PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 120, Number 1, January 1994

HILBERT'S TENTH PROBLEM FOR RATIONAL FUNCTION FIELDS IN CHARACTERISTIC 2

CARLOS R. VIDELA

(Communicated by Andreas R. Blass)

ABSTRACT. In *Hilbert's Tenth problem for fields of rational functions over finite fields* (Invent. Math. **103** (1991)) Pheidas showed that Hilbert's Tenth problem over a field of rational functions with constant field a finite field of characteristic other than 2 is undecidable. We show that the same holds for characteristic 2.

1. INTRODUCTION

To obtain his result, Pheidas establishes four lemmas, the first three valid only for characteristic $p \geq 3$. They are:

Lemma 1.1. *Let F be a field of characteristic $p \geq 3$. An $x \in F(t)$ is a p^sth power of t for some $s \in \mathbb{N}$ if and only if $\exists u, v \in F(t)$ such that*

$$x - t = u^p - u, \qquad \tfrac{1}{x} - \tfrac{1}{t} = v^p - v.$$

Lemma 1.2. *Let F be a field of characteristic $p \geq 3$. For $x \in F(t)$ let $u = (x^p + t)/(x^p - t)$. Then u has only simple zeros and simple poles.*

Lemma 1.3. *Let F be a field of characteristic $p \geq 3$. Let $x, y \in F(t)$, $xy \neq 0$. Let $u = (x^p + t)/(x^p - t)$ and $v = (y + t^{p^s})/(y - t^{p^s})$ for some $s \geq 0$. Then $y = x^{p^{s+1}}$ if and only if $\exists \sigma, \tau, \mu, \theta, \delta$ in $F(t)$ such that*

$$v^2 - u^2 = \sigma^p - \sigma, \qquad \frac{1}{v^2} - \frac{1}{u^2} = \tau^p - \tau,$$

$$v^2 t^{p^s} - u^2 t = \mu^p - \mu, \qquad \frac{1}{v^2 t^{p^s}} - \frac{1}{u^2 t} = \theta^p - \theta, \qquad v - u = \delta^p - \delta.$$

Lemma 1.4. *Let F be a field of nonzero characteristic p. Assume F finite with p^n elements. Write $r = p^n$, and let $x \in F(t)$. Then $\operatorname{ord}_t(x) \geq 0$ if and only if $\exists s \in \mathbb{N} - \{0\}$ such that $\exists a, a_1, \ldots, a_{r-1} \in F(t)$ with $(1 - t^{p^{s-1}})tx^p/(1 + tx^p) = (a^r - a) + ta_1^r + \cdots + t^{r-1}a_{r-1}^r$.*

We mention Lemma 1.4 because it is an open problem to find something analogous for infinite fields. In characteristic 2 Lemma 1.1 is false. For example,

Received by the editors January 4, 1992 and, in revised form, April 23, 1992; the results of this paper were presented at the XXV Congreso Nacional de la Sociedad Matemática Mexicana, during October, 1992, held in Xalapa, Veracruz.

1991 *Mathematics Subject Classification.* Primary 03B25, 12L05.

take $x = (1+t+t^3)^2 t/(1+t^2+t^3)^2$. Then we have

$$x + t = \left(\frac{t^3}{1+t^2+t^3}\right)^2 + \frac{t^3}{1+t^2+t^3},$$

$$\frac{1}{x} + \frac{1}{t} = \left(\frac{1}{1+t+t^3}\right)^2 + \frac{1}{1+t+t^3}.$$

2. Proofs

For Lemma 1.1 we need to add more equations. In this section F is a field of characteristic 2.

Lemma 2.1. *Let $x \in F(t)$. Then $x \in \{t^{2^s} : s \geq 1\} \Leftrightarrow \exists u, v, w, s \in F(t)$ such that*

(1) $x + t = u^2 + u$,
(2) $u = w^2 + t$,
(3) $\frac{1}{x} + \frac{1}{t} = v^2 + v$,
(4) $v = s^2 + \frac{1}{t}$.

Notice that one direction is easy. If $x = t^{2^s}$ with $s \geq 2$, take $u = t^{2^{s-1}} + \cdots + t^2 + t = (t^{2^{s-2}} + \cdots + t)^2 + t$. For v take

$$\frac{1}{t^{2^{s-1}}} + \cdots + \frac{1}{t^2} + \frac{1}{t} = \left(\frac{1}{t^{2^{s-2}}} + \cdots + \frac{1}{t}\right)^2 + \frac{1}{t}.$$

If $s = 1$ take $u = t$ and $w = 0$; $v = \frac{1}{t}$ and $s = 0$.

In the other direction, it is enough to prove the result in $\tilde{F}(t)$. So from now on we assume we work in $\tilde{F}(t)$. First, two facts.

Fact 2.1. *If a rational function x is of the form $u^2 + u$ then the poles of x have multiplicities divisible by 2.*

Proof. Straightforward calculation.

