FUNDAMENTA
MATHEMATICAE
182 (2004)

Diophantine undecidability for addition and divisibility in polynomial rings

by

Thanases Pheidas (Heraklion)

Abstract. We prove that the positive-existential theory of addition and divisibility in a ring of polynomials in two variables $A[t_1, t_2]$ over an integral domain A is undecidable and that the universal-existential theory of $A[t_1]$ is undecidable.

1. Introduction. Let B be a commutative ring. The relation of *divisibility* in B, denoted by $|$, is defined by

$$x \,|\, y \quad \text{if and only if} \quad \exists z \in B\ [y = xz].$$

By $(B; +; |; C)$ we denote B considered as a model of the language L which contains the symbol $+$ for addition, the relation symbol $|$ for divisibility, constants for the elements of the subset C of B and, for each element $c \in C$, a symbol for multiplication by c: $x \to cx$. A formula of L is *existential* (resp. *positive-existential*) if it is of the form $\exists x_1, \ldots, x_n \in B[\phi(x_1, \ldots, x_n)]$, where ϕ is a quantifier-free formula of L (resp. a positive quantifier-free formula, i.e. a disjunction of conjunctions of formulas of the form $f_1(x_1, \ldots, x_n) \diamond f_2(x_1, \ldots, x_n)$, where $\diamond$ is one of $=$ and $|$, and f_1 and f_2 are terms of L). The *positive-existential* theory of $(B; +; |; C)$ is the set of all positive-existential formulas of L which hold true in $(B; +; |; C)$. The *ring-theory* (resp. *positive-existential ring-theory*) of B is the theory of B (resp. positive-existential theory of B) in the language which extends L by a symbol for multiplication.

Addition and divisibility have been studied for several years. In [17] J. Robinson proved that the first order theory of addition and divisibility in the rational integers $\mathbb{Z}$ is undecidable. Lipshitz [7] (and, independently, Bel'tyukov [1]) proved that the existential theory of addition and divisibility in $\mathbb{Z}$ is decidable; the same is true in any ring of algebraic integers of an

2000 *Mathematics Subject Classification*: Primary 03B25, 12L05; Secondary 11U05.

The results of this article were part of the Ph.D. thesis of the author, at Purdue University, under the supervision of Leonard Lipshitz and with support of a David Ross grant. The author expresses his gratitude.

The author thanks the referee for very helpful suggestions.

imaginary quadratic number field. Let $\mathcal{O}_K$ be the ring of algebraic integers in the number field K. In [6] and [8] Lipshitz proved that if K is neither $\mathbb{Q}$ nor imaginary quadratic then multiplication is positive-existentially definable from addition and divisibility, and thus the positive-existential theory of addition and divisibility in $\mathcal{O}_K$ is decidable if and only if the positive existential ring-theory (also called *diophantine theory*) of $\mathcal{O}_K$ is decidable. In all known cases the diophantine theory of $\mathcal{O}_K$ is undecidable and it has been conjectured by Denef and Lipshitz that the same holds true in all $\mathcal{O}_K$ (this is the analogue of Hilbert's tenth problem for the rings $\mathcal{O}_K$; for a survey see [18], [13] and [14]). Therefore it is expected that the positive-existential theory of addition and divisibility in any $\mathcal{O}_K$ is undecidable if K is of degree other than 1 or 2 over $\mathbb{Q}$.

In [12] it was proved that the existential theory of addition and divisibility in a ring of polynomials $F[t]$ of one variable, over a field F, with constants for the elements $0, 1, t$, is decidable if and only if the existential ring-theory of F is decidable. In the present article we show that this result does not extend to polynomials in two variables. In fact, given an integral domain A, we will reduce the undecidability of the positive-existential theory of the structure $(A[t_1, t_2]; +; |; \{0, 1, t_1, t_2\})$ of addition and divisibility in the ring of polynomials $A[t_1, t_2]$, with constant symbols for the elements $0, 1, t_1, t_2$, to the undecidability of the positive-existential theory of the structure $(A[t, t^{-1}]; +; |; \{0, 1, t\})$ of addition and divisibility in $A[t, t^{-1}]$ with constant symbols for $0, 1, t$. We will prove

