TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 333, Number 1, September 1992

HILBERT'S TENTH PROBLEM FOR RINGS OF ALGEBRAIC FUNCTIONS IN ONE VARIABLE OVER FIELDS OF CONSTANTS OF POSITIVE CHARACTERISTIC

ALEXANDRA SHLAPENTOKH

ABSTRACT. The author builds an undecidable model of integers with certain relations and operations in the rings of S-integers of algebraic function fields in one variable over fields of constants of positive characteristic, in order to show that Hilbert's Tenth Problem has no solution there.

1. INTRODUCTION

Hilbert's Tenth Problem can be phrased as the following question: Is there an algorithm to determine, given an integer polynomial equation $f(x_1, \dots, x_n) = 0$, whether this equation has integer solutions? This question was answered negatively by M. Davis, J. Robinson, H. Putnam, and Y. Matijasevich. (See [1].) An analogous question can be asked of algebraic number fields, various polynomial rings and rings of algebraic functions. One way to resolve the problem negatively would be to construct a model of integers with certain operations and relations which would make the positive existential theory of that model undecidable, and to show that if Hilbert's Tenth Problem had solution in the ring under consideration, the constructed model would also become decidable.

J. Denef carried through such a construction in the polynomial rings of positive characteristic. (See [2].) The present paper extends this construction to the rings of S-integers of algebraic function fields in one variable over fields of constants of positive characteristic.

First we need to define a certain relation on rational integers which will be used in the construction of the above-mentioned undecidable model.

Definition 1.1. Let $x, y \in \mathbb{Z}$, p a rational prime. Then we will write "$x|^p y$" if $\exists k \in \mathbb{N}$ such that $y = \pm x p^k$.

The undecidability result which we are going to use in this paper is due to Denef (see [2]).

Theorem 1.1. *The positive existential theory of* $(\mathbb{Z}, +, |, |^p)$ *is undecidable.*

Received by the editors June 4, 1990. This paper has been presented at the AMS Research Conference in Amherst, July 1990.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 03Cxx, 03B25, 11Rxx, 11U05, 11U09.

In other words there is no uniform algorithm to tell whether there are solutions in rational integers to the following:

$$\left[\bigwedge_{i=1}^{n} F_i(a_1, \dots, a_k) \mid^p G_i(a_1, \dots, a_k)\right]$$

and

$$\left[\bigwedge_{i=1}^{m} H_i(b_1, \dots, b_j) \mid K_i(b_1, , \dots, b_j)\right],$$

where F_i, G_i, H_i, K_i are polynomials of degree 1 or less and $\bigwedge_{i=1}^{n}$ is a finite conjunction.

It is not hard to show that if the quotient field of the ring under consideration is not algebraically closed, expressions like "$h(x_1, \dots, x_n) = 0$ AND $g(y_1, \dots, y_m) = 0$" and "$h(x_1, \dots, x_n) = 0$ OR $g(y_1, \dots, y_m) = 0$" can be substituted by a single polynomial equation. (See [1].) Therefore, to resolve Hilbert's Tenth Problem it is enough to show that there is no algorithm to determine whether *a finite system of polynomial equations with coefficients in the ring* has solutions in the ring.

We will use the following terminology. Given an algebraic function field K of finite degree, an element f of K and a valuation p of K we will say that "f has a zero at p" if $\operatorname{ord}_p f > 0$, "$f$ has a pole at p" if $\operatorname{ord}_p f < 0$, and "$f$ is a unit of p" if $\operatorname{ord}_p f = 0$.

2. Pell equations in the rings of characteristic $p > 2$

The Pell equation $v^2 - dt^2 = 1$ plays a very important role in the proofs presented in this paper. In this section we will investigate the properties of the Pell equation in the rings of characteristic $p > 2$.

Definition 2.1. Let K be an algebraic function field, S a finite set of its valuations of size n. Then define a *ring of S-integers* $O_{K,S} \subset K$ to be the ring

$$O_{K,S} = \{x \in K, \ \forall p \notin S \operatorname{ord}_p x \geq 0\}.$$

In other words, $O_{K,S}$ is the ring of all the elements of K which have no poles outside S.

Definition 2.2. Let K be an algebraic function field, let $d \in O_{K,S}$ and assume d is not a square of K. Then define $H_{K,d,S}$ to be the following subset of $K(d^{1/2})$:

$$H_{K,d,S} = \{x - d^{1/2}y \mid x, y \in O_{K,S}, \ x^2 - dy^2 = 1\}.$$

Lemma 2.1. *Let K, d be as in the Definitions* 2.1 *and* 2.2. *Then $H_{K,d,S}$ is a group under multiplication.*

Proof. Denote $K(d^{1/2})$ by M, let $\varepsilon = x - d^{1/2}y$, $\delta = u - d^{1/2}w \in H_{K,d,S}$, and let $\varepsilon\delta = t - d^{1/2}v$, $x, y, u, w \in O_{K,S}$, $t, v \in K$. In fact, since $t = xu + dyw$, $v = xw + yu$, we see that t, v are also in $O_{K,S}$. Next we have the following implication chain. $\varepsilon, \delta \in H_{K,d,S} \Rightarrow N_{M/K}(\varepsilon) = 1$, $N_{M/K}(\delta) = 1 \Rightarrow N_{M/K}(\varepsilon\delta) = 1 \Rightarrow t^2 - dv^2 = 1$. This demonstrates that the set is closed under multiplication. Next we show that all the elements of the set have their inverses in the set. If $v - d^{1/2}t \in H_{K,d,S}$ then $(v - d^{1/2}t)^{-1} = v + d^{1/2}t = v - d^{1/2}(-t) \in H_{K,d,S}$ and, therefore, the lemma holds.

Lemma 2.2. *Let K, d be as above with the additional requirement that d is not a unit of $O_{K,S}$. Then the only constants in $H_{K,d,S}$ are ± 1.*

Proof. Suppose $x - d^{1/2}y \in H_{K,d,S}$ and $x - d^{1/2}y$ is a constant. $x^2 - dy^2 = 1$ implies that $x + d^{1/2}y = (x - d^{1/2}y)^{-1}$ is also a constant and, therefore, $2d^{1/2}y$ is a constant too. If y is not 0, this signifies that d is a unit and we get a contradiction with out assumption on d. Therefore $y = 0$ and $x = \pm 1$.

Lemma 2.3. *Assume $d \in O_{K,S}$ and is not a square of K. Let $x_1 - d^{1/2}y_1 \in H_{K,d,S}$ and let $x_m, y_m \in O_{K,S}$ be defined as*

$$x_m - \sqrt{d}y_m = (x_1 - \sqrt{d}y_1)^m, \tag{2.1}$$

where $m \in \mathbb{Z}$. Then $x_m - \sqrt{d}y_m \in H_{K,d,S}$ and the following statements are true:

$$x_{-m} = x_m, \qquad y_{-m} = -y_m, \tag{2.2}$$

$$x_{m\pm k} = x_m x_k \pm d y_m y_k, \qquad y_{m\pm k} = x_k y_m \pm x_m y_k, \tag{2.3}$$

$$k \mid m \Rightarrow y_k \mid y_m, \tag{2.4}$$

$$2k \mid m \Rightarrow x_k \mid y_m, \qquad m = (2l+1)k \Rightarrow x_k \mid x_m, \tag{2.5}$$

$$x_{m(\pm p^k)} = (x_m)^{p^k}. \tag{2.6}$$

Additionally, if $d = a^2 - 1$ and $x_1 = a$ and $y_1 = 1$, then

$$a - 1 \mid x_m - 1. \tag{2.7}$$

Proof. The proof easily follows from the fact that $H_{K,d,S}$ is a group (by Lemma 2.1), and from the binomial theorem.

Lemma 2.4. *Let w be an element of $O_{K,S}$ such that $\operatorname{ord}_{p_i} w \neq 0$ for all $p_i \in S$. Then if $H(T)$ is a polynomial in T over the field of constants of K, such that $H(T) \neq cT^k$ for any $k \in \mathbb{N}$ and any constant c, $H(w)$ is not a unit of $O_{K,S}$.*

Proof. Let $H(w) = \sum_{i=0}^{n} a_i w^i$, and let i, $0 \le i < n$, be the smallest index such that $a_i \neq 0$. Since it is enough to show that a factor of $H(w)$ is not a unit, we can divide by w^i and consider the resulting polynomial of degree at least 1. Therefore, without loss of generality, we can assume that a_0 is not 0. In this case $H(w)$ will share with w all of its poles and none of its zeros. Therefore, none of the zeros of $H(w)$ can come from the valuations of S. Since $H(w)$ is not constant, that fact implies that $H(w)$ must have a zero outside S and, therefore, cannot be a unit of $O_{K,S}$.

Lemma 2.5. *Suppose w is as described in Lemma 2.4 and let $F(T)$, $G(T)$ be separable polynomials over the field of constants of K. Then $F(w) \mid G(w)$ in $O_{K,S}$ implies $F(T) \mid G(T)$ as polynomials.*

Note. If $F(T)$, $G(T)$ have their coefficients in some finite field, then the conditions of the lemma are satisfied, since any extension of a finite field is separable.

Proof. Extend the field of constants by adding the roots of $F(T)$ and $G(T)$. Over that extended field we will have

$$F(w) = (w - a_1) \cdots (w - a_m), \tag{2.8}$$

$$G(w) = (w - b_1) \cdots (w - b_k), \tag{2.9}$$

where $a_1, \dots, a_m, b_1, \dots, b_k$ are algebraic over the field of constants of K.

Let $E = K(a_1, \dots, b_k)$ and let W be the set of all valuations extending valuations of S in E. Then E is separable over K and $O_{E,W}$ is the integral closure of $O_{K,S}$ in E. By our assumptions, $\operatorname{ord}_{p_i} w \neq 0$, $\forall p_i \in S$ and, hence, $\operatorname{ord}_{q_i} w \neq 0$, $\forall q_i \in W$. Therefore, by Lemma 2.4 applied to E, $w - a_i$, $i = 1, \dots, m$, is not a unit of $O_{E,V}$ for a_i a constant of $O_{E,V}$. The same, of course, applies to $w - b_i$, $i = 1, \dots, k$. Moreover, if a, b are constants of E, $w - a$ and $w - b$ cannot share any zeros unless $a = b$. Hence, if $F(w) = (w - a_1)\cdots(w - a_m) \mid G(w) = (w - b_1)\cdots(w - b_k)$ for any factor $w - a_i$ of $F(w)$, we must have $b_j = a_i$ for some j. It is also clear that the multiplicity of terms on the right must be at least as big as multiplicity on the left. Hence, $F(T) \mid G(T)$ as polynomials. Q.E.D.

Lemma 2.6. *Let w be as in the previous lemmas with the added condition that $\operatorname{ord}_{p_i} w$ is odd positive for $i = 1, \dots, n$ and negative for $i = 1$. Let $d = s^2 - 1$, where $s = w + 1$ and let $x_1 = s$, $y_1 = 1$. Then the following statements are true.*

1. *x_m, y_m are polynomials in s (and in w) over the field of constants with* $\deg(x_m) = |m|$ *and* $\deg(y_m) = |m| - 1$.
2. $y_k \mid y_m \Rightarrow k \mid m$.

