Pacific Journal of Mathematics

HILBERT'S TENTH PROBLEM FOR ALGEBRAIC FUNCTION FIELDS OVER INFINITE FIELDS OF CONSTANTS OF POSITIVE CHARACTERISTIC

Alexandra Shlapentokh

Volume 193 No. 2 April 2000

PACIFIC JOURNAL OF MATHEMATICS
Vol. 193, No. 2, 2000

HILBERT'S TENTH PROBLEM FOR ALGEBRAIC FUNCTION FIELDS OVER INFINITE FIELDS OF CONSTANTS OF POSITIVE CHARACTERISTIC

Alexandra Shlapentokh

Let K be an algebraic function field of characteristic $p > 2$. Let C be the algebraic closure of a finite field in K. Assume that C has an extension of degree p. Assume also that K contains a subfield K_1, possibly equal to C, and elements u, x such that u is transcendental over K_1, x is algebraic over $C(u)$ and $K = K_1(u, x)$. Then the Diophantine problem of K is undecidable.

Let G be an algebraic function field in one variable whose constant field is algebraic over a finite field and is not algebraically closed. Then for any prime $\mathfrak{p}$ of G, the set of elements of G integral at $\mathfrak{p}$ is Diophantine over G.

1. Introduction.

The interest in the questions of Diophantine definability and decidability goes back to a question which was posed by Hilbert: Given an arbitrary polynomial equation in several variables over $\mathbb{Z}$, is there a uniform algorithm to determine whether such an equation has solutions in $\mathbb{Z}$. This question, otherwise known as Hilbert's 10th problem, has been answered negatively in the work of M. Davis, H. Putnam, J. Robinson and Yu. Matijasevich. (See [5] and [6].) Since the time when this result was obtained, similar questions have been raised for other fields and rings. Arguably the two most interesting and difficult problems in the area are the questions of Diophantine decidability of $\mathbb{Q}$ and the rings of algebraic integers of arbitrary number fields. One way to resolve the question of Diophantine decidability over a ring of characteristic 0 is to construct a Diophantine definition of $\mathbb{Z}$ over such a ring. This notion is defined below.

Definition 1.1. Let R be a ring and let $A \subset R$. Then we say that A has a Diophantine definition over R if there exists a polynomial $f(t, x_1, \dots, x_n) \in R[t, x_1, \dots, x_n]$ such that for any $t \in R$,

$$\exists x_1, \dots, x_n \in R, f(t, x_1, \dots, x_n) = 0 \Longleftrightarrow t \in A.$$

If the quotient field of R is not algebraically closed, it can be shown that we can allow Diophantine definitions to consist of several polynomials without changing the nature of the relationship. (For more details see [6].) Such Diophantine definitions have been obtained for $\mathbb{Z}$ over rings of algebraic integers of the following fields: Totally real extensions of $\mathbb{Q}$, their extensions of degree 2, fields with exactly one pair of complex conjugate embeddings, some fields of degree 4, and some totally real infinite extensions of $\mathbb{Q}$. For more details concerning these results see [7], [11], [12], [25], [30], [29], [37]. However, not much progress has been made towards resolving the Diophantine problem of $\mathbb{Q}$. Further, one of the consequences of a series of conjectures by Barry Mazur and Colliot-Thélène, Swinnerton-Dyer and Skorobogatov is that $\mathbb{Z}$ does not have a Diophantine definition over $\mathbb{Q}$, and thus one would have to look for some other method for resolving the Diophantine problem of $\mathbb{Q}$. (Mazur's conjectures can be found in [23] and [24]. However, Colliot-Thélène, Swinnerton-Dyer and Skorobogatov have found a counterexample to the strongest of the conjectures in the papers cited above. Their modification of Mazur's conjecture in view of the counterexample can be found in [4].) In [40], the author of this paper has demonstrated that in certain totally real algebraic number fields there exist recursive integrally closed rings of algebraic numbers where infinite number of primes can appear in denominators and where rational integers have Diophantine definition. (This implies, of course, that Hilbert's Tenth Problem is undecidable over these rings.) The result above was not proved for $\mathbb{Q}$. The general problem of existence of Diophantine definitions of rational and algebraic integers over integrally closed subrings of number fields (including the fields themselves) remains open.

The problem turned out to be much more tractable over function fields. At this point there are several results pertaining to Diophantine undecidability of various function fields and rings. More specifically, we know that the Diophantine problem of the following function fields is undecidable: the rational function fields of characteristic 0 whose constant fields are subfields of some p-adic fields or are formally real (see [9] and [19]), the rational function fields in two variables over $\mathbb{C}$ (see [18]), the rational function fields over the finite fields of constants (see [25], [41]), rational function fields of positive characteristic whose constant fields do not contain the algebraic closure of a finite field ([17]), and algebraic function fields over finite fields of constants ([38]). Results concerning various function rings can be found in [27], [31], [32], [34], [35], [36].

In this paper we extend the undecidability results of Pheidas, Kim and Roush, and the author of this paper to a new class of fields of algebraic functions: Algebraic function fields of positive characteristic p such that the algebraic closure of a finite field contained in the fields under consideration

has an extension of degree p. More specifically, we will prove the following theorems.

Theorem. *Let K be an algebraic function field of characteristic $p > 2$. Let C be the algebraic closure of a finite field in K. Assume that C has an extension of degree p. Assume also that K contains a subfield K_1, possibly equal to C, and elements u, x such that u is transcendental over K_1, x is algebraic over $C(u)$ and $K = K_1(u, x)$. Then the Diophantine problem of K is undecidable.*

Theorem. *Let G be an algebraic function field whose constant field C is algebraic over a finite field of characteristic $p > 0$. Assume further, that C is not algebraically closed. Then for any prime $\mathfrak{B}$ of G the set of all elements of G integral with respect to $\mathfrak{B}$ is Diophantine over G.*

The proof of the undecidability result is based on the idea first introduced by Denef in [10] and further developed by Pheidas in [26], Kim and Roush in [17], and the author of this paper in [38]. This idea can be summarized by the following lemma.

Lemma 1.2. *Let K be an algebraic function field of characteristic $p > 0$. Let $t \in K$ be a nonconstant element of K. Let C_p be the finite field of p elements, and let G be the algebraic closure of $C_p(t)$ in K. Let $\mathfrak{p}$ be a prime of K which lies above a nontrivial prime of G, and assume that the following sets are Diophantine over K.*

$$p(K) = \{(x, w) \in K^2 | \exists s \in \mathbb{N},\ w = x^{p^s}\}$$

$$INT(\mathfrak{p}),$$

where if $w \in K \cap INT(\mathfrak{p})$ then $\operatorname{ord}_{\mathfrak{p}} w \geq 0$, and if $w \in G$ and $\operatorname{ord}_{\mathfrak{p}} w \geq 0$, then $w \in INT(\mathfrak{p})$. Then the Diophantine problem of K is undecidable.

(The proof of the lemma can be easily derived from the proof of [38, Lemma 1.5].)

Section two of the paper is devoted to showing that $p(K)$ is Diophantine over K, while section three contains a proof of the fact that $INT(\mathfrak{p})$ is Diophantine over K. Before we leave this section, we will state one more easy but useful lemma concerning Diophantine definitions.

Lemma 1.3. *Let L be a field, and let*

$$P(w, u_1, \ldots, u_m) = 0 \tag{1.1}$$

be a polynomial equation over L. Let

$$\{P_s(w, x_1, \ldots, x_n, y_1, \ldots, y_r) = 0, s = 1, \ldots, v\} \tag{1.2}$$

be a set of equations over L. Then, assuming $k > 0$ is the degree of P in w, there exists a set of equations

$$\{Q_l(u_1, \dots, u_m, t_{1,0}, \dots, t_{n,k-1}, y_1, \dots, y_r) = 0,\ l = 1, \dots, e\} \tag{1.3}$$

over L such that for any $u_1, \dots, u_m, y_1, \dots, y_r \in L$, the system (1.1) and (1.2) has solutions w in the algebraic closure of L and $x_1, \dots, x_n \in L(w)$ if and only if for some $t_{1,0} \dots, t_{n,k-1} \in L$, $t_{1,0}, \dots, t_{n,k-1}$, $u_1, \dots, u_m$, $y_1, \dots, y_r$ are solutions of the system (1.3).

Proof. Fix $u_1, \dots, u_m, y_1, \dots, y_r \in L$ and assume initially that the values of $u_1, \dots, u_m$ under consideration will not make the leading coefficient of P with respect to w zero. Under this assumption we can use Equation (1.1) to compute $\{A_{i,j}(u_1, \dots, u_m) \in L(u_1, \dots, u_m)\}$ such that for any $i \in \mathbb{N}$,

$$w^i = \sum_{j=0}^{k-1} A_{i,j} w^j. \tag{1.4}$$

Next consider the following system of equations:

$$\left\{ P_s\left(w, \sum_{i=0}^{k-1} t_{i,1} w^i, \dots, \sum_{i=0}^{k-1} t_{i,n} w^i, y_1, \dots, y_r \right) = 0, s = 1, \dots, v \right\}. \tag{1.5}$$

If we treat $\{1, \dots, w^{k-1}\}$ as if they were linearly independent over $L(u_1, \dots, u_m, y_1, \dots, y_r)$ and use Equation (1.4), we can replace the system (1.5) by a system of the form (1.3), where every P_i is replaced by k equations corresponding to the coefficients of the first k powers of w. Suppose now (1.2) has solutions as described in the statement of the lemma. Since $0 < [L(w) : L] \leq k$, for $i = 1, \dots, n, x_i = \sum_{i=0}^{k-1} a_{i,j} w^j$, where $a_i \in L$. (If $[L(w) : L] < k$ then for $j = [L(w) : L], \dots, k$, we can set $a_{i,j} = 0$.) Thus, the system (1.3) will clearly be satisfied with $t_{i,j} = a_{i,j}$. Conversely, if for some $a_{i,j}, = Q_l(u_1, \dots, u_m, a_{1,0}, \dots, a_{n,k-1}, y_1, \dots, y_r) = 0, l = 1, \dots, e$, then given the construction of Q_l's and assuming w is a root of P,

$$P_s\left(w, \sum_{i=0}^{k-1} a_{i,1} w^i, \dots, \sum_{i=0}^{k-1} a_{i,n} w^i, y_1, \dots, y_r \right) = 0, s = 1, \dots, v.$$

Finally, we remove the assumption that the leading coefficient of P with respect to w is not zero. To accomplish that we need to consider the following cases: The k-th coefficient is not zero; the k-th coefficient is zero but $k-1$-st coefficient is not zero; ... ; only the free term is nonzero. Conditions for each case can be written down in a Diophantine fashion and all the conditions can be combined together in a Diophantine fashion also.

For the remainder of the paper we will use the following notations.

Notations 1.4.

- K will denote an algebraic function field over a field of constants C_K of characteristic $p > 2$. In other words, K is a finite algebraic extension of $C_K(w)$ for some $w \in K$ transcendental over C_K.
- C will denote the algebraic closure of a finite field in C_K.
- u will denote a nonconstant element of K.
- G will denote the algebraic closure of $C(u)$ in K.
- Given $x_1, \dots, x_m \in G$, $G_{x_1,\dots,x_m}$ will denote a subfield of G containing $x_1, \dots, x_m$ and such that $C_{x_1,\dots,x_m}$ - the constant field of $G_{x_1,\dots,x_m}$ is finite.
- t will denote an element of $G \setminus C$ such that the divisor of t is of the form $\mathfrak{p}/\mathfrak{q}$, where $\mathfrak{p}$, $\mathfrak{q}$ are K primes of degree q^h for some rational prime number q and a natural number h. Further, $K/C_K(t)$ is separable and $q^h = n = [K : C_K(t)]$.
- $\tilde{C}_K = C_{\tilde{K}}$, where $\tilde{K} = \tilde{C}_K K$, will denote the algebraic closure of C_K.
- r will denote the number of primes ramifying in the extension $\tilde{C}_K K/\tilde{C}_K(t)$.
- $|C| \geq N(n+2r+5)$, where $N(n+2r+5)$ is a positive constant defined in the proof of Theorem 6.11, or C is infinite.
- C has an extension of degree q, where q is a rational prime possibly equal to p.
- x will denote a generator of G over $C(t)$. (Such a generator exists by Lemma 6.18 and our assumption that $K/C_K(t)$ is separable.)
- $c_0 = 0, c_1 \neq \pm 1, \dots c_{n+2r+5} \neq \pm 1$ will denote the elements of C such that for $i = 0, 1, \dots, n+2r+5$, the divisor of $t - c_i$ is of the form $\mathfrak{p}_i/\mathfrak{q}$, where $\mathfrak{p}_i$ is a prime divisor. For $i \neq j$, for any natural number s, $c_i^{p^s} \neq c_j$.
- For all i, $\mathfrak{P}_i$ will denote the prime of $C_K(t)$ lying below $\mathfrak{p}_i$, while $\mathfrak{P}$ and $\mathfrak{Q}$ will denote $C_K(t)$-primes below $\mathfrak{p}$ and $\mathfrak{q}$ respectively. For all i, $\mathfrak{P}_i$, $\mathfrak{P}$ and $\mathfrak{Q}$ do not split in the extension $K/C_K(t)$.
- r_i will denote the smallest positive integer such that $c_i^{p^{r_i}} = c_i$. We will let $d_{ij} = c_i^{p^j}, 0 \leq j \leq r_i$.

(The existence of an algebraic function field K over a sufficiently large or infinite field of constants containing t and $c_1, \dots, c_{2r+n+5}$ satisfying the conditions above follows from Theorem 6.11. In Section 5 of the paper we will give a fuller description of the class of fields satisfying our assumptions.)

2. P-th Power Equations: The case of $p = q$.

In this section we will show that over an algebraic function field K of characteristic $p > 0$, under some assumptions on the constant field, the set $p(K)$ is Diophantine. The method we are going to use has its origins in a paper

of Pheidas (see [26]). It was extended by the author to prove an analogous result for an algebraic function field over a *finite* field of constants. Unfortunately, in its original form, this extension cannot be used to prove the results pertaining to the algebraic function fields over infinite fields of constants, since it relied on the fact that the class numbers of global fields are finite. To prove the results mentioned above in our case, we will use the fact that under our assumptions on the constant field, the algebraic function field K will have a rational subextension of degree p^h.

Lemma 2.1. *Let F/G be a finite separable extension of fields of positive characteristic p. Let $\alpha \in F$ be such that all the coefficients of its monic irreducible polynomial over G are p-th powers in G. Then α is a p-th power in F.*

Proof. Let $a_0^p + \ldots + a_{m-1}^p T^{m-1} + T^m$ be the monic irreducible polynomial of α over G. Let β be the element of the algebraic closure of F such that $\beta^p = \alpha$. Then β is of degree at most m over G. On the other hand, $G(\alpha) \subseteq G(\beta)$. Therefore, $G(\alpha) = G(\beta)$.

Lemma 2.2. *Let F/G be a finite separable extension of fields of positive characteristic p. Let $[F : G] = n$. Let $x \in F$ be such that $F = G(x)$ and for distinct $a_0^p, \ldots, a_n^p \in G$, $\mathbf{N}_{F/G}(a_i^p - x) = y_i^p$. Then x is a p-th power in F.*

Proof. Let $H(T) = A_0 + A_1 T + A_{n-1} T^{n-1} + T^n$ be the monic irreducible polynomial of x over G. Then for $i = 0, \ldots, n$, $H(a_i^p) = y_i^p$. Further, we have the following linear system of equations:

$$\begin{pmatrix} 1 & a_0^p & \ldots & a_0^{p(n-1)} & a_0^{pn} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & a_n^p & \ldots & a_n^{p(n-1)} & a_n^{pn} \end{pmatrix} \begin{pmatrix} A_0 \\ \ldots \\ 1 \end{pmatrix} = \begin{pmatrix} y_0^p \\ \ldots \\ y_n^p \end{pmatrix}.$$

Using Cramer's rule to solve the system, it is not hard to conclude that for $i = 0, \ldots, n$, A_i is a p-th power in G. Then, by Lemma 2.1, x is a p-th power in F.

Lemma 2.3. *Let $w \in K$, let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ be primes of K and let $a_1, \ldots, a_{r+1} \in C$ be a set of distinct constants. Then the set $\{w + a_1, \ldots, w + a_{r+1}\}$ contains at least one element of K having no zero at any of the primes $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$.*

Proof. The lemma follows from the fact that each prime $\mathfrak{a}_i$ can be a zero of at most one element of the set $\{w + a_1, \ldots, w + a_{r+1}\}$.

Lemma 2.4. *Let $w \in K$, let $a, b \in C$. Then all the zeros of $\frac{w+a}{w+b}$ are zeros of $w + a$ and all the poles of $\frac{w+a}{w+b}$ are zeros of $w + b$. Further, the height of $\frac{w+a}{w+b}$ is equal to the height of w. (Here by height we mean the degree of zero or pole divisor of an algebraic function.)*

Proof. Let $\mathfrak{p}$ be a prime of K. Then $\mathfrak{p}$ is a pole w if and only if $\mathfrak{p}$ is a pole of $w+a$ and a pole of $w+b$. Moreover, the order of the pole at all the three functions will be the same. On the other hand, any zero of $\frac{w+a}{w+b}$ will come from zeros of $w+a$ or poles of $w+b$. So let $\mathfrak{p}$ be a pole of $w+b$. Then $\mathrm{ord}_{\mathfrak{p}}(w+a) = \mathrm{ord}_{\mathfrak{p}}(w+b)$ and therefore $\mathrm{ord}_{\mathfrak{p}}\frac{w+a}{w+b} = 0$. A similar argument shows that $\frac{w+a}{w+b}$ is a unit at any valuation which is a pole of $w+a$. Consequently, all zeros of $\frac{w+a}{w+b}$ are zeros of $w+a$ and all the poles of $\frac{w+a}{w+b}$ are zeros of $w+b$.