THEOREM 1.1. *Let A be an integral domain. Let t be a variable and $A[t]$ the ring of polynomials of the variable t with coefficients in A. Let L be the language with symbols for addition and divisibility in $A[t, t^{-1}]$, with symbols for* 0, 1 *and t and a symbol for multiplication by t. Write $(A[t, t^{-1}]; +; |; \{0, 1, t\})$ for the structure of $A[t, t^{-1}]$ as a model of L. Then*:

(i) *The positive-existential theory of $(A[t, t^{-1}]; +; |; \{0, 1, t\})$ is undecidable.*

(ii) *If A has characteristic zero and contains the field of rational numbers $\mathbb{Q}$ then the following are positive-existentially definable in L over $(A[t, t^{-1}]; +; |; \{0, 1, t\})$*: (a) *the set $\mathbb{Z}$ of rational integers and* (b) *the graph of multiplication in $\mathbb{Z}$ (thus the ring-structure of $\mathbb{Z}$ is positive-existentially definable).*

(iii) *If A has prime characteristic $p > 0$ then the following are positive-existentially definable in L over $(A[t, t^{-1}]; +; |; \{0, 1, t\})$*: (a) *the set $E[t, t^{-1}]$, where E is the field of elements of A, algebraic over the field $\mathbb{F}_p$ with p elements and* (b) *the graph of multiplication in $E[t, t^{-1}]$ (thus the subring $E[t, t^{-1}]$ and its ring-structure are positive-existentially definable).*

(iv) *The positive-existential ring-theory of* $E[t, t^{-1}]$ (E *is as in* (iii)) *is undecidable.*

As a consequence we obtain

COROLLARY 1.1. *Let* A *be as in Theorem* 1.1 *and let* t_1 *and* t_2 *be distinct variables. Then the positive-existential theory of the structure* $(A[t_1, t_2]; +; |; \{0, 1, t_1, t_2\})$ *is undecidable.*

Proof. The quotient ring $A[t_1, t_2]/(1 - t_1t_2)$ (of $A[t_1, t_2]$ by the ideal generated by $1 - t_1t_2$) is an integral domain, isomorphic to $A[t, t^{-1}]$ under the natural extension σ of the map which associates t to t_1 and t^{-1} to t_2. For any $x, y \in A[t_1, t_2]$,

$$\sigma(x) \text{ divides } \sigma(y) \text{ in } A[t, t^{-1}] \quad \text{if and only if}$$
$$\exists z \in A[t_1, t_2]\,[x \text{ divides } y + z(1 - t_1t_2) \text{ in } A[t_1, t_2]].$$

Hence, if the positive-existential theory of addition and divisibility with constants $0, 1, t_1, t_2$ in $A[t_1, t_2]$ (i.e. of the structure $(A[t_1, t_2]; +; |; \{0, 1, t_1, t_2\})$) were decidable, then the similar problem in $A[t, t^{-1}]$ with constants $0, 1, t$ (i.e. the positive-existential theory of $(A[t, t^{-1}]; +; |; \{0, 1, t\})$) would also be decidable, which contradicts Theorem 1.1. ∎

In [3] and [4] J. Denef proved that the diophantine problem in any polynomial ring over an integral domain is undecidable. Corollary 1.1 obviously gives a stronger result for the case of two or more variables. Besides, our treatment of addition and divisibility in $A[t, t^{-1}]$ is related to the methods of Denef in the following way: Consider the equation $x^2 - (t^2 - 1)y^2 = 1$ over $A[t]$. As is proved in [3] and [4], if $\mathrm{char}(A) \neq 2$, then the solutions of this equation are given by (x_n, y_n), where $x_n + dy_n = \pm(t + d)^n$ and d is a root of the polynomial $X^2 - (t^2 - 1)$. It is easy to show that, in order to prove that the positive-existential ring-theory of $A[t]$ is undecidable, it suffices to prove that the positive-existential ring-theory of $A[t, d]$ is undecidable, in the language which, besides symbols for addition, multiplication, 0 and 1, contains also constant-symbols for t and d. Write $\varepsilon = t + d$. Then $t = (\varepsilon + \varepsilon^{-1})/2$ and $d = (\varepsilon - \varepsilon^{-1})/2$, so if 2 is a unit in A, we have $A[t][d] = A[\varepsilon, \varepsilon^{-1}]$. Therefore, to prove that the diophantine ring-theory of $A[t, d]$ is undecidable, it suffices to show that the positive-existential theory of addition and divisibility in $A[\varepsilon, \varepsilon^{-1}]$ is undecidable (in a language which contains a symbol for the constant ε), which follows from Theorem 1.1.

