Invent. math. 103, 1–8 (1991)

Inventiones mathematicae

Hilbert's Tenth Problem for fields of rational functions over finite fields

Thanases Pheidas*
Department of Mathematics, Florida International University, Miami, FL 33199, USA

Oblatum 1-XI-1989

Summary. We prove that there is no algorithm to solve arbitrary polynomial equations over a field of rational functions in one letter with constants in a finite field of characteristic other than 2 and hence, Hilbert's Tenth Problem for any such field is undecidable.

Introduction

If R is a commutative ring, a *Diophantine equation* over R is an equation $P(x_1, \ldots, x_m) = 0$ where P is a polynomial in the variables $x_1, \ldots, x_m$ with coefficients in R. A relation Q in R^k is Diophantine if $Q = \{(x_1, \ldots, x_k) \in R^k: \exists y_1, \ldots, y_m \in R \ (P(x_1, \ldots, x_k, y_1, \ldots, y_m) = 0)\}$ where $P = 0$ is a Diophantine equation over R. When R is not a finitely generated module over Z, we limit our attention to the Diophantine equations whose coefficients are in a finitely generated module over $\mathbf{Z}$. In particular if R is a ring of polynomials, a field of rational functions or a field of Laurent series in a letter t, we only consider Diophantine equations whose coefficients lie in the natural image of $Z[t]$ in R.

In [9], Y. Matijasevic proved that there is no algorithm to determine whether any given Diophantine equation over the ring of rational integers has an integer solution or not, thereby answering in the negative Hilbert's Tenth Problem (which asked such an algorithm to be found). Since then the analog of this answer to Hilbert's Tenth Problem has been proved for various rings, most notably various rings of algebraic integers [5], [6] and [12], rings of polynomials [3], [4] and fields of rational functions over real fields [4].

A related question is whether the theory of some ring R is decidable, that is, whether there is an algorithm to determine which sentences of first order logic about R are true and which are not true; the sentences that we are concerned with

* Supported in part by NSF Grant DMS 8605198.
Current address: Department of Mathematics, University of Illinois, 1409 West Green Street, IL 61801, USA

are the ones which can be built using addition, multiplication, a fixed finite number of constants and quantifiers. In this context, Hilbert's Tenth Problem is the question about the decidability of the Diophantine theory of R, i.e. the set of sentences which are questions about the solvability of a system of Diophantine equations in R.

J. Robinson proved in [13] that the theory of the rational numbers is undecidable. In [7] Ershov proved that the theory of a field of rational functions over a finite field of characteristic greater than 2 is undecidable; the case of characteristic 2 was proved by Penzin in [10]. In [14], Rumely proved that the theory of global fields is essentially undecidable. In [1], Cherlin proved that the theory of a field of rational functions over an infinite perfect field is undecidable. The decidability question about an arbitrary field of rational functions over any field still remains open, even in the important case that the field of constants is an algebraically closed field of zero characteristic (like the field of complex numbers).

In this paper we prove

Theorem. *Hilbert's Tenth Problem for a field of rational functions in a letter t with coefficients in a finite field of positive characteristic other than 2, is undecidable.*

The idea of the proof is to code the rational integers into the orders of elements x of $F(t)$ (F a finite field of characteristic $p \geqq 3$) at the prime t (denoted $\mathrm{ord}_t x$). Lemma 4 shows that the relation "$\mathrm{ord}_t x \geqq 0$" is Diophantine in $F(t)$. Lemma 3 shows that the relation "*y is a p^s-th power of x*" is Diophantine in $F(t)$ and so, by Lemma 4, the relation $\exists s(\mathrm{ord}_t y = p^s \mathrm{ord}_t x)$ is Diophantine in $F(t)$. So we can code in the Diophantine theory of $F(t)$ the Diophantine theory of the rational integers with inequality, addition (since $\mathrm{ord}_t x + \mathrm{ord}_t y = \mathrm{ord}_t(xy)$) and the relation "$n|_p m$" defined by $n|_p m$ if and only if $\exists s(m = p^s n)$. In [11] it was proved that the Diophantine theory of the natural numbers with addition and $|_p$ is undecidable. It follows that the Diophantine theory of the rational integers with inequality, addition and $|_p$ is undecidable and hence the Diophantine theory of $F(t)$ is undecidable.