Finally, note that $\frac{w+a}{w+b} = 1 + \frac{a-b}{w+b}$. Let $H_K(\frac{w+a}{w+b})$ denote the K-height of $\frac{w+a}{w+b}$. Then we have the following equalities.

$$H_K\left(\frac{w+a}{w+b}\right) = H_K\left(1+\frac{a-b}{w+b}\right) = H_K\left(\frac{a-b}{w+b}\right) = H_K(w+b) = H_K(w).$$

The last equality follows from the fact, mentioned above, that the pole divisors of $w+b$ and w are the same.

Lemma 2.5. *Let $u, v, z \in \tilde{C}_K K = \tilde{K}$, let $y \in \tilde{C}_K(z)$, and assume y, z do not have zeros or poles at any valuation of $\tilde{K}$ ramifying in the extension $\tilde{K}/\tilde{C}_K(z)$. Further, assume*

$$y - z = u^p - u \tag{2.1}$$

$$y^{-1} - z^{-1} = v^p - v. \tag{2.2}$$

Then $y = z^{p^s}$, for some natural number $s \geq 0$. (Note that in $\tilde{C}_K(z)$, the zeros and the poles of z are simple. Assuming that z has no zeros or poles at any valuations ramifying in the extension $\tilde{K}/\tilde{C}_K(z)$ amounts, therefore, to assuming that all zeros and poles of z are simple in $\tilde{K}$.)

Proof. The argument below is very similar to the one used in [**26**, Lemma 1, pages 3-4], with the following difference. In this lemma we do not assume that u, v are rational functions in z over $\tilde{C}_K$ and therefore we will have to use the concept of local derivation with respect to a prime in place of the derivative defined in the usual manner on a rational function field. (For a discussion of local and global derivations see [**22**, pages 9-10] and [**13**, pages 144-148].) Let $\mathfrak{A}/\mathfrak{B}$ be the divisor of $z \in \tilde{K}$, where $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime integral divisors. Further, by assumption all the prime factors of $\mathfrak{A}$ and $\mathfrak{B}$ are distinct. Next note that all the poles of $v^p - v$ and $u^p - u$ in $\tilde{K}$ are of orders divisible by p. Since from the above discussion we know that all the zeros and poles of z are of orders equal to ± 1, we must conclude from (2.1) and (2.2) that the divisor of y is of the form $\mathfrak{U}^p\mathfrak{V}$, where all the prime factors of $\mathfrak{V}$ come from $\mathfrak{A}$ or $\mathfrak{B}$ and are distinct. Further, the factors of $\mathfrak{A}$ will appear to the first power in $\mathfrak{V}$; and the factors of $\mathfrak{B}$ will appear to the

power -1 in $\mathfrak{V}$. Indeed, let $\mathfrak{t}$ be a prime which is not a factor of $\mathfrak{A}$ or $\mathfrak{B}$. Without loss of generality assume $\mathfrak{t}$ is a pole of y. Then, since $\mathrm{ord}_{\mathfrak{t}} z = 0$,

$$0 > \mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}}(z - y) = \mathrm{ord}_{\mathfrak{t}}(u^p - u) \cong 0 \text{ modulo } p.$$

Now let $\mathfrak{t}$ be a factor of $\mathfrak{A}$ or $\mathfrak{B}$. Again, without loss of generality, assume that $\mathfrak{t}$ is a pole of y. If $\mathfrak{t}$ is a factor of $\mathfrak{A}$, then $\mathrm{ord}_{\mathfrak{t}}(y - z) = \mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}}(u^p - u)$. Since we assumed $\mathfrak{t}$ to be a pole of y, we must conclude that $\mathfrak{t}$ is a pole of u and thus $\mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}}(u^p - u) \cong 0$ modulo p. If, on the other hand, $\mathfrak{t}$ is a factor of $\mathfrak{B}$. Then we have two possibilities: $\mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}} z = -1$ or again $\mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}}(u^p - u) \cong 0$ modulo p.

On the other hand, since $y \in \tilde{C}_K(z)$, where $\mathfrak{A}$ and $\mathfrak{B}$ are prime divisors, we must conclude that the divisor of y is actually of the form $\mathfrak{U}^p \mathfrak{A}^a \mathfrak{B}^b$, with either $a, b = 0$ or $a = 1, b = -1$. (This follows from the observation that the degree of the zero and the pole divisor of y must be the same. In particular, the degrees must be equal modulo p.) If $a, b = 0$, taking into account the fact that no prime which is a pole or zero of y ramifies in the extension $\tilde{K}/\tilde{C}_K(z)$, we can conclude that the divisor of y in the rational field is also a p-th power of another divisor. Thus, since in the rational field every zero degree divisor is principal, y is a p-th power. Suppose, on the other hand that $a = 1, b = -1$. Then we can conclude using an argument similar to the one above, that yz^{-1} is a p-th power in the rational field. Thus, (2.1) can be rewritten as

$$z(f - 1)^p = u^p - u, \tag{2.3}$$

where $f \in \tilde{C}_K(z)$. Since $f - 1$ is a rational function in z, we can further rewrite (2.3) as

$$z(f_1^p / f_2^p) = u^p - u, \tag{2.4}$$

where f_1, f_2 are relatively prime polynomials in z over $\tilde{C}$ and f_2 is monic. From this equation it is clear that any valuation which is a pole of u, is either a pole of z or a zero of f_2. Further, the absolute value of the order of any pole of u at any valuation which is a zero of f_2, must be the same as the order of f_2 at this valuation. Therefore, $s = f_2 u$ will have poles only at the valuations which are poles of z. Thus we can rewrite (2.4) in the form

$$-z f_1^p + s^p = s f_2^{p-1}.$$

Let $\mathfrak{c}$ be a zero of f_2. Then, since f_2 is a polynomial in z, $\mathfrak{c}$ is not a pole of z. Since, $p - 1 \geq 2$, s is integral over $\tilde{C}_K[z], \mathrm{ord}_{\mathfrak{c}}(s^p - z f_1^p) \geq 2$.

In general, for any $x \in \tilde{K}$ and any $\tilde{K}$-prime $\mathfrak{a}$, let $\partial x / \partial \mathfrak{a}$ denote the local derivative of x with respect to $\mathfrak{a}$. Further, if x has a zero at $\mathfrak{a}$ of order greater than 1, then $\partial x / \partial \mathfrak{a}$ will have a zero at $\mathfrak{a}$. Now observe that

$$\mathrm{ord}_{\mathfrak{c}} \partial(-z f_1^p + s^p)/\partial \mathfrak{c} = \mathrm{ord}_{\mathfrak{c}} \frac{d(-z f_1^p + s^p)}{dz} = \mathrm{ord}_{\mathfrak{c}}(-f_1^p),$$

by Lemma 6.17, since, by assumption f_2 does not have any zeros at valuations ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$. Thus, f_1 has a zero at $\mathfrak{c}$. But f_1 and f_2 are supposed to be relatively prime polynomials. Hence, f_2 does not have any zeros, and thus is equal to 1. Therefore, y is a polynomial in z. Similarly, we can show that $1/y$ is a polynomial in $1/z$. Hence, y is a power of z, and more specifically, unless $y = z$, y must be a power of z divisible by p. If $y = z$ we are done. Otherwise, we have shown that y is a p-th power of another rational function in z over $\tilde{C}_K$. From this point on, the proof of the lemma proceeds in the fashion identical to the proof which can be found in [**26**, Lemma 1, pages 3, 4].

Lemma 2.6. *Let* w, u, u_{i,j_i,k,j_k}, v_{i,j_i,k,j_k}, $i,k = 0,\dots,(r+n+2)$, $j_i = 1,\dots,r_i$, $j_k = 1,\dots,r_k$ *be elements of* K *satisfying the following equations for all* $i,k = 0,\dots,(r+n+2)$, *and some* $1 \le j_i \le r_i$, $1 \le j_k \le r_k$.

$$w - t = u^p - u \tag{2.5}$$

$$w^{-1} - t^{-1} = v^p - v \tag{2.6}$$

$$w_{i,j_i,k,j_k} = \frac{w - d_{i,j_i}}{w - d_{k,j_k}}, \tag{2.7}$$

$$t_{i,k} = \frac{t - c_i}{t - c_k} \tag{2.8}$$

$$w_{i,j_i,k,j_k} - t_{i,k} = u^p_{i,j_i,k,j_k} - u_{i,j_i,k,j_k} \tag{2.9}$$

$$\frac{1}{w_{i,j_i,k,j_k}} - \frac{1}{t_{i,k}} = v^p_{i,j_i,k,j_k} - v_{i,j_i,k,j_k}. \tag{2.10}$$

Then $w = t^{p^s}$ *for some natural number* $s \ge 0$.

Proof. First of all note that $\mathfrak{Q}$, and $\mathfrak{P}_i$ for all i will remain prime in the extension $\tilde{C}_K(t)/C_K(t)$ and their factors will be unramified in the extension $\tilde{K}/\tilde{C}_K$. Indeed, the first assertion is true because all the listed primes are of degree one in $C_K(t)$ and thus will remain prime under any constant field extension. The second assertion is true by Lemma 6.16. Thus, for all i,k, $t_{i,k}$ has neither zeros nor poles at any prime ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$.

Next we note that by Lemma 2.3, for some $i = 0,\dots,(n+r+2)$ there exist distinct $k_1,\dots,k_{n+1} \in \{0,\dots,(r+n+2)\} \setminus \{i\}$ such that for any $1 \le j_i \le r_i, 1 \le j_{k_l} \le r_{k_l}, w_{i,j_i,k_l,j_{k_l}}, l = 1,\dots,n+1$ does not have zeros or poles at any prime ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$. Indeed, we can select the required indices in the following manner. First consider the set $\{w - d_{i,j_i}, i = 0,\dots,n+r+2, 1 \le j_i \le r_i\}$. Note, that by assumption, for all $(i,j_i), d_{i,j_i}$ is a constant and all these constants are distinct. Let $\{m_u, u = 1\dots,s\}$ be the set of all the elements of the set $\{0,\dots,n+r+2\}$ such that for some j_{m_u} in the set $\{1,\dots,r_{m_u}\}$, $w - d_{m_u,j_{m_u}}$ has a zero at a valuation of $\tilde{K}$ ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$. Then by Lemma

2.3, $s \leq r$. Therefore, the set $\{0, \dots, n+r+2\} \setminus \{m_1, \dots, m_s\}$ contains at least $n+3$ elements. Choose i in this set. Finally choose $k_1, \dots, k_{n+1}$ in the set $\{0, \dots, n+r+2\} \setminus \{m_1, \dots, m_s, i\}$, containing at least $n+2$ elements. Next consider, $w_{i,j_i,k_l,j_{k_l}} = \frac{w-d_{i,j_i}}{w-d_{k_l,j_{k_l}}}$, where $1 \leq j_i \leq r_i, k_l \in \{0, \dots, n+r+2\} \setminus \{m_1, \dots, m_s, i\}, 1 \leq j_{k_l} \leq r_{k_l}$. Note that neither numerator, nor denominator of this fraction has a zero at a valuation ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$. Thus, by Lemma 2.4, $w_{i,j_i,k_l,j_{k_l}}$ has no zeros or poles at any valuation ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$.

If $w \in C_K(t)$ then we can apply Lemma 2.5 to conclude that our lemma is true. Thus, we may assume $w \notin C_K(t)$. This would imply that $w_{i,j_i,k_l,j_{k_l}} \notin C_K(t)$ for all i, j_i, k_l, j_{k_l} Further, by an argument similar to the one used in the proof of Lemma 2.5, for all $l = 1, \dots, n+1$, Equations (2.9) and (2.10) imply that for some j_i, j_{k_l} the divisor of $w_{i,j_i,k_l,j_{k_l}}$ is of the form $\mathfrak{A}^p \mathfrak{p}_{k_l}^a \mathfrak{p}_i^b$, where a is either -1 or 0 and b is either 1 or 0. Let $K_w = C_K(w,t)$, and note that for all $i, k, j_i, j_k, w_{i,j_i,k,j_k} \in K_w$ and $[K_w : C_K(t)] = p^m$, where $0 < m \leq h$. (The left inequality is strict due to our assumption that $w \notin C_K(t)$.) Further, since for all $l = 1, \dots, n+1, w_{i,j_i,k_l,j_{k_l}}$ does not have any zeros or poles ramifying in the extension $K/C_K(t)$, the divisor of $w_{i,j_i,k_l,j_{k_l}}$ will be of the form $\mathfrak{A}_{K_w}^p \mathfrak{P}_{i,w}^a \mathfrak{P}_{k_l,w}^b$ in K_w, where $\mathfrak{A}_{K_w}$ is the K_w-divisor below the divisor $\mathfrak{A}$, and for all i, $\mathfrak{P}_{i,w}$ denotes the prime below $\mathfrak{p}_i$ in $C_K(t,w)$. Next we note that for all $l = 1, \dots, n+1$ the divisor of $\mathbf{N}_{K_w/C_K(t)}(w_{i,j_i,k_l,j_{k_l}})$ is equal to the corresponding norm of the divisor of $w_{i,j_i,k_l,j_{k_l}}$. On the other hand,

$$\mathbf{N}_{K_w/C_K(t)} \mathfrak{P}_{i,w} = \mathfrak{P}_i^{f(\mathfrak{P}_{i,w}/\mathfrak{P}_i)} = \mathfrak{P}_i^{p^m}.$$

Thus, for all $l = 1, \dots, n+1$, the divisor of the norm of $w_{i,j_i,k_l,j_{k_l}}$ in $C_K(t)$ is a p-th power of some other divisor of $C_K(t)$. Since in $C_K(t)$ every zero degree divisor is principal, we must conclude that for all $l = 1, \dots, n+1$, the $K/C_K(t)$ norm of $w_{i,j_i,k_l,j_{k_l}}$ is a p-th power of some element of $C_K(t)$. On the other hand,

$$\begin{aligned} w_{i,j_i,k_l j_{k_l}}^{-1} &= \frac{w - d_{k_l,j_{k_l}}}{w - d_{i,j_i}} = 1 + \frac{d_{i,j_i} - d_{k_l,j_{k_l}}}{w - d_{i,j_i}} \\ &= (d_{i,j_i} - d_{k_l,j_{k_l}}) \left(\frac{1}{d_{i,j_i} - d_{k_l,j_{k_l}}} - \frac{1}{d_{i,j_i} - w} \right). \end{aligned}$$

Thus, we can conclude that for $l = 1, \dots, n+1$,

$$\mathbf{N}_{K_w/C_K(t)} \left(\frac{1}{d_{i,j_i} - d_{k_l,j_{k_l}}} - \frac{1}{d_{i,j_i} - w} \right)$$

is a p-th power. Then, by Lemma 2.2, taking into account our assumption that for all natural numbers s, for $r \neq j, c_r^{p^s} \neq c_j$, we can conclude that $w - d_{i,j_i}$ is a p-th power in K. Consequently, w is a p-th power in K. Thus, $w = \tilde{w}^p$ for some $\tilde{w} \in K$. Next observe the following.

$$w_{i,j_i,k,j_k} = \frac{w - d_{i,j_i}}{w - d_{k,j_k}} = \frac{w - c_i^{p^{j_i}}}{w - c_k^{p^{j_k}}} = \left(\frac{\tilde{w} - c_i^{p^{m_i}}}{\tilde{w} - c_k^{p^{m_k}}}\right)^p = (\tilde{w}_{i,m_i,k,m_k})^p,$$

where $m_i = j_i - 1, m_k = j_k - 1$, if $j_k, j_i > 1$ and $m_i = r_i, m_k = r_k$, if $j_k = 1, j_i = 1$. Note that since for all k, j_k took all values $1, \ldots, r_k$, the same will be true of m_k. Thus Equations (2.9) and (2.10) can be rewritten in the following manner.

$$\tilde{w}_{i,m_i,k,m_k} - t_{i,k} = (u^p_{i,j_i,k,j_k} - \tilde{w}^p_{i,m_i,k,m_k}) - (u_{i,j_i,k,j_k} - \tilde{w}_{i,m_i,k,m_k}), \tag{2.11}$$

$$\frac{1}{\tilde{w}_{i,m_i,k,m_k}} - \frac{1}{t_{i,k}} = \left(v^p_{i,j_i,k,j_k} - \frac{1}{\tilde{w}^p_{i,m_i,k,m_k}}\right) - \left(v_{i,j_i,k,j_k} - \frac{1}{\tilde{w}_{i,m_i,k,m_k}}\right), \tag{2.12}$$

where $1 \leq m_i \leq r_i, 1 \leq m_k \leq r_k$. Equations (2.5) and (2.6) can be rewritten in a similar fashion. Therefore, the previous argument applies to $\tilde{w}$. Note also that the height of $\tilde{w}$ is strictly less than the height of w. Thus after finitely many iterations of this process, we will find ourselves in a situation where (2.5) and (2.6) hold for a $\bar{w} \in K$, whose height is less or equal to the height of t. This would imply that the divisor of $\bar{w}$ and t are the same. In other words, $\bar{w} = at$, where a is a constant. Thus, $(a-1)t = u^p - u$. However, unless $a = 1$, we have a contradiction. Therefore, if we assume that the height of $\bar{w}$ is less or equal to the height of t, we must conclude that $\bar{w} = t$. Consequently, for some natural number s, $w = t^{p^s}$.

