AN UNDECIDABILITY RESULT FOR POWER SERIES RINGS OF POSITIVE CHARACTERISTIC. II

THANASES PHEIDAS

ABSTRACT. We prove that the existential problem for a power series ring over an integral domain of positive characteristic with a predicate which represents the powers of the indeterminate is undecidable. We prove the same result for any ring which is contained in a power series ring and contains the corresponding ring of polynomials.

Introduction and notation. Let F be an integral domain. Let K be its quotient field. $F[t]$ denotes the ring of polynomials in t with coefficients in F . $K(t)$ denotes the function field of K , i.e. the quotient field of $F[t]$. $F[[t]]$ denotes the power series ring in the indeterminate t . $K((t))$ denotes the Laurent series ring over K , i.e. the quotient field of $F[[t]]$. $P(x)$ means that $\exists n \in \mathbb{Z}_+ (x = t^n)$ ($\mathbb{Z}_+$ is the set of positive integers). $L = \{+, \cdot, P, 0, 1, t\}$.

In [1 and 8], Ax and Kochen and Ershov proved that if F is a field of characteristic zero with decidable theory, then the theory of $F[[t]]$ in the language of discrete valuation rings augmented by P admits elimination of those quantifiers which range over $F[[t]]$ and is therefore decidable. In [5] Cohen gave such a concrete elimination. In [9] Macintyre proved that such an elimination exists in p -adic fields in an improved language. In [13] Weispfenning gave such a concrete elimination which applies in more general situations, such as rings of power series of characteristic zero.

It is known that the situation in nonzero characteristic is radically different. This was known to Ax though it was never published. In [2] Becker, Denef, and Lipshitz proved that in many cases the theory of $K((t))$ is undecidable. In particular this holds whenever K is a finite field. With some analysis of the proof one sees that the result can be stated in the following way: The universal existential theory of $F[[t]]$ in L is undecidable for several fields F of positive characteristic.

Unfortunately the proof cannot be generalized for arbitrary F . Moreover the question about the decidability or undecidability of the existential problem of $F[[t]]$ in L is left open, even in the case where F is a finite field. Some interesting relative results can be found in [3 and 4] by Cherlin.

In the present paper we give the answer to two of the above questions. Theorem 2 says that for any integral domain F of positive characteristic, the existential theory of $F[[t]]$ in L is undecidable. In [12] we proved a similar result for a limited class of integral domains using methods different from the present paper's.

Received by the editors April 8, 1986. The results of this paper have been presented to the Logic Seminar of Rutgers University at New Brunswick in March 1986 and to the 1986 meeting of the ASL at Indianapolis.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 03B25, 12L05; Secondary 10B40, 12B99, 12J10, 13F25, 13J05.

The author would like to thank the referee for helpful criticism.

The main ideas of the proof are the following: For n, m in N (the set of natural numbers $\{0, 1, 2, \dots\}$) let $n /_p m$ mean that $\exists s \in N (m = p^s n)$. We first code effectively the Diophantine problem (i.e. the positive existential problem) of N , with the operation $+$ and the relation $/_p$, into the existential problem of $F[[t]]$. This is done in Lemma 1. Next we prove that the Diophantine problem for N with $+$ and $/_p$ is undecidable. This is done by giving a Diophantine definition of multiplication in N in the language $L_0 = \{0, 1, +, /_p\}$. Finally we observe that the proofs work for every ring R which includes $F[t]$ and is included in $K((t))$.

In [6], Denef used the relation $/_p$ for the first time in order to show that the Diophantine problem of a polynomial ring of positive characteristic is undecidable. He did that by coding addition, divisibility, and $/_p$ for the integers in the Diophantine problems of these rings, and by showing that the Diophantine problem for N in the language of addition, divisibility, and $/_p$ is undecidable. A similar technique was used by the author in [11].

A consequence of the above results is that the Diophantine problem of $K(t)$ in the language L is undecidable. The common analogy between function fields and the rational numbers suggests that the Diophantine theory of the rational numbers in the language of rings together with a predicate for the powers of two might be undecidable. In our opinion this is an interesting problem in the direction of investigating the decidability properties of the Diophantine theory of the rationals, an outstanding problem of this area of mathematics.