Proof. First of all, we have to show that d is not a square of K. Indeed, $d = s^2 - 1 = w(w+2)$, $\operatorname{ord}_{p_i} d = \operatorname{ord}_{p_i} w + \operatorname{ord}_{p_i}(w+2) = \operatorname{ord}_{p_i} w =$ odd integer, for $i = 2, \dots, n$. So, assuming S contains more than one valuation, d is not a square. If S has only one valuation then d is not a square for the following reason. First of all, in this case the only invertible elements of $O_{K,S}$ are the constants. Secondly, if d is a square, then $s^2 - 1 = f^2$, $(s - f)(s + f) = 1$. Hence, $s \pm f$ must be a constant. Then s must be a constant. This is impossible, however, because by our assumption s has a pole at p_1.

We now proceed with the proof of the first assertion. Noting that $x_{-m} = x_m$ and $y_{-m} = -y_m$, we can assume $m \geq 0$. Then by the binomial theorem

$$x_m = \sum_{m-i \cong 0 \pmod 2} \binom{m}{i} s^i (s^2 - 1)^{(m-i)/2}. \tag{2.10}$$

The highest power of s in each term is m, the coefficient corresponding to that term is 2^{m-1} (it is the sum of either odd- or even-numbered binomial coefficients) which is not 0 since the characteristic is assumed to be different from 2. On the other hand

$$y_m = \sum_{m-i-1 \cong 0 \pmod 2} \binom{m}{i} s^i (s^2 - 1)^{(m-i-1)/2}. \tag{2.11}$$

Here the highest power of s in every term is $m - 1$ and the coefficient corresponding to that power is also 2^{m-1} (this is the other half of the sum of the binomial coefficients). Hence, as before, it is not 0. Since $x_m(s) = x_m(w + 1)$, $y_m(s) = y_m(w + 1)$, the degrees of x_m and y_m as polynomials in w are the same as their degrees as polynomials in s.

To prove the second assertion, we will start with showing that if $0 \leq k < m$, $y_m(s) = y_m(w + 1)$ cannot divide $y_k(s) = y_k(w + 1)$ in $O_{K,S}$ unless $k = 0$. Suppose $k > 0$, $k < m$, and $y_m \mid y_k$. $y_m(s) = y_m(w+1)$ is a polynomial in w

of degree $m-1$ over the field constants and $y_k(s) = y_k(w+1)$ is a polynomial of degree $k-1$ in w over the same field. By Lemma 2.5, $y_m(w+1) \mid y_k(w+1)$ if and only if $y_m(T+1) \mid y_k(T+1)$ as polynomials in T over the field of constants. But then $\deg(y_m(T+1)) \leq \deg(y_k(T+1))$, unless $y_k(T+1) \equiv 0$. That is either $m-1 \leq k-1$ or $y_k(T+1) \equiv 0$. The inequality contradicts our assumption on k and m, and, therefore, $y_k(T+1) \equiv 0$. This can happen only if $k = 0$.

Now suppose $y_k \mid y_m$. $m = kq + r$, where $0 \leq r < k$. By Lemma 2.3, we then have $y_m = x_{kq}y_r + y_{kq}x_r$ and by Lemma 2.3, $y_k \mid y_{kq}$. On the other hand, by Lemma 2.4, $y_k(w+1)$ is not a unit and, therefore, it must have zeros at valuations not in S. For any such valuation p, $\operatorname{ord}_p x_{kq} = 0$. Otherwise, as p is not in S, $\operatorname{ord}_p x_{kq} > 0$ and

$$\operatorname{ord}_p 1 = \operatorname{ord}_p(x_{kq}^2 - dy_{kq}^2) = \operatorname{ord}_p(x_{kq}^2 - dg^2y_k^2) > 0,$$

where $y_{kq} = gy_k$, $g \in O_{K,S}$. Therefore, $y_k \mid y_r$, with $r < k$. By the argument above, $r = 0$ and $k \mid m$.

Lemma 2.7. *Let w be as in the previous lemma, let $s = w+1$, let $d = s^2 - 1$, and let $D = (2s-1)^2 - 1$. Then the groups*

$$H_{K,d,S} = \{f - (s^2-1)^{1/2}g,\ f, s \in O_K \mid f^2 - (s^2-1)g^2 = 1\},$$
$$H_{K,D,S} = \{f - ((2s-1)^2-1)^{1/2}g,\ f, s \in O_K \mid f^2 - ((2s-1)^2-1)g^2 = 1\}$$

are cyclic $\operatorname{mod} \{\pm 1\}$. *The indices of the subgroups of $H_{K,d,S}$ and $H_{K,D,S}$ generated by $\pm(s - (s^2-1)^{1/2})$ and $\pm((2s-1) - (2s-1)^{1/2})$ respectively, are divisors of* $|\operatorname{ord}_{p_1} w|$.

Proof. Consider $H_{K,d,S}$. First of all, we want to show that $p_2, \dots, p_n$ will all ramify in $M = K((s^2-1)^{1/2})$. $\operatorname{Ord}_{p_i}(s^2-1) = \operatorname{ord}_{p_i} w(w+2) = \operatorname{ord}_{p_i} w =$ odd number for $i = 2, \dots, n$. Let β_i lie above p_i in M. Then

$$2\operatorname{ord}_{\beta_i}(s^2-1)^{1/2} = \operatorname{ord}_{\beta_i}(s^2-1) = k\operatorname{ord}_{p_i}(s^2-1)$$

where k is the exponent of the highest power of β_i dividing p_i. Since $\operatorname{ord}_{p_i}(s^2-1)$ is odd for $i = 2, \dots, n$ we must conclude from the above equalities that $k = 2$, that is, p_i's are ramified for $i = 2, \dots, n$.

Consider now an element $\varepsilon = x - d^{1/2}y = (x + d^{1/2}y)^{-1} \in H_{K,d,S}$. Let β be a valuation of $M = K(d^{1/2})$ such that $\operatorname{ord}_\beta \varepsilon > 0$ (< 0). Then $\operatorname{ord}_\beta \varepsilon^{-1} < 0$ (> 0). So $\operatorname{ord}_\beta(\varepsilon + \varepsilon^{-1}) < 0$, i.e. $\operatorname{ord}_\beta x < 0$. Therefore, all of the poles and zeros of ε must come from the valuations extending valuations from S. On the other hand, ε is of norm 1, and so its zeros and poles cannot correspond to valuations which either do not split or are completely ramified in M. Indeed, if β, a valuation of M, is the only valuation lying above p, a valuation of K, and ε is not a unit at β, then $N_{M/K}(\varepsilon)$ is not a unit at p. Hence, p_1, the only valuation of S which is not necessarily totally ramified in M, must split in M into β_{11} and β_{12} which would generate zeros and poles for ε. Since the degree of zeros must be equal to the degree of poles we must also have $\operatorname{ord}_{\beta_{11}} \varepsilon = -\operatorname{ord}_{\beta_{12}} \varepsilon$.

Consider now a homomorphism from $H_{K,d,S}$ into $\mathbb{Z}$:

$$\varepsilon \to \operatorname{ord}_{\beta_{11}} \varepsilon.$$

The image of this homomorphism is an additive subgroup of integers and, therefore, the image is cyclic. The kernel of the map contains elements of M without zeros or poles, and consequently must be a set of constants of M. However, the only constants of $H_{K,d,S}$, by Lemma 2.2, are ± 1. Hence the $H_{K,d,S}$ must be cyclic mod ± 1.

Now, assume that $x - d^{1/2}y$ is a generator of $H_{K,d,S}$. Without loss of generality we can also assume that

$$\mathrm{ord}_{\beta_{11}}(x - (s^2-1)^{1/2}y) = -\mathrm{ord}_{\beta_{11}}(x + (s^2-1)^{1/2}y) < 0.$$

Hence,

$$\begin{aligned}\mathrm{ord}_{\beta_{11}}(x - (s^2-1)^{1/2}y) &= \mathrm{ord}_{\beta_{11}}[(x - (s^2-1)^{1/2}y) + (x + (s^2-1)^{1/2}y)]\\ &= \mathrm{ord}_{\beta_{11}} 2x = \mathrm{ord}_{\beta_{11}} x = \mathrm{ord}_{p_1} x.\end{aligned}$$

Hence, if $(s - (s^2-1)^{1/2}) = (x - (s^2-1)^{1/2}y)^k$ then $|\mathrm{ord}_{p_1} s| = |k\, \mathrm{ord}_{p_1} x|$. On the other hand, $\mathrm{ord}_{p_1} s = \mathrm{ord}_{p_1}(w+1)$ and hence, the statement of the lemma holds for $H_{K,d,S}$.

$(2s-1)^2 - 1 = (2s-2)(2s) = 4(s-1)s = 4w(w+1)$. Therefore,

$$\begin{aligned}\mathrm{ord}_{p_i}((2s-1)^2-1) &= \mathrm{ord}_{p_i} w + \mathrm{ord}_{p_i}(w+1)\\ &= \text{odd positive number for } i = 2, \dots, n.\end{aligned}$$

Hence, $p_2, \dots, p_n$ will ramify in $K((2s-1)^2-1)^{1/2}$ for the same reasons they ramify in M. Moreover, $\mathrm{ord}_{p_1} 2s - 1 = \mathrm{ord}_{p_1} s$. Hence, the proof of the assertion concerning $H_{K,D,S}$ will proceed in the same way as the proof of the assertion concerning $H_{K,d,S}$.

Lemma 2.8. *Let* s, w, $H_{K,d,S}$, $H_{K,D,S}$ *be as in the previous lemma and assume additionally that* $\mathrm{ord}_{p_1} s = -2^j p^k$, *where* $j, k \in \mathbb{N}$, *and* p *is the characteristic of the field. Assume also that* W *is not a unit. Then* $s - (s^2-1)^{1/2}$ *and* $(2s-1) - ((2s-1)^2-1)^{1/2}$ *generate* $H_{K,d,S}$ *and* $H_{K,D,S}$ *respectively modulo* $\{\pm 1\}$.

Proof. Let $(x - (s^2-1)^{1/2}y)^2 = s - (s^2-1)^{1/2}$. Then $x^2 + (s^2-1)y^2 = s$, $2xy = 1$, $y = 1/2x$. Hence,

$$x^2 + (s^2-1)(1/4x^2) = s, \tag{2.12}$$

$$4x^4 - 4sx^2 + (s^2-1) = 0, \tag{2.13}$$

$$x^2 = \frac{s \pm \sqrt{s^2 - s^2 + 1}}{2} = \frac{(s \pm 1)}{2}. \tag{2.14}$$

Therefore, $s \pm 1$ is a unit and this contradicts our assumptions on s.

Suppose now we have

$$(x - \sqrt{(2s-1)^2 - 1y})^2 = (2s-1) - \sqrt{(2s-1)^2 - 1}.$$

Carrying out the same argument as above we will arrive at $x^2 = ((2s-1) \pm 1)/2$, $s = x^2$ or $(s-1) = x^2$. That is, $s-1$ or s is a unit, which is again impossible by our assumptions on $w = s-1$.

Now assume $(x - (s^2-1)^{1/2}y)^p = s - (s^2-1)^{1/2}$. Then $y(s^2-1)^{p-1/2} = 1$. This is impossible, since $s^2 - 1 = w(w+2)$ is not a unit. On the other hand,

$$(x - \sqrt{(2s-1)^2 - 1y})^p = (2s-1) - \sqrt{(2s-1)^2 - 1}$$

is impossible for the same reason.

By Lemma 2.6, if $s - (s^2 - 1)^{1/2}$ and $(2s - 1) - \sqrt{(2s-1)^2 - 1}$ do not generate $H_{K,d,S}$ and $H_{K,D,S}$, respectively, they must be either pth or 2nd powers of some other units of the respective quadratic extensions of K. Since it is impossible, they must generate the groups.

