 1140.11356 MR 2054753

[Shl06] Shlapentokh, A.: Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields. Cambridge Univ. Press (2006) Zbl 1196.11166 MR 2297245

[Tar53] Tarski, A.: Undecidable Theories. Stud. Logic Found. Math., North-Holland, Amsterdam (1953) Zbl 0053.00401 MR 0058532

[Vid94] Videla, C.: Hilbert's tenth problem for rational function fields in characteristic 2. Proc. Amer. Math. Soc. **120**, 249–253 (1994) Zbl 0795.03015 MR 1159179

[Wei74] Weil, A.: Basic Number Theory. Springer (1974) Zbl 0326.12001 MR 0427267