Corollary 2.7. *The set* $\{w \in K | \exists s \in \mathbb{N},\ w = t^{p^s}\}$ *is Diophantine over* K.

Proof. First we note that for any $x \in K$ and any $s \in \mathbb{N}$

$$x^{p^s} - x = (x^{p^{s-1}} + x^{p^{s-2}} + \cdots + x)^p - (x^{p^{s-1}} + x^{p^{s-2}} + \cdots + x). \tag{2.13}$$

Next we want to show that assuming $w = t^{p^s}$, Equations (2.5)-(2.10) can be satisfied over K. In view of equality (2.13), it is enough to show that for some $1 \leq j_i \leq r_i, 1 \leq j_k \leq r_k$, $w_{i,j_i,k,j_k} = (t_{i,k})^{p^s}$. Choose $j_i \cong s$ modulo r_i. (Such a j_i exists since the set of all possible values of j_i contains a representative of every class modulo r_i.) Then $c_i^{p^s} = (c_i^{p^{j_i}})^{p^{mr_i}} = c_i^{p^{j_i}}$. Similarly, choose $j_k \cong s$ modulo r_k so that $c_k^{p^s} = c_k^{p^{j_k}}$. Now the desired conclusion follows from Equations (2.7) and Equations (2.8).

Lemma 2.8. *Let $\sigma, \mu \in K$. Assume that all the primes that are poles of σ or μ do not ramify in the extension $\tilde{K}/\tilde{C}_K(t)$. Further, assume the following equality is true.*

$$t(\sigma^p - \sigma) = \mu^p - \mu. \tag{2.14}$$

Then $\sigma^p - \sigma = \mu^p - \mu = 0$.

Proof. Let $\mathfrak{A}$, $\mathfrak{B}$ be integral divisors of K, relatively prime to each other and to $\mathfrak{p}$ and $\mathfrak{q}$, such that the divisor of σ is of the form $\frac{\mathfrak{A}}{\mathfrak{B}}\mathfrak{p}^i\mathfrak{q}^k$, where i, k are integers. Then it is not hard to see that for some integral divisor $\mathfrak{C}$, relatively prime to $\mathfrak{B}$, $\mathfrak{p}$ and $\mathfrak{q}$, some integers j, m, the divisor of μ is of the form $\frac{\mathfrak{C}}{\mathfrak{B}}\mathfrak{p}^j\mathfrak{q}^m$. Indeed, let $\mathfrak{t}$ be a pole of μ such that $\mathfrak{t} \neq \mathfrak{p}$ and $\mathfrak{t} \neq \mathfrak{q}$. Then

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

Conversely, let $\mathfrak{t}$ be a pole of σ such that $\mathfrak{t} \neq \mathfrak{p}$ and $\mathfrak{t} \neq \mathfrak{q}$. Then

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

By the Strong Approximation Theorem there exists $b \in K$ such that the divisor of b is of the form $\mathfrak{B}\mathfrak{D}/\mathfrak{q}^l$, where $\mathfrak{D}$ is an integral divisor relatively prime to $\mathfrak{A}, \mathfrak{C}, \mathfrak{p}, \mathfrak{q}$ and l is a natural number. Then $b\sigma = s_1 t^i, b\mu = s_2 t^j$, where s_1, s_2 are integral over $C_K[t]$ and have zero divisors relatively prime to $\mathfrak{p}$ and $\mathfrak{B}$. Indeed, consider the divisors of $b\sigma$:

$$\frac{\mathfrak{B}\mathfrak{D}}{\mathfrak{q}^l}\frac{\mathfrak{A}}{\mathfrak{B}}\mathfrak{p}^i\mathfrak{q}^k = \mathfrak{D}\mathfrak{A}\mathfrak{p}^i\mathfrak{q}^{k-l} = \mathfrak{D}\mathfrak{A}\mathfrak{q}^{k-l+i}\frac{\mathfrak{p}^i}{\mathfrak{q}^i}.$$

Thus the divisor of s_1 is of the form $\mathfrak{D}\mathfrak{A}\mathfrak{q}^{k-l+i}$ and therefore, $\mathfrak{q}$ is the only pole of s_1, making it integral over $C_k[t]$. 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 through by b^p we will obtain the following equation.

$$t(s_1^p t^{ip} - b^{p-1}s_1 t^i) = s_2^p t^{jp} - b^{p-1}s_2 t^j. \tag{2.15}$$

Suppose $i < 0$. Then the left side of (2.15) has a pole of order $ip + 1$ at $\mathfrak{p}$. This would imply that $j < 0$ and the right side has a pole of order jp at $\mathfrak{p}$. Thus, we can assume that i, j are both nonnegative. We can now rewrite (2.15) in the form

$$(s_1^p t^{ip+1} - s_2^p t^{jp}) = b^{p-1}(s_1 t^{i+1} - s_2 t^j). \tag{2.16}$$

Let $\mathfrak{t}$ be any prime factor of $\mathfrak{B}$ in $\tilde{K}$. Then $\mathfrak{t}$ does not ramify in the extension $\tilde{K}/C_{\tilde{K}}(t)$ and since $p > 2$, $\mathrm{ord}_{\mathfrak{t}}(s_1^p t^{ip+1} - s_2^p t^{jp}) \geq 2$. Thus, $\mathrm{ord}_{\mathfrak{t}}\partial(s_1^p t^{ip+1} - s_2^p t^{jp})/\partial\mathfrak{t} > 0$. Since $\mathfrak{t}$ is not ramified in the extension $\tilde{K}/C_{\tilde{K}}(t)$, by Lemma 6.17, $\mathrm{ord}_{\mathfrak{t}}\partial(s_1^p t^{ip+1} - s_2^p t^{jp})/\partial\mathfrak{t} = \mathrm{ord}_{\mathfrak{t}}d(s_1^p t^{ip+1} - s_2^p t^{jp})/dt = \mathrm{ord}_{\mathfrak{t}}(s_1^p t^{ip})$. Therefore, since $\mathfrak{t}$, by assumption is not a zero of t, s_1 has a zero at $\mathfrak{t}$. This, however, is impossible. Consequently, $\mathfrak{B}$ is a trivial divisor, and in (2.14)

all the functions are integral over $C_K[t]$, i.e., they can have poles at $\mathfrak{q}$ only. Assuming μ is not a constant and thus has a pole at $\mathfrak{q}$, we note that the left side has a pole at $\mathfrak{q}$ of order equivalent to 1 modulo p, while the right side has the pole $\mathfrak{q}$ of order equivalent to 0 modulo p. Thus, μ is a constant. But the only way the product of t and a function integral over $C_K[t]$ can be a constant is for that function to be equal to zero. Consequently, the statement of the lemma is true.

Lemma 2.9. *Let $v \in K$ and assume for some distinct $a_0 = 0, a_1, \ldots, a_n \in C_K$, the divisor of $v + a_0, \ldots, v + a_n$ is a p-th power of some other divisor of K. Then, assuming for all i, $v + a_i$ does not have any zeros or poles at any prime ramifying in the extension $K/C_K(t)$, v is a p-th power in K.*

Proof. First assume $v \in C_K(t)$. Since $v + a_i$ does not have any zeros or poles at primes ramifying in the extension $K/C_K(t)$, the divisor of $v + a_i$ in $C_K(t)$ is a p-th power of another $C_K(t)$ divisor. Since in $C_K(t)$ every zero degree divisor is principal, v is a p-th power in $C_K(t)$ and therefore in K. Next assume $v \notin C_K(t)$. Note that no zero or pole of $v + a_i$ is at any valuation ramifying in the extension $K/C_K(t, v)$. Hence, in $C_K(t, v)$ the divisor of $v + a_i$ is also a p-th power of another divisor. Finally note that $\mathbf{N}_{C_K(t,v)/C_K(t)}(v + a_i)$ will be a p-th power in $C_K(t)$ and apply Lemma 2.2.

Lemma 2.10. *Let $x, v \in K \setminus \{0\}$, let $u = \frac{x^p+t}{x^p-t}$. Further, assume that the following equations hold for all $i, k = 0, \ldots, (2r + n + 5)$, some $1 \leq j_i \leq r_i, 1 \leq j_k \leq r_k$, and some $s \geq 0$.*

$$u_{i,k,g} = \frac{u^g + c_i}{u^g + c_k}, g = -1, 1. \tag{2.17}$$

$$v_{i,j_i,k,j_k,g} = \frac{v^g + d_{i,j_i}}{v^g + d_{k,j_k}}, g = -1, 1. \tag{2.18}$$

$$v_{i,j_i,k,j_k,g}^{2e} t^{mp^s} - u_{i,k,g}^{2e} t^m = \mu_{i,j_i,k,j_k,e,m,g}^p - \mu_{i,j_i,k,j_k,e,m,g}, \quad e = -1, 1, m = 0, 1, g = -1, 1. \tag{2.19}$$

$$v_{i,j_i,k,j_k,g}^e - u_{i,k,g}^e = \sigma_{i,j_i,k,j_k,e,g}^p - \sigma_{i,j_i,k,j_k,e,g}, e = -1, 1, g = -1, 1. \tag{2.20}$$

$$(u^g + c_i)^e - (v^g + d_{i,j_i})^e = \mu_{i,j_i,e,g}^p - \mu_{i,j_i,e,g}, e = -1, 1, g = -1, 1. \tag{2.21}$$

Then for some natural number k, $v = u^{p^k}$.

Proof. First of all, we claim that for all i, k, g, $u_{i,k,g}$ has no multiple zeros or poles except possibly at the primes ramifying in $\tilde{K}/\tilde{C}_K(t)$, $\mathfrak{p}$ or $\mathfrak{q}$. Indeed, by Lemma 2.4, all the poles of $u_{i,k,g}$ are zeros of $u^g + c_k$ and all the zeros of $u_{i,k,g}$ are zeros $u^g + c_i$. However, by Lemma 4.5 of [38] and by assumption on c_i and c_k, all the zeros of $u^g + c_k$ and $u^g + c_i$ are simple, except possibly

for zeros at $\mathfrak{p}$, $\mathfrak{q}$, or primes ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$. For future use, we also note that u is not a p-th power in K, assuming $x \neq 0$. (This can be established by computing the derivative of u, which is not 0, if x is not 0.) We will show that if $s > 0$ then v is a p-th power in K, and if $s = 0$ then $u = v$. Suppose $s > 0$ and let $g = 1$. Next note that by Lemma 2.3, by an argument similar to the one used in Lemma 2.6, there exist $0 \leq i \leq (2r+5+n), 0 \leq k_l \leq (2r+n+5), l = 1, \dots, n+1, k_l \neq i, k_l \neq k_m$ for $m \neq l$, such that for all $1 \leq j_i \leq r_i, 1 \leq j_{k_l} \leq r_{k_l}$, $u_{i,k_l,1}$ and $v_{i,j_i,k_l,j_{k_l},1}$ have no zeros or poles at the primes of $\tilde{K}$ ramifying in the extension $\tilde{K}/\tilde{C}(t)$, or $\mathfrak{p}$ or $\mathfrak{q}$. Note that for thus selected indices, all the poles and zeros of $u_{i,k_l,1}$ are simple for $l = 1, \dots, n+1$.

Pick an $i, k_1, \dots, k_{n+1}, j_i, j_{k_1}, \dots, j_{k_{n+1}}$ such that Equations (2.17)-(2.21) are satisfied for these indices and $u_{i,k_1,1}, v_{i,j_i,k_1,j_{k_1},1}, \dots, u_{i,k_{n+1},1}$, $v_{i,j_i,k_{n+1},j_{k_{n+1}},1}$ have no poles or zeros at primes ramifying in the extension $\tilde{K}/\tilde{C}(t)$, or at $\mathfrak{p}$ or $\mathfrak{q}$. Further, by an argument similar to the one used in the proof of Lemma 2.5, either for $l = 1, \dots, n+1$, the divisor of $v_{i,j_i,k_l,j_{k_l},1}$ in $\tilde{K}$ is a p-th power of another divisor or for some l and some prime $\mathfrak{t}$ not ramifying in $\tilde{K}/\tilde{C}(t)$ and not equal to $\mathfrak{p}$ or to $\mathfrak{q}$, $\mathrm{ord}_{\mathfrak{t}} v_{i,j_i,k_l,j_{k_l},1} = \pm 1$. In the first case, given the assumption that $v_{i,j_i,k_l,j_{k_l},1}$'s do not have poles or zeros at ramifying primes and Lemma 2.9, v is a p-th power in K. So suppose the second alternative holds. In this case, without loss of generality, assume $\mathfrak{t}$ is a pole of $v_{i,j_i,k_l,j_{k_l},1}$. Next consider the following equations

$$v^2_{i,j_i,k_l,j_{k_l},1} t^{p^s} - u^2_{i,k_l,1} t = \mu^p_{i,j_i,k_l,j_{k_l},1,1,1} - \mu_{i,j_i,k_l,j_{k_l},1,1,1}, \tag{2.22}$$

$$v^2_{i,j_i,k_l,j_{k_l},1} - u^2_{i,k_l,1} = \mu^p_{i,j_i,k,j_k,0,1,1} - \mu_{i,j_i,k,j_k,0,1,1}, \tag{2.23}$$

obtained from (2.19) by first making $e = 1, m = 1$ and then $e = 1, m = 0$. (If $\mathfrak{t}$ were a zero of $v_{i,j_i,k_l,j_{k_l},1}, e$ would be equal to -1 in both equations.) Since t does not have a pole or zero at $\mathfrak{t}$ and $p > 2$, we must conclude that

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

and

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

Thus,

$$\begin{aligned}
&\mathrm{ord}_{\mathfrak{t}} v^2_{i,j_i,k_l,j_{k_l},1}(t^{p^s} - t) \\
&= \mathrm{ord}_{\mathfrak{t}}(\mu^p_{i,j_i,k_l,j_{k_l},1,1,1} - \mu_{i,j_i,k_l,j_{k_l},1,1,1} - t\mu^p_{i,j_i,k_l,j_{k_l},0,1,1} + t\mu_{i,j_i,k_l,j_{k_l},0,1,1}) \\
&\geq 0.
\end{aligned}$$

Finally, we must deduce that $\mathrm{ord}_{\mathfrak{t}}(t^{p^s} - t) \geq 2|\mathrm{ord}_{\mathfrak{t}} v|$. But in $C_K(t)$ all the zeros of $(t^{p^s} - t)$ are simple. Thus, this function can have multiple zeros only

at primes ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$. By assumption $\mathfrak{t}$ is not one of these primes and thus we have a contradiction, unless v is a p-th power.

Suppose now that $s = 0$. Set $g = 1$ again and let $i, k_1, \dots, k_{n+1}$ be selected as above. Then from (2.22) and (2.23) we obtain

$$\mu^p_{i,j_i,k,j_k,1,1,1} - \mu_{i,j_i,k,j_k,1,1} = t(\mu^p_{i,j_i,k,j_k,0,1,1} - \mu_{i,j_i,k,j_k,0,1,1}).$$

Note here that all the poles of $\mu_{i,j_i,k,j_k,1,1,1}$ and $\mu_{i,j_i,k,j_k,0,1,1}$ are poles of $u_{i,k_l,1}, v_{i,j_i,k_l,j_{k_l},1}$ or t, and thus are not any valuation ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$. By Lemma 2.8 we can then conclude that

$$v^2_{i,j_i,k_l,j_{k_l},1} - u^2_{i,k_l,1} = 0.$$

Thus, $v_{i,j_i,k_l,j_{k_l},1} = \pm u_{i,k_l,1}$. Since all the poles of $u_{i,k_l,1}$ are simple, (2.20) with $k = k_l$ rules out "$-$". Therefore,

$$v_{i,j_i,k_l,j_{k_l},1} = u_{i,k_l,1}. \tag{2.24}$$

Rewriting (2.24) we obtain

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

or

$$v = au + b, \tag{2.25}$$

where a, b are constants.