The outstanding open problem of the area concerns Hilbert's Tenth Problem for the rational numbers. In number theory it has often been observed that there is a strong similarity of the properties of the rational numbers with the common properties of fields of rational functions over finite fields when it comes to solvability of Diophantine equations. In view of this similarity our result supports the idea that the Diophantine theory of the rationals is undecidable. Unfortunately, our treatment depends heavily on the characteristic of the field in question and is thereby not uniform. A more uniform approach would possibly be an important step towards finding techniques which are applicable to the rationals.

Acknowledgements. I should say that I am thankful to J. Denef for communicating to me the question which is answered here and for several inspiring conversations on the subject. His idea to code the integers into the endomorphisms of an elliptic curve, as in [4], seems to me the strongest possibility for a uniform proof of the present result. I am also thankful to Leonard Lipshitz for his encouragement and help in my first efforts towards the present results.

Notation. In the sequel $\mathbf{Z}$ is the set of rational integers, $\mathbf{N}$ the set of natural numbers $\{0, 1, 2, \ldots\}$, F a finite field with p^n elements where p is the characteristic of F. $\tilde{F}$ is a fixed algebraic closure of F. t is a letter, $F[t]$ the ring of polynomials in t with coefficients in F, $F(t)$ the field of rational functions, that is, quotients of

polynomials in t with coefficients in F and $F((t))$ the field of Laurent series, i.e. formal series of the form $a_{-k}t^{-k} + \ldots + a_0 + a_1 t + \ldots$ with $a_i \in F$ and $k \in \mathbf{N}$. Given an $x \in F(t)$, x can be written uniquely as $x = \frac{a}{b}$ where $a, b \in F[t]$, a and b are coprime and b is monic (that is, the highest degree coefficient of b is 1); we call a the *numerator* and b the *denominator* of x. A zero of x is a root (in $\tilde{F}$) of a and a pole of x is a root (in $\tilde{F}$) of b.

A prime in $F(t)$ is an irreducible monic polynomial in $F[t]$. If q is a prime in $F(t)$, x is in $F(t)$ and $x \neq 0$ we can always write $x = q^k y$ where q does not divide the numerator or denominator of y and $k \in Z$; we call k the order of x at q and denote it by $\operatorname{ord}_q x$. By convention, $\operatorname{ord}_q 0 = \infty$.

The multiplicity of a zero or a pole of x and the derivative of x with respect to t, x', are defined as usual.

The algebraic facts about finite fields and fields of rational functions can be found in [8]. A fact that will be used is that $F[t]$ is a free module over $F[t^{p^s}]$ of dimension p^s; the set $\{1, t, t^2, \ldots, t^{p^s-1}\}$ is a basis.

Lemma 1. *Let F be a field of characteristic $p \geqq 3$ (not necessarily finite). An x in $F(t)$ is a p^s-th power of t for some $s \in \mathbf{N}$ if and only if $\exists u, v \in F(t)$ $(x - t = u^p - u$ and $x^{-1} - t^{-1} = v^p - v)$.*

Proof. If $x = t$ then take $u = v = 0$; So assume that $s > 0$ and $x = t^{p^s}$. Then

$$x - t = (t^{p^{s-1}} + t^{p^{s-2}} + \ldots + t)^p - (t^{p^{s-1}} + t^{p^{s-2}} + \ldots + t)$$

and

$$x^{-1} - t^{-1} = (t^{-p^{s-1}} + t^{-p^{s-2}} + \ldots + t^{-1})^p - (t^{-p^{s-1}} + t^{-p^{s-2}} + \ldots + t^{-1}) .$$

Now we prove the converse. It is sufficient to prove that the result is valid in $\tilde{F}(t)$, hence we work in $\tilde{F}(t)$. If $x = z^p$ with $z \in \tilde{F}(t)$ and $x - t = u^p - u$, $x^{-1} - t^{-1} = v^p - v$ then

$$z - t = (u - z)^p - (u - z) \quad \text{and} \quad z^{-1} - t^{-1} = (v - z^{-1})^p - (v - z^{-1}) ,$$

so if it can be proved that $z = t^{p^s}$ for some $s \in \mathbf{N}$ then $x = z^p = t^{p^{s+1}}$; hence we may assume without loss of generality that x is not a p-th power in $\tilde{F}(t)$. *So* x has either a zero or a pole whose multiplicity is not divisible by p. But each pole of $u^p - u$ has multiplicity divisible by p. Hence, by the equation $x - t = u^p - u$, each pole of x is a pole of $u^p - u$ and so it has multiplicity divisible by p. Similarly by the equation $x^{-1} - t^{-1} = v^p - v$, each zero of x other than 0 has multiplicity divisible by p. So x is of the form