Some of the ideas of the present article have their origin in the aforementioned papers of Denef and Lipshitz.

P. Pappas proved in [11] that the diophantine theory of the ring $A[t, t^{-1}]$ is undecidable if $\mathrm{char}(A) = 0$. More results on addition and divisibility can be found in [2], [5], [9], [15], [16] and [19]. The solution to Hilbert's tenth problem was given in [10].

Theorem 1.1 is proved in Sections 3 (the case of characteristic zero), 4 and 5 (the case of positive characteristic). In Section 6 we prove:

THEOREM 1.2. *Assume that A is an integral domain containing the quotient field of its prime ring (that is, if A is of zero characteristic then the field $\mathbb{Q}$ of rational numbers is contained in A). Then the universal-existential theory of addition and divisibility in $A[t]$ is undecidable. In particular the elementary theory of addition and divisibility in $A[t]$ is undecidable.*

We note that our proof of Theorem 1.2 in the case of zero characteristic actually shows that the positive-existential theory of addition, divisibility and the relation "$x \in \{t^n : n \in \mathbb{N}\}$" in $A[t]$ is undecidable (for A as in Theorem 1.2). An analogous fact does not follow in the case of nonzero characteristic. We think that in that case the problem may be decidable. If this turns out to be correct then, by the analogy that often occurs between the polynomial rings over finite fields and the rational integers, one may expect that the positive-existential theory of addition, divisibility and the relation "x is a power of 2" in the rational integers may be decidable; this is a problem asked by J. Robinson in a letter to L. Lipshitz.

We use the following notation: $\mathbb{N} = \{1, 2, \ldots\}$ is the set of natural numbers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, and $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ is the set of integers. Throughout this article A is an integral domain of characteristic $\mathrm{char}(A)$ (it can be either 0 or a prime $p > 0$).

2. Definability in the language of addition and divisibility. We will work in the structure $(A[t, t^{-1}]; +; |; \{0, 1, t\})$ of addition and divisibility in the ring $A[t, t^{-1}]$ (sometimes called "Laurent polynomials") with constant symbols for $0, 1, t$. The divisibility relation will be understood in $A[t, t^{-1}]$, unless stated otherwise. The language L that we will use is the set of symbols $L = \{+, |, 0, 1, t\}$, representing the obvious relations, operations and elements of $A[t, t^{-1}]$ (we will not make the usual distinction between the symbols of the language and the relations that interpret them because the distinction will always be clear from the context).

In the following lemma we include the algebraic properties of $A[t, t^{-1}]$ that we will use. The proofs are easy and are left to the reader.

LEMMA 2.1. (i) *For any $x \in A[t, t^{-1}]$ there is an integer power t^n of t with $n \in \mathbb{N}_0$ so that $t^n x \in A[t]$.*

(ii) *Each element x of $A[t, t^{-1}]$ can be written uniquely as $x = t^n z$, where $n \in \mathbb{Z}$ and $z \in A[t]$ is not divisible by t in $A[t]$.*

(iii) *If $x, y \in A[t]$ and t does not divide x in $A[t]$ then $x \mid y$ in $A[t, t^{-1}]$ if and only if x divides y in $A[t]$.*

(iv) *All the units in $A[t, t^{-1}]$ are of the form αt^n for some $n \in \mathbb{Z}$ and some unit $\alpha \in A$.*

(v) *If A is a unique factorization domain, then the ring $A[t, t^{-1}]$ is a unique factorization domain as well.*

LEMMA 2.2. (i) *If $n, m \in \mathbb{Z}$ then n divides m in $\mathbb{Z}$ if and only if $t^n - 1 \mid t^m - 1$ in $A[t, t^{-1}]$.*

(ii) *If $k \in \mathbb{Z} \setminus \{0\}$ and $n \in \mathbb{Z}$ then*

$$\frac{t^{kn} - 1}{t^k - 1} \equiv n \bmod (t^k - 1).$$

(iii) *If $k \in \mathbb{Z}$ then*

$$\frac{t^k - 1}{t - 1} \equiv 1 \bmod (t + 1) \quad \textit{if and only if} \quad k \textit{ is odd.}$$