Now keep $s = 0$, set $g = -1$, pick new distinct $i, k_1, \dots, k_{n+1}$ such that $u_{i,k_l,-1}, v_{i,j_i,k_l,j_{k_l},-1}, l = 1, \dots, n+1$ do not have any zeros or poles at valuations ramifying in the extension $\tilde{K}/\tilde{C}_K(t)$, at $\mathfrak{p}$ or $\mathfrak{q}$. Repeat the argument above (with $s = 0$) for $g = -1$ to conclude that

$$v^{-1} = \bar{a}u^{-1} + \bar{b}, \tag{2.26}$$

where $\bar{a}, \bar{b}$ are also constants. Equation (2.25) stipulates that u and v have the same poles. If $\bar{b} \neq 0$, then (2.26) stipulates that u and v have no poles in common. Since u is not constant, and therefore, v is not constant, we must deduce that $\bar{b} = 0$ and $u = av$ for some constant a. If $a \neq 1$, from (2.21), we conclude, using $g = 1$ for all i, that all the zeros of $u + c_i$ are of order divisible by p. Indeed, consider $\frac{1}{u+c_i}$ and $\frac{1}{u+a^{-1}d_{i,j}}$. Either $ac_i = c_i^{p_{j_i}} = d_{i,j_i}$ and

$$\frac{1}{u + c_i} - \frac{1}{v + d_{i,j_i}} = \frac{1}{u + c_i} - a^{-1}\frac{1}{u + c_i} = (1 - a^{-1})/(u + c_i),$$

or $u + c_i$ and $v + d_{i,j_i} = au + d_{i,j_i}$ have no common zeros, and $\frac{1}{u+c_i} - \frac{1}{v+d_{i,j_i}}$ has poles at all the valuations at which $\frac{1}{u+c_i}$ has poles, and these poles are of the same order as the poles of $\frac{1}{u+c_i}$. Since this cannot happen, $a = 1$.

If $s > 0$ and v is a p-th power, then Equations (2.18)-(2.21) can be rewritten in the same fashion as equations in Lemma 2.6 with s being replaced by $s-1$ and v replaced by its p-th root. Therefore, after finitely many iterations of this rewriting procedure we will be in the case of $s = 0$. Hence, for some natural number k, $v = u^{p^k}$.

Corollary 2.11. *Let $x \in K$, and let $u = \frac{x^p+t}{x^p-t}$. Then the set $\{w \in K \| \exists s \in \mathbb{N},\ w = u^{p^s}\}$ is Diophantine over K.*

Proof. Given Lemma 2.10, it is enough to show that if $w = u^{p^s}$ for some natural number s, Equations (2.17) - (2.21) can be satisfied in the remaining variables over K. The proof of this assertion is identical to the proof of Corollary 2.7.

Finally we state the main result of this section.

Theorem 2.12. *The set $\{(x, y) \in K^2 \| \exists s \in \mathbb{N},\ y = x^{p^s}\}$ is Diophantine over K.*

Given Corollaries 2.7 and 2.11, the proof of this theorem will be identical to the proof of Theorem 5.12 of [**38**].

3. Integrality at One Prime: The case of $q = p$.

In this section we will show that integrality at one prime is a Diophantine condition over an algebraic function field of characteristic $p > 0$ whose constant field has an extension of degree $p > 0$.

Lemma 3.1. *Let L be a local field or an algebraic function field of positive characteristic p. Let $v \in L$ and let α be a root of the equation*

$$x^p - x - v = 0. \tag{3.1}$$

Then either $\alpha \in L$ or α is of degree p over L. Further, in the second case the extension $L(\alpha)/L$ is cyclic of degree p and the only primes possibly ramified in this extension are the poles of v. On the other hand, if for some L-prime $\mathfrak{a}$, $\mathrm{ord}_{\mathfrak{a}} v \not\cong 0$ modulo p and $\mathrm{ord}_{\mathfrak{a}} v < 0$, then a factor of $\mathfrak{a}$ in $L(\alpha)$ will be ramified completely.

Proof. Let $\alpha = \alpha_1, \ldots, \alpha_p$ be all the roots of (3.1) in the algebraic closure of L. Then we can number the roots so that $\alpha_i = \alpha + i - 1$. Thus, either the left side of (3.1) factors completely or it is irreducible. In the second case α is of degree p over L and $L(\alpha)$ contains all the conjugates of α over L. Thus, the extension $L(\alpha)/L$ is Galois of degree p, and therefore is cyclic. Next consider the different of α. This different is a constant. By [**3**, Lemma 2, page 71], this implies that no prime of L at which α is integral has any ramified factors in the extension $L(\alpha)/L$. Finally, suppose $\mathfrak{a}$ is a prime of L described in the statement of the lemma. Let $\tilde{\mathfrak{a}}$ be an $L(\alpha)$ prime above $\mathfrak{a}$. Then $\mathrm{ord}_{\tilde{\mathfrak{a}}} v \cong 0$ modulo p. Thus, $\tilde{\mathfrak{a}}$ must be totally ramified over $\mathfrak{a}$.

Lemma 3.2. *Let M/K be a Galois extension of algebraic function fields of degree n. Let $\mathfrak{p}$ be a prime of K which does not split in M. Let $h \in K$ be such that $\operatorname{ord}_{\mathfrak{p}} h \not\equiv 0$ modulo n. Then h is not a norm of an element of M.*

Lemma 3.3. *Let H/F be an unramified extension of local fields of degree n. Let $\mathfrak{t}$ be the prime of F. Let $x \in F$ be such that $\operatorname{ord}_{\mathfrak{t}} x \cong 0$ modulo n. Then x is a norm of some element of H.*

Proof. Let π be a local uniformizing parameter for $\mathfrak{t}$. Then $x = \pi^n \varepsilon$, where ε is a unit. Since π^n is an F-norm, x is an F-norm if and only if ε is an F norm. The last statement is true by [**42**, Corollary, page 226].

Lemma 3.4. *Let L be an algebraic function field. Let $\mathfrak{C}$ and $\mathfrak{B}$ be prime divisors of L. Let $v \in L$ be such that the divisor of v is of the form $\mathfrak{C}^{-1}\mathfrak{V}$, where $\mathfrak{V}$ is a divisor of L which has no common factors with $\mathfrak{C}$ or $\mathfrak{B}$. Further, assume v is equivalent to $b^p - b$ modulo $\mathfrak{B}$, where $b \in C_L$, the constant field of L. (Such a v exists by the Weak Approximation theorem.) Let β be a root of (3.1). Let $R_{\mathfrak{B}}$ be the residue field of $\mathfrak{B}$ in L and assume it is separable over C_L. Let δ be an element of the algebraic closure of C_L, such that $C_L(\delta)$ is isomorphic to the Galois closure of $R_{\mathfrak{B}}$ over C_L. Let $\bar{L} = L(\beta, \delta)$. Then in $\bar{L}$,*

$$\mathfrak{C} = \prod \mathfrak{c}_i^p, \tag{3.2}$$

and

$$\mathfrak{B} = \prod \mathfrak{b}_i, \tag{3.3}$$

where for $i \neq j$, $\mathfrak{b}_i \neq \mathfrak{b}_j$, $\mathfrak{c}_i \neq \mathfrak{c}_j$, and for all i, $\mathfrak{b}_i$ is of degree 1.

Proof. By Lemma 3.1, $[L(\beta) : L] = p$, and the prime above $\mathfrak{C}$ in $L(\beta)$ is totally ramified. Thus, in $L(\beta)$, $\mathfrak{C} = \mathfrak{c}^p$. Note that by Lemma 3.1, $\mathfrak{B}$ does not have ramifying factors in the extension $L(\beta)/L$. On the other hand, the left side of (3.1) will factor completely modulo $\mathfrak{B}$. Since all the coefficients of the left side (3.1) are integral at $\mathfrak{B}$ and $\mathfrak{B}$ is not a zero of the discriminant of this polynomial, β generates a local integral basis with respect to $\mathfrak{B}$. Thus the fact that left side of (3.1) will factor completely modulo $\mathfrak{B}$ implies that $\mathfrak{b}$ will split completely in $L(\beta)$. Thus, the residue fields of the factors of $\mathfrak{B}$ in $L(\beta)$ are the same as the residue field of $\mathfrak{B}$ in L. Next note that the constant fields of L and $L(\beta)$ are the same because $\mathfrak{C}$ has a completely ramified factor in this separable extension. Hence the residue fields of the factors of $\mathfrak{b}$ in $L(\beta)$ are separable over $C_{L(\beta)} = C_L$. Consequently, we can apply Lemma 6.14 to assert that in $L(\beta, \delta)$ all the factors of $\mathfrak{b}$ will be of degree 1. Finally we note that no factor of $\mathfrak{b}$ is ramified in the extension $L(\beta, \delta)/L$, so that all the factors in the product (3.3) are distinct. Similarly, no prime ramifies in the extension $L(\beta, \delta)/L(\beta)$, and all the factors in the product (3.2) are distinct.

Lemma 3.5. *Let $\mathfrak{b}$ be a prime of K and let $\mathfrak{B}$ be a prime of G below $\mathfrak{b}$. Assume $\mathfrak{B}$ is not trivial. Let $R_{\mathfrak{B}}$ be the residue field of $\mathfrak{B}$ in G, and let $\delta_{\mathfrak{B}}$ be a generator of the extension of C isomorphic to $R_{\mathfrak{B}}$. Let $\bar{K}$ be a separable extension of K where $\mathfrak{b}$ splits into factors of degree 1. Let $\hat{G}$ be the algebraic closure of G in $\bar{K}$. Then $\hat{G}$ contains $\delta_{\mathfrak{B}}$.*

Proof. Let $\mathfrak{b} = \prod_{i=1}^{m} \mathfrak{b}_i$ be the factorization of $\mathfrak{b}$ in $\bar{K}$. Then each $\mathfrak{b}_i$ lies over a nontrivial prime $\mathfrak{B}_i$ of $\hat{G}$. (This is true because each $\mathfrak{B}_i$ is an extension of $\mathfrak{B}$.) Let $x \in G$ be such that its residue class generates $R_{\mathfrak{B}}$ over C, and let $F(T) \in C[T]$ be the irreducible polynomial of the residue class of x over C. Then $F(\delta_{\mathfrak{B}}) = 0$ and $F(x) \cong 0$ modulo $\mathfrak{B}$. On the other hand, since $\mathfrak{b}_1$ is of degree 1, there exists $a \in C_{\bar{K}}$ such that $x - a \cong 0$ modulo $\mathfrak{b}_1$. Hence, $0 \cong F(x) \cong F(a)$ modulo $\mathfrak{b}_1$. But $F(a)$ is a constant. Therefore, $F(a) = 0$. Since every extension of C is Galois, and a is a conjugate of $\delta_{\mathfrak{B}}$ over C, $\delta_{\mathfrak{B}} \in C(a) \subset \hat{G}$.

Lemma 3.6. *Let $\mathfrak{a}$ be a prime of K with a nontrivial restriction to G. Let $\mathfrak{A}$ be the prime below $\mathfrak{a}$ in G. Let $\bar{K} \supset \bar{G}$ be finite separable extensions of K and G respectively. Let $\bar{\mathfrak{a}}$ be a prime above $\mathfrak{a}$ in $\bar{K}$. Let $\bar{\mathfrak{A}}$ be the prime below $\bar{\mathfrak{a}}$ in $\bar{G}$. Then $\bar{\mathfrak{A}}$ lies above $\mathfrak{A}$ in $\bar{G}$ (and thus is not a trivial prime of $\bar{G}$). Further, if we assume that $e(\bar{\mathfrak{a}}/\mathfrak{a}) = e(\bar{\mathfrak{A}}/\mathfrak{A})$, then $e(\bar{\mathfrak{a}}/\bar{\mathfrak{A}}) = e(\mathfrak{a}/\mathfrak{A})$.*

Proof. Let $\bar{\mathfrak{a}}$ and $\bar{\mathfrak{A}}$ be as in the statement of the lemma. Then, since $\bar{\mathfrak{a}}$ restricts to $\bar{\mathfrak{A}}$ in $\bar{G}$ and to $\mathfrak{A}$ in G, we must conclude that the restriction of $\bar{\mathfrak{A}}$ to G is also $\mathfrak{A}$. Further, we have the following equality. $e(\bar{\mathfrak{a}}/\bar{\mathfrak{A}})e(\bar{\mathfrak{A}}/\mathfrak{A}) = e(\bar{\mathfrak{a}}/\mathfrak{a})e(\mathfrak{a}/\mathfrak{A})$. Thus, $e(\bar{\mathfrak{a}}/\bar{\mathfrak{A}}) = e(\mathfrak{a}/\mathfrak{A})$.

Lemma 3.7. *Let $\mathfrak{a}, \mathfrak{b}$ be two primes of K, restricting to nontrivial primes $\mathfrak{A}$ and $\mathfrak{B}$ of G respectively. Assume the residue field of $\mathfrak{b}$ is separable over C_K. Further, assume that $\mathfrak{b}$ and $\mathfrak{a}$ are unramified over G and are the only factors of $\mathfrak{B}$ and $\mathfrak{A}$ in K. Let $f \in G$ be such that its divisor is of the form*

$$\frac{\mathfrak{B}^s}{\mathfrak{A}\mathfrak{U}}, \tag{3.4}$$

where $\mathfrak{U}$ is an integral divisor of G relatively prime to $\mathfrak{B}$ and $\mathfrak{A}$, and s is a natural number such that $s \ncong 0$ modulo p. Let $v \in G$ be such that it has a pole of order 1 at all the primes which are factors of the pole divisor of f and is equivalent to $b^p - b$ modulo $\mathfrak{B}$ for some $b \in C$. (Such an $f \in G$ exists by the Strong Approximation Theorem.) Let δ_G, an element of the algebraic closure of C, be a generator of the residue field of $\mathfrak{B}$ over C and let δ_K, an element of the algebraic closure of C_K, be a generator of the Galois closure of the residue field of $\mathfrak{b}$ over C_K. Let β be a root of (3.1) in the algebraic closure of K. Let $w \in G$, and let $\mathfrak{A}_w$, $\mathfrak{B}_w$, $\mathfrak{U}_w$ be the primes and the divisor below $\mathfrak{A}$ and $\mathfrak{B}$ and $\mathfrak{U}$ respectively in $G_{t,x,v,w,f}$. Let $\bar{G}_w = G_{x,t,v,w,f,\beta}$. Let $\bar{K} = K(\beta, \delta_K), \bar{G} = G(\beta, \delta_G)$. Then the following statements are true.

1) $\bar{G}_w \subset \bar{G} \subset \bar{K}$.
2) $\bar{G}/\bar{G}_w$ *is a separable (possibly infinite) constant field extension, and thus no prime ramifies in this extension.*
3) *The primes* $\mathfrak{A}_w$ *and* $\mathfrak{B}_w$ *are distinct in* $\bar{G}_w$.
4) *In* $\bar{K}$, $\mathfrak{b} = \prod \mathfrak{b}_i$, *where* $\mathfrak{b}_i$ *are distinct prime divisors of degree* 1.
5) *In* $\bar{G}$, $\mathfrak{B} = \prod \mathfrak{B}_i$, *where* $\mathfrak{B}_i$ *are distinct prime divisors of degree* 1.
6) *For each* i *there exists* j *such that* $\mathfrak{b}_i$ *lies above* $\mathfrak{B}_j$ *and* $e(\mathfrak{b}_i/\mathfrak{B}_j) = 1$.
7) *In* $\bar{K}$, $\mathfrak{a} = \prod \mathfrak{a}_i^p$, *where* $\mathfrak{a}_i$ *are distinct prime divisors.*
8) *In* $\bar{G}$, $\mathfrak{A} = \prod \mathfrak{A}_i^p$, *where* $\mathfrak{A}_i$ *are distinct prime divisors.*
9) *For each* i *there exists* j *such that* $\mathfrak{a}_i$ *lies above* $\mathfrak{A}_j$ *and* $e(\mathfrak{a}_i/\mathfrak{A}_j) = 1$.
10) *In* $\bar{G}_w$, $\mathfrak{A}_w = \mathfrak{a}_w^p$ *for some prime* $\mathfrak{a}_w$ *of* $\bar{G}_w$.
11) *There exist* $z_1 \in \bar{G}$ *such that its divisor is of the form* $\mathfrak{T}\mathfrak{A}_1^{-1}$, *where* $\mathfrak{T}$ *is a divisor of* $\bar{G}$ *relatively prime to* $\mathfrak{B}$ *and* $\mathfrak{A}$, *such that for some* $b \in C$, $z_1 \cong b^p - b$ *modulo* $\mathfrak{B}$.
12) *Let* $k > 0, k \not\cong 0$ *modulo* p *be greater than the highest order of any pole of* z_1 *in* $\bar{K}$. *Then there exists* $z_2 \in \bar{G}$ *such that its divisor is of the form* $\mathfrak{W}\mathfrak{A}_1^{-p^l}$, *where* $p^l > p^2k$ *and* $\mathfrak{W}$ *is an integral divisor of* $\bar{G}$ *relatively prime to* $\mathfrak{B}$ *and* $\mathfrak{A}$. *Further,* $z_2 \cong 1$ *modulo* $\mathfrak{B}$.
13) *Let* $z = z_1 z_2$. *Then in* $\bar{G}$, z *has a pole of order* $p^l + 1 > p^2k$ *at* $\mathfrak{A}_1$ *and is equivalent to* $b^p - b$ *modulo* $\mathfrak{B}$. *All the other poles of* z *are of order less than* k.
14) *In* $\bar{G}_w(z)$, z *has a pole of order* $p^l + 1 > p^2k$ *at the prime below* $\mathfrak{A}_1$ *and is equivalent to* $b^p - b$ *modulo the divisor below* $\mathfrak{B}$.
15) *In* $\bar{G}$, $\mathfrak{U}$ *is a* p*-th power of another divisor.*
16) *In* $\bar{G}_w$, $\mathfrak{U}_w$ *is a* p*-th power of another divisor.*

Proof. 1. First of all, $x, t \in G$ by construction, $v, f, w \in G$ by assumption. Therefore, $G_{x,t,v,f.w} \subset G$, and $\bar{G}_w = G_{x,t,v,f,w,\beta} \subset G(\beta, \delta_G) = \bar{G}$. Secondly, by Lemma 6.14, $\mathfrak{b}$ will split into factors of degree 1 in $\bar{K}$. Therefore, $\delta_G \in K(\delta_K)$ by Lemma 3.5. Hence, $\bar{G} \subset \bar{K}$.