$$x = z^p t^k$$

for some $z \in \tilde{F}(t)$. By $x^{-1} - t^{-1} = v^p - v$, k is either 1 or divisible by p. Since x is not a p-th power, k is not divisible by p, so $k = 1$, so $x = tz^p$. So

$$x - t = t(z - 1)^p$$

and hence

$$t(z - 1)^p = u^p - u .$$

Write $z - 1 = \frac{a}{b}$, $u = \frac{c}{d}$ with $a, b, c, d \in \tilde{F}[t]$ so that a, b are coprime, c, d are coprime and b, d are monic. Clearly b is coprime to t since 0 is not a pole of $x - t$ (otherwise $x - t = u^p - u$ and $x = z^p t^k$ would force k to be divisible by p which has been shown not to be the case). Then since $ta^p/b^p = (c^p - cd^{p-1})/d^p$ and b is not

divisible by t we conclude that $b = d$ and

$$ta^p = c^p - cb^{p-1}\ .$$

So b^{p-1} divides $(-c)^p + ta^p$ in $\tilde{F}[t]$; since $p > 2$, $p - 1 \geqq 2$ and so b divides the derivative of $(-c)^p + ta^p$ with respect to t, so b divides a^p in $\tilde{F}[t]$ (note that the derivative of $(-c)^p + ta^p$ with respect to t is a^p). Since a, b are coprime it follows that b is a unit in $\tilde{F}[t]$; since b is monic we conclude that $b = 1$, so

$$ta^p = c^p - c\ ;$$

if $a \neq 0$ then the degree of the left hand side of the last equality would be congruent to 1 *modulo* p while the right hand side has degree divisible by p. We conclude that $a = 0$, hence $z = 1$, so $x = t$ which concludes the proof.

Lemma 2. *Let F be an arbitrary field of characteristic $p \geqq 3$. Let $x \in F(t)$ and write $u = (x^p + t)/(x^p - t)$. Then u has only simple zeros and simple poles.*

Proof. Write $x = \frac{a}{b}$ with $a, b \in F[t]$, a, b coprime. Then $u = (a^p + tb^p)/(a^p - tb^p)$. Let q be a prime of $F[t]$ so that q^2 divides $a^p + tb^p$. Then q divides the derivative of $a^p + tb^p$ with respect to t, so q divides b^p. Since q divides $a^p + tb^p$ and b^p it follows that q divides a^p so q divides a which contradicts the hypothesis that a and b are coprime. So u has only simple zeros. The result for the poles of u is proved similarly.

Lemma 3. *Let F be an arbitrary field of characteristic $p > 2$. Let $x, y \in F(t)$ and $xy \neq 0$. Let $u = (x^p + t)/(x^p - t)$, $v = (y + t^{p^s})/(y - t^{p^s})$, for some $s \geqq 0$. Then $y = x^{p^{s+1}}$ if and only if there are $\sigma, \tau, \mu, \theta, \delta$ in $F(t)$ so that*

$$v^2 - u^2 = \sigma^p - \sigma \tag{1}$$

$$v^{-2} - u^{-2} = \tau^p - \tau \tag{2}$$

$$v^2 t^{p^s} - u^2 t = \mu^p - \mu \tag{3}$$

$$v^{-2} t^{-p^s} - u^{-2} t^{-1} = \theta^p - \theta \tag{4}$$

$$v - u = \delta^p - \delta \tag{5}$$

Proof. If $y = x^{p^{s+1}}$ then $v = u^{p^s}$ so $v^2 = (u^2)^{p^s}$ and $v^2 t^{p^s} = (u^2 t)^{p^s}$ and the existence of $\sigma, \tau, \mu, \theta$ and δ follows as in the proof of Lemma 1.

So we assume (1)–(5) and we prove that $y = x^{p^{s+1}}$. We assume without loss of generality that F is algebraically closed.