In the sequel F is an integral domain of characteristic $p > 0$. For $n, m \in Z$, n/m means that n divides m and $n /_p m$ means that $\exists s \in N (m = p^s n)$.

1. Reduction of the existential problem for $F[[t]]$ in L to the Diophantine problem for N in L_0 .

LEMMA 1. (a) Let $n, m \in Z_+$. Then $n /_p m$ if and only if $\exists a \in K((t)) (t^{-m} - t^{-n} = a^p - a \text{ and } m \geq n)$.

(b) The Diophantine problem for N with $+$ and $/_p$ can be coded effectively into the existential problem for $F[[t]]$ in L .

(c) Let R be a ring such that $F[t] \subset R \subset K((t))$. Then the Diophantine problem in N for $+$ and $/_p$ can be effectively coded into the existential theory of R in the language L .

PROOF. (a) If $m = p^s n$ then $t^{-m} - t^{-n} = (t^{-n \cdot p^{s-1}} + t^{-n \cdot p^{s-2}} + \dots + t^{-n})^p - (t^{-n \cdot p^{s-1}} + \dots + t^{-n})$.

We now prove the converse. Let $n = p^r k$ with $p \nmid k$. Then, as we proved, there is a b so that $t^{-n} - t^{-k} = b^p - b$. Hence $t^{-m} - t^{-k} = (a+b)^p - (a+b)$. Let $m = p^l i$, with $p \nmid i$. Then for some $c \in K((t))$ we have $t^{-m} - t^{-i} = c^p - c$. Then we have $t^{-i} - t^{-k} = (a+b-c)^p - (a+b-c)$. The term of $(a+b-c)^p - (a+b-c)$ corresponding to the lowest exponent is a p th power. Since neither i nor k is divisible by p we conclude that $t^{-i} = t^{-k}$ and so $i = k$. So $m = p^l k$ and $n = p^r k$. Since $m \geq n$ we conclude that $l \geq r$ and so $n /_p m$.

(b) A Diophantine statement over $K((t))$ is equivalent to an existential statement over $F[[t]]$. So the relation $/_p$ is existentially definable in $F[[t]]$. Namely $n /_p m$ if and only if $\exists a, b, c, z \in F[[t]] (c^p(t^n - t^m) = t^n t^m (b^p - c^{p-1} b) \text{ and } c \neq 0 \text{ and } t^m = z t^n)$. Also $m = n + k$ if and only if $t^m = t^n t^k$.

(c) The existential definition of $m = n + k$ and $/_p$ in R is the same as for $F[[t]]$.

2. The Diophantine problem for N in the language $L_0 = \{0, 1, +, /_p\}$ is undecidable. In this section p is a positive prime integer.

LEMMA 2. (a) If $n, m \in \mathbb{Z}_+$ and $s \in N$ then $m = p^s n$ if and only if $n /_p m$, $n + 1 /_p m + p^s$, and $n + p /_p m + p^{s+1}$.

(b) Given n, m, p^s , the relation $m = p^s n$ is Diophantine over N in the language L_0 .

PROOF. (a) Let $m = p^s n$. Then $n /_p m$, $m + p^s = p^s(n + 1)$, and $m + p^{s+1} = p^s(n + p)$, so $n + 1 /_p m + p^s$ and $n + p /_p m + p^{s+1}$.

We now prove the converse. For suitable $r, q, k \geq 0$ we have $m = p^r n$, $m + p^s = p^q(n + 1)$, and $m + p^{s+1} = p^k(n + p)$. So we get $m = p^r n$, $p^r n + p^s = p^q(n + 1)$, and $p^r n + p^{s+1} = p^k(n + p)$. We assume that $n \neq 0$ (the case $n = 0$ is trivial). From the last two relations we obtain $n(p^r - p^q) = p^q - p^s$ and $n(p^r - p^k) = p^{k+1} - p^{s+1}$. If $r = q$ or $q = s$ then we obtain $r = q = s$. If $r = k$ or $k = s$ then we obtain $r = k = s$. So it is enough to prove the conclusion under the hypothesis that $r \neq q$, $q \neq s$, $r \neq k$, and $k \neq s$. From now on we accept these relations as part of the hypothesis. From the above relations, eliminating n we obtain