2. $\bar{G} = C(t, x, \beta, \delta_G) = C\bar{G}_w(\beta)$.

3. Since $v \in \bar{G}_w$ has a pole at $\mathfrak{A}_w$ but not at $\mathfrak{B}_w$, these primes must be distinct in $\bar{G}_w$.

4,5,7,8,10,15,16. These statements follow from Lemma 3.4.

6,9. These statements follow from Lemma 3.6.

11, 12. These statements follow from Lemma 6.15.

13. This statement follows from a direct calculation of the orders of poles of z.

14. This statement follows from the fact that $\bar{G}/\bar{G}_w(z)$ is also a separable constant field extension and thus no prime is ramified.

Lemma 3.8. *Let* $\mathfrak{b}$, $\mathfrak{a}$, $\mathfrak{A}$, $\mathfrak{B}$, $\bar{G}$, $\bar{K}$, $\mathfrak{a}_i$, $\mathfrak{A}_i$, $\mathfrak{b}_i$, $\mathfrak{B}_i$, f, z, s, k *be as in Lemma 3.7. Let* $w \in K$. *If* $w \in G$ *then let* $\bar{G}_w$ *be as in Lemma 3.7. Let* $a \in C_{\bar{K}}$ *be*

such that the equation

$$x^p - x - a = 0 \tag{3.5}$$

has no solution in $C_{\bar{K}}$, the constant field of $\bar{K}$, while a is algebraic over a finite field. If $w \in G$, without loss of generality, we can assume that $a \in G_w$. (G_w can be any subfield of G containing the elements listed above and such that its constant field is finite.) Let

$$h = f^{-1} w^{p(s+1)} + f^{-p}. \tag{3.6}$$

Let β_w be a root of the equation

$$x^p - x - (h^{-k} + z) = 0. \tag{3.7}$$

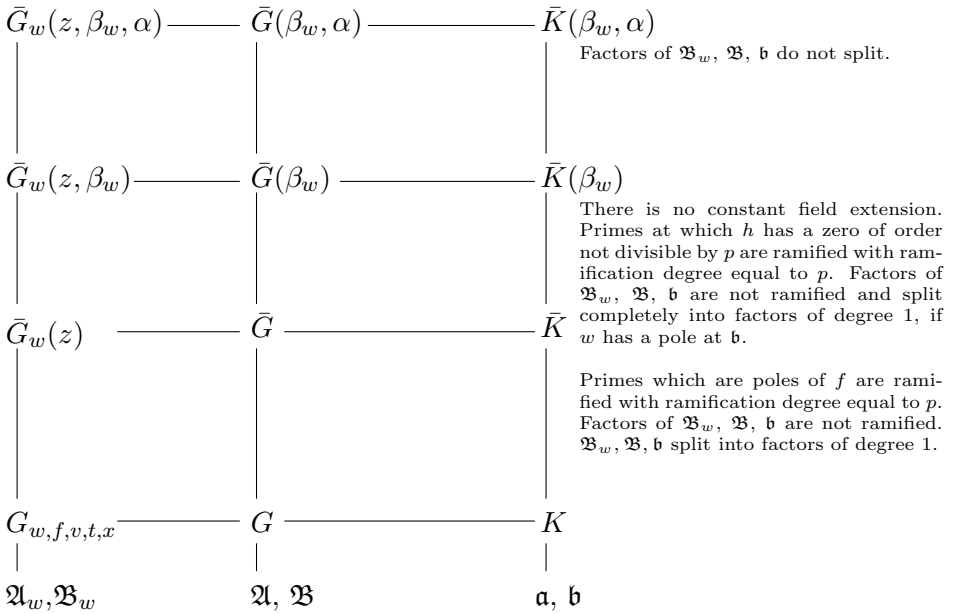
Let α be a root of the Equation (3.5). Then the following statements are true.

1) *If $w \in K$ has a pole at $\mathfrak{b}$, then the equation*

$$\prod_{i=0}^{p-1} (a_0 + a_1(\alpha + i) + \cdots + a_{p-1}(\alpha + i)^{p-1}) = h \tag{3.8}$$

   has no solution $(a_0, \ldots, a_{p-1}) \in \bar{K}(\beta_w)$.
2) *If $w \in G$ has no pole at $\mathfrak{B}$, then Equation (3.8) will have a solution $(a_0, \ldots, a_{p-1}) \in \bar{G}_w(z, \beta_w) \subset \bar{G}(\beta_w)$.*

Proof. The following figure describes the extensions involved. The two left columns correspond to the case of $w \in G$.



Before we proceed with the proof we will discuss the following three points. First of all, we will show below that for all $w \in G$,

$$[\bar{K}(\beta_w) : \bar{K}] = [\bar{K}(\beta_w, \alpha) : \bar{K}(\beta_w)] = p, \tag{3.9}$$

$$[\bar{G}(\beta_w) : \bar{G}] = [\bar{G}(\beta_w, \alpha) : \bar{G}(\beta_w)] = p, \tag{3.10}$$

$$[\bar{G}_w(\beta_w, z) : \bar{G}_w(z)] = [\bar{G}_w(z, \beta_w, \alpha) : \bar{G}_w(z, \beta_w)] = p, \tag{3.11}$$

while (3.9) holds for all $w \in K$. Secondly, it is not hard to see that the existence of solutions $a_0, \ldots, a_{p-1} \in \bar{K}(\beta_w)$ to (3.8) is equivalent to existence of $u \in \bar{K}(\alpha, \beta_w)$ such that

$$\mathbf{N}_{\bar{K}(\alpha,\beta_w)/\bar{K}(\beta_w)}(u) = h. \tag{3.12}$$

Finally, assume $w \in G$. Then it is also not hard to see that (3.8) has solutions in $\bar{G}_w(z, \beta_w)$ if and only if there exists $u \in \bar{G}_w(z, \alpha, \beta_w)$ such that

$$\mathbf{N}_{\bar{G}_w(z,\alpha,\beta_w)/\bar{G}_w(z,\beta_w)}(u) = h. \tag{3.13}$$

In order to show that (3.9)-(3.11) hold, we will show that in extensions $\bar{K}(\beta_w)/\bar{K}$, $\bar{G}(\beta_w)/\bar{G}$, and $\bar{G}_w(\beta_w, z)/\bar{G}_w(z)$ at least one prime will have ramification degree p while the degree of each extension listed above is at most p. (As above, when we consider the last two extensions, we assume that $w \in G$.) Since all the extensions listed above are separable, the presence of a totally ramified prime will imply that there is no constant field extension in either of the three extensions. Thus, since α was of degree p over $C_{\bar{K}}, C$ and C_w- the constant field of G_w, it will remain of degree p over the constant fields of $\bar{K}(\beta_w), \bar{G}(\beta_w)$ and $\bar{G}_w(\beta_w, z)$. We can assume without loss of generality that a $\bar{K}$-prime $\mathfrak{a}_1$ lies above a $\bar{G}$-prime $\mathfrak{A}_1$. In this case, by Lemma 3.7, in $\bar{K}$, f has a pole of order p at $\mathfrak{a}_1$, so that f^{-1} and f^{-p} have zeros of order p and p^2 respectively at $\mathfrak{a}_1$. Therefore, if w has a pole at $\mathfrak{a}_1$,

$$\operatorname{ord}_{\mathfrak{a}_1} h = \operatorname{ord}_{\mathfrak{a}_1} f^{-1} w^{(s+1)p} + f^{-p} = ps \operatorname{ord}_{\mathfrak{a}_1} w < 0.$$

If w is a unit at $\mathfrak{a}_1$, then

$$\operatorname{ord}_{\mathfrak{a}_1} h = \operatorname{ord}_{\mathfrak{a}_1} f^{-1} w^{p(s+1)} + f^{-p} = -\operatorname{ord}_{\mathfrak{a}_1} f = p.$$

If w has a zero at $\mathfrak{a}_1$, then

$$\operatorname{ord}_{\mathfrak{a}_1} h = \operatorname{ord}_{\mathfrak{a}_1} f^{-1} w^{p(s+1)} + f^{-p} = -p \operatorname{ord}_{\mathfrak{a}_1} f = p^2.$$

Thus, at $\mathfrak{a}_1$, h either has a pole or a zero of degree at most p^2. Now consider $h^{-k} + z$. Since at $\mathfrak{a}_1$, z has a pole of order greater than $p^2 k$, $\operatorname{ord}_{\mathfrak{a}_1}(h^{-k} + z) = \operatorname{ord}_{\mathfrak{a}_1} z = -(p^l + 1)$. Therefore, by Lemma 3.1, $\mathfrak{a}_1$ will ramify completely in the extension $\bar{K}(\beta_w)/\bar{K}$. Hence, this extension is of degree p. Since at least one prime is ramified completely and the extension is separable, the constant field of $\bar{K}(\beta_w)$ is the same as the constant field of $\bar{K}$. Thus α is of degree p over $\bar{K}(\beta_w)$. Further we remind the reader that if $w \in G$, $h \in \bar{G}_w(z) \subset \bar{G}$. In these fields, $h^{-k} + z$ will have a pole of order not divisible by p at primes

below $\mathfrak{a}_1$. Therefore, by Lemma 3.1 these primes in $\bar{G}_w(z)(\beta_w)$ and in $\bar{G}(\beta_w)$ respectively will have factors with ramification degree p. Consequently, the degrees of the corresponding extensions will be equal to p. Finally, α will remain of degree p over $\bar{G}_w(z)(\beta_w)$ and $\bar{G}(\beta_w)$ for the reasons described above.

For future use, in the case $w \in G$, also note that in all of the three fields, any valuation that is a zero of h is also a pole of $(h^{-k}+z)$. Further, the order of $(h^{-k}+z)$ at any such valuation, except for $\mathfrak{a}_1$ and primes below it, is divisible by p if and only if the order of h at this valuation is divisible by p. Thus, if h has a zero at $\mathfrak{t}$ and $\mathrm{ord}_{\mathfrak{t}} h \not\cong 0$ modulo p in $\bar{G}_w$, then $\mathfrak{t}$ ramifies completely in the extensions $\bar{K}(\beta_w)/\bar{K}$, $\bar{G}(\beta_w)/\bar{G}$, $\bar{G}_w(z,\beta_w)/\bar{G}_w(z)$.

We will now proceed to the proof of the lemma.

1) Suppose $w \in K$ has a pole at $\mathfrak{b}$. Then in K,

$$\mathrm{ord}_{\mathfrak{b}} h = \mathrm{ord}_{\mathfrak{b}}(f^{-1}w^{p(s+1)} + f^{-p}) = p(s+1)\mathrm{ord}_{\mathfrak{b}} w - s \not\cong 0 \text{ modulo } p.$$

Further,

$$\mathrm{ord}_{\mathfrak{b}} h < 0.$$

Further, by construction, no factor of $\mathfrak{b}$ ramifies in the extension $\bar{K}/K$. Thus, in $\bar{K}$, for any factor $\mathfrak{g}$ of $\mathfrak{b}$, $\mathrm{ord}_{\mathfrak{g}} h \not\cong 0$ modulo p and h has a pole at all factors of $\mathfrak{b}$.

Next observe the following. Since h has a pole at $\mathfrak{b}$, and z does not have a pole at any factor of $\mathfrak{b}$, $h^{-k}+z$ does not have a pole at any factor of $\mathfrak{b}$, and so, by Lemma 3.1, no factor of $\mathfrak{b}$ ramifies in the extension $\bar{K}(\beta_w)/\bar{K}$. Thus, the order of h at any factor of $\mathfrak{b}$ is not divisible by p in $\bar{K}(\beta_w)$.

Note also that every factor of $\mathfrak{b}$ is relatively prime to the discriminant of β_w. Further, $h^{-k}+z \cong b^p - b$ modulo every factor of $\mathfrak{b}$ in $\bar{K}$ and thus the left side of (3.7) factors completely modulo every factor of $\mathfrak{b}$. Therefore, by [**21**, Proposition 25, page 27, Proposition 16, page 67], every factor of $\mathfrak{b}$ will split completely in the extension $\bar{K}(\beta_w)/\bar{K}$. Since this extension has no constant field subextension, and every factor of $\mathfrak{b}$ is of degree 1 in $\bar{K}$, we must conclude that in $\bar{K}(\beta_w)$ all factors of $\mathfrak{b}$ are also of degree 1.

Since $\bar{K}$ and $\bar{K}(\beta_w)$ have the same constant field, (3.5) still has no solution in $\bar{K}(\beta_w)$ and consequently, (3.5) has no solution modulo any factor of $\mathfrak{b}$ in $\bar{K}(\beta_w)$. Thus, by [**21**, Proposition 25, page 27, Proposition 16, page 67], every factor of $\mathfrak{b}$ in $\bar{K}(\beta_w)$ remains prime in $\bar{K}(\beta_w,\alpha)$. Hence, by Lemma 3.2, (3.12) will have no solution in $\bar{K}(\alpha,\beta_w)$.

2) Suppose now w does not have a pole at $\mathfrak{b}$ and $w \in G$. We will show that in this case (3.13) will have a solution in $\bar{G}_w(z,\alpha,\beta_w)$.

By the Strong Hasse Norm Principal (see [2, Page 185] or [42, Propositions 10,11, pages 182-183; Theorem 2, page 206]), it is enough to show that for all primes $\mathfrak{t}$ of $\bar{G}_w(z,\beta_w)$, h is a local norm. Note that no prime ramifies in the extension $\bar{G}_w(z,\alpha,\beta_w)/\bar{G}_w(z,\beta_w)$. Thus if h is a unit at $\mathfrak{t}$, it is automatically a local norm at $\mathfrak{t}$ by [42, Corollary, page 226]. Suppose $\mathfrak{t}$ is a pole of h. Then either it is a factor of $\mathfrak{B}_w$ or it is a pole of w. Since w has no pole at $\mathfrak{B}_w$, direct calculation assures us that h will have a pole at every factor of $\mathfrak{B}$ of order divisible by p. On the other hand, if $\mathfrak{t}$ is a pole of w, then again by direct calculation one can see that h will also have a pole at $\mathfrak{t}$ of order divisible by p. Indeed, the only case which has to be considered with some care is the case of $\mathfrak{t}$ being a pole of f or a zero of f^{-1}. In this case,

$$\begin{aligned}\operatorname{ord}_{\mathfrak{t}} h &= \operatorname{ord}_{\mathfrak{t}}\left(f^{-1}w^{p(s+1)} + f^{-p}\right)\\ &= \min\left(\operatorname{ord}_{\mathfrak{t}}\left(f^{-1}w^{p(s+1)}\right),\ \operatorname{ord}_{\mathfrak{t}} f^{-p}\right)\\ &= \operatorname{ord}_{\mathfrak{t}}\left(f^{-1}w^{p(s+1)}\right).\end{aligned}$$

We should note here that by Lemma 3.7, $\mathfrak{t}$ is ramified over $G_{w,f,v,t,x}$ with ramification degree divisible by p. On the other hand, $f \in G_{w,f,v,t,x}$. Thus, $\operatorname{ord}_{\mathfrak{t}}(f^{-1}) \cong 0$ modulo p. Hence, $\operatorname{ord}_{\mathfrak{t}} h \cong 0$ modulo p.

Assume now that $\mathfrak{t}$ is a zero of h. If $\mathfrak{t}$ is a factor of $\mathfrak{A}_w$ then it is ramified with ramification degree divisible by p over $G_{x,t,v,w,f}$ and since $h \in G_{x,t,v,w,f}$, we can conclude that h has a zero of order divisible by p at $\mathfrak{t}$. If $\mathfrak{t}$ is not a factor of $\mathfrak{A}_w$, then it is ramified with ramification degree divisible by p over $\bar{G}_w(z)$ and again we conclude that h has a zero of order divisible by p at $\mathfrak{t}$. Thus, in all the cases cited above, by Lemma 3.3, h is a local norm at $\mathfrak{t}$.

Theorem 3.9. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be primes of K satisfying conditions described in Lemma 3.7. Then the set $INT(\mathfrak{b})$ is Diophantine over K.*

4. Integrality at one prime: The case of $q \neq p$.

In this section we will show that in the case C has an extension of degree $q \neq p$, the set of elements of G integral at a prime is Diophantine over G. Most of the work necessary to prove this proposition has been done in [39], but we will need to take care of some details. In this section we will assume $q \neq p$.

Lemma 4.1. *Let L be an algebraic function field, let $a \in L$. Let q be a rational prime distinct from the characteristic of the field. Then a prime $\mathfrak{t}$ of K ramifies in the extension $K(a^{1/q})/K$ if and only if $\operatorname{ord}_{\mathfrak{t}} a \ncong 0$ modulo q.*

Proof. If $\mathrm{ord}_{\mathfrak{t}} a \ncong 0$ modulo q then $\mathfrak{t}$ will clearly ramify in the extension. Suppose now $\mathrm{ord}_{\mathfrak{t}} a \cong 0$ modulo q. Since we can multiply or divide a by the qth power of some local uniformizing parameter without changing the extension, without loss of generality we can assume that $\mathrm{ord}_{\mathfrak{t}} a = 0$. But in this case the discriminant of the power basis of $a^{1/q}$ will be a unit at $\mathfrak{t}$, and thus $\mathfrak{t}$ will be unramified.