Fact 2.2. *Let $x \in F(t)$, $x = a^2 t/b^2$, $(a, b) = 1$, and $(t, b) = 1$. Then the equations*

(1) $x + t = u^2 + u$,
(2) $u = w^2 + t$,
(3) $\frac{1}{x} + \frac{1}{t} = v^2 + v$,
(4) $v = s^2 + \frac{1}{t}$

cannot have solutions u, v, w, s, in $F(t)$.

Proof. Let $u = c/d$, $(c, d) = 1$, $w = m/n$, $(m, n) = 1$, $v = e/f$, $(e, f) = 1$, and $s = k/h$, $(k, h) = 1$. From (1) we get $t(a^2 + b^2)/b^2 = c(c + d)/d^2$. It follows that $b = d$. Equation (2) yields $c/b = (m^2 + n^2 t)/n^2$. Hence b is a square.

From (3) we get $(a^2 + b^2)/ta^2 = e(e + f)/f^2$.

Hence $t | a^2 + b^2$, from which we get that $a_0^2 + b_0^2 = 0$ (here a_0 and b_0 are the constant terms of the polynomials a and b). So $a_0 = b_0$, and $a = f$. From (4) we get $e/a = (k^2 t + h^2)/h^2 t$. If $(h^2 t, k^2 t + h^2) = 1$ then $a = h^2 t$ from which $a_0 = 0$; i.e., the polynomial a has no constant term. But then $b_0 = 0$ and so

$t|b$, which is a contradiction. On the other hand, if $(h^2t, k^2t+h^2) = q \neq 1$, it follows that $q = t$ and $t|h$. Write $h = th'$. So

$$\frac{e}{a} = \frac{t(k^2+th'^2)}{t^3h'^2} = \frac{k^2+th'^2}{t^2h'^2}.$$

Now we have $(k^2+th'^2, t^2h'^2) = 1$. The polynomial a is therefore divisible by t^2; in particular, $a_0 = 0$ again. This proves the fact.

We are now ready for the proof of Lemma 1.1.

Proof of Lemma 2.1. Suppose x is not a square. From Fact 2.1 and (1) and (3) (of the lemma) we have $x = a^2t^k/b^2$. The case $k < 1$ cannot happen; otherwise, $t = 0$ is a pole (and hence of even multiplicity) and x is a square, which we assume is not the case. It follows that $k = 1$. Notice that we also have $(t, b) = 1$ for otherwise we would have $t = 0$ a pole of x with odd multiplicity. Therefore, by Fact 2.2, we may assume that x is a square.

Let $x = z^2$. We consider two cases:

Case 1: $z = r^2$. By taking $u' = u+z$, $w' = w+r$, $v' = v+\frac{1}{z}$, and $s' = s+\frac{1}{r}$ we see that z satisfies (1)–(4). Hence if we establish that $z \in \{t^{2^s} : s \geq 1\}$ we get $x \in \{t^{2^s} : s \geq 1\}$. So we are left with

Case 2: z is not a square. As before (use (1) and (2) applied to z) we have $z = a^2t/b^2$, $(a, b) = 1$, $(t, b) = 1$. Assume b monic. Let u, w satisfy $x+t = w^2+u$, $u = w^2+t$. Then we have $z+t = (u+z)^2+(u+z)$. Writing $u+z = \frac{c}{d}$, $(c, d) = 1$, $w = \frac{m}{n}$, $(m, n) = 1$, we have that (as above in Fact 2.2) $b = d$ and

$$\frac{c}{d} = \frac{c}{b} = \frac{m^2}{n^2} + t + \frac{a^2}{b^2}t = \frac{(bm)^2+(nb)^2t+(na)^2t}{(nb)^2}.$$

If $((bm)^2+(nb)^2t+(na)^2t, (nb)^2) = 1$ then we have that $b = n^2b^2$ and hence $n^2b = 1$. It follows that $b = 1$. So $t(a^2+1) = c(c+1)$ (from (1) applied to z). If $a^2+1 \neq 0$, the left-hand side has odd degree whereas the right-hand side has even degree, so $a = 1$ and $z = t$ and $x = t^2$.

Now suppose $((bm)^2+(nb)^2t+(na)^2t, (nb)^2) = q \neq 1$.

If $q|n$ then the fraction c/b is of the form $c'/n'b^2$ with $(c', n'b^2) = 1$ (after cancelling q). Hence $n'b = 1$, so $b = 1$ and we are done. If $q \nmid n$ then there exists a nonconstant polynomial p such that $p|q$, $p|b$, $p \nmid n$, and $p|(bm)^2+(nb)^2t+(na)^2t$. Therefore, $p|a^2t$ and so $p|t$; hence, $t|b$, which is a contradiction. This finishes the proof.