(iv) *Let u be a unit in $A[t, t^{-1}]$. Then $\exists n \in \mathbb{Z}\ [u = t^n]$ if and only if $t - 1 \mid u - 1$ in $A[t, t^{-1}]$.*

Proof. (i) The "only if" part is trivial. We prove the "if" part. For any $n \in \mathbb{Z}$, $t^{-n} - 1 = -t^{-n}(t^n - 1)$, hence we assume with no loss of generality that $m, n \geq 0$. If $n = 0$ then the result is clear. So let $n > 0$ and let $m = rn + l$ with $0 \leq l < n$. Since $t^n - 1 \mid t^m - 1$, we have $t^n - 1 \mid (t^m - 1) - (t^{rn} - 1)t^l = t^l - 1$, which, by working in $A[t]$ and applying Lemma 2.1(iii), implies that $t^l = 1$, hence $l = 0$.

(ii) For $n = 0$ the result is clear. For $n > 0$ we have

$$\frac{t^{kn} - 1}{t^k - 1} = 1 + t^k + t^{2k} + \cdots + t^{(n-1)k} \equiv n \bmod (t^k - 1).$$

For $n < 0$ we have

$$\frac{t^{kn} - 1}{t^k - 1} = -t^{kn}\,\frac{t^{-kn} - 1}{t^k - 1} \equiv n \bmod (t^k - 1).$$

(iii) For $k > 0$ we have

$$\frac{t^k - 1}{t - 1} = 1 + t + \cdots + t^{k-1} \equiv \begin{cases} 0 \bmod (t + 1) & \text{if } k \text{ is even,} \\ 1 \bmod (t + 1) & \text{if } k \text{ is odd.} \end{cases}$$

The case $k \leq 0$ is left to the reader.

(iv) The "only if" part is obvious. We prove the "if" part. By Lemma 2.1(iv), $u = \alpha t^n$ for some $n \in \mathbb{Z}$ and some unit $\alpha \in A$. Since $t - 1 \mid u - 1 = \alpha(t^n - 1) + \alpha - 1$ we have $t - 1 \mid \alpha - 1$ and so, by Lemma 2.1(iii), $t - 1$ divides $\alpha - 1$ in $A[t]$, hence $\alpha = 1$. ∎

For the following lemmas we will be writing expressions of the form $u - 1$, where u is a term of the language L, as if they were terms of the language. It is easy to replace those formulas by equivalent L-formulas, which, if the initial formulas are positive-existential, are positive-existential as well.

LEMMA 2.3. (i) *If* $\mathrm{char}(A) \neq 2$ *and* 2 *is a unit in* A, *then for any* $n \in \mathbb{Z}$, $t^n \neq 1$ *if and only if there is a* $k \in \mathbb{Z}$ *and there are* $a, b \in A[t, t^{-1}]$ *such that the following formula* $\psi_1(t^n, t^k, a, b)$ *holds true*:

$$t^k - 1 \,|\, t^n - 1 \ \wedge\ t^2 - 1 \,|\, (t^k - 1) - (t - 1) \ \wedge\ t^n - 1 \,|\, a \ \wedge \\ (t-1)(t^k-1) \,|\, b \ \wedge\ a + b = t^k - 1$$

(*clearly* $\psi_1(x, y, a, b)$ *is a formula of* L).

(ii) *If* 2 *is not a unit in* A *then for any* $n \in \mathbb{Z}$, $t^n \neq 1$ *if and only if there is a* $k \in \mathbb{Z}$ *and there are* $a, b \in A[t, t^{-1}]$ *such that the following formula* $\psi_2(t^n, t^k, a, b)$ *holds true*:

$$(t^3 - 1 \,|\, t \cdot t^k - 1 \ \vee\ t^3 - 1 \,|\, t^k - t) \ \wedge\ t^k - 1 \,|\, t^n - 1 \ \wedge \\ (t-1)(t^k-1) \,|\, a \ \wedge\ t^k - 1 \,|\, b \ \wedge\ t^n - 1 = t^k - 1 + a + 2b$$

(*clearly* $\psi_2(x, y, a, b)$ *is a formula of* L.)
(*In the case* $\mathrm{char}(A) = 2$, *the term* $2b$ *is equal to* 0 *and therefore it may be deleted*).