Lemma 2.9. *Let $G(T)$ be a polynomial over the field of constants of K, and assume $G(s) = 0$ for some nonconstant element s of K. Then $G(T) \equiv 0$ as a polynomial.*

Proof. If $G(T)$ is not identically zero as a polynomial then s is algebraic over the field of constants and, therefore, is a constant itself. This would contradict our assumption on s.

In case S contains only one valuation the situation is simpler than in the case of bigger S.

Lemma 2.10. *Assume S contains only one valuation q. Then for any integral nonconstant $s \in K$, $H_{K,d,S}$ is a cyclic group under multiplication modulo ± 1, generated by $s - (s^2 - 1)^{1/2}$.*

Proof. Let $M = K(\sqrt{s^2 - 1})$, and let V be the set of all the valuations of M lying above the unique valuation of S. $s^2 - 1$ is not a unit of $O_{K,S}$ because, under our assumptions, $O_{K,S}$ has no nonconstant units. Consider now an element of M, $\varepsilon = s - (s^2 - 1)^{1/2}$. It is a nonconstant unit of $O_{M,V}$ with $N_{M/K}(s - (s^2 - 1)^{1/2}) = 1$. By arguments similar to the ones from the preceding lemmas, all the zeros and poles of ε must come from valuations extending the unique valuation in S. M can have at most two such valuations. Since at least two valuations are needed for a zero and a pole of $s - \sqrt{s^2 - 1}$, M must have two such valuations. Call them q_{11} and q_{12}.

Let $\omega = x - (s^2 - 1)^{1/2} y$ be an element of H. Then $\operatorname{ord}_{q_{11}} \omega = -\operatorname{ord}_{q_{12}} \omega$. Consider now the following homomorphism from $H_{K,d,S}$ into the rational integers:

$$\omega \to \operatorname{ord}_{q_{11}} \omega .$$

Any element of the kernel of that map is an element of $H_{K,d,S}$ with no zeros or poles, that is a constant. The only constants in $H_{K,d,S}$ are ± 1, by Lemma 2.2. Hence, $H_{K,d,S}$ is cyclic $\mod \{\pm 1\}$.

Next we will show that $\varepsilon = s - (s^2 - 1)^{1/2}$ is the generator $\mod \{\pm 1\}$. Suppose $\varepsilon = \omega^m$ for some $\omega \in H_{K,d,S}$, that is $\varepsilon = (x^2 - (s-1)^{1/2} y)^m$. From Lemma 2.3, $y \mid 1$ and either $x \mid 1$ or $x \mid s$, depending on whether m is odd or even. As has been mentioned before, $O_{K,S}$ has no other units but constants. Hence y is a constant. Since $x^2 - (s^2 - 1)y^2 = 1$, x is not a constant, otherwise $s^2 - 1$ is a constant, and therefore m is odd, whereas $x \mid s$. Then, however, we have

$$(us)^2 - (s^2 - 1)y^2 = 1, \tag{2.15}$$

$$u^2 s^2 - s^2 y^2 = 1 - y^2 . \tag{2.16}$$

Unless $y^2 = 1$, (2.16) implies s is a constant. Consequently, $y^2 = u^2 = 1$ and $m = \pm 1$.

Lemma 2.11. *Let d, D, s be defined as in Lemmas 2.7 and 2.8, and let $x_m(s) - d^{1/2} y_m(s) = (s - d^{1/2})^m$, $x_h(2s-1) - D^{1/2} y_h(2s-1) = ((2s-1) - D^{1/2})^h$ where*

m, $h \in \mathbb{Z}$, and assume

$$\pm x_m(s) = \pm\frac{1}{2}x_h(2s-1) + \frac{1}{2}, \tag{2.17}$$

with the signs not necessarily synchronized. Then $m = \pm h = \pm p^k$ and both signs are actually "+" 's.

Proof. Since by Lemma 2.3, $x_{-m}(s) = x_m(s)$, we can assume without loss of generality that $m, h \geq 0$. Under this assumption, we will show that $m = h$. By Lemma 2.7, $x_m(s)$ is a polynomial in s of degree m over the field of constants, and $x_h(2s-1)$ is also a polynomial in s over the field of constants but of degree h. Hence, by Lemma 2.10, $x_m(s)$ and $\frac{1}{2}x_h(2s-1)$ must be identical polynomials, and, in particular, their degrees must be the same. Let $h = qp^k$, where $(q, p) = 1$. Then we have the following.

$$\pm x_h(s) = \pm x_{qp^k}(s) = \pm(x_q(s))p^k = (\pm x_q(s))^{p^k}. \tag{2.18}$$

$$\begin{aligned} \pm\frac{1}{2}x_h(2s-1) + 1 &= \pm\frac{1}{2}x_{qp^k}(2s-1) + 1 \\ &= \pm\frac{1}{2}(x_q(2s-1))^{p^k} + 1 \\ &= \left(\pm\frac{1}{2}x_q(2s-1) + 1\right)^{p^k}, \end{aligned} \tag{2.19}$$

since $2^{p^k} \cong 2 \pmod p$. Therefore, we can rewrite (2.17) as

$$\pm x_q(s) = \pm\frac{1}{2}x_q(2s-1) + \frac{1}{2}. \tag{2.20}$$

Suppose now that

$$x_q(s) = A_q s^q + A_{q-1}s^{q-1} + \cdots + A_0, \tag{2.21}$$

$$\begin{aligned} x_q(2s-1) &= A_q(2s-1)^q + A_{q-1}(2s-1)^{q-1} + \cdots + A_0 \\ &= A_q 2^q s^q + (A_q q 2^{q-1}s^{q-1} + A_{q-1}2^{q-1}s^{q-1}) \\ &\quad + \text{terms of lower order in } s. \end{aligned} \tag{2.22}$$

From (2.20)–(2.22) we then derive, if $q > 1$,

$$\pm 2A_{q-1} = \pm q2^{q-1}A_q \pm 2^{q-1}A_{q-1}. \tag{2.23}$$

Next we show that $A_{q-1} = 0$. Returning to the definition of $x_q(s)$ we see that

$$\begin{aligned} x_q(s) &= s^q + \binom{q}{2}s^{q-2}(s^2-1) + \cdots + \binom{q}{2r}s^{q-2r}(s^2-1)^r \\ &= \sum\binom{q}{2r}s^{q-2r}\sum\binom{r}{i}s^{2i}(-1)^{r-i} \\ &= \sum_{\substack{0\leq r\leq q/2 \\ 0\leq i\leq r}}(-1)^{r-i}\binom{q}{2r}\binom{r}{i}s^{q-2r+2i}. \end{aligned} \tag{2.24}$$

The only powers of s which appear in $x_q(s)$ with possible nonzero coefficients are of the form $q-$even number and $q-1$ is not among them. Hence, $A_{q-1} = 0$

and, therefore, from the above, $q2^{q-1}A_q = 0$. A_q is not zero since $q > 0$, and $x_q(s)$ is a polynomial of degree q in s by Lemma 2.7. Moreover, no power of 2 is zero $\bmod p$. Hence, q must be zero $\bmod p$. This contradicts our assumption, and so $q = 1$. Now,

$$\frac{1}{2}x_{p^k}(2s-1) = \frac{1}{2}(2^{p^k}s^{p^k} - 1) = x_{p^k}(s) - \frac{1}{2}. \tag{2.25}$$

Hence, the only possible choice of signs on both sides is "+".

Lemma 2.12. *Suppose $w \in O_{K,S}$ is not a unit and, if S contains more than one valuation, assume additionally that w has the following properties.*

1. $\mathrm{ord}_{p_i} w$ *is positive odd for* $i = 2, \dots, m$.
2. $\mathrm{ord}_{p_1} w$ *is* $-2^j p^k$ *where* $j, k \geq 0$.

Let $s = w + 1$. (We will say that s satisfies "pth-power conditions.") Then for any $f \in O_{K,S}$ the equations

$$f^2 - (s^2 - 1)h^2 = 1, \tag{2.26}$$

$$(2f - 1)^2 - ((2s - 1)^2 - 1)g^2 = 1, \tag{2.27}$$

have solutions in $O_{K,S}$ in variables g and h if and only if $\exists l \in \mathbb{N}$ such that $f = s^{p^l} \Leftrightarrow f = x_{\pm p^l}(s)$. (In case $|S| = 1$, no assumptions on w are necessary beyond being nonconstant.)

For future reference denote (2.26) and (2.27) by $\mathrm{PPE}(f, s, g, h)$. Here "PPE" stands for "pth power equations." Then the statement of the lemma can be rewritten as:

If $s \in O_{K,S}$ satisfies "pth-power conditions" then $\forall f \in O_{K,S}$,

$$\exists g, h \in O_{K,S} \mathrm{PPE}(f, s, g, h) \Leftrightarrow \exists l \in \mathbb{N},\ f = s^{p^l}.$$

Proof. Let $H_{K,d,S}$ and $H_{K,D,S}$ be defined as in previous lemmas. Then, by Lemma 2.8, for the case of S containing more than one valuation, and by Lemma 2.10 for the case of a unique valuation in S, $s - (s^2 - 1)^{1/2}$, $(2s - 1) - \sqrt{(2s-1)^2 - 1}$ generate $H_{K,d,S}$ and $H_{K,D,S}$ respectively modulo ± 1. So suppose (2.26) and (2.27) are satisfied in $O_{K,S}$. By the above considerations we can conclude that

$$2f - 1 = \pm x_m(2s - 1), \qquad f = \pm x_h(s), \tag{2.28}$$

where $x_h(s)$ and $x_m(2s-1)$ are defined in the previous lemma. Therefore, from (2.26) and (2.27) we derive (2.17) and conclude that both signs in (2.28) are "+", $m = h = \pm p^k$, by Lemma 2.11, and $f = x_{\pm p^k}(s) = s^{p^k}$ for some integer $k \geq 0$, by Lemma 2.3. Conversely, suppose $f = s^{p^k}$. Then set $h = (s^2 - 1)^{(p^k-1)/2}$ and (2.26) is satisfied. Since $2f - 1 = (2s - 1)^{p^k}$, if $g = ((2s - 1)^2 - 1)^{(p^k-1)/2}$ (2.27) is satisfied.

3. Construction of a model of $(\mathbb{Z}, |, +, |_p)$ in the rings of algebraic function of characteristic $p > 2$

Definition 3.1. Let $f, g \in O_{K,S}$. Then define $(f, g) = 1$ to mean

$$\forall p \notin S\ (\mathrm{ord}_p f > 0 \text{ or } \mathrm{ord}_p g > 0) \Rightarrow \mathrm{ord}_p(f + g) = 0.$$

(In other words, f and g have no common zeros, except possibly at valuations of S.)