$$(1) \quad (p^r - p^q)(p^{k+1} - p^{s+1}) = (p^q - p^s)(p^r - p^k).$$

Before we proceed with the proof we prove the following

PROPOSITION. Let $i, j, k, q \in N - \{0\}$. Assume that p is a positive prime integer and that $(p^i - 1)(p^j - 1) = (p^k - 1)(p^q - 1)$. Then either $i = k$ and $j = q$, or $i = q$ and $j = k$.

PROOF. Because of symmetry we may assume with no loss of generality that $i \geq j, k \geq q$, and $j \leq q$. We consider these relations as part of the hypothesis. We obtain $p^{i+j} - p^i - p^j = p^{k+q} - p^k - p^q$ and hence $p^i - p^{i-j} - 1 = p^{k+q-j} - p^{k-j} - p^{q-j}$. We have that p^{q-j} divides all $p^i, p^{i-j}, p^{k+q-j}, p^{k-j}$. Hence p^{q-j} divides 1 so $q = j$. Hence $p^i - 1 = p^k - 1$, so $i = k$.

We now proceed with the proof of the lemma.

We distinguish the following cases:

Case 1: $r \geq q, k \geq s, q \geq s, r \geq k$. We obtain $(p^{r-q} - 1)(p^{k-s} - 1)p^{q+s+1} = (p^{q-s} - 1)(p^{r-k} - 1)p^{s+k}$. Hence $q + s + 1 = s + k$ and (by the Proposition) either $r - q = q - s$ and $k - s = r - k$, or $k - s = q - s$ and $r - q = r - k$. In the first case we get $r + s = 2q$ and $r + s = 2k$, so $k = q$ which contradicts the relation $q + s + 1 = s + k$. In the second case $k = q$ leading to the same conclusion.

Case 2: $r \geq q, k \geq s, q \leq s, r \leq k$. We obtain $(p^{r-q} - 1)(p^{k-s} - 1)p^{q+s+1} = (p^{s-q} - 1)(p^{k-r} - 1)p^{q+r}$. So $q + s + 1 = q + r$ and (by the Proposition) either $r - q = s - q$ and $k - s = k - r$, or $r - q = k - r$ and $k - s = s - q$. In the first case we obtain $r = s$ which contradicts the relation $q + s + 1 = q + r$. In the second case we have $k + q = 2r$ and $k + q = 2s$, so $r = s$, leading to the same conclusion.

Case 3: $r \leq q, k \leq s, q \geq s, r \geq k$. We obtain $(p^{q-r} - 1)(p^{s-k} - 1)p^{r+k+1} = (p^{q-s} - 1)(p^{r-k} - 1)p^{s+k}$. So $r + k + 1 = s + k$ and either $q - r = q - s$ and $s - k = r - k$, or $q - r = r - k$ and $s - k = q - s$. In the first case we obtain $r = s$ while in the second $q + k = 2r$ and $q + k = 2s$, so $r = s$, which contradicts the relation $r + k + 1 = s + k$.

Case 4: $r \leq q, k \leq s, q \leq s, r \leq k$. We obtain $(p^{q-r} - 1)(p^{s-k} - 1)p^{r+k+1} = (p^{s-q} - 1)(p^{k-r} - 1)p^{q+r}$. So $r + k + 1 = q + r$ and either $q - r = s - q$ and

$s - k = k - r$, or $q - r = k - r$ and $s - k = s - q$. In the first case we obtain $r + s = 2q$ and $r + s = 2k$, hence $k = q$ while in the second $q = k$ which contradicts the relation $r + k + 1 = q + r$.