If y is a p-th power, $y = z^p$, and $s > 0$, then set

$v_0 = (z + t^{p^{s-1}})/(z - t^{p^{s-1}})$ so $v = v_0^p$. We obtain

by (1), $$v_0^2 - u^2 = (\sigma - v_0^2)^p - (\sigma - v_0^2)\ , \tag{1'}$$

by (2), $$v_0^{-2} - u^{-2} = (\tau - v_0^{-2})^p - (\tau - v_0^{-2})\ , \tag{2'}$$

by (3), $$v_0^2 t^{p^{s-1}} - u^2 t = (\mu - v_0^2 t^{p^{s-1}})^p - (\mu - v_0^2 t^{p^{s-1}}) \tag{3'}$$

by (4), $$v_0^{-2} t^{-p^{s-1}} - u^{-2} t^{-1} = (\theta - v_0^{-2} t^{-p^{s-1}})^p - (\theta - v_0^{-2} t^{-p^{s-1}}) \tag{4'}$$

and by (5), $$v_0 - u = (\delta - v_0)^p - (\delta - v_0) \tag{5'}.$$

Hence if from (1')–(5') it follows that $v_0 = u^{p^{s-1}}$, then $v = u^{p^s}$ and so $y = x^{p^{s+1}}$ (the last assertion follows by straightforward calculation). So we assume without loss of generality that either y is not a p-th power, or $s = 0$.

Assume that $s > 0$ and y is not a p-th power. If v is a p-th power, say $v = h^p$, then $(y + t^{p^s})/(y - t^{p^s}) = h^p$, so $y(1 - h^p) = -t^{p^s}(1 + h^p)$; Since the characteristic of F is not 2, we have $h^p \neq 1$, therefore y is a p-th power, which contradicts the hypothesis; Hence v is not a p-th power. Assume that q is a prime of $F[t]$ other than t so that $\mathrm{ord}_q v$ is negative and not divisible by p. Clearly if $\mathrm{ord}_q(\sigma^p - \sigma)$ is negative then it is equal to $p \cdot \mathrm{ord}_q \sigma$ hence it is divisible by p. Since $\mathrm{ord}_q v$ is not divisible by p and by Lemma 2 $\mathrm{ord}_q u$ is either 0 or is not divisible by p, (1) implies that $\mathrm{ord}_q u^2 = ord_q v^2$. Since by Lemma 2 u has simple poles, $\mathrm{ord}_q u = -1$ so $\mathrm{ord}_q\ v = -1$ and $\mathrm{ord}_q(\sigma^p - \sigma) \geqq 0$. Similarly by (3) we obtain $\mathrm{ord}_q(\mu^p - \mu) \geqq 0$ so

$$\mathrm{ord}_q(v^2(t^{p^s} - t)) = \mathrm{ord}_q(\mu^p - \mu - t(\sigma^p - \sigma)) \geqq 0 .$$

But then, since $\mathrm{ord}_q v = -1$, we obtain $\mathrm{ord}_q(t^{p^s} - t) \geqq 2$. It is now easy to see that if $s \neq 0$ then $t^{p^s} - t$ has only simple zeros (since the derivative of $t^{p^s} - t$ with respect to t is -1), so we have a contradiction. Since $s \neq 0$ we conclude that all poles of v other than 0 have multiplicities divisible by p. Similarly, by (2) and (4) we conclude that all zeros of v other than 0 have multiplicities divisible by p. So v is of the form

$$v = r^p \cdot t^j .$$

It is easy to see that $\mathrm{ord}_t u = 0$. Hence, if $j < 0$ then by (1) it follows that j is divisible by p. Similarly, if $j > 0$ then by (2) it follows that j is divisible by p. So j is divisible by p, which contradicts the hypothesis that v is not a p-th power.

Hence the only remaining case to be considered is the case $s = 0$. Assume that $s = 0$. Then (3) becomes

$$t(v^2 - u^2) = \mu^p - \mu ,$$

so, in combination with (1) we obtain

$$t(\sigma^p - \sigma) = \mu^p - \mu .$$

Write $\sigma = t^i a/b$, $\mu = t^j c/d$ where $a, b, c, d \in F[t]$, the pairs a, b and c, d are coprime, b, d are monic, each of a, b, c, d is coprime to t and $i, j \in Z$. By $t(\sigma^p - \sigma) = \mu^p - \mu$ we obtain