Lemma 2.2. *Let F be a field of characteristic 2, and $x \in F(t)$. Then $u = (x^2+t^2+t)/(x^2+t)$ has only simple zeros and simple poles.*

Proof. Let $x = a/b$, $(a, b) = 1$. Then $u = (a^2+b^2t^2+b^2t)/(a^2+b^2t)$. If a prime $q \in F[t]$ is such that $q^2s = a^2+b^2t$ then the derivative $q^2s' = b^2$. Hence $q|a$; we get $q = 1$; similarly for the zeros of u.

Lemma 2.3. *Let F be a field of characteristic 2. Let $x, y \in F(t)$, $xy \neq 0$. Put*

$$u = \frac{x^2+t^2+t}{x^2+t} \quad \text{and} \quad v = \frac{y+t^{2^{s+1}}+t^{2^s}}{y+t^{2^s}}$$

where $s \geq 0$. Then $y = x^{2^{s+1}}$ if and only if $\exists p, q, w, z \in F(t)$ such that

(1) $u+v = p^2+p$,

(2) $v^2t^{2^s} + u^2t = q^2 + q$,
(3) $\frac{1}{u} + \frac{1}{v} = w^2 + w$,
(4) $1/v^2t^{2^s} + 1/u^2t = z^2 + z$.

Proof. First assume that $y = x^{2^{s+1}}$. Then $u^{2^s} = v$, so that $v^2 = (u^2)^{2^s}$ and $v^2t^{2^s} = (u^2t)^{2^s}$. It is clear what p, q, w, and z should be.

Conversely, assume we work in $\widetilde{F}(t)$. First observe that if $y = z^2$ and $s \geq 1$ and if we let $v_0 = (z + t^{2^s} + t^{2^{s-1}})/(z + t^{2^{s-1}})$, so that $v_0^2 = v$, then we have

$$v_0 + u = (p + v_0)^2 + (p + v_0),$$
$$v_0^2t^{2^{s-1}} + u^2t = (q + v_0^2t^{2^{s-1}})^2 + (q + v_0^2t^{2^{s-1}}),$$
$$\frac{1}{v_0} + \frac{1}{u} = \left(w + \frac{1}{v_0}\right)^2 + \left(w + \frac{1}{v_0}\right),$$
$$\frac{1}{v_0^2t^{2^{s-1}}} + \frac{1}{u^2t} = \left(z + \frac{1}{v_0^2t^{2^{s-1}}}\right)^2 + \left(z + \frac{1}{v_0^2t^{2^{s-1}}}\right).$$

Hence, if we showed that $z = x^{2^s}$, we get $y = x^{2^{s+1}}$. So assume that either $s = 0$ or y is not a square.

Case 1. $s = 0$. From (2) $t(u + v)^2 = q^2 + q$. Combining with (1) we have $t(p^4 + p^2) = q^2 + q$. Let $p = t^ia/b$, $q = t^jc/d$ with $(a, b) = 1$, $(t, ab) = 1$, $(c, d) = 1$, $(t, cd) = 1$, and $i, j \in \mathbb{Z}$. Then we have

$$\frac{t(t^{4i}a^4 + t^{2i}a^2b^2)}{b^4} = \frac{t^{2j}c^2 + t^jcd}{d^2}.$$

Hence $d = b^2$. Consider the equation $t(t^{4i}a^4 + t^{2i}a^2b^2) = t^{2j}c^2 + t^jcd$. If $i < 0$ then the order at t of the left-hand side is $4i + 1$, which is negative. The order of the right-hand side must be negative and so it is equal to $2j$, a contradiction. So $i \geq 0$ and $j \geq 0$. We have $b^2(t^{2i}a^2 + t^jc) = t^{2j}c^2 + t^{4i+1}a^4$. Differentiating, we get $b^2(t^{2i}a^2 + t^jc)' = a^4t^{4i}$. Hence $b|a^4t^{4i}$ and so $b = 1$ (we may assume b monic).

So we have $t(t^{4i}a^4 + t^{2i}a^2) = t^{2j}c^2 + t^jc$. By comparing degrees one must have that both sides are equal to 0; hence, $p^2 + p = 0$, so $u = v$, which implies $y = x^2$.

Case 2. $s \geq 1$ and y not a square. The proof of Pheidas works; split the situation into two subcases: v a square and v not a square. If v is a square then y is a square, which is a contradiction. If v is not a square then argue that all poles and zeros of v have multiplicity divisible by 2, and hence v is a square!

Final comments

The rest of Pheidas's argument applies without change, so one has the unsolvability of Hilbert's tenth problem. It is not clear to me why more equations are needed in characteristic 2 or rather why two are enough in odd characteristic in Lemma 2.1.

References

1. Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991).

Departamento de Matemáticas, CINVESTAV-IPN, México, D. F. 07000, México
E-mail address: cvidela@cinvesmx.bitnet