Lemma 4.2. *Let L be an algebraic function field containing primitive q-th roots of unity. Let $\mathfrak{C}$ and $\mathfrak{B}$ be prime divisors of L. Let $v \in K$ be such that the divisor of v is of the form $\mathfrak{C}^{-1}\mathfrak{U}$, where $\mathfrak{U}$ is a divisor of L which has no common factors with $\mathfrak{C}$ or $\mathfrak{B}$. Further, assume v is equivalent to $b^q \neq 0$ modulo $\mathfrak{B}$, where $b \in C_L$. (Such a v exists by the Weak Approximation theorem.) Let β be a root of*

$$T^q - v = 0. \tag{4.1}$$

Let $R_{\mathfrak{B}}$ be the residue field of $\mathfrak{B}$ in L and assume it is separable over C_L, the constant field of L. Let δ be an element of the algebraic closure of C_L such that $C_L(\delta)$ is isomorphic to the Galois closure of $R_{\mathfrak{B}}$ over C_L. Let $\bar{L} = L(\beta, \delta)$. Then in $\bar{L}$

$$\mathfrak{C} = \prod \mathfrak{c}_i^q,$$

and

$$\mathfrak{B} = \prod \mathfrak{b}_i,$$

where for $i \neq j$, $\mathfrak{b}_i \neq \mathfrak{b}_j, \mathfrak{c}_i \neq \mathfrak{c}_j$, and for all $i, \mathfrak{b}_i$ is of degree 1.

(The proof of this lemma is analogous to the one for Lemma 3.4.)

Lemma 4.3. *Let $f \in G$ have the divisor of the form (3.4), but with s not congruent to 0 modulo q. Let $v \in G$ be such that it has a pole of order 1 at all the primes which are factors of the pole divisor of f and is equivalent to b^q modulo $\mathfrak{B}$ for some $b \neq 0$ in the field of p elements. (Such an $f \in G$ exists by the Strong Approximation Theorem.) Let δ_G, an element of the algebraic closure of C, be a generator of the residue field of $\mathfrak{B}$ over C. Let β be a root of (4.1) in the algebraic closure of G. Let $w \in G$, and let $\mathfrak{A}_w$, $\mathfrak{B}_w$, $\mathfrak{U}_w$ be the primes and the divisor below $\mathfrak{A}$ and $\mathfrak{B}$ and $\mathfrak{U}$ respectively in $G_{t,x,v,w,f}$. Let $\bar{G}_w = G_{x,t,v,w,f,\beta}$. Let $\bar{G} = G(\beta, \delta_G)$. Then the following statements are true.*

1) *$\bar{G}_w \subset \bar{G}$.*
2) *$\bar{G}/\bar{G}_w$ is separable (possibly infinite) constant field extension, and thus no prime ramifies in this extension.*
3) *The primes $\mathfrak{A}_w$ and $\mathfrak{B}_w$ are distinct in $\bar{G}_w$.*
4) *In $\bar{G}$, $\mathfrak{B} = \prod \mathfrak{B}_i$, where $\mathfrak{B}_i$ are distinct prime divisors of degree 1.*
5) *In $\bar{G}$, $\mathfrak{A} = \prod \mathfrak{A}_i^q$, where $\mathfrak{A}_i$ are distinct prime divisors.*
6) *In $\bar{G}_w$, $\mathfrak{A}_w = \mathfrak{a}_w^q$, where $\mathfrak{a}_w$ is a prime of $\bar{G}_w$.*

7) *There exist* $z_1 \in \bar{G}$ *such that its divisor is of the form* $\mathfrak{T}\mathfrak{A}_1^{-1}$, *where* $\mathfrak{T}$ *is a divisor of* $\bar{G}$ *relatively prime to* $\mathfrak{B}$ *and* $\mathfrak{A}$, *such that for some* $b \in C, b \neq 0, z_1 \cong b^q$ *modulo* $\mathfrak{B}$.
8) *Let* $k > 0$ *be the highest order of any pole of* z_1 *in* $\bar{G}$. *Then there exists* $z_2 \in \bar{G}$ *such that its divisor is of the form* $\mathfrak{W}\mathfrak{A}_1^{-q^l}$, *where* $\mathfrak{W}$ *is an integral divisor of* $\bar{G}$ *relatively prime to* $\mathfrak{B}$ *and* $\mathfrak{A}$, *and* $q^l > kq^2$. *Further,* $z_2 \cong 1$ *modulo* $\mathfrak{B}$.
9) *Let* $z = z_1 z_2$. *Then in* $\bar{G}$, z *has a pole of order* $q^l + 1 > k$ *at* $\mathfrak{A}_1$ *and is equivalent to* b^q *modulo* $\mathfrak{B}$.
10) *In* $\bar{G}_w(z)$, z *has a pole of order* $q^l + 1 > q^2 k$ *at the prime below* $\mathfrak{A}_1$ *and is equivalent to* b^q *modulo the divisor below* $\mathfrak{B}$.
11) *In* $\bar{G}$, $\mathfrak{U}$ *is a* q*-th power of another divisor.*
12) *In* $\bar{G}_w$, $\mathfrak{U}_w$ *is a* q*-th power of another divisor.*

(The proof of this lemma is analogous to the proof of Lemma 3.7.)

Lemma 4.4. *Let* $\mathfrak{A}$, $\mathfrak{B}$, $\bar{G}$, $\bar{G}_w$, $\mathfrak{A}_i$, $\mathfrak{B}_i, f, w, z$ *be as in Lemma 4.3. Let* $a \in \bar{G}$ *be such that the equation*

$$x^q - a = 0 \tag{4.2}$$

has no solution in $\bar{G}$. *As above assume without loss of generality that* $a \in \bar{G}_w$. *Let* h *be defined by* (3.6) *but with* q *in place of* p. *Let* β_w *be a root of the equation*

$$T^q - (h^{-k} + z) = 0. \tag{4.3}$$

Let α *be a root of the equation* (4.2). *Then the following statements are true.*

1) *If* $w \in G$ *has a pole at* $\mathfrak{B}$, *then the equation*

$$\prod_{i=0}^{q-1}(a_0 + a_1\xi_q^i\alpha + \cdots + a_{q-1}\xi_q^{i(q-1)}\alpha^{q-1}) = h \tag{4.4}$$

has no solution $(a_0, \ldots, a_{q-1}) \in \bar{G}(\beta_w)$, *where* ξ_q *is a* q*-th primitive root of unity.*
2) *If* $w \in G$ *has no pole at* $\mathfrak{B}$, *then Equation* (4.4) *will have a solution* $(a_0, \ldots, a_{q-1}) \in \bar{G}_w(z, \beta_w) \subset \bar{G}(\beta_w)$.

(The proof of this lemma is analogous to the proof of Lemma 3.8.)

Lemma 4.4 is the last part required for the proof of the following theorem.

Theorem 4.5. *Let* G *be an algebraic function field whose constant field* C *is algebraic over a finite field of characteristic* $p > 0$. *Assume further, that* C *is not algebraically closed. Then for any prime* $\mathfrak{B}$ *of* G *the set of all elements of* G *integral with respect to* $\mathfrak{B}$ *is Diophantine over* G.

Proof. If C is not algebraically closed, then it has an extension of degree q, where q is a prime. (This can be easily derived from [**20**, Theorem 13, page

185].) Further, it is not hard to show that this extension will be generated either by an equation of the form (3.5) or (4.1). By Lemma 6.6, any finite extension of C will have also have an extension of degree q. Thus, a as described in the proofs of Lemmas 3.8 and 4.4 exist. Finally, we note that by Lemma 1.3, Equations (3.8) and (4.4) can be rewritten as an equivalent system of equations over G. (By the equivalent system, we mean a system of equations over G such that for every $w \in G$, this system will have solutions in G if and only if (3.8), ((4.4) respectively) has solutions in $\bar{G}(\beta_w)$.)

5. Diophantine Undecidability.

In this section we will summarize the discussion above and describe in more detail classes of fields to which our result is applicable.

Theorem 5.1. *Let K be a recursive field satisfying the assumptions of Notations 1.4 with $q = p$. Then Diophantine problem of K is undecidable.*

Proof. The proof of this theorem will follow from Lemma 1.2, Theorem 2.12, Theorem 3.9 assuming we demonstrate existence of primes $\mathfrak{a}$ and $\mathfrak{b}$ as described in the statement of Theorem 3.9. We can let $\mathfrak{a} = \mathfrak{p}$ and $\mathfrak{b} = \mathfrak{q}$, where $\mathfrak{p}$ and $\mathfrak{q}$ are described in Notations 1.4.

Theorem 5.2. *Let K be a recursive field of characteristic $p > 2$. Let C be the algebraic closure of a finite field in K. Assume C has an extension of degree p. Assume further that K has a subfield K_1, possibly equal to C, and an element u transcendental over K_1 such that for some x algebraic over $C(u)$, $K = K_1(u, x)$. Then Diophantine problem of K is undecidable.*

Proof. We can consider K as an algebraic function field over a constant field $K_1 = C_K$. By Theorem 6.11, we know that a finite extension of G contains element t and constants $c_1, \ldots$ as described in Notations 1.4. Further, by Lemma 6.13, in the corresponding finite extension of K, t and $c_1, \ldots$ will also posses the required properties. Thus, by Theorem 5.1, the Diophantine problem of K is undecidable.

6. Appendix.

Notations 6.1. In this section the term "algebraic function field K over a constant field C" we will always mean a finite algebraic extension of a rational function field $C(w)$, where w is transcendental over C and C is algebraically closed in K.

Lemma 6.2. *Let H/L be a finite separable extension of algebraic function fields and let C_H be the constant field of H. Let $\mathfrak{u}$ be an integral divisor of L. Then* $\text{degree}_H(\mathfrak{u}) = [H : C_H L]\text{degree}_L(\mathfrak{u})$.

(See [**1**, Theorem 9, page 279 and Theorem 14, page 282].)

Lemma 6.3. *Let M/H be a Galois extension of algebraic function fields over the same field of constants C, algebraic over a finite field. Let F be an algebraic extension of C. Then MF/HF is a Galois extension whose Galois group is isomorphic to the original one.*

Lemma 6.4. *Let C be a field algebraic over a finite field, and let t be transcendental over C. Let H be a finite separable extension of $C(t)$ generated by $\alpha \in H$. Let C_0 be any subfield of C. Then the extension $H/C_0(\alpha, t)$ is a constant field extension.*

Lemma 6.5. *Let H be an algebraic function field over a perfect field of constants C and let t be a nonconstant element of H. Then the following conditions are equivalent.*

1) *t is not a p-th power in H.*
2) *The extension $H/C(t)$ is finite and separable.*

(See [22, page 94].)

Lemma 6.6. *Let C be a field algebraic a over finite field of characteristic $p > 0$. Let q be a rational prime possibly equal to p such that C has an extension of degree q. For any natural number n, let F_n be the finite field of p^n elements. Let $F = \bigcup_i^\infty F_{q^i}$. Then there exists a natural number r such that $F \cap C = F_{q^r}$.*

Proof. First of all, we note the following well known facts concerning the finite fields:

$$F_m F_n = F_{lcm(m,n)}; \tag{6.1}$$

F_m is of degree m over the field of p elements and it consists of all the solutions to the equation $x^{p^m} - x = 0$. (See [20, pages 184 - 185].) Next let α be an element of the algebraic closure of a finite field such that $[C(\alpha) : C] = q$. Let $a_0, \ldots, a_{q-1}$ be the coefficients of the irreducible polynomial of α over C. Let m be the smallest positive integer such that $\alpha^{p^m} = \alpha$. Then from (6.1) we conclude that $m = q[F_1(a_0, \ldots, a_{q-1}) : F_1]$. Let $m = q^t k$, where $(k, q) = 1$. Then $F_{q^{t-1}} \subset F_{q^{t-1}k} \subset C$ but $F_{q^t} \not\subset C$. Otherwise, C contains $F_{q^t} F_{m/q} = F_m$ and thus α.

Lemma 6.7. *Let A_1 be a field algebraic over a finite field. Let A_2 be a finite algebraic extension of A_1. Let α be an element of the algebraic closure of A_1 such that for some rational prime $q, (q, [A_1(\alpha) : A_1]) = 1$. Then $(q, [A_2(\alpha) : A_2]) = 1$.*

Proof. Let $F(T) = a_0 + \ldots + T^k$ be the monic irreducible polynomial of α over A_2. Then $a_0, \ldots, a_{k-1} \in A_1(\alpha)$ since these are symmetric functions of conjugates of α over A_2 which are also conjugates of α over $A_1 \subset A_2$. Thus, $A_3 = A_1(a_0, \ldots, a_{k-1}) \subset A_1(\alpha) \cap A_2$. Since $A_3 \subset A_2, [A_2(\alpha) : A_2] \leq [A_3(\alpha) : A_3]$. On the other hand, since $a_0, \ldots, a_{k-1} \subset A_3$, $[A_3(\alpha) : A_3] \leq$

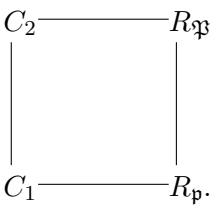
$[A_2(\alpha) : A_2]$. Thus, $[A_2(\alpha) : A_2] = [A_3(\alpha) : A_3]$. On the other hand, $A_3(\alpha) \subset A_1(\alpha)$ and $A_1(\alpha) \subset A_3(\alpha)$ so that $A_1(\alpha) = A_3(\alpha)$. Thus,

$$[A_2(\alpha) : A_2] = [A_3(\alpha) : A_3] = [A_1(\alpha) : A_3] = [A_1(\alpha) : A_1]/[A_3 : A_1],$$

and the lemma is true.

Lemma 6.8. *Let H be an algebraic function field whose constant field C_1 is algebraic over a finite field. Let $\mathfrak{p}$ be a prime of H. Let C be an algebraic extension of C_1 such that for any field $C_2 \subset C$ such that C_2/C_1 is a finite extension, $[C_2 : C_1]$ is prime to the degree$_H$ of $\mathfrak{p}$. Then $\mathfrak{p}$ remains prime in CH.*

Proof. Suppose $\mathfrak{p}$ splits in CH, then for some C_2 as described in the statement of the lemma, $\mathfrak{p}$ splits in C_2H. (This is true because in CH, $\mathfrak{p}$ will have at least two factors, and therefore there will be an element α integral at one but not at the other. Hence, $\mathfrak{p}$ will have to split in $C_1(\alpha)H$.) Let $m = [C_2 : C_1]$ and let $\mathfrak{P}$ be a prime above $\mathfrak{p}$ in C_2H. Since C_2/C_1 is a separable extension, by Theorem 14 on page 282 of [1], C_2 is the constant field of C_2H. Next consider the following diagram:



Here $R_{\mathfrak{p}}$ and $R_{\mathfrak{P}}$ are residue fields of $\mathfrak{p}$ and $\mathfrak{P}$ respectively. Further, from the diagram we can conclude that

$$[R_{\mathfrak{P}} : C_1] = [R_{\mathfrak{P}} : R_{\mathfrak{p}}][R_{\mathfrak{p}} : C_1] = [R_{\mathfrak{P}} : C_2][C_2 : C_1],$$

or, in other words,

$$f(\mathfrak{P}/\mathfrak{p})\text{degree}_{C_1H}(\mathfrak{p}) = \text{degree}_{C_2H}(\mathfrak{P})m.$$

Thus, since $(m, \text{degree}_{C_1H}(\mathfrak{p})) = 1$, we must conclude that $\text{degree}_{C_1H}(\mathfrak{p})$ divides $\text{degree}_{C_2H}(\mathfrak{P})$. Hence, $\text{degree}_{C_2H}(\mathfrak{P})$ is at least as big as $\text{degree}_{C_1H}(\mathfrak{p})$ $= \text{degree}_{C_2H}(\mathfrak{p}) \geq \text{degree}_{C_2H}(\mathfrak{P})$. (Here we use the fact that degree of a divisor stays the same under separable constant extensions by Lemma 6.2.) Thus, we must conclude that $\text{degree}_{C_2H}(\mathfrak{p}) = \text{degree}(\mathfrak{P})_{C_2H}$ and $\mathfrak{P}$ is the only prime of C_2H above $\mathfrak{p}$.

Our next task is to prove the main technical theorem of this section. The proof of this theorem will be similar to the proof of Theorem 3.6 of [38]. The differences will stem from the fact that we have an infinite constant field here (as opposed to the finite constant field in the theorem cited above), and seek primes which are linear polynomials in a certain element t of K. The proof of the theorem relies on two technical lemmas which we state below.