$$t(t^{pi}a^p - t^i ab^{p-1})/b^p = (t^{pj}c^p - t^j cd^{p-1})/d^p ,$$

so $b = d$, and hence

$$t(t^{pi}a^p - t^i ab^{p-1}) = t^{pj}c^p - t^j cb^{p-1} .$$

If $i < 0$ then the order at t of the left hand side is $pi + 1$ which must be negative, so $j < 0$; but then the order at t of the right hand side is pj, so $pi + 1 = pj$ which is a contradiction. So $i \geqq 0$ and hence $j \geqq 0$. We have

$$b^{p-1}(t^j c - t^{i+1} a) = t^{pj}c^p - t^{pi+1}a^p$$

so b^{p-1} divides $t^{pj}c^p - t^{pi+1}a^p$. Since $p > 2$, b divides the derivative with respect to t of $t^{pj}c^p - t^{pi+1}a^p$, so b divides $t^{pi}a^p$ and since b is coprime to t, b divides a^p which, since a and b are coprime, implies that b is a unit in $F[t]$; since b is monic we conclude that $b = 1$. So

$$t(t^{pi}a^p - t^i a) = t^{pj}c^p - t^j c .$$

If the two sides of the last equality are different from zero, then the left hand side has degree congruent to 1 *modulo p* while the right hand side has degree divisible by p; We conclude that both the sides of the equality are equal to zero and therefore

$\sigma^p - \sigma = 0$. Consequently $v^2 = u^2$; so $u = \pm v$. Assume that $u = -v$. Then $u - v = 2u$ and by (5)

$$2u = u - v = -(\delta^p - \delta) .$$

Since $2u$ has only simple poles (by Lemma 2) and the poles of $\delta^p - \delta$ have multiplicity divisible by p we conclude that $\delta \in F[t]$, so $u \in F[t]$. Let $x = e/f$ with $e, f \in F[t]$, e, f coprime and f monic. Then $u = (e^p + tf^p)/(e^p - tf^p)$. Clearly (since the characteristics is not equal to 2), $e^p + tf^p$ and $e^p - tf^p$ either have t as a greatest common divisor or are coprime. In the first case t divides e^p, so the degree of e^p is at least p, hence the denominator of u, $(e^p - tf^p)/t$, has degree at least $p - 1$, which contradicts the fact that u is in $F[t]$. In the second case, since $u \in F[t]$ we have $e^p - tf^p \in F$, which implies that tf^p is a p-th power (since F is assumed algebraically closed) which implies that $f = 0$, a contradiction. So $u = v$ and hence $x^p = y$, which proves the Lemma.

Lemma 4. *Assume that F is a finite field with p^n elements, of characteristic $p > 0$. Write $r = p^n$. Let $x \in F(t)$. Then $\mathrm{ord}_t x \geqq 0$ if and only if there is an $s \in \mathbf{N} - \{0\}$ so that*

$$\exists a, a_1, \ldots, a_{r-1} \in F(t)[(1 - t^{p^s - 1})tx^p/(1 + tx^p) = a^r - a + ta_1^r + t^2 a_2^r + \ldots + t^{r-1} a_{r-1}^r].$$

Proof. Assume that

$$(1 - t^{p^s - 1})tx^p/(1 + tx^p) = a^r - a + ta_1^r + t^2 a_2^r + \ldots + t^{r-1} a_{r-1}^r$$

for some $a, a_1, \ldots, a_{r-1} \in F(t)$. The right hand side, viewed as a Laurent series in $F((t))$ has constant term zero since the constant term of each $t^i a_i^r$ is zero and the constant term of a^r is equal to the constant term of a (recall that for any $c \in F$, $c^r = c$).

We want to see what the constant term of the left hand side can be. If $\mathrm{ord}_t x \geqq 0$ then $\mathrm{ord}_t[(tx^p/(1 + tx^p)] > 0$, so

$$\mathrm{ord}_t[(1 - t^{p^s - 1})tx^p/(1 + tx^p)] > 0$$

and so the constant term of $(1 - t^{p^s - 1})tx^p/(1 + tx^p)$ is zero. Now assume that $\mathrm{ord}_t x = -k = < 0$. Then $\mathrm{ord}_t(tx^p) = 1 - pk$ and $\mathrm{ord}_t(1 + tx^p) = 1 - pk$ so $\mathrm{ord}_t[(1 - t^{p^s - 1})tx^p/(1 + tx^p)] = 0$ and hence the constant term of $(1 - t^{p^s - 1})tx^p/(1 + tx^p)$ is different from zero.