Case 5: $r \geq q$, $k \leq s$, $q \geq s$, $r \leq k$. We obtain $(p^{r-q} - 1)(p^{s-k} - 1)p^{q+k+1} = (p^{q-s} - 1)(p^{k-r} - 1)p^{s+r}$. So $q + k + 1 = s + r$ and either $r - q = q - s$ and $s - k = k - r$, or $r - q = k - r$ and $s - k = q - s$. In the first case we have $r + s = 2q$ and $r + s = 2k$, so $k = q$. In the second case we have $k + q = 2r$ and $k + q = 2s$, so $r = s$. By $q + k + 1 = s + r$ we obtain in the first case $2k + 1 = r + s$ which together with $r + s = 2k$ gives a contradiction. In the second case we get $2s + 1 = s + r$, so $s + 1 = r$ which contradicts $r = s$.

Case 6: $r \geq q$, $k \leq s$, $q \leq s$, $r \geq k$. We obtain $(p^{r-q} - 1)(p^{s-k} - 1)p^{q+k+1} = (p^{s-q} - 1)(p^{r-k} - 1)p^{q+k}$. So $q + k + 1 = q + k$ which is a contradiction.

Case 7: $r \leq q$, $k \geq s$, $q \geq s$, $r \leq k$. We obtain $(p^{q-r} - 1)(p^{k-s} - 1)p^{r+s+1} = (p^{q-s} - 1)(p^{k-r} - 1)p^{s+r}$, so $r + s + 1 = s + r$ which is a contradiction.

Case 8: $r \leq q$, $k \geq s$, $q \leq s$, $r \geq k$. We obtain $(p^{q-r} - 1)(p^{k-s} - 1)p^{r+s+1} = (p^{s-q} - 1)(p^{r-k} - 1)p^{q+k}$. So $r + s + 1 = q + k$ and either $q - r = s - q$ and $k - s = r - k$, or $q - r = r - k$ and $k - s = s - q$. In the first case we obtain $r + s = 2q$ and $r + s = 2k$ so $k = q$, so $2k + 1 = q + k$, so $k + 1 = q$, a contradiction. In the second case we obtain $q + k = 2r$ and $k + q = 2s$, so $r = s$, so $r + s + 1 = 2s$, so $r + 1 = s$, a contradiction.

It is easy to see that all the other relative positions of r, q, k, s lead to one side of (1) having different sign from the other, so these are all the cases. Hence the result follows.

(b) Follows from (a).

PROPOSITION. (a) Let $n, m \in \mathbb{Z}_+$. Then n/m if and only if $p^n - 1/p^m - 1$.

(b) If $s, r \in \mathbb{Z}_+$ and $s \geq 1$ then $(p^{sr} - 1)/(p^s - 1) \equiv r \pmod{p^s - 1}$.

PROOF. (a) We prove that the right-hand relation implies n/m since the other direction is trivial. Let $m = qn + r$ with $0 \leq r < n$. Then $p^n - 1/p^r - 1$. But then $p^r - 1 < p^n - 1$, so $p^r = 1$, so $r = 0$.

(b) $(p^{sr} - 1)/(p^s - 1) = p^{s(r-1)} + p^{s(r-2)} + \dots + p^s + 1$ and $p^s \equiv 1 \pmod{p^s - 1}$ hence the result follows.

LEMMA 3. For $m, n \in \mathbb{N}$, we have $m = n^2$ if and only if

$$\exists s, r \in \mathbb{Z}_+ ((p^{2s} - 1)/(p^r - 1), (p^r - 1)/(p^{2s} - 1) \equiv n \pmod{p^{2s} - 1}, n < p^s - 1, \\ ((p^r - 1)/(p^{2s} - 1))^2 \equiv m \pmod{p^{2s} - 1} \text{ and } m < p^{2s} - 1).$$

PROOF. Assume that the right-hand side is true. Then by the relations $(p^r - 1)/(p^{2s} - 1) \equiv n \pmod{p^{2s} - 1}$ and $((p^r - 1)/(p^{2s} - 1))^2 \equiv m \pmod{p^{2s} - 1}$ we obtain $m \equiv n^2 \pmod{p^{2s} - 1}$. Since $n < p^s - 1$ we have $n^2 < p^{2s} - 1$. Since also $m < p^{2s} - 1$ we obtain $m = n^2$.

