PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 99, Number 2, February 1987

AN UNDECIDABILITY RESULT FOR POWER SERIES RINGS OF POSITIVE CHARACTERISTIC

THANASES PHEIDAS

ABSTRACT. We prove that the existential theory of a power series ring in one variable over an integral domain F of positive characteristic, with cross section, is undecidable whenever F does not contain an e such that $e^p - e = 1$. For example, the result is valid if $F = Z_p$ (the p-element field where p is a prime).

Introduction. Let F be an integral domain of positive characteristic such that F does not contain an e with $e^p - e = 1$. Let t be a variable. $F[[t]]$ denotes the power series ring in t with coefficients from F and $K((t))$ denotes the field of Laurent series in t with coefficients from K, where K is the quotient field of F.

We use an idea in [**2**] and a result of [**6**] in order to code effectively the Diophantine problem for the rational integers into the existential problem for $F[[t]]$ in the language $L = \{0, I, +, \cdot, P\}$, where P represents the set $\{0, t, t^2, \dots, t^n, \dots\}$.

The present result combined with the results of [**2**, **3**, and **5**] gives a better understanding of the decidability properties of these rings in the above language. Unfortunately, this result gives no indication of what happens if the predicate P is dropped.

I would like to thank Jan Denef for proofreading and correcting some mistakes in a previous version of this paper.

An important lemma. The following lemma is taken from [**2**]. We give its proof for the sake of completeness.

LEMMA 1. *Let Z_p be the finite field with p elements, where p is a prime rational integer. Let $x \in Z_p((t))$. Then the constant term of x is equal to zero if and only if there are $a, x_1, \dots, x_{p-1}$ in $Z_p((t))$ so that $x = a^p - a + x_1^p t + \cdots + x_{p-1}^p t^{p-1}$.*

PROOF. It is easy to see that if $y \in F[[t]]$ and t divides y, then there is a $b \in F[[t]]$ so that $b^p - b = y$, namely $b = -(y + y^p + y^{p^2} + y^{p^3} + \cdots)$ (since y is divisible by t, it is easily checked that the expression $y + y^p + y^{p^2} + y^{p^3} + \cdots$ represents a power series in $F[[t]]$).

Moreover the form $a^p - a + x_1^p t + \cdots + x_{p-1}^p t^{p-1}$ is additive, i.e. if $x = a^p - a + x_1^p t + \cdots + x_{p-1}^p t^{p-1}$ and $y = b^p - b + y_1^p t + \cdots + y_{p-1}^p t^{p-1}$, then

$$x + y = (a+b)^p - (a+b) + (x_1 + y_1)^p t + \cdots + (x_{p-1} + y_{p-1})^p t^{p-1}.$$

So if $x = y + z$ with $y \in Z_p[[t]]$ and $z \in Z_p[t^{-1}]$ with t dividing y and the constant term of x is zero, x can be written in the above form if and only if z can be written

Received by the editors January 13, 1986.

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

in this form. Moreover, it is enough to check this only in the case that z is a monomial. So let $z = ct^{-np^s}$ where $x \in Z_p$, n is a positive rational integer not divisible by p, and s a natural number. If $s \neq 0$, then $z = a^p - a + ct^{-n}$ where $a = c(t^{-np^{s-1}} + t^{-np^{s-2}} + \cdots + t^{-n})$. So we are reduced to the case $z = ct^{-n}$, where n is not divisible by p. But then $-n$ can be written in the form $-n = -kp + i$ where $0 < i < p$ so $z = (ct^{-k})^p t^i$. Of course, in the above we made use of the fact that for any $c \in Z_p$ we have $c^p = c$.

For the converse we observe that if $x = a^p - a + x_1^p t + \cdots + x_{p-1}^p t^{p-1}$, then the constant term of x is equal to the constant term of $a^p - a$ which is necessarily zero (again using the fact that for any $c \in Z_p$ we have $c^p - c = 0$). Q.E.D.

We need the following fact:

FACT. If $y \in F[[t]]$ and t divides y, then all the solutions of $x^p - x = y$ in $F[[t]]$ are $-[c + (y + y^p + \cdots)]$, where c ranges over all the elements of the prime subfield Z_p of F. In particular, the only solution whose order is greater than zero is $-(y + y^p + \cdots)$.

The proof of this fact is elementary, using the observation that we stated at the beginning of the proof of Lemma 1.