We conclude that we must have

$$\mathrm{ord}_t x \geqq 0 .$$

We now prove the converse. Assume that $\mathrm{ord}_t x \geqq 0$. Since $2tx^p/(1 + tx^p) = 1 - ((1 - tx^p)/(1 + tx^p))$ it follows by Lemma 2 that $tx^p/(1 + tx^p)$ has only simple poles.

We claim that if d is a polynomial in $F[t]$ with only simple roots which is not divisible by t in $F[t]$ then there is an s in $N - \{0\}$ so that d divides $t^{p^s - 1} - 1$ in $F[t]$; to see this observe that since t does not divide d, since the ring $R = F[t]/(d)$ is finite, the elements $1, t, t^2, t^3, \ldots$ of it cannot all be distinct, so for some distinct k, m in $\mathbf{N}$, d divides $t^k - t^m$ in $F[t]$; assuming without loss of generality that $m < k$ we have that d divides $t^{k-m} - 1$. If $k - m$ is a multiple of p, $k - m = hp$ then d divides $t^{hp} - 1 = (t^h - 1)^p$ and since d has only simple roots we conclude that d divides $t^h - 1$. So we can assume that $k - m$ is not divisible by p. Since p does not

divide $k-m$, p is a unit in the finite ring $\mathbf{Z}/(k-m)$ and so $k-m$ divides p^s-1 for some $s\in\mathbf{N}-\{0\}$. So $t^{k-m}-1$ divides $t^{p^s-1}-1$ in $F[t]$ and therefore d divides $t^{p^s-1}-1$, hence the claim is proved.

Since $\mathrm{ord}_t x \geqq 0$, the denominator of $tx^p/(1+tx^p)$ is a polynomial in $F[t]$ which is not divisible by t and which, as we have noticed again in the proof of the current Lemma, has only simple roots; so it divides $1-t^{p^s-1}$ for some $s\in\mathbf{N}-\{0\}$ as we proved before. Since $\mathrm{ord}_t x \geqq 0$, $(1-t^{p^s-1})tx^p/(1+tx^p)$ is a polynomial in $F[t]$ which is divisible by t. So it is sufficient to prove that any polynomial v which is divisible by t in $F[t]$ can be written as

$$v = a^r - a + ta_1^r + t^2a_2^r + \ldots + t^{r-1}a_{r-1}^r, \text{ with } a, a_1, \ldots, a_{r-1}\in F[t] .$$

So assume that $v\in F[t]$ and v is divisible by t in $F[t]$. $F[t]$ is a free module of dimension r over the ring $F[t^r]$ with basis $\{1, t, \ldots, t^{r-1}\}$ and so v can be written uniquely as

$$v = v_0^r + tv_1^r + \ldots + t^{r-1}v_{r-1}^r, \text{ with } v_0, \ldots, v_{r-1}\in F[t] .$$

The degree of each $t^i v_i^r$ is congruent to i *modulo* r, so there is no cancellation among leading terms of the $t^i v_i^r$ hence $\deg v \geqq \deg(t^i v_i^r)$ for each i for which $v_i \neq 0$. In particular, if $v_0 \neq 0$, $\deg v \geqq r \deg v_0$. Since t divides v we have that t divides v_0, so either $v_0 = 0$ or $\deg v > \deg v_0$. We have

$$v = v_0 + [v_0^r - v_0 + tv_1^r + \ldots + t^r v_{r-1}^r]$$

and by induction on the degree of v, we may assume that

$$v_0 = b^r - b + tb_1^r + \ldots + tb_{r-1}^r ,$$

so

$$v = (v_0 + b)^r - (v_0 + b) + t(v_1 + b_1)^r + \ldots + t^{r-1}(v_{r-1} + b_{r-1})^r$$

which concludes the proof.

Proof of the Theorem. It is easy to see that if Q_1, Q_2 are Diophantine relations in $F(t)$ then $Q_1 \cap Q_2$ and $Q_1 \cup Q_2$ are Diophantine relations in $F(t)$. By Lemma 1 the set $\{t^{p^s}: s\in\mathbf{N}\}$ is Diophantine in $F(t)$. So, by Lemma 4, for any $x\in F(t)$, the relation $\mathrm{ord}_t x \geqq 0$ is Diophantine in $F(t)$. By Lemma 3, the relation $\exists s\in\mathbf{N}\ (y = x^{p^s})$ is Diophantine in $F(t)$. So the relation $\exists s\in\mathbf{N}\ (\mathrm{ord}_t y = p^s \mathrm{ord}_t x)$ is Diophantine in $F(t)$ since it is equivalent to

$$\exists z\in F(t),\ s\in\mathbf{N}\ (z = x^{p^s} \text{ and } \mathrm{ord}_t(y/z) \geqq 0 \text{ and } \mathrm{ord}_t(z/y) \geqq 0) .$$