Now assume that $m = n^2$. Let s be any integer so that $p^s - 1 > n^2 = m$. Let $r = 2ns$. By the Proposition we have $p^{2s} - 1/p^r - 1$ and $(p^r - 1)/(p^{2s} - 1) \equiv n \pmod{p^{2s} - 1}$, so $((p^r - 1)/(p^{2s} - 1))^2 \equiv m \pmod{p^{2s} - 1}$.

COROLLARY. The relation $m = nk$ is Diophantine over $\mathbb{N}$ in the language $L_0 = \{0, 1, +, /_p\}$.

PROOF. By Lemma 2 we have that the right-hand side of Lemma 3 is Diophantine over N in L_0 . Hence the relation $m = n^2$ is Diophantine in L_0 . We have that $m = nk$ if and only if $(n + k)^2 = n^2 + 2m + k^2$ and this proves the assertion of the Corollary.

THEOREM 1. *The Diophantine problem for N in the language $\{0, 1, +, /_p\}$ is undecidable.*

PROOF. By the Corollary we can effectively code the Diophantine problem for N in the language $\{0, 1, +, \cdot\}$ into the Diophantine problem for N in the language $\{0, 1, +, /_p\}$. The former is known to be undecidable since Hilbert's Tenth Problem has a negative answer (cf. [10]). Hence the latter is undecidable as well.

By Lemma 1 and Theorem 1 we obtain

THEOREM 2. *Let R be a ring such that $F[t] \subset R \subset K((t))$. Then the existential problem for R in the language L is undecidable.*

REMARK. If we adopt the convention that 0 is not in P then the relation $x \neq 0$ has a Diophantine definition in R in the above language. So under this convention the Diophantine problem of R is undecidable. But such a convention would be rather artificial.

BIBLIOGRAPHY

1. J. Ax and S. Kochen, *Diophantine problems over local fields. III. Decidable fields*, Ann. of Math. (2) **83** (1966), 437–456.
2. J. Becker, J. Denef and L. Lipshitz, *Further remarks on the elementary theory of formal power series rings*, Model Theory of Algebra and Arithmetic (Proc. Karpacz, Poland 1979), Lecture Notes in Math., vol. 834, Springer-Verlag, 1980.
3. G. L. Cherlin, *Definability in power series rings of nonzero characteristic*, Models and Sets, Lecture Notes in Math., Springer-Verlag, 1984, pp. 102–112.
4. —, *Undecidability of rational function fields in nonzero characteristic*, Logic Colloq., no. 82, North-Holland, Amsterdam.
5. P. J. Cohen, *Decision procedures for real and p -adic fields*, Comm. Pure Appl. Math. **22** (1969), 131–151.
6. J. Denef, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloq., no. 78, North-Holland, Amsterdam, 1979.
7. J. Denef and L. Lipshitz, *An effective form of Greenberg's Theorem* (preprint).
8. Yu. L. Ersov, *On the elementary theory of maximal normed fields*, Dokl. Akad. Nauk SSSR **165** (1965).
9. A. Macintyre, *On definable subsets of p -adic fields*, J. Symbolic Logic **41** (1976), 605–610.
10. Y. Matiyasevic, *Enumerable sets are Diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282.
11. T. Pheidas, *The Diophantine problem for addition and divisibility in polynomial rings*, Thesis, Purdue Univ., 1985.
12. —, *An undecidability result for power series rings of positive characteristic*, Proc. Amer. Math. Soc. **99** (1987), 364–366.
13. V. Weispfenning, *Quantifier elimination and decision procedures for valued fields*, Logic Colloq., no. 83, Aachen, and Lecture Notes in Math., vol. 1103, Springer-Verlag, 1984.

DEPARTMENT OF MATHEMATICAL SCIENCES, FLORIDA INTERNATIONAL UNIVERSITY, TAMAMI CAMPUS, MIAMI, FLORIDA 33199

Current address: Computer Technology Institute, Post Office Box 1122, 26110 Patras, Greece