Lemma 3.1. *Let K, S be defined as before. Then the set of constants of K is Diophantine over $O_{K,S}$.*

Proof. If $O_{K,S}$ contains only finitely many constants we are done. So assume that $O_{K,S}$ has infinitely many constants. Let $|S| = n$; then $O_{K,S}$ must have a constant of an order bigger than $n+1$. (Otherwise all the constants of K are contained in a finite field of the size $p^k > n+1$.) So let t be such a constant, and consider the following system of equations:

$$(j+t)x_1 = 1, \tag{3.1.1}$$

$$(j+t^2)x_2 = 1, \tag{3.1.2}$$

$$\dots$$

$$(j+t^{n+1})x_{n+1} = 1. \tag{3.1.n+1}$$

We will show that this system of equations has solutions j, $x_1, \dots, x_{n+1}$ in $O_{K,S}$ if and only if j is a constant. So suppose this system is satisfied in $O_{K,S}$. If j is not a constant then $j+t^i$ is also not a constant for $i = 1, \dots, n+1$ and, therefore, each of these elements, being a nonconstant unit of $O_{K,S}$, must have a zero at a valuation of S. But S contains only n valuations, so at least two of the above mentioned elements, $j+t^i$ and $j+t^k$, $i \neq k$, must share a zero at some valuation p of s. Therefore, the

$$\operatorname{ord}_p(t^i - t^k) > 0. \tag{3.2}$$

On the other hand, t is a constant, and the only way (3.2) is going to hold is for $t^i - t^k = 0$. This equality cannot hold, however, since $0 < i, k \leq n+1$ and order of t is, by assumption, bigger than $n+1$. Therefore, our supposition that j was not a constant is false.

Conversely, if j is a constant different from $-t^i$, $1 \leq i \leq n+1$, $j+t^k$ is a nonzero constant for any integer $1 \leq k \leq n+1$, and therefore it is invertible in $O_{K,S}$.

Lemma 3.2. *Let s be a fixed element of $O_{K,S}$. Then the set*

$$\{f \in O_{K,S} \mid (f, s) = 1\}$$

is Diophantine over $O_{K,S}$.

Proof. Let $\prod q_i^{a_i}$ be the non-S part of the divisor of s. For every i, residue class field of q_i is a finite extension of the field of constants of degree d_i. If $u \in O_{K,S}$ and $u \not\cong 0 \bmod q_i$, then u must satisfy $\bmod q_i$ a polynomial of degree less or equal to d_i with constant coefficients and a nonzero free term. Moreover, if

$$a_{0i} + q_{1i}u + \dots + a_{d_i i}u^{d_i} \cong 0 \pmod{q_i},$$

then

$$(a_{0i} + a_{1i}s + \dots + a_{d_i i}u^{d_i})^{a_i} \cong 0 \pmod{q_i^{a_i}}.$$

So we can conclude that the following statements are equivalent.

1. $\prod_j (a_{0i} + a_{1i}u + \dots + a_{d_i i}u^{d_i})^{a_j} \cong 0 \bmod s$, a_{ij} are constants, $a_{0i} \neq 0$.
2. $(s, u) = 1$.

By Lemma 3.1 the set of constants of K is Diophantine over $O_{K,S}$. It is easy to see, that the set of nonzero constants of K is also Diophantine over $O_{K,S}$, and so the first statement can be rewritten in a completely Diophantine fashion.

Lemma 3.3. *Let $y \in O_{K,S}$ be a nonconstant such that $\operatorname{ord}_p y \neq 0$ $\forall p \in S$, and let $F(T)$ and $G(T)$ be polynomials in the variable T over some finite subfield C of the constant field of K with $F(0) \neq 0$ or $G(0) \neq 0$. Furthermore, assume that $(F(y), G(y)) = 1$. Then $\exists a > b \in \mathbb{N}$ such that $(G(y))^{p^a - p^b} \cong 1 \bmod F(y)$.*

Proof. First of all, we will show that $(F(T), G(T)) = 1$ as polynomials over C. Suppose not, that is suppose $\exists H(T) \in C[T]$ such that $H(T) \mid F(T)$ and $H(T) \mid G(T)$. Since either $F(T)$ or $G(T)$ is not divisible by T, $H(T)$ is not a power of T times a constant. Therefore, $H(y)$ is not a unit of $O_{K,S}$, by Lemma 2.4. On the other hand, $H(y)$ will be a common divisor of $G(y)$ and $F(y)$ and we have a contradiction with the fact that $(F(y), G(y)) = 1$.

Next, consider a finite ring $C[T]/F(T)$ which contains a multiplicative group of all the nonzero divisors of the ring. The equivalence class of $G(T)$, $[G(T)]$, will not be a zero divisor in the ring, since as polynomials in T, $F(T)$ and $G(T)$ are relatively prime, by the argument above. Hence, $[G(T)]$ will belong to the finite multiplicative group of the ring and, consequently, $[G(T)]^u = [1]$, where u is the size of the group. Let $u = p^x u_1$, where $(u_1, p) = 1$. Then for some z, $p^z \cong 1 \bmod u_1$. Therefore, $u \mid p^x(p^z - 1)$ and $G(T)^{p^{x+z} - p^x} \cong 1 \bmod F(T)$ in $C[T]$, and consequently, $G(y)^{p^{x+z} - p^x} \cong 1 \bmod F(y)$ in $O_{K,S}$. Q.E.D.

Lemma 3.4. *Assume S contains at least two valuations and let w_1 and w_2 be such that they are not units of $O_{K,S}$ and for $j = 1, 2$, $i = 1, \dots, m$, $\operatorname{ord}_{p_j} w_j = -2^{h_j} p^{k_j}$, $h_j, k_j \in \mathbb{N}$, $\operatorname{ord}_{p_i} w_j =$ odd positive, for $i \neq j$, $\operatorname{ord}_{p_1} w_2 \geq |\operatorname{ord}_{p_1} w_1|$. Let $s_i = w_i + 1$, $i = 1, 2$, and let*

$$z(m) = \left\{ n \in \mathbb{N} \mid n \geq \log_p m \geq \left[\log_p \frac{m |\operatorname{ord}_{p_1} s_1|}{\operatorname{ord}_{p_1} w_2} \right] \right\}, \tag{3.3}$$

$$T(m, z) = w_2^{p^z} (w_2^{p^z} x_m(s_1) + 1), \tag{3.4}$$

where, as before,

$$x_m(s_1) - (s_1^2 - 1)^{1/2} y_m(s_1) = \left[s_1 - (s_1^2 - 1)^{1/2} \right]^m,$$

and $x_m(s_1), y_m(s_1) \in O_{K,S}$. Then, $s_1^{p^k}$, $s_2^{p^e}$, for any $e, k \geq 0$, and any $T(m, z) + 1$ such that $z \in z(m)$ for some m, satisfy the "pth-power conditions."

Proof. Any pth power of s_1 and s_2 will satisfy the "pth-power conditions" by definition of these conditions. To show that $T(m, z) + 1$ satisfies the conditions if $z \in z(m)$, we have to determine what kind of zeros and poles $x_m(s_1)$ has at the valuations contained in S. As has been shown before,

$$\begin{aligned} x_m(s_1) &= \sum_{2i\leq m}\binom{m}{2i}s_1^{m-2i}(s_1^2-1)^i \\ &= \sum_{2i\leq m}\binom{m}{2i}(w_1+1)^{m-2i}(w_1(w_1+2))^i \\ &= \sum_{2i\leq m}\binom{m}{2i}w_1^m + \text{terms of lower order in } w_1 \\ &\qquad\qquad\qquad \text{with coefficients in } \mathbb{Z}_p. \end{aligned} \tag{3.5}$$

Hence,

$$\operatorname{ord}_{p_1} x_m(s_1) = m \operatorname{ord}_{p_1} w_1 = -m2^j p^k \tag{3.6}$$

and

$$\operatorname{ord}_{p_i} x_m(s_1) = 0 \quad \text{for } i = 2, \dots, m. \tag{3.7}$$

Therefore, from (3.3) and (3.6) we obtain for $z \in z(m)$

$$p^z \operatorname{ord}_{p_1} w_2 > -m \operatorname{ord}_{p_1} s_1 . \tag{3.8}$$

Denote $T(z, m)$ by T. Then

$$\begin{aligned} \operatorname{ord}_{p_1} T &= p^z \operatorname{ord}_{p_1} w_2 + \min(p^z \operatorname{ord}_{p_1} w_2 + m \operatorname{ord}_{p_1} s_1 , 0) \\ &= p^z \operatorname{ord}_{p_1} w_2 , \end{aligned} \tag{3.9}$$

and so

$$\operatorname{ord}_{p_1} T = 2k+1, \qquad k \in \mathbb{N}. \tag{3.10}$$

On the other hand,

$$\begin{aligned} \operatorname{ord}_{p_2} T &= p^z \operatorname{ord}_{p_2} w_2 + \min(p^z \operatorname{ord}_{p_2} w_2 + \operatorname{ord}_{p_2} x_m(s_1), 0) \\ &= p^z \operatorname{ord}_{p_2} w_2 + p^z \operatorname{ord}_{p_2} w_2 , \end{aligned} \tag{3.11}$$

and

$$\operatorname{ord}_{p_2} T = 2p^z \operatorname{ord}_{p_2} w_2 = -2^{h_2+1}p^{k_2+z} . \tag{3.12}$$

At the same time,

$$\begin{aligned} \operatorname{ord}_{p_i} T &= p^z \operatorname{ord}_{p_i} w_2 + \min(p^z \operatorname{ord}_{p_i} w_2 + \operatorname{ord}_{p_i} x_m(s_1), 0) \\ &= p^z \operatorname{ord}_{p_i} w_2 = 2j+1, \qquad j \in \mathbb{N},\ i = 3, \dots, n. \end{aligned} \tag{3.13}$$

Since T is integral at all the other valuations of K, $T+1 = T(m, z)+1$ satisfies the "pth-power conditions."

Lemma 3.5. *Let* $s_1 = w_1 + 1$, $s_2 = w_2 + 1$, $X = x_m(s_1)$ *be defined as before, let* $U \in O_{K,S}$ *be given, and let* $z_1 \in z(1)$ *and* $T_1 = T(1, z_1)$ *be fixed. Then the following system of equations and conditions* (3.14)–(3.27) *can be satisfied in all* *the other variables in* $O_{K,S}$ *if and only if* $U = X^{p^i}$, *for some* $i \in \mathbb{N}$.

(3.14) $\mathrm{PPE}(g, s_2, g_1, g_2)$,

(3.15) $\mathrm{PPE}(u, s_1, u_1, u_2)$,

(3.16) $\mathrm{PPE}(h, T_1 + 1, h_1, h_2)$,

(3.17) $Y = \dfrac{h-1}{g-1}$,

(3.18) $(Y, w_2) = 1$,

(3.19) $f = \dfrac{Y-1}{g-1}$,

(3.20) $R = \dfrac{f-1}{u-1}$

(3.21) $Xw = R - 1$,

(3.22) $T - (g-1)((g-1)X + 1)$

(3.23) $\mathrm{PPE}(G, T+1, G_1, G_2)$,

(3.24) $\mathrm{PPE}(H, g, H_1, H_2)$,

(3.25) $Z = \dfrac{G-1}{H-1}$,

(3.26) $(Z, w_2) = 1$,

(3.27) $U = \dfrac{Z-1}{H-1}$.