We code a rational integer k into the class of all elements x of $F(t)$ so that $\mathrm{ord}_t x = k$. Addition in the rational integers corresponds to multiplication of elements of $F(t)$, $\mathrm{ord}_t(xy) = \mathrm{ord}_t x + \mathrm{ord}_t y$, and inequality corresponds to the relation $\mathrm{ord}_t(y/x) \geqq 0$. The relation $k|_p m$ defined by $\exists s\in\mathbf{N}\ (m = p^s k)$ corresponds to $\exists s\in\mathbf{N}\ (\mathrm{ord}_t y = p^s \mathrm{ord}_t x)$ in $F(t)$. So we obtain a model of $\mathbf{Z}$ with inequality, $\geqq$, addition, $+$, and the relation $|_p$. So if the Diophantine theory of $F(t)$ were decidable then the Diophantine theory of $\mathbf{Z}$ with $\geqq$, $+$, $|_p$ would be decidable as well. In [11] it was proved that the Diophantine theory of $\mathbf{N}$ with $+$ and $|_p$ is undecidable. It follows that the Diophantine theory of $\mathbf{Z}$ with $\geqq$, $+$ and $|_p$ is undecidable (since $\mathbf{N}$ is Diophantine in $\mathbf{Z}$ with $\geqq$) and hence the Diophantine theory of $F(t)$ is undecidable.

We observe that Lemmas 1, 2 and 3 are valid in any field of positive characteristic other than 2. So the present result would be extended to any field of rational

functions in positive characteristic other than 2 if a general Diophantine definition of $\text{ord}_t x \geqq 0$ were found. We believe that such a definition exists and will not be very difficult to find in case F is not algebraically closed. The case that F is algebraically closed probably requires more significant utilization of sophisticated algebraic tools. The case $\text{char} F = 2$ may be tractable with slight modifications of the present proof.

References

1. Cherlin, G.: Undecidability of rational function fields in nonzero characteristic, Logic colloquium '82, Lolli, G., Logo, G., Marcja A. (eds), pp. 85–95. North Holland 1984
2. Davis, M., Matijasevic, Yu., Robinson, J.: Diophantine equations: Positive Aspects of a negative solution. Proc. Symp. Pure Math. **28**, 323–378 (1976)
3. Denef, J.: The Diophantine problem for polynomial rings of positive characteristic, Logic Colloquium '78, Boffa, M., van Dalen, D., McAloon, K. (eds), pp. 131–145. North Holland 1979
4. Denef, J.: The Diophantine problem for polynomial rings and fields of rational functions. Trans. Am. Math. Soc. **242**, 391–399 (1978)
5. Denef, J.: Diophantine sets over algebraic integer rings II. Trans. Am. Math. Soc. **257**, 227–336 (1980)
6. Denef, J., Lipshitz, L.: Diophantine sets over some rings of algebraic integers. J. Lond. Math. Soc. **18**, 385–391 (1978)
7. Ersov, Yu.: Undecidability of certain fields. Dokl. Akad. Nauk SSSR **161**, 349–352 (1965)
8. Lang, S.: Algebra. Reading, MA: Addison Wesley 1971
9. Matijasevic, Yu.: Enumerable sets are Diophantine. Dokl. Akad. Nauk SSSR **191**, 279–282 (1970)
10. Penzin, Yu.: Undecidability of fields of rational functions over fields of characteristic 2. Algebra Logic **12**, 205–219 (1973)
11. Pheidas, T.: An undecidability result for power series rings of positive characteristic II. Proc. Am. Math. Soc. **100**, 526–530 (1987)
12. Pheidas, T.: Hilbert's Tenth Problem for a class of rings of algebraic integers. Proc. Am. Math. Soc. **104**, 611–620 (1988)
13. Robinson, J.: Definability and decision problems in arithmetic. J. Symb. Logic **14**, 98–114 (1949)
14. Rumely, R.: Undecidability and definability for the theory of global fields. Trans. Am. Math. Soc. **262**, 195–217 (1980)