The two main lemmas and the conclusion. We want to code the natural numbers with addition, divisibility, and the relation $/_p$, where $n/_p m$ means $\exists s \geq 0 (m = p^s n)$, into the existential problem for $F[[t]]$ with cross section.

We use the powers of t as representing the natural numbers.

The relation $m = n + k$ is expressed by $t^m = t^n t^k$. Hence we need to show that we can code the relations $/$ (which from now on denotes divisibility in the integers) and $/_p$. Lemmas 2 and 3 show these two facts, correspondingly.

LEMMA 2. *n/m if and only if the constant term of $[t^m(1 - t^n)]^{-1} - 1$ is equal to zero.*

PROOF. ($\rightarrow$) We have $[1 - t^n]^{-1} = 1 + t^n + t^{2n} + \cdots$, so, if $m = nk$ then

$$[t^m(1 - t^n)]^{-1} = (t^{nk})^{-1} + (t^{n(k-1)})^{-1} + \cdots + (t^n)^{-1} + 1 + t^n + \cdots$$

so the constant term of $[t^m(1 - t^n)]^{-1} - 1$ is equal to zero.

($\leftarrow$) We have again $[t^m(1 - t^n)]^{-1} = t^{-m}(1 + t^n + \cdots)$, so if the constant term of $[t^m(1 - t^n)]^{-1}$ is 1, then for some integer k we have $t^{-m}t^{kn} = 1$, so $m = kn$.

LEMMA 3. *$n/_p m$ iff the mth term of $(t^n + t^{np} + t^{np^2} + \cdots) - t^m$ is zero, i.e. if and only if the constant term of $t^{-m}[(t^n + t^{np} + \cdots) - t^{-m}]$ is equal to zero.*

PROOF. ($\rightarrow$) If for some s we have $m = p^s n$, then the result follows.

($\leftarrow$) Since the term t^m must cancel with some term of the form t^{np} we obtain $m = np^s$.

THEOREM. *One can code effectively the Diophantine problem for the natural numbers into the existential problem for the ring $F[[t]]$ with cross section. Hence, since the former is undecidable the latter is undecidable as well.*

PROOF. All the expressions that we used in Lemmas 2 and 3 are elements of $Z_p[[t]]$. Hence, the constant term of $[t^m(1 - t^n)]^{-1} - 1$ is zero if and only if $\exists a, x_1, \ldots, x_{p-1} \in K((t))$ such that $[t^m(1-t^n)]^{-1} - 1 = a^p - a + tx_1^p + \cdots + x_{p-1}^p t^{p-1}$ (here we use the fact that for each $e \in F$, $e^p - e \neq 1$). Hence, by Lemma 1 and

the Fact, the relations $/$ and $/_p$ are Diophantine over $F((t))$ with cross sections, hence existentially definable over $F[[t]]$ with cross section. In [**6**] it is proved that the Diophantine problem for the natural numbers can be effectively coded into the Diophantine theory of the rational integers with addition, divisibility, and the relation $/_p$. It is a triviality that the Diophantine problem for the rational integers with $+$, $/$, and $/_p$ can be effectively coded into the Diophantine problem for the natural numbers with $+$, $/$, and $/_p$. This completes the proof.

REMARK. If the set denoted by P does not contain 0, i.e. if $P = \{t, t^2, \dots\}$, then the above theorem implies that the Diophantine problem for $F[[t]]$ with cross section is undecidable, since the relation $x \neq 0$ for any $x \in Z_p[[t]]$ is Diophantine: $x \neq 0$ iff $\exists y \in P, z\ (xz = y)$.

REFERENCES

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, pp. 1–9.
3. G. L. Cherlin, *Definability in power series rings of nonzero characteristic*, Models and Sets, Lecture Notes in Math., vol. 1103, Springer-Verlag, 1984, pp. 102–112.
4. P. J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. **22** (1969), 131–151.
5. J. Denef and L. Lipshitz, *A constructive analogue of Greenberg's Theorem in positive characteristic*, preprint.
6. J. Denef, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloq., no. 78, North-Holland, 1979.
7. A. Macintyre, *On definable subsets of p-adic fields*, J. Symbolic Logic **41** (1976), 605–610.
8. V. Weispfenning, *Quantifier elimination and decision procedures for valued fields*, Logic Colloq., no. 83, Aachen, Lecture Notes in Math., Springer-Verlag, 1986, pp. 419–472.

DEPARTMENT OF MATHEMATICS, FLORIDA INTERNATIONAL UNIVERSITY, TAMIAMI CAMPUS, MIAMI, FLORIDA 33199