Proof. Assume initially that (3.14)–(3.27) are satisfied in $O_{K,S}$. Then we have the following implications:

(3.14.*) $\mathrm{PPE}(g, s_2, g_1, g_2) \Rightarrow (g = s_2^{p^k} = w_2^{p^k} + 1)$;

(3.15.*) $\mathrm{PPE}(u, s_1, u_1, u_2) \Rightarrow (u = s_1^{p^l} = w_1^{p^l} + 1)$;

since by Lemma 3.4, s_1 and s_2 satisfy the "pth-power conditions." Similarly, we obtain

$$\mathrm{PPE}(h, T_1 + 1, h_1, h_2) \Rightarrow (h = [w_2^{p^{z_1}}(w_2^{p^{z_1}} s_1 + 1)]^{p^r} + 1),$$

since by definition, $T(1) = w_2^{p^{z_1}}(w_2^{p^{z_1}} x_1(s_1) + 1)$, $x_1(s_1) = s_1$, and by Lemma 3.4, any $T(m, z) + 1$, with $z \in z(m)$ for some natural m, satisfies p-power conditions. Given expressions for h and g we have a new expression for Y, which, in turn, implies an inequality for exponents, that follows from the facts that $Y \in O_{K,S}$, w_2 is not a unit of $O_{K,S}$, and $(w_2, w_2^{p^{z_1}} s_1 + 1) = 1$:

(3.17.*) $Y = \dfrac{h-1}{g-1} \Rightarrow (Y = w_2^{p^{z_1+r-k}}(w_2^{p^{z_1}} s_1 + 1)^{p^r},\ z_1 + r - k \geq 0)$.

The primality condition in (3.18) establishes the inequality for exponents in the other direction and implies that the equality must hold. The equality allows us to rewrite the expression for Y:

(3.18.*) $(Y, w_2) = 1 \Rightarrow (Y = w_2^{p^{r+z_1}} s_1^{p^r} + 1,\ r = k - z_1)$.

Given the new expression for Y and the already established expression for g we can obtain a new expression for f from (3.19):

(3.19.*) $f = \dfrac{Y-1}{g-1} \Rightarrow (f = s_1^{p^r})$.

Given, the expressions for f and u, we can obtain a new expression for R which also implies an inequality on the exponents:

$$R = \frac{f-1}{u-1} \Rightarrow \left(R = \frac{s_1^{p^r}-1}{s_1^{p^l}-1} = \frac{w_1^{p^r}}{w_1^{p^l}}, \ \iota \leq r \right). \tag{3.20.*}$$

We can interpret (3.21) as a divisibility condition in $O_{K,S}$. That divisibility condition will imply that $x_m(s_1) = x_m(w_1+1)$, a polynomial in w_1 of degree m over $\mathbb{Z}_p$, divides $w_1^{p^r-p^1}-1$, a polynomial of degree p^r-p^l in w_1 over the $\mathbb{Z}_p$. Therefore, by Lemma 2.4 and Lemma 2.5, $m \leq p^r - p^1 \leq p^r \leq p^k$ that is,

$$Xw = R-1 \Rightarrow (X \mid w_1^{p^r-p^l}-1, \ m \leq p^r \leq p^k). \tag{3.21.*}$$

Using, again, the already obtained expression for g, we can derive a new expression for T and ascertain that $T = T(m, k)$ with $k \in z(m)$.

$$\begin{aligned} &T = (g-1)((g-1)X+1) \\ &\Rightarrow (T = w_2^{p^k}(w_2^{p^k} x_m(s_1)+1) \\ &\qquad\qquad \text{with } k \geq \log_p m \Rightarrow T = T(m, k), \ k \in z(m)). \end{aligned} \tag{3.22.*}$$

If $T = T(m, k)$, with $k \in z(m)$ then $T+1$ satisfies the "pth-power conditions" and, therefore, we obtain the following from (3.23):

$$\begin{aligned} &\mathrm{PPE}(G, T+1, G_1, G_2) \\ &\Rightarrow (G = (T+1)^{p^i} = (g-1)^{p^i}(((g-1)X+1)^{p^i}+1). \end{aligned} \tag{3.23.*}$$

From (3.24) we obtain an expression for H in terms of g, using the fact that g satisfies the "pth-power conditions" by Lemma 3.4.

$$\mathrm{PPE}(H, g, H_1, H_2) \Rightarrow (H = g^{p^j}). \tag{3.24.*}$$

Next from (3.25) we will obtain a new expression for Z together with the inequality on the exponents.

$$Z = \frac{G-1}{H-1} \Rightarrow (Z = (g-1)^{p^i-p^j}((g-1)X+1)^{p^i}, \ i \geq j). \tag{3.25.*}$$

As in the case of implication (3.18.*), the primality condition (3.26) gives us an inequality on exponents in the opposite direction, and, ultimately, assures that exponents i and j are equal. That fact, in turn, gives us a simplified expression for Z.

$$(Z, w_2) = 1 \Rightarrow (Z = ((g-1)X+1)^{p^i}, i = j). \tag{3.26.*}$$

Ultimately, given the derived expressions for Z and H, we obtain the required expression for U.

$$U = \frac{Z-1}{H-1} \Rightarrow (U = X^{p^i}). \tag{3.27.*}$$

Conversely, suppose $U = X^{p^i} = x_m(s_1)^{p^i}$ is given and $z_1 \in z(1)$ and $T_1 = T(1, z_1)$ are fixed. We will show how equations and conditions (3.14)–(3.27) can be satisfied in $O_{K,S}$. First of all, we will note that $(X, w_1) = 1$ and therefore, by Lemma 3.3, there exist natural numbers $1 \leq r$ such that $X \mid w_1^{p^r-p^l}-1$. Set $R = w_1^{p^r-p^l}$, $w = (R-1)/X$. Then $w \in O_{K,S}$ and (3.21) is satisfied. To satisfy (3.20) set $f = s_1^{p^r}$, $u = s_1^{p^l}$. Next set $k = r + z_1$, $g = s_2^{p^k}$, $g_1 = y_{p^k}(2s_2 - 1)$, $g_2 = y_{p^k}(s_2)$ to satisfy (3.14). Set

$$Y = w_2^{p^{r+z_1}} s_1^{p^r} + 1, \qquad f = \frac{Y-1}{g-1}$$

and (3.18) and (3.19) are satisfied.

Set $h = (T_1^{p^r} + 1)$, $h_1 = y_{p^r}(2T_1 + 1)$, $h_2 = y_{p^r}(T_1 + 1)$, and (3.16) and (3.17) are satisfied. Let $u_1 = y_{p^l}(2s_1 - 1)$, $u_2 = y_{p^l}(s_1)$ which would satisfy (3.15). Next set $T = w_2^{p^k}(w_2^{p^k} x_m(s_1) + 1)$ and (3.22) is satisfied. If $G = (T+1)^{p^i} = x_{p^i}(T+1)$, $G_1 = y_{p^i}(2T+1)$, $G_2 = y_{p^i}(T+1)_{p^i}(T)$ and (3.23) is satisfied. Similarly, let $H = g^{p^i} = x_{p^i}(g)$, $H_1 = y_{p^i}(2g-1)$, $H_2 = y_{p^i}(g)$ to satisfy (3.24). Now set $Z = ((g-1)X + 1)^{p^i} = (w_2^{p^k} X + 1)^{p^i}$, and (3.25), (3.26) are now satisfied. Finally (3.27) is now satisfied also. Q.E.D.

Definition 3.1. Let $\mathfrak{U} = \prod p_i^{a_i}$ be a divisor of K and let $f \in K$. We will say that $f \cong 0 \bmod \mathfrak{U}$ if $\operatorname{ord}_{p_i} f \geq a_i$ for $i = 1, \dots, m$ and for every other valuation q of K, $q \neq p_i$, $\operatorname{ord}_q f \geq 0$.

Lemma 3.6. [1] *Let $V = \{q_1, \dots, q_k\}$ be any finite set of valuations of K and let $\{a_2, \dots, a_k\}$ be a $(k-1)$-tuple of positive integers. Then if the size e of the field of constants of K is greater than k, $\exists w \in K$ such that $\operatorname{ord}_{q_i} w = a_i$ for $i = 2, \dots, k$, $\operatorname{ord}_{q_1} w = -2^a$ for some positive integer a, and $\operatorname{ord}_q w \geq 0$ for all $q \notin V$.*

Proof. Let $\mathfrak{U}$ be a divisor of K, such that $\deg(\mathfrak{U}^{-1}) > 2g - 2$, where g is the genus of K. Then by a corollary to the Riemann-Roch theorem,

$$l(\mathfrak{U}) = \deg(\mathfrak{U}^{-1}) - g + 1, \tag{3.28}$$

where $l(\mathfrak{U})$ is the dimension of $\mathfrak{X}(\mathfrak{U})$, the vector space of functions which are 0 mod $\mathfrak{U}$, over the field of constants.

Consider now the divisors

$$\mathfrak{U}_{1i} = q_1^{-2^{m_i}} q_i^{a_i}, \tag{3.29}$$

$$\mathfrak{U}_{2i} = q_1^{-2^{m_i}} q_i^{a_i+1}, \tag{3.30}$$

$$\mathfrak{U}_{1ij} = q_1^{-2^{m_i}} q_i^{a_i} q_j, \tag{3.31}$$

$$\mathfrak{U}_{3i} = q_1^{-2^{m_i}+1} q_i^{a_i}, \tag{3.32}$$

where $i, j = 2, \dots, k$, so that q_i, q_j range over all the elements of V not equal to q_1 and $i \neq j$. Note that $\mathfrak{X}(\mathfrak{U}_{2i})$, $\mathfrak{X}(\mathfrak{U}_{1ij})$, $\mathfrak{X}(\mathfrak{U}_{3i})$ are all subspaces of $\mathfrak{X}(\mathfrak{U}_{1i})$. Select m so large that $\forall m_i \geq m$,

$$\deg(\mathfrak{U}_{hi}^{-1}) > 2g - 1, \tag{3.33}$$

$$\deg(\mathfrak{U}_{1ij}^{-1}) > 2g - 1, \tag{3.34}$$

for $h = 1, 2, 3$, $i, j = 2, \dots, k$, $i \neq j$. Now define $m_2, \dots, m_k$ as follows: $m_2 = m_3 = m$, $m_{i+1} = m_i + 1$, $i = 4, \dots, k$.

[1] The proof of this lemma was suggested to me by Michael Fried of the University of California at Irvine.