Lemma 6.9. *Let M be a Galois extension of an algebraic function field L over a finite field of constants, let C_L be the constant field of L, let C_M be the constant field of M, let t be a nonconstant element of L. Let $\sigma \in \mathrm{Gal}(M/L)$, and let $\mathcal{C} = \{\tau\sigma\tau^{-1} | \tau \in \mathrm{Gal}(M/L)\}$. Further, let p^r be the size of C_L, let $\phi = \phi_{C_L}$ be the generator of $\mathrm{Gal}(C_M/C_L)$ sending each element $c \in C_M$ to c^{p^r}, and assume that for every $\psi \in \mathcal{C}, \psi_{|C_M} = \phi^a$ for some natural integer a different from zero. Then if $k \cong a$ modulo $[C_M : C_L]$, $m = [M : C_M L]$, $d = [L : C_L(t)]$, and $C_k(M/L, \mathcal{C}) = \{\mathfrak{p} | \mathfrak{p}$ is a prime of L, $\mathrm{degree}(\mathfrak{p}) = k$, $\mathfrak{p}$ is unramified over $C_L(t)$, and for some β above $\mathfrak{p}$ the Frobenius automorphism of β belongs to $\mathcal{C}\}$,*

$$\left| C_k(M/L,\mathcal{C}) - \frac{|\mathcal{C}|}{km} p^{rk} \right| < \frac{|\mathcal{C}|}{km}((m+2g_M)p^{rk/2} + m(3g_L+1)p^{kr/4} + 2(g_M+dm)) < \frac{|\mathcal{C}|}{k}(7g_M+4d)p^{rk/2}, \tag{6.2}$$

where g_M, g_L are genus' of M and L respectively.

(For the first inequality see [15, Proposition 13.4] and [14, Lemma 5.7, p. 59]. The second inequality follows from [3, Corollary 2, page 106], [1, Theorem 22, page 291], and the fact that the extension M/L is separable.)

Lemma 6.10. *Let M be a Galois extension of an algebraic function field L over a finite field of constants, and assume U is an algebraic function field such that $L \subset U \subset M$, and U is not necessarily Galois over L. Let C_M and C_L denote the constant fields of M and L respectively. Further, let $\mathfrak{p}$ be a prime of L which does not split in U. Let $\mathfrak{p}_U$ be the prime above $\mathfrak{p}$ in U, let β be a prime of M above $\mathfrak{p}$, let $G(\beta)$ be the decomposition group of β, and let $\sigma \in G(\beta)$ be such that its coset modulo the inertia group of β induces the Frobenius automorphism $\phi_{R_\mathfrak{p}}$ on the residue field of $\mathfrak{p}$. Then $\sigma^{f(\mathfrak{p}_U/\mathfrak{p})} \in \mathrm{Gal}(M/U)$, and $f(\mathfrak{p}_U/\mathfrak{p}) = [U : L]$ is the smallest positive exponent such that the corresponding power of σ is in $\mathrm{Gal}(M/U)$. Further, $\sigma_{|C_M} = \phi_{C_L}^{\mathrm{degree}(\mathfrak{p})}$, where ϕ_{C_L} is the Frobenius automorphism of C_L.*

Conversely, suppose β is a prime of M not ramified over L. Let $\mathfrak{p}$ be a prime of L below β and let σ be the Frobenius automorphism of β. Assume further that for some coset $\mathrm{Gal}(M/U)\tau$ of $\mathrm{Gal}(M/U)$ in $\mathrm{Gal}(M/L)$, $\mathrm{Gal}(M/U)\tau\sigma^{[U:L]} = \mathrm{Gal}(M/U)\tau$, while this equality does not hold for any smaller exponent. Then $\mathfrak{p}$ does not split in U.

(See [38, Lemma 3.3] for part one of the lemma and [16, Proposition 2.8, page 101] for part two of the lemma.)

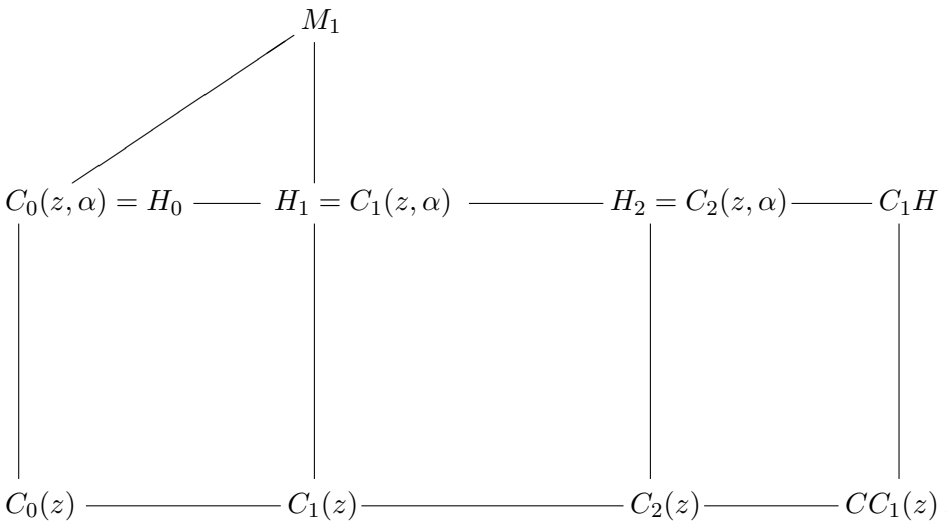
Theorem 6.11. *Let C be an infinite field algebraic over a finite field of characteristic $p > 0$. Assume C has an extension of degree q, where q is*

a rational prime (possibly equal to p). Let H be an algebraic function field whose field of constants is equal to C. Then for any sufficiently large positive integer h, a finite constant extension of H contains a nonconstant element t, infinitely many constants $c_0 = 0, c_1, \dots$, such that for all $i = 0, \dots$, the divisor of $t + c_i$ in H is of the form $\mathfrak{p}_i/\mathfrak{q}$, where $\mathfrak{p}_i$, $\mathfrak{q}$ are primes of H of degree q^h.

Proof. We will first establish existence of t, and then derive the existence of the required constants. Let z be a nonconstant element of H which is not a p-th power. (Such an element exists by the Weak Approximation Theorem.) Then by Lemma 6.5 the extension $H/C(z)$ is finite and separable and therefore is simple. Thus, for some $\alpha \in H, H = C(z, \alpha)$. Let $C_0 = \bigcup_i^\infty F_{q^i} \cap C$. Let C_1 be the constant field of M_1, the normal closure of $C_0(\alpha, z)$ over $C_0(z)$. Let $H_1 = C_1(\alpha, z)$. Then M_1/H_1 and $M_1/C_1(z)$ are Galois extension and all three fields have the same field of constants.

Let C_2 be a finite extension of C_1 contained in C_1C. Let $H_2 = C_2(z, \alpha)$ and note that H_2/H_1 is a separable constant field extension such that, by Lemma 6.7 and by construction of C_0, its degree is not divisible by q. Indeed, let $\alpha_1, \alpha_2, \dots \in C$ be the generators of C over C_0. Then the degree of α_i over C_0 and consequently, by Lemma 6.7, over $C_1(\alpha_1, \dots, \alpha_{i-1})$ is not divisible by q. Let $\beta \in C_2$, then $\beta \in C_1(\alpha_1, \alpha_2, \dots)$ and consequently the degree of β over C_1 is not divisible by q.

The following diagram describes the extensions involved.



Fix a positive integer h. Let $|C_1| = p^{r_1}$. Then $C_1(z)$ has exactly $\frac{p^{r_1 q^h} - p^{r_1 q^{h-1}}}{q^h}$ irreducible polynomials of degree q^h. ($p^{r_1 q^h} - p^{r_1 q^{h-1}}$ is the number of elements of the algebraic closure of C_1 of degree q^h over C_1.

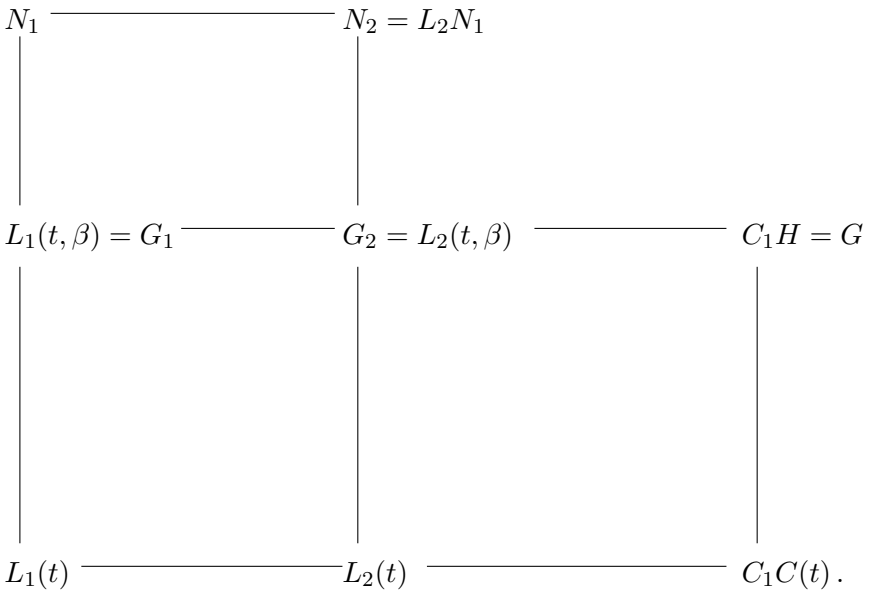
Each of these elements has exactly q^h conjugates.) Let h_{H_1} be the class number of H_1. Then for any sufficiently large h, $C_1(z)$ will contain at least $h_{H_1}+2$ primes of degree q^h.

Next consider the Galois extension $M_1/C_1(z)$. Let $\mathfrak{t}$ be a prime of $C_1(z)$ of degree q^h. Assume $\mathfrak{t}$ splits completely in M_1. Then, we claim, it splits completely in H_1 and its factors in H_1 are all of degree q^h. Indeed, assume $\mathfrak{t}=\prod_{i=1}^{[H_1:C_1(z)]}\mathfrak{T}_i$ is the factorization of $\mathfrak{t}$ in H_1. For each i, the relative degree of $\mathfrak{T}_i$ over $\mathfrak{t}$ is equal to one. This fact together with the fact that there is no constant field extension from $C_1(z)$ to H_1 implies that $C_1(z)$ degree of $\mathfrak{t}$ must be the same as the H_1 degree of $\mathfrak{T}_i$. Thus, for sufficiently large h, H_1 has at least $h_{H_1}+2$ primes of degree q^h. Let $\mathfrak{b}_1,\dots,\mathfrak{b}_{h_{H_1}+2}$ be these primes. Next consider the following $h_{H_1}+1$ H_1-divisors of degree zero: $\mathfrak{b}_2/\mathfrak{b}_1,\dots,\mathfrak{b}_{h_{H_1}}/\mathfrak{b}_1$. At least two of these divisors belong to the same divisor class, and thus for some $1\le i,j\le h_{H_1}+2$, $\mathfrak{b}_i/\mathfrak{b}_j$ is a principal divisor. Thus, there exists $t\in H_1$ such that its divisor is of the form $\mathfrak{p}/\mathfrak{q}$, where $\mathfrak{p},\mathfrak{q}$ are primes of H_1 of degree q^h.

Finally, we note that by Lemma 6.8, divisors $\mathfrak{p}$ and $\mathfrak{q}$ will remain prime in C_1H. Further, since degree of divisors does not change under separable constant field extensions, $\mathfrak{p}$ and $\mathfrak{q}$ will retain their degree. Therefore, C_1H, a finite constant extension of H, will possess the required element t.

We will next address the issue of the existence of the constants $c_1,\dots$ described in the statement of the lemma. To this end let $G=C_1H$ and denote its constant field by $C_G=C_1C$. Note that t is of order 1 at a prime of G and therefore is not a p-th power in G. Thus, the extension $G/C_G(t)$ is separable and finite by Lemma 6.5. Hence, there exists $\beta\in G$ such that $G=C_G(t,\beta)$. Next let L_1 be a finite subfield of C_G such that the following conditions are satisfied: The extension $G/L_1(\beta,t)=G_1$ is an (infinite) constant field extension, the constant field of $L_1(\beta,t)$ is L_1, and $C_1\subset L_1$. The first condition can be satisfied by any finite field L_1 by Lemma 6.4. Also, by definition of C_1, as in the argument above, the second condition implies that the extension C_G/L_1 contains no finite subextension of degree divisible by q. Note that the prime $\mathfrak{p}_1$ below $\mathfrak{p}$ in G_1 has the same degree in G_1 as $\mathfrak{p}$ in G, by Lemma 6.2. Thus, since there is no constant field extension from $L_1(t)$ to G_1, we can conclude that $[G_1:L_1(t)]$ is equal to the degree of $\mathfrak{p}_1$: q^h. Let N_1 be the Galois closure of G_1 over $L_1(t)$. Next let $L_2\subset C_G$ be any finite extension of L_1. Let $G_2=L_2(t,\beta)=L_2G_1$. Let $N_2=L_2N_1$. Note that the extensions $N_2/L_2(t,\beta)$ and $N_2/L_2(t)$ are Galois. From the above discussion, it follows that the G_2-divisor of t is of the form $\mathfrak{p}_2/\mathfrak{q}_2$, where $\mathfrak{p}_2$ and $\mathfrak{q}_2$ are G_2-primes of degree q^h. Further, since L_2/L_1 is a separable extension and since G_1 and $L_1(t)$ share the same constant field, G_2 and $L_2(t)$ have the same constant field L_2 and $[G_1:L_1(t)]=[G_2:L_2(t)]$ by [**1**, Theorem 11, page 280 and Theorem 14, page 282]. Additionally, $[N_2:L_2(t)]\le[N_1:L_1(t)]$, while

the genus' of N_2 and G_2 are equal to genus' of N_1 and G_1 respectively by [1, Theorem 22, page 291]. The following diagram describes the extensions involved.



Let $\mathfrak{b}_2$ be a factor of $\mathfrak{p}_2$ in N_2. Further, let $\sigma_2 \in \mathrm{Gal}(N_2/L_2(t))$ be an element of the decomposition group $G(\mathfrak{b}_2)$ of $\mathfrak{b}_2$ such that the equivalence class of σ_2 modulo the inertia group of $\mathfrak{b}_2$ is mapped onto the Frobenius automorphism ϕ_{L_2} of L_2 under the canonical homomorphism sending $G(\mathfrak{b}_2)$ to $\mathrm{Gal}(R_{2\mathfrak{b}_2}/L_2)$. Here $R_{2\mathfrak{b}_2}$ is the residue field of $\mathfrak{b}_2$. Then by the first part of Lemma 6.10 we have the following.

1) $\sigma_2^{[G_2:L_2(t)]} \in \mathrm{Gal}(N_2/G_2)$.
2) $[G_2 : L_2(t)]$ is the smallest positive exponent such that the corresponding power of σ_2 is in $\mathrm{Gal}(N_2/G_2)$.
3) σ_2 restricted to the constant field of N_2 is equal to ϕ_{L_2} where ϕ_{L_2} is the Frobenius automorphism of L_2.

Next let $\mathfrak{a}_2$ be a prime of $L_2(t)$ such that σ_2 is the Frobenius automorphism of some N_2-factor $\mathfrak{g}_2$ of $\mathfrak{a}_2$ in N_2. Then by the second part of Lemma 6.10 we can conclude that $\mathfrak{a}_2$ does not split in G_2.

Next we note that in the notations of Lemma 6.9, $a = 1$, and thus, assuming $\mathcal{C}$ is the conjugacy class of σ_2 in $\mathrm{Gal}(N_2/L_2(t))$,

$$
\begin{aligned}
&|C_1(N_2/L_2(t), \mathcal{C})| \\
&> \frac{|\mathcal{C}|}{[N_2 : L_2(t)]}|L_2| - |\mathcal{C}|(7g_{N_2} + 4)|L_2|^{1/2} \qquad (6.3)\\
&> |L_2|^{1/2}\left(\frac{1}{[N_1 : L_1(t)]}|L_2|^{1/2} - ([N_1 : L_1(t)](7g_{N_1} + 4))\right). \qquad (6.4)
\end{aligned}
$$

Hence, we can conclude that for sufficiently large $|L_2|$, arbitrarily large number of degree one primes of $L_2(t)$ will not split in G_2. For each natural number m, let $N(m)$ be the lower bound on the size of L_2 sufficient for the number of the non-splitting degree one primes to be greater than m. Let $\mathfrak{a}_2$, as above, be such a prime. Then, since there is no constant field extension from $L_2(t)$ to G_2, $[G_2 : L_2(t)] = f(\mathfrak{p}_2/\mathfrak{p}_2 \cap L_2(t)) = q^h = f(\mathfrak{g}_2 \cap G_2/\mathfrak{a}_2)$. Thus, again using the fact that there is no constant field extension from $L_2(t)$ to G_2, we conclude that $\mathfrak{g}_2 \cap G_2$ is of degree q^h in G_2 and will not split in the extension G/G_2.

Finally, we note that, that any degree one prime of $C_2(t)$ which is not a pole of t, is the zero of the element of the form $t + c$, where $c \in L_2$. Thus, keeping in mind that the pole of $t+c$ is the same as pole of t, we can conclude that the divisor of $t + c$ in G will be of the required form.