Let $d_i = \deg(q_i)$. Then under our assumptions on m and by the above-stated corollary to the Riemann-Roch theorem, we now have

$$l(\mathfrak{U}_{1i}) = 2^{m_i} d_1 - a_i d_i - g + 1\,, \tag{3.35}$$

$$l(\mathfrak{U}_{2i}) = 2^{m_i} d_1 - (a_i + 1) d_i - g + 1\,, \tag{3.36}$$

$$l(\mathfrak{U}_{1ij}) = 2^{m_i} d_1 - a_i d_i - d_j - g + 1\,, \tag{3.37}$$

$$l(\mathfrak{U}_{3i}) = (2^{m_i} - 1) d_1 - a_i d_i - g + 1\,. \tag{3.38}$$

Our assumptions on m also guarantee that all of these vector spaces have dimensions ≥ 1. Moreover, $\mathfrak{X}(\mathfrak{U}_{2i})$, $\mathfrak{X}(\mathfrak{U}_{3i})$, and $\mathfrak{X}(\mathfrak{U}_{1ij})$ are all subspaces of $\mathfrak{X}(\mathfrak{U}_{1i})$ of lower dimension. We have to consider separately the case of the infinite constant field and the case of the finite constant field. If the constant field is finite, it is, by assumption, of the size $k < e < \infty$. Then

$$|\mathfrak{X}(\mathfrak{U}_{1i})| = e^{2^{m_i} d_1 - a_i d_i - g + 1}\,, \tag{3.39}$$

$$|\mathfrak{X}(\mathfrak{U}_{2i})| = e^{2^{m_i} d_1 - (a_i+1) d_i - g + 1}\,, \tag{3.40}$$

$$|\mathfrak{X}(\mathfrak{U}_{1ij})| = e^{2^{m_i} d_1 - a_i d_i - d_j - g + 1}\,, \tag{3.41}$$

$$|\mathfrak{X}(\mathfrak{U}_{3i})| = e^{(2^{m_i} - 1) d_1 - a_i d_i - g + 1}\,. \tag{3.42}$$

$$\begin{aligned} |\mathfrak{X}_i| &= |((\mathfrak{X}(\mathfrak{U}_{1i}) \backslash \mathfrak{X}(\mathfrak{U}_{2i})) \backslash \mathfrak{X}(\mathfrak{U}_{3i})) \backslash \bigcup_{j \neq i} \mathfrak{X}(\mathfrak{U}_{1ij})| \\ &\geq e^{2^{m_i} d_1 - a_i d_i - g + 1} - e^{2^{m_i} d_1 - (a_i+1) d_i - g + 1} \\ &\quad - \sum_{\substack{j=2 \\ j \neq i}}^{k} e^{2^{m_i} d_1 - a_i d_i - d_j - g + 1} - e^{(2^{m_i} - 1) d_1 - a_i d_i - g + 1} \\ &= e^{2^{m_i} d_1 - a_i d_i - g + 1} \left(1 - \sum_{i=1}^{k} e^{-d_i}\right) \\ &\geq e^{2^{m_i} d_1 - a^i d_i - g + 1} \left(1 - \sum_{i=1}^{k} e^{-1}\right) > 0\,. \end{aligned} \tag{3.43}$$

Since the difference in the sizes of spaces is an integer, we can conclude it is at least 1. So

$$\mathfrak{X}_i = ((\mathfrak{X}(\mathfrak{U}_{1i}) \backslash \mathfrak{X}(\mathfrak{U}_{2i})) \backslash \mathfrak{X}(\mathfrak{U}_{3i})) \backslash \bigcup_{j \neq i} \mathfrak{X}(\mathfrak{U}_{1ij}) \neq \varnothing\,. \tag{3.44}$$

If the field of constants is infinite, (3.44) follows from the fact that we are taking out finitely many lower-dimensional subspaces.

Let $v_i \in \mathfrak{X}_i$, then w has poles only at p_1 and $\operatorname{ord}_{p_1} v_i \geq -2^{m_i}$, v_i has a zero of order at least a_i at p_i, and v_i is integral at all the valuations not in V. On the other hand, v_i is not in $\mathfrak{X}(\mathfrak{U}_{2i})$, which means that $\operatorname{ord}_{p_i} v_i = a_i$. Also, since v_i is not in $\mathfrak{X}(\mathfrak{U}_{1ij})$ for any $j \neq i$, $\operatorname{ord}_{p_j} v_i = 0$ for all such j's. Moreover, since v_i is not in $\mathfrak{X}(\mathfrak{U}_{3i})$, $\operatorname{ord}_{p_1} v_i = -2^{m_i}$. Now let $w = v_2 \cdots v_k$. Then $\operatorname{ord}_{p_i} w = a_i$ for $i = 2, \ldots, k$, $\operatorname{ord}_q w_1 \geq 0$ for $q \notin V$, and

$$\begin{aligned} \operatorname{ord}_{p_1} w &= 2^m + 2^m + 2^{m+1} + \cdots + 2^{m+k-2} \\ &= 2^m + 2^m(2^{k-1} - 1) = 2^{m+k-1}\,. \end{aligned}$$

Therefore, w will satisfy all the requirements.

Lemma 3.7. *Assume the field of constants of K is of size $e > n+1$. Then $O_{K,S}$ contains w_1 and w_2 such that $s_1 = w_1 + 1$ and $s_2 = w_2 + 1$ satisfy "pth-power conditions" with respect to p_1 and p_2 respectively, $w_2 s_1$ has a positive order at p_1, and w_1 and w_2 are not units of $O_{K,S}$.*

Proof. Let $q \notin S$ and define $T = S \cup \{q\}$. In the future, we will refer to q as p_{n+1}. Apply the previous lemma to $V = T$ and $a_i = 1$ for $i = 2, \dots, n+1$. The resulting element is going to be w_1. Next apply Lemma 3.6 to $V = T$ again, except let p_2 play the role of q_1 and let p_1 play the role of q_2. Also let $a_2 = -\operatorname{ord}_{p_1} w_1 + 1$, $a_i = 1$, for $i = 3, \dots, n+1$.

Lemma 3.8. *Let K and S be defined as before and let the constant field of K be of size $e \leq n+1 = |S|+1$. Then there exists a separable extension of K, L with a set of valuations V containing all the valuations of L extending valuations in S, with the property that the size of the field of constants of L is greater than $|V|+1$.*

Proof. Consider an extension of the constant field of K of degree m. As an extension of a finite field it will be separable. Our new constant field will be of size e^m. On the other hand, every valuation of S could have split into at most m new valuations. So in the extended field we can have at most mn valuations extending valuations of S. Hence, let m be any positive integer such that $e^m > mn+1$, let α be algebraic over the field of constants of K of degree at least m, and let $L = K(\alpha)$; then such an L will satisfy the requirements of the lemma.

Lemma 3.9. *Let $L-K$ be a finite separable extension of algebraic function fields. Let S be a finite set of valuations of K, and V the set of all the valuations of L extending valuations of S. Let $\{\omega_1, \dots, \omega_m\}$ be a basis of L over K with $\omega_i \in O_{L,V}$. Then $\exists c \in O_{K,S}$, such that $\forall x \in O_{L,V}$, $cx = \sum_{i=1}^{m} a_i \omega_i$, $a_i \in O_{K,S}$.*

Proof. By Lemma 1 [3, p. 54] the statement of Lemma 3.10 is true for the case of S containing just one valuation. Now let $x \in O_{L,V}$ and assume x has poles at valuations of V other than the ones extending p_1. By Lemma 3.6 one can find an element $w \in L$ with a pole only at a valuation extending p_1 and with zeros of any prescribed order at all the valuations of V not extending p_1. In particular, we can assume that the order of those zeros is greater then the order of the poles of x at valuations of V not extending p_1.

Consider now $N_{L/K}(w)x$. This element will have poles only at the valuations extending p_1. Therefore, we can apply the above mentioned lemma of [3], to conclude that $\exists C \in O_{K,S}$ such that $CN_{L/K}(w)x = \sum_{i=1}^{n} a_i \omega_i$, with $a_i \in O_{K,S}$. Since, w belonged to the integral closure of $O_{K,S}$ in L, $N_{L/K}(w) \in O_{K,S}$ and, therefore, we can let $c = CN_{L/K}(w)$ to complete the proof of the lemma.

Theorem 3.1. *Let K be any algebraic function field of one variable over a field of constants of characteristic $p > 2$, S a finite set of its valuations. Then Hilbert's Tenth Problem has no solution in $O_{K,S}$.*

Proof. If S contains just one valuation assume s_1 is any nonconstant element of $O_{K,S}$, and in the case of more than one valuation in S assume initially that the field of constants of K contains at least $n+2$ distinct elements where

n is the number of valuations in S. In that case let $p_1, \dots, p_n$ be all of the valuations of S and let p_{n+1} as before, be a valuation not in S. Then by Lemma 3.7, $O_{K,S}$ contains elements w_1 and w_2 such that $\operatorname{ord}_{p_i} w_j = 1$, for $i \neq j$, $i = 1, \dots, n+1$, $j = 1, 2 \operatorname{ord}_{p_j} w_j = -2^{a_j}$, and $\operatorname{ord}_{p_1} w_1 w_2 > 0$. Let $s_1 = w_1 + 1$ and consider the following divisibility condition over the rational integers.

$$\sum_{i=1}^{k} a_i m_i \mid \sum_{i=1}^{k} b_i m_i. \tag{3.45}$$

We claim that (3.45) has solutions $m_1, \dots, m_k$ in $\mathbb{Z}$ if and only if

$$X_i^2 - (s_1^2 - 1)Y_i^2 = 1, \qquad i = 1, \dots, k, \tag{3.46}$$

$$U - (s_1^2 - 1)^{1/2} V = \prod_{i=1}^{k} (X_i - (s_1^2 - 1)^{1/2} Y)_i^{a_i}, \tag{3.47}$$

$$G - (s_1^2 - 1)^{1/2} T = \prod_{i=1}^{k} (X_i - (s_1^2 - 1)^{1/2} Y_i)^{b_i}, \tag{3.48}$$

$$T = Vw, \tag{3.49}$$

$$X_i \cong 1 \bmod (w_1) \tag{3.50}$$

have solutions in $O_{K,S}$. Indeed, by Lemmas 2.3, 2.8, and 2.10, this system of equations (3.46)–(3.50) has solutions in $O_{K,S}$ if and only if $\exists m_1, \dots, m_k \in \mathbb{Z}$ such that $X_i = x_{m_i}(s_1)$, $Y_i = y_{m_i}(s_1)$, $V = y_{\sum a_i m_i}(s_1)$, $T = y_{\sum b_i m_i}(s_1)$, and $y_{\sum a_i m_i} \mid y_{\sum b_i m_i}$ in $O_{K,S}$. By Lemma 2.6, the last conditions hold if and only if (3.45) holds.

On the other hand, consider

$$\sum_{i=1}^{k} a_i m_i \Big|^{p} \sum_{i=1}^{k} b_i m_i. \tag{3.51}$$

We claim that (3.51) has solutions $(m_1, \dots, m_k)$ in $\mathbb{Z}$ if and only if the following system of equations has solutions in $O_{K,S}$:

$$X_i^2 - (s_1^2 - 1)Y_i^2 = 1, \qquad i = 1, \dots, k, \tag{3.52}$$

$$U - (s_1^2 - 1)^{1/2} V = \prod_{i=1} (X_i - (s_1^2 - 1)^{1/2} Y)_i^{a_i}, \tag{3.53}$$

$$G - (s_1^2 - 1)^{1/2} T = \prod_{i=1} (X_i - (s_1^2 - 1)^{1/2} Y)_i^{b_i}, \tag{3.54}$$

$$\exists j \in \mathbb{N}\ G = U^{p^j}, \tag{3.55}$$

$$X_i \cong 1 \bmod (w_1). \tag{3.56}$$

Indeed, by the above-mentioned Lemmas 2.3, 2.8, and 2.10, this system of equations (3.52)–(3.57) has solutions in $O_{K,S}$ if and only if $\exists m_1, \dots, m_k \in \mathbb{Z}$ such that $X_i = x_{m_i}(s_1)$, $U = x_{\sum a_i m_i}$, $G = x_{\sum b_i m_i}$, and $\sum b_i m_i = \pm p^j \sum a_i m_i$, that is (3.51) has solutions in $\mathbb{Z}$.

On the other hand, we know that by Lemmas 2.12 and 3.5 respectively, we can substitute equations (2.26) and (2.27) for (3.55) in case S has just one valuation and we can substitute equations (3.14)–(3.27) for (3.55) if we have more than one valuation in S. So (3.51) has solutions in $\mathbb{Z}$ if and only if a certain finite system of polynomial equations has solutions in K. Hence, we have constructed a model of $(\mathbb{Z}, |^p, |, +)$ which is Diophantine over $O_{K,S}$. Therefore, by Theorem 1.1, Hilbert's Tenth Problem has no solution in that ring.

Now we will treat the case of K whose field of constants has fewer than $n+2$ elements. By Lemma 3.8 there exists a finite separable extension E of K such that the size of constant field of E is greater than $1+|V|$, where V is the set of all the valuations lying above S in E. Therefore, we can apply the first part of the theorem to E to produce a polynomial equation $F(z_1, \dots, z_r) = 0$ over $O_{E,V}$ which will have solutions in $O_{E,V}$ if and only if (3.45) ((3.50)) have solutions in $\mathbb{Z}$. Let $\{\omega_1, \dots, \omega_m\}$ be a basis of E over K with $\omega_i \in O_{E,V}$ and c as in Lemma 3.9. Also let $F(z_1, \dots, z_r) = \sum a_{i_1\cdots i_r} z_i^{i_1} \cdots z_r^{i_r}$. Consider now the following equivalence chain:

$$\exists\{z_i\} \in O_{E,V}F(z_1, \dots, z_r) = 0 \tag{3.55}$$

$$\Updownarrow$$

$$\exists\{z_i\} \in O_{E,V}\sum a_{i_1\cdots i_r} z_1^{i_1} \cdots z_r^{i_r} = 0 \tag{3.56}$$

$$\Updownarrow$$

$$\exists b_{j,e} \in O_{K,S}, \qquad j = 1, \dots, m,\ e = 1, \dots, r,$$

$$\sum b_{j,e}\omega_j \cong 0 \bmod c, \qquad e = 1, \dots, r, \tag{3.57}$$

$$\sum \Big(\sum c_{ji_1\cdots i_r}\frac{\omega_j}{c}\Big)\Big(\sum b_{j1}\frac{\omega_j}{c}\Big)^{i_1} \cdots \Big(\sum b_{jr}\frac{\omega_j}{c}\Big)^{i_r} = 0 \tag{3.58}$$

$$\Updownarrow$$

$$\exists b_{j,e}, \qquad j = 1, \dots, m,\ e = 1, \dots, r,$$

$$\sum b_{j,e}\omega_j \cong 0 \bmod c, \qquad e = 1, \dots, r, \tag{3.59}$$

$$g_1(b_{11}, \dots, b_{mr}) = 0, \tag{3.60.1}$$

$$\dots$$

$$g_m(b_{11}, \dots, b_{mr}) = 0, \tag{3.60.m}$$

where g_h are polynomial over K with coefficients of the form $a/c^{(\deg(F)+1)}$, $a \in O_{K,S}$. The last equivalence follows from the fact that any product of ω's can again be rewritten as linear combination of ω's with coefficients of the form a/c, $a \in O_{K,S}$, so altogether we will need at most $\deg(F)+1$ power of c in the denominator. Therefore, (3.55) having solution in $O_{E,V}$ is now equivalent to the system (3.59)–(3.60.m) having solutions in $O_{K,S}$. By multiplying through by the appropriate power of c we can clear the denominators of all the coefficients and make sure they are in $O_{K,S}$.

The only remaining detail is rewriting (3.59) without references to ω's which are not elements of K. This can be done in the following way. Since the field of constants of K is finite, elements of $O_{K,S}$ are divided into finitely many residue classes $\bmod c$. Now let $(\mu_{11}, \dots, \mu_{mr})$ be a mr-tuple of representatives of the residue classes $\bmod c$. Out of all such mr-tuples consider those with the property that if $b_{11} \cong \mu_{11}, \dots, b_{mr} \cong \mu_{mr}$ then the equivalences (3.59) are satisfied. Let $\{(\mu_{11}^{(i)}, \dots, \mu_{mr}^{(i)})\}$, $i = 1, \dots, q$, be the list of all such mr-

tuples. Hence, (3.59) can be replaced by $\{b_{jh} \cong \mu_{jh}^{(1)} \bmod c,\ j = 1, \dots, m,\ e = 1, \dots, r\}$ or ... or $\{b_{jh} \cong \mu_{jh}^{(q)},\ j = 1, \dots, m,\ e = 1, \dots, r\}$. This completes the proof of the theorem.

4. The case of characteristic equal to 2

To treat the case of characteristic equal to 2 we have to use a quadratic equation different from the Pell equation. We will make use of the equation introduced by Denef in [2].

Lemma 4.1. *Let K be an algebraic function field of characteristic 2 and let S, as before, be a finite set of valuations of K. Let $\alpha(a)$ be the root of the following equation in the algebraic closure of K.*

$$f^2 + af + 1 = 0, \tag{4.1}$$

where $a \in O_{K,S}$ and a is not a constant. Assume $\alpha(a)$, $\alpha(a(a+1)) \notin K$, and define $(x_m(a), y_m(a))$ to be elements of $O_{K,S}$ such that

$$x_m(a) - \alpha(a)y_m(a) = (\alpha(a))^m = (a + \alpha(a))^{-m}.$$

Then the following statements hold.

$(x_m(a), y_m(a))$, $m \in \mathbb{Z}$, are solutions to the equation

$$f^2 + afg + g^2 = 1. \tag{4.2}$$

Moreover, x_m, y_m, x_n, y_n, x_{m+n}, y_{m+n} have the following properties:

$$x_{m+n}(a) = x_m(a)x_n(a) - y_m(a)y_n(a). \tag{4.3}$$

$$y_{m+n}(a) = x_m(a)y_n(a) + y_m(a)x_n(a) - ay_m(a)y_n(a). \tag{4.4}$$

$x_m(a)$, $y_m(a)$ are polynomials in a over $\mathbb{Z}_2$.

$$\deg(x_m(a)) = (|m| - 2) \quad \mathit{if}\, |m| \geq 2, \tag{4.5}$$

$$\deg(y_m(a)) = (|m| - 1) \quad \mathit{if}\, |m| \geq 2 \tag{4.6}$$

as polynomials in a.

$$x_{-m}(a) = x_m(a) + ay_m(a). \tag{4.7}$$

$$y_{-m}(a) = y_m(a). \tag{4.8}$$

$$n \mid m \Rightarrow y_n(a) \mid y_m(a). \tag{4.9}$$

$$y_{m2^n}(a) = (a^{2^n}/a)(y_m(a))^{2^n}. \tag{4.10}$$

$$y_{2^n}(a) = a^{2^n}/a, \quad \mathit{if}\, n \geq 0. \tag{4.11}$$

$$(a+1)y_m(a(a+1)) = a(y_m(a))^2 + y_m(a) \leftrightarrow m = \pm 2^n \quad \mathit{for\ some}\ n \in \mathbb{N}. \tag{4.12}$$

Proof. The assertion that $(x_m(a), y_m(a))$ are solutions to (4.2) can be verified directly, and properties (4.3), (4.4) are proved in a way similar to the proof of the analogous properties of the Pell equation solutions in the case of characteristic $p \neq 2$.

(4.5) and (4.6) are proved by induction as follows. $x_1 = 0$, $y_1 = 1$, $x_2 = x_1^2 - y_1^2 = -1$, $y_2 = 2x_1y_1 - ay_1^2 = -a$ establishes the starting point of the induction.

$\deg(x_{m+1}) = \deg(-y_m y_1) = (m-1)\deg(a)$. $\deg(y_{m+1}) = \deg(x_m y_1 - a y_1 y_m) = m\deg(a)$ completes this induction.

(4.7) and (4.8) can be shown directly by multiplication. We can derive (4.9) in the same way as for the Pell equation in the case of characteristic $p > 2$.

Next we establish (4.10) and (4.11) by induction. We have

$$\begin{aligned}(x_{m2^n}(a) - \alpha(a)y_{m2^n}(a)) &= (x_{m2^{n-1}}(a) - \alpha(a)y_{m2^{n-1}}(a))^2\\ &= x^2_{m2^{n-1}}(a) + \alpha(a)^2 y^2_{m2^{n-1}}(a)\\ &= x^2_{m2^{n-1}}(a) + (-1 - a\alpha(a))y^2_{m2^{n-1}}(a),\end{aligned}$$

and hence, $y_{m2^n}(a) = a y^2_{m2^{n-1}}(a) = a(a^{2^{n-1}}/a)^2(y_m(a))^{2^n} = (a^{2^n}/a)(y_m(a))^{2^n}$. Since $y_1(a) = 1$, the case for $m = 1$ follows.

Next we will prove (4.12). Since $y_{-m} = y_m$, without loss of generality we can assume that $m \geq 0$. Suppose $m = q2^n$, where $(q, 2) = 1$. Then

$$\begin{aligned}y_m(a(a+1)) &= y_{q2^n}(a(a+1))\\ &= ((a(a+1))^{2^n}/a(a+1))(y_q(a(a+1)))^{2n},\end{aligned}\tag{4.13}$$

and

$$(a+1)y_m(a(a+1)) = (a^{2^n}(a+1)^{2^n}/a)(y_q(a(a+1))^{2^n}.\tag{4.14}$$

On the other hand,

$$\begin{aligned}a y_m^2(a) + y_m(a) &= a(a^{2^n}/a)^2(y_q(a))^{2^{n+1}} + (a^{2^n}/a)y_q(a)^{2^n}\\ &= (a^{2^{n+1}}/a)(y_q(a))^{2^{n+1}} + (a^{2^n}/a)y_q(a)^{2^n},\end{aligned}\tag{4.15}$$

and consequently,

$$a^{2^n}(a+1)^{2^n}(y_q(a(a+1)))^{2^n} = a^{2^{n+1}}(y_q(a))^{2^{n+1}} + a^{2^n}(y_q(a)^{2^n}).\tag{4.16}$$

Raising both sides of the equality to the power $1/2^n$, we get

$$a(a+1)y_q(a(a+1)) = a^2 y_q(a)^2 + a y_q(a).\tag{4.17}$$

Canceling a from both sides, we obtain

$$(a+1)y_q(a(a+1)) = a y_q(a)^2 + y_q(a).\tag{4.18}$$

By (4.6), $y_q(a)$ and $y_q(a(a+1))$ are polynomials of degree $q-1$ over $\mathbb{Z}_2$ in a and $a(a+1)$ respectively. Therefore,

$$\begin{aligned}y_q(a) &= A_{q-1}a^{q-1} + A_{q-2}a^{q-2} + \cdots,\\ y_q(a(a+1)) &= A_{q-1}a^{q-1}(a+1)^{q-1} + A_{q-2}a^{q-2}(a+1)^{q-2} + \cdots\end{aligned}$$

and (4.18) can be rewritten as

$$\begin{aligned}&A_{q-1}a^{q-1}(a+1)^q + A_{q-2}a^{q-2}(a+1)^{q-1} + \cdots\\ &\quad = A_{q-1}a^{2q-1} + A_{q-2}a^{2q-3} + \cdots + A_{q-1}a^{q-1} + \cdots.\end{aligned}\tag{4.19}$$

In order for (4.19) to hold, by Lemma 2.9, the coefficients corresponding to every power of a must be equal on both sides. Let us compare the coefficients corresponding to a^{2q-2}. The coefficient from the left-hand side is $A_{q-1}q$ and the coefficient from the right-hand side is

$$\begin{cases}0 & \text{if } 2q-2 > q-1,\\ A_{q-1} & \text{if } 2q-2 = q-1,\end{cases}$$

i.e. that coefficient is

$$\begin{cases} 0 & \text{if } q > 1\,, \\ A_0 & \text{if } q = 1\,. \end{cases}$$

Since q is odd and A_{q-1} is not 0 by (4.6), we must conclude that q is 1 and $m = 2^n$.