Lemma 6.12. *Let F/G be a finite separable extension of algebraic function fields. Let $\mathfrak{a}$ be a prime of G which does not split in F, i.e., $\mathfrak{a}$ has only one unramified prime factor $\mathfrak{A}$ in F and $f(\mathfrak{A}/\mathfrak{a}) = [F : G]$. Then there exist $\alpha \in F$ such that $F = G(\alpha)$, α is integral with respect to $\mathfrak{a}$ and such that $\mathfrak{a}$ is not a zero of the discriminant of α.*

Proof. Let $\alpha \in F$ be such that its residue class modulo $\mathfrak{A}$ generates the residue field of $\mathfrak{A}$ over the residue field of $\mathfrak{a}$. (Such an element exists because the residue field of $\mathfrak{A}$ is separable, by assumption, over the residue field of $\mathfrak{a}$.) Then α must be integral with respect to $\mathfrak{A}$ and thus with respect to $\mathfrak{a}$. Further, since the residue class of α is of degree $[F : G]$ over the residue field of $\mathfrak{a}$, $F = G(\alpha)$. Finally, since the residue class of α generate the residue field of $\mathfrak{A}$ over the residue field of $\mathfrak{a}$, $\mathfrak{a}$ cannot be a zero of the discriminant of α. (Otherwise the irreducible polynomial of α modulo $\mathfrak{a}$ will have multiple roots. This is impossible since by assumption the residue field extension is separable.)

Lemma 6.13. *Let H be an algebraic function field over a field of constants C_H. Let K be a constant field extension of H. Let C_K be the constant field of K and assume H is algebraically closed in K. Let $t \in H \setminus C_H$ be such that $H/C_H(t)$ is separable. Let $\mathfrak{a}$ be a prime of $C_H(t)$ remaining prime in*

H and such that its residue field is separable over C_H. Then $\mathfrak{a}$ will have just one prime factor in K.

Proof. Without loss of generality assume $\mathfrak{a}$ is not a pole of t and let $P(t)$ be the polynomial in t over C_H corresponding to $\mathfrak{a}$. By Lemma 6.12, there exists $\alpha \in H$ such that $H = C_H(\alpha, t)$, α is integral with respect to $\mathfrak{a}$, and $\mathfrak{a}$ is not a zero of the discriminant of α. Let $G(T)$ be the monic irreducible polynomial of α over $C_H(t)$. Then, given our assumptions on α and $\mathfrak{a}$, by [**21**, Proposition 25, page 27], $G(T)$ does not split modulo $\mathfrak{a}$. Next consider $P(t)$ over $C_K(t)$. Since H is algebraically closed in K, C_H is algebraically closed in C_K, and thus $P(t)$ will not factor in $C_K(t)$ by [**1**, Theorem 11, page 280]. Hence, $\mathfrak{a}$ will remain prime in $C_K(t)$. Next we want to show that $G(T)$ will not factor modulo $\mathfrak{a}$ over $C_K(t)$. First of all, observe that since $P(t)$ is separable over C_H, the residue field of $\mathfrak{a}$ as a prime of $C_H(t)$ is algebraically closed in the residue field of $\mathfrak{a}$ as a prime $C_K(t)$ by [**1**, Theorem 13, page 281]. Let $\bar{G}(T)$ is the image of $G(T)$ modulo $\mathfrak{a}$. By assumption, $\bar{G}(T)$ is irreducible over the residue field of $\mathfrak{a}$ as a prime of $C_H(t)$. Finally, since the residue field of $\mathfrak{a}$ as a prime of $C_H(t)$ is algebraically closed in the residue field of $\mathfrak{a}$ as a prime $C_K(t)$, again by [**1**, Theorem 11, page 280], $\bar{G}(T)$ will remain prime over the residue field of $\mathfrak{a}$ in $C_K(t)$. Since $K = C_K H = C_K(t, \alpha)$, we can use [**21**, Proposition 25, page 27] to conclude that $\mathfrak{a}$ will remain prime in K.

Lemma 6.14. *Let K be an algebraic function field over a field of constants C_K. Let $\mathfrak{t}$ be a prime of K. Let $R_{\mathfrak{t}}$ be the residue field of $\mathfrak{t}$ isomorphic to a finite extension of $C_{\mathfrak{t}}$ of C_K. Assume that $C_{\mathfrak{t}}$ is separable over C_K. Let C_{Gal} be the Galois closure of $C_{\mathfrak{t}}$ over C_K. Then in the extension $C_{\mathrm{Gal}}K/K$, $\mathfrak{t}$ will split into degree 1 factors. Further, the same statement will apply to any separable constant field extension of $C_{\mathrm{Gal}}K$.*

Proof. Let $\alpha \in K$ be such that the residue class of α modulo $\mathfrak{t}$ generates $C_{\mathfrak{t}}$ over C_K. Let $F(T) \in C_K[T]$ be the monic irreducible polynomial of the residue class of α over C_K. By assumption $F(T)$ is a separable polynomial. Let C_{Gal} be the splitting field of F. Let $a_1, \ldots, a_m$ be all the distinct roots of $F(T)$ in the algebraic closure of C_K. Since $F(T)$ does not factor over K (otherwise some symmetric function of a subset of $a_1, \ldots, a_m$ would be in $K \setminus C_K$), $a_1, \ldots, a_m$ are conjugates over C_K and K. Next note that $\mathbf{N}_{K(a_i)/K}(\alpha - a_i) = F(\alpha) \cong 0$ modulo $\mathfrak{t}$. Thus, for each i, $(\alpha - a_i)$ has a zero at a factor of $\mathfrak{t}$ in $K(a_i)$ and $K(a_1, \ldots, a_m)$. Further, $\alpha - a_i$ and $\alpha - a_j$ have no common zeros for $i \neq j$ because these elements differ by a nonzero constant. Hence, $\mathfrak{t}$ has at least degree$(F(T))$ factors in $K(a_1, \ldots, a_m)$. On the other hand, degree of $\mathfrak{t}$ over K is equal to the degree of $F(T)$ and this degree remains the same in $K(a_1, \ldots, a_m)$- a separable constant field extension of K. Thus all the factors of $\mathfrak{t}$ in $C_{\mathrm{Gal}}K$ are of degree 1. Finally, under any

separable constant field extension of $C_{\mathrm{Gal}}K$ all the divisors including factors of $\mathfrak{t}$ will retain their degree.

Lemma 6.15. *Let $\{\mathfrak{q}, \mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ be a set of primes of K. Let $\{b_1, \dots, b_m\}$ be a set of elements of K such that for each $i = 1, \dots, m, b_i$ is integral at $\mathfrak{p}_i$. Let $\{n_1, \dots, n_m\}$ be a set of natural numbers. Then there exists $y \in K$ satisfying the following requirements:*

1) $\mathrm{ord}_{\mathfrak{q}} y = -p^l$, *for some* $l \in \mathbb{N}$;
2) y *is integral at all the other primes of* K;
3) $\mathrm{ord}_{\mathfrak{p}_i}(y - b_i) \geq n_i$.

Proof. By the Strong Approximation Theorem ([14, page 21, Proposition 2.11]), there exists $y_1 \in K$ such that $\mathrm{ord}_{\mathfrak{p}_i}(y_1 - b_i) \geq n_i$, y_1 has a pole at $\mathfrak{q}$ and is integral at all the other primes. By a corollary of the Riemann-Roch Theorem, for any sufficiently large l, which we can assume to be greater than $\log_p(\mathrm{ord}_{\mathfrak{q}} y_1)$, there exists $y_2 \in K$ with a sole pole of order p^l at $\mathfrak{q}$, and for each $i = 1, \dots, m$, with a zero of order greater than $\mathrm{ord}_{\mathfrak{p}_i}(y_1 - b_i)$ at $\mathfrak{p}_i$. Next consider $y = y_1 + y_2$. Note that y will have the pole of the required order and $\mathrm{ord}_{\mathfrak{p}_i}(y - b_i) = \mathrm{ord}_{\mathfrak{p}_i}(y_1 + y_2 - b_i) \geq n_i$.

Lemma 6.16. *Let K be an algebraic function field over a field of constants C_K. Let t be a nonconstant element of K such that the extension $K/C_K(t)$ is finite and separable. Let $\tilde{C}_K$ be the algebraic closure of C_K and let $\tilde{K} = \tilde{C}_K K$. Then the extension $\tilde{K}/\tilde{C}_K(t)$ is separable. Further, let $\tilde{\mathfrak{T}}$ be a prime of $\tilde{C}_K(t)$ with ramified factors in $\tilde{K}$. Let $\mathfrak{T}$ be the prime below $\tilde{\mathfrak{T}}$ in $C_K(t)$. Then $\mathfrak{T}$ has ramified factors in K.*

Proof. Since $K/C_K(t)$ is a finite and separable extension, this extension is simple. Let α be a generator. Then the monic irreducible polynomial of α over $C_k(t)$ has no multiple roots. On the other hand, α will also generate $\tilde{K}$ over $\tilde{C}_K(t)$, and hence $\tilde{K}/\tilde{C}_K(t)$ is separable.

Next let $\hat{C}_K$ be the inseparable closure of C_K and let $\hat{K} = \hat{C}_K K$. Then the extension $\tilde{C}_K/\hat{C}_K$ is separable. Further, since $K/C_K(t)$ is separable, $n = [\hat{K} : \hat{C}_K(t)] = [K : C_K(t)]$. Assume $\mathfrak{T}$ has no ramified factors in K. Let $\{\omega_1, \dots, \omega_n\}$ be an integral basis with respect to $\mathfrak{T}$. Then by [3, Lemma 2, page 71], $\mathfrak{T}$ is neither a zero nor a pole of the discriminant of this basis. But $\{\omega_i\}_{i=1,\dots,n}$ is also a basis of $\hat{K}/\hat{C}_K(t)$. Thus, by the above cited lemma, no factor of $\mathfrak{T}$ in $\hat{C}_K(t)$ has ramified factors in $\hat{K}$. Finally consider the extension tower $\tilde{K} - \hat{K} - \hat{C}_K(t)$. Since the extension $\tilde{K}/\hat{K}$ is a separable constant field extension, no primes ramify. Thus, $\tilde{\mathfrak{T}}$, any factor of $\mathfrak{T}$ in $\hat{C}_K(t)$, has no ramified factors in $\tilde{K}$. Finally, we note that the extension $\tilde{K}/\tilde{C}_K(t)$ is a subextension of $\tilde{K}/\hat{C}_K(t)$, and thus $\tilde{\mathfrak{T}}$ has no ramified factors in $\tilde{K}$.

Lemma 6.17. *Let $\tilde{K}$ be an algebraic function field over an algebraically closed field of constants $\tilde{C}_K$. Let t be transcendental over $\tilde{C}_K$. Let $\tilde{K}$ be a separable extension of $\tilde{C}(t)$. Let $\mathfrak{t}$ be a prime of $\tilde{K}$ not ramifying in the extension $\tilde{K}/\tilde{C}(t)$ and not a pole of t. Let $x \in \tilde{K}$. Then $\mathrm{ord}_{\mathfrak{t}}\partial x/\partial \mathfrak{t} = \mathrm{ord}_{\mathfrak{t}} dx/dt$.*

Proof. By [22, page 96], $\mathrm{ord}_{\mathfrak{t}}\partial x/\partial \mathfrak{t} = \mathrm{ord}_{\mathfrak{t}}\partial t/\partial \mathfrak{t} + \mathrm{ord}_{\mathfrak{t}} dx/dt$. However, if $\mathfrak{t}$ is not ramified over $\tilde{C}(t)$, for some $a \in \tilde{C}$, $t + a$ is a local uniformizing parameter for $\mathfrak{t}$. Therefore, $\mathrm{ord}_{\mathfrak{t}}\partial t/\partial \mathfrak{t} = 0$.

Lemma 6.18. *Let K be an algebraic function field over the constant field C_K. Let C be the algebraic closure of a finite field in K. Let G be the algebraic closure of $C(u)$ in K, where $u \in K \setminus C_K$ and K is separable over $C_K(u)$. Then the extension $G/C(u)$ is finite.*

Proof. First of all, observe that $C(u)$ is algebraically closed in $C_K(u)$. Next, let $f \in G$. Then by [1, Theorem 11, page 280], $[C(f,u) : C(u)] = [C_K(f,u) : C_K(u)] \leq [K : C_K(u)]$. Thus, since G is separable over $C(u)$, the extension $G/C(u)$ must be finite.

References

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1986.

[2] J.W.S. Cassels and A. Frölich, *Algebraic Number Theory*, Thompson Book Co, Washington, D.C., 1967.

[3] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, **6**, AMS, 1951.

[4] J.-L. Colliot-Thélène, A.N. Skorobogatov and P. Swinnerton-Dyer, *Double Fibres and Double Covers: Paucity of Rational Points*, preprint.

[5] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly, **80** (1973), 233-269.

[6] M. Davis, Yu. Matijasevich and J. Robinson, *Positive Aspects of a Negative Solution*, Proc. Sympos. Pure Math., AMS, Providence, RI, 1976

[7] J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc., **48** (1975), 214-220.

[8] ———, *Diophantine sets over $\mathbb{Z}[T]$*, Proc. Amer. Math. Soc., **69** (1978), 148-150.

[9] ———, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc., **242** (1978), 391-399.

[10] ———, *The Diophantine Problem for Polynomial Rings of Positive characteristic*, Logic Colloquium 78, M. Boffa, D. van Dalen, K. MacAloon (eds.), North Holland, (1979), 131-145.

[11] ———, *Diophantine sets of algebraic integers*, II, Trans. of Amer. Math. Soc., **257**(**1**) (1980), 227-236.

[12] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc., **18**(**2**) (1978), 385-391.

[13] M. Eichler, *Introduction to Algebraic Numbers and Algebraic Functions*, Academic Press, New York, 1966.

[14] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, New York, 1986.

[15] W.-D. Geyer and M. Jarden, *Bounded Realization of l-groups over Global Fields*, to appear in Nagoya Mathematical Journal.

[16] G. Januz, *Algebraic Number Fields*, Academic Press, New York, 1973.

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

[18] ———, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, Journal of Algebra, **150**(**1**) (1992), 35-44.

[19] ———, *Diophantine unsolvability over p-adic function fields*, Journal of Algebra, **176** (1995), 83-110.

[20] S. Lang, *Algebra*, Addison Wesley, Reading, MA, 1971.

[21] ———, *Algebraic Number Theory*, Addison-Wesley, Reading, MA, 1970.

[22] R. Mason, *Diophantine Equations over Function Fields*, London Mathematical Society Lecture Notes Series, 96, Cambridge University Press, Cambridge, 1984.

[23] B. Mazur, *The topology of rational points*, Experimental Mathematics, **1**(**1**) (1992), 35-45.

[24] ———, *Questions of decidability and undecidability in number theory*, Journal of Symbolic Logic, **59**(**2**) (June 1994), 353-371.

[25] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. of Amer. Math. Soc., **104**(**2**) (1988).

[26] ———, *Hilbert's tenth problem for fields of rational functions over finite fields*, Inventiones Mathematicae, **103** (1991), 1-8.

[27] ———, *The diophantine theory of a ring of analytic functions*, Journal für die reine und angewandte Mathematik, **463** (1995), 153-167.

[28] ———, *An undecidability result for power series rings of positive characteristic*, II, Proceedings of American Mathematical Society, **100** (1987), 526-530.

[29] H. N. Shapiro and A. Shlapentokh, *Diophantine relations between algebraic number fields*, Communications on Pure and Applied Math., **XLII** (1989), 1113-1122.

[30] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Communications on Pure and Applied Math., **XLII** (1989), 939-962.

[31] ———, *Hilbert's tenth problem for rings of algebraic functions of characteristic zero*, Journal of Number Theory, **40**(**2**) (1992), 218-236.

[32] ———, *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Transaction of AMS, **333**(**1**) (1992), 275-298.

[33] ———, *A Diophantine definition of rational integers in some rings of algebraic numbers*, Notre Dame Journal of Formal Logic, **33**(**3**) (1992), 299-321.

[34] ———, *Diophantine relations between rings of S-integers of fields of algebraic functions in one variable over constant fields of positive characteristic*, Journal of Symbolic Logic, **58**(**1**) (March 1993), 158-192.

[35] ———, *Diophantine classes of holomorphy rings of global fields*, Journal of Algebra, **169**(**1**) (October 1, 1994), 139-175.

[36] ———, *Diophantine undecidability for some holomorphy rings of algebraic function fields of characteristic* 0, Communications in Algebra, **22**(**11**) (1994), 4379-4404.

[37] ———, *Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of* $\mathbb{Q}$, Annals of Pure and Applied Logic, **68** (1994), 299-325.

[38] ———, *Diophantine undecidability over algebraic function fields over finite fields of constants*, Journal of Number Theory, **58**(**2**) (June 1996), 317-342.

[39] ———, *The logic of pseudo S-integers*, Israel Journal of Mathematics, **101** (1997), 229-254.

[40] ———, *Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator*, Inventiones Mathematicae, **129** (1997), 489-507.

[41] C. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proceedings of American Math. Society, **120**(**1**), (January 1994), 249-253.

[42] A. Weil, *Basic Number Theory*, Springer Verlag, New York, 1974.

Received September 23, 1998 and revised January 15, 1999. The research for this paper has been partially supported by NSA grants MDA904-96-1-0019 and MDA904-98-1-0510.

East Carolina University
Greenville, NC 27858
E-mail address: shlapentokh@math.ecu.edu