We still have to verify that (4.12) holds for $m = 2^n$. By (4.11) we have

$$(4.20) \qquad (a+1)y_{2n}(a(a+1)) = (a+1)\frac{a^{2n}(a+1)^{2^n}}{a(a+1)} = \frac{a^{2^n}(a+1)^{2^n}}{a}\,,$$

$$(4.21) \qquad ay_{2^n}(a)^2 + y_{2^n}(a) = a\frac{a^{2^{n+1}}}{a^2} + \frac{a^{2^n}}{a}\,.$$

It is easy to see that the right sides of (4.21) and (4.22) are indeed equal.

Lemma 4.2. *Let* a *be such that* $\operatorname{ord}_p a \neq 0$ *for all* $p \in S$. *Then*

$$y_m(a) \mid y_n(a) \Rightarrow m \mid n\,.$$

Proof. The proof of this lemma is similar to the proof of the analogous result for the Pell equation solutions in the case $p > 2$.

Next we determine a set a conditions under which, as in the case of Pell equation, $(x_m(a), y_m(a))$ are the only solutions to (4.2).

Lemma 4.3. *If* S *contains just one valuation then for any nonconstant* a, $(x_m(a), y_m(a))$ *are the only solutions to* (4.2).

If S *has more than one valuation let* $p_1, \dots, p_n$ *be all the valuations in* S, p_{n+1} *a valuation of* K *not in* S, *and assume* $\operatorname{ord}_{p_1} a = -2^k$, $\operatorname{ord}_{p_i} a$ *is odd and positive,* $i = 2, \dots, n+1$, $\operatorname{ord}_q a \geq 0$ *for any* $q \notin S \cup \{p_{n+1}\}$. *Then, again,* $(x_m(a), y_m(a))$ *are the only solutions to* (4.2).

Proof. In the case where S contains just one valuation, the proof of the lemma is similar to the proof of the analogous lemma concerning the Pell equation in the fields of characteristic greater than 2. So assume S has more than one valuation, let p be any valuation of K, and let β lie above p in $K(\alpha)$. We will show that $\operatorname{ord}_\beta \alpha = 0$, unless $p = p_1$. Suppose $\operatorname{ord}_\beta \alpha > 0$. Then from (4.1), $\operatorname{ord}_\beta a\alpha = 0$ and, therefore, $\operatorname{ord}_\beta a < 0$. Since a has a pole at only one valuation p_1, β must be above p_1. On the other hand, suppose $\operatorname{ord}_\beta \alpha < 0$, then (4.1) implies that $2\operatorname{ord}_\beta \alpha = \operatorname{ord}_\beta a + \operatorname{ord}_\beta \alpha$. That is, $\operatorname{ord}_\beta a < 0$ and β must lie above p_1 again. This argument also shows that p_1 splits into two distinct valuations β_{11} and β_{12} in $K(\alpha)$, $\operatorname{ord}_{\beta_{11}} \alpha = -\operatorname{ord}_{\beta_{12}} \alpha = \operatorname{ord}_{p_1} a$, with β_{11} being a pole of α.

Next we will show that $p_2, \dots, p_n$ will totally ramify in $K(\alpha)$. Indeed, from (4.1), $(\alpha+1)^2 = a\alpha$. Therefore, if β_i lies above p_i, we have $2\operatorname{ord}_{\beta_i}(\alpha+1) = \operatorname{ord}_{\beta_i} a = k\operatorname{ord}_{p_i} a$, where k is the highest power of β_i dividing p_i. The above equality implies k is even, and hence, must be 2.

Now let (x, y) be solutions to (4.1). Then $x + \alpha y$ is a unit of norm 1, and therefore, as in the case of the Pell equation, all of its poles and zeros must come from β_{11} and β_{12}, and, moreover, $\operatorname{ord}_{\beta_{11}}(x - \alpha y) = -\operatorname{ord}_{\beta_{12}}(x - \alpha y)$. Therefore, by mapping all such units to their orders at β_{11} we can establish an isomorphism between the group of solutions to (4.2) and a subgroup of rational integers under addition which will enable us to conclude that the group of solutions to (4.2) is cyclic.

Lastly, we show that α is the generator of the solution group. As we have established before, $|\operatorname{ord}_{\beta_{11}} \alpha| = |\operatorname{ord}_{p_1} a| = 2^k$. Therefore, if α is not a generator, $(x - \alpha y)^2 = \alpha$, for some $x, y \in O_{K,S}$ solutions to (4.2). Then, however, $x^2 - \alpha^2 y^2 = x^2 + (\alpha a + 1)y^2 = x^2 + y^2 + \alpha a y^2 = \alpha$ and $x^2 = y^2 = a^{-1}$. This is impossible, because a has a zero at at least one valuation not in S, and therefore is not invertible in $O_{K,S}$.

As in the case of characteristic greater than 2, if S contains just one valuation we can relax conditions on a and still show that $(x_m(a), y_m(a))$ are the only solutions to (4.2).

Lemma 4.4. *Assume S contains only one valuation p and a is* any nonconstant element *of $O_{K,S}$; then $(x_m(a), y_m(a))$, $m \in \mathbb{Z}$, are the only solutions to* (4.2).

Proof. First of all we show that $\alpha \notin K$. If it did, α would be a nonconstant unit of $O_{K,S}$, which has only constant units. Now let $\varepsilon = x + y\alpha$, $x, y \in O_{K,S}$, be a solution to (4.2). Then ε must be a unit of the integral closure of $O_{K,S}$ in $K(\alpha)$ and, therefore, must be a unit at any valuation not lying above p. On the other hand, $N_{K(\alpha)/K}(\varepsilon) = 1$, so p must split into β_1 and β_2 with $\operatorname{ord}_{\beta_1} \varepsilon = \operatorname{ord}_{\beta_2} \varepsilon$. As in the previous lemma, we will use the map $\varepsilon \to \operatorname{ord}_{\beta_1} \varepsilon$ to establish the fact that the group of solutions to (4.2) is cyclic. Next we want to establish that α is the generator. Suppose $(x + \alpha y)^n = \alpha$, with $x, y \in O_{K,S}$. Then it is easy to see from the formula equivalent to (4.9) that $y \mid 1$, and therefore y is a constant. From (4.2), we then get that either x is a nonzero constant or $y = 1$ and $x = 0$. If we assume the first alternative then α is a constant also, which would contradict our assumptions on a. Therefore, $y = 1$, $x = 0$, $n = 1$, i.e., α generates all the solutions.

Lemma 4.5. *If S contains just one valuation then let a be any nonconstant element. If S contains $n > 1$ valuations $p_1, \dots, p_n$, let p_{n+1} be a valuation not in S and let a be as described in Lemma* 4.2. *Then the following equivalence holds.*

$$\left.\begin{array}{ll} (4.23) & X^2 + aXY + Y^2 = 1, \\ (4.24) & U^2 + a(a+1)UT + T^2 = 1 \\ (4.25) & (a+1)T = aY^2 + Y. \end{array}\right\} \Leftrightarrow (4.26) \quad \exists k \in N, \ aY = a^{2^k}.$$

Proof. We will assume initially that (4.23)–(4.25) hold, and we will show that (4.26) is true. If S contains only one valuation, $(X, Y) = (x_m(a), y_m(a))$, $(U, T) = (x_r(a(a+1)), y_r(a(a+1))$ by Lemma 4.3 with $m, r \in \mathbb{Z}$. If S contains $n > 1$ valuations then, by Lemma 4.2, $Y = y_m(a)$ for some $m \in \mathbb{N}$. Moreover, $\operatorname{ord}_{p_1} a(a+1) = \operatorname{ord}_{p_1} a + \operatorname{ord}_{p_1}(a+1) = 2\operatorname{ord}_{p_1}(a) = -2^{k+1}$, and $\operatorname{ord}_{p_i} a(a+1) = \operatorname{ord}_{p_i} a + \operatorname{ord}_{p_i}(a+1) = \operatorname{ord}_{p_i} a$ is odd and positive for $i = 2, \dots, n+1$. So $a(a+1)$ satisfies the requirements of Lemma 4.2 and we can conclude that $T = y_j(a(a+1))$. If $m = \pm 1$ or $j = \pm 1$, then $Y = T = 1$ and $k = 0$ will satisfy (4.26). If, on the other hand, $|m| \geq 2$ and $|j| \geq 2$, we know by Lemma 4.1 that $y_m(a)$ should be a polynomial of degree $|m| - 2$ in a over the field of constants, and $y_j(a(a+1))$ should be a polynomial of degree $2|j| - 4$ in a over the field of constants, and so the only way for (4.25) to hold is for $|j| = |m|$. Therefore, we can apply Lemma 4.2 to conclude that $m = \pm 2^k$ for some natural k.

Conversely, suppose (4.26) holds, then by Lemma 4.1, (4.23)–(4.25) can be satisfied by $X = x_m(a)$, $Y = y_m(a)$, $U = x_m(a(a+1))$, and $T = y_m(a(a+1))$.

We have succeeded in making condition (4.26) Diophantine for a certain class of a's. From this point on we can proceed as in the case of characteristic greater than 2 to prove the following theorem.

Theorem 4.1. *Let K be an algebraic function field in one variable of characteristic 2, S a finite set of its valuations. Then Hilbert's Tenth Problem has no solution in $O_{K,S}$.*

5. Hilbert's Tenth problem in some extensions of infinite degree

First of all, we want to describe the infinite extensions we will consider. Let K be a field of algebraic functions of infinite degree and positive characteristic and let F be any finite degree subfield of K whose set of valuations contains a valuation p with the following property. Every finite degree subfield of K containing F will have only one valuation above p. Given such a finite degree field M containing F, define a set of valuations $S(M) = \{p(M)\}$, where $p(M)$ is the unique valuation of M lying above p. Under these conditions we will let $O_{K,p} = \bigcup O_{M,S(M)'}$, where the union is taken over all finite degree fields M containing F. For the above-described field K, we have the following theorem.

Theorem 5.1. *Hilbert's Tenth Problem has no solution in $O_{K,p}$.*

Proof. To begin with, we will consider the Pell equation for the characteristic greater than 2 and equation (4.2) for characteristic 2, over $O_{M,S(M)'}$ where we assume that $a \in F$. We can note that since S contains only one valuation, solutions to the Pell equation or equation (4.2) will be generated by $a-(a^2-1)^{1/2}$ and α, respectively, by Lemmas 2.10 and 4.3. Consider now the Pell equation and equation (4.2) over $O_{K,p}$. Let (x, y) be a pair of solutions. Let $M = F(x, y)$. Then, by the argument above, $x-(a^2-1)^{1/2}y = (a-(a^2-1)^{1/2})^n$, for characteristic greater than 2, and $x + \alpha y = \alpha^n$ for characteristic 2, and some integer n. Therefore, we can assert that $a - (a^2 - 1)^{1/2}$ and α will generate the solutions for the Pell equation and equation (4.2), respectively, over $O_{K,p}$. From this point on, one can proceed as in the cases of extensions of finite degree when S contained just one valuation.

Acknowledgment

The author would like to thank the referee for valuable comments.

References

1. M. Davis, Yu. Matijasevich, and J. Robinson, *Positive aspects of a negative solution*, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R.I., 1976, pp. 323–378.
2. J. Denef, *The Diophantine Problem for polynomial rings of positive characteristic*, Logic Colloquium 78 (M. Boffa, D. van Dalen, K. MacAloon, eds.), North-Holland, Amsterdam, 1979, pp. 131–145.
3. C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Amer. Math. Soc., Providence, R.I., 1951.

Department of Mathematics, East Carolina University, Greenville, North Carolina 27858