(iii) *For any* $m, n \in \mathbb{Z}$, $m \neq n$ *if and only if there is an* $r \in \mathbb{Z}$ *such that the following formula* $\psi_3(t^r, t^m, t^n)$ *is true*:

$$r \neq 0 \ \wedge\ t^m - t^n \,|\, t^r - 1.$$

Proof. (i) For the "if" direction: The relation $t^2 - 1 \,|\, (t^k - 1) - (t - 1)$ is equivalent to $t + 1 \,|\, \frac{t^k - 1}{t - 1} - 1$ and this, by Lemma 2.2(iii), implies that k is odd. Assume that $n = 0$. Then by the relation $t^n - 1 \,|\, a$ we have $a = 0$, and hence, by the relations $(t-1)(t^k-1) \,|\, b$ and $a + b = t^k - 1$, we obtain $(t-1)(t^k-1) \,|\, t^k - 1$. Since k is odd, it is not zero, hence we obtain $t - 1 \,|\, 1$, so $t - 1$ is a unit in $A[t, t^{-1}]$, which contradicts Lemma 2.1(iv). Hence $n \neq 0$ and $t^n \neq 1$.

For the "only if": Let $n = 2^s k$ with k odd. The first two divisibility relations follow from Lemma 2.2. By Lemma 2.2(ii) we obtain

$$\frac{t^n - 1}{t^k - 1} \equiv 2^s \bmod (t^k - 1), \quad \text{so} \quad \frac{t^n - 1}{t^k - 1} \equiv 2^s \bmod (t - 1).$$

Hence, for some $z \in A[t, t^{-1}]$ we have $\frac{t^n - 1}{t^k - 1} = z(t-1) + 2^s$, so, since 2 is a unit in A, we have

$$2^{-s}(t^n - 1) - 2^{-s} z (t-1)(t^k - 1) = t^k - 1.$$

Let $a = 2^{-s}(t^n - 1)$ and $b = -2^{-s} z (t-1)(t^k - 1)$.

(ii) By Lemma 2.2(ii), the condition $t^3 - 1 \,|\, t^{k+1} - 1 \vee t^3 - 1 \,|\, t^k - t$ is equivalent to $k \equiv 2$ or $1 \bmod 3$.

The "if" direction: Assume that the right hand side is true and that $n = 0$. Since $k \equiv 2$ or $1 \bmod 3$ we have $k \neq 0$. From the relations $(t-1)(t^k-1) \,|\, a$ and $t^k - 1 \,|\, b$ we infer that there are $z, w \in A[t, t^{-1}]$ so that $a = (t^k - 1)(t-1)z$

and $b = (t^k - 1)w$. So the relation $t^n - 1 = t^k - 1 + a + 2b$ gives $0 = 1 + (t-1)z + 2w$. Hence $0 \equiv 1 + 2w \bmod (t-1)$. The ring $A[t, t^{-1}]/(t-1)$ is isomorphic to A through the natural isomorphism and hence the latter relation implies that 2 is a unit in A, which contradicts our hypothesis.

The "only if" direction: Let $n = 3^s k$ with $k \not\equiv 0 \bmod 3$ (the relations are meant in $\mathbb{Z}$). Then $k \equiv 1$ or $2 \bmod 3$, $t^k - 1 \mid t^n - 1$ and

$$\frac{t^n - 1}{t^k - 1} \equiv 3^s \bmod (t^k - 1), \quad \text{so} \quad \frac{t^m - 1}{t^k - 1} \equiv 3^s \bmod (t - 1).$$

So there is a $z \in A[t, t^{-1}]$ such that $\frac{t^n-1}{t^k-1} = 3^s + z(t-1)$. Write 3^s as $3^s = 1 + 2w$ for some suitable $w \in A$. Then

$$\frac{t^n - 1}{t^k - 1} = 1 + z(t-1) + 2w.$$

Let $a = z(t-1)(t^k - 1)$ and $b = w(t^k - 1)$.

(iii) is trivial. ∎

LEMMA 2.4. *Assume that A is an integral domain. Then the following hold in $A[t, t^{-1}]$:*

(i) *If $m, n, k \in \mathbb{Z}$, $mnk \neq 0$ and $n \neq k$ then $m = n + k$ if and only if the following formula $\tau(t^n, t^k, t^m)$ is true*:

$$t^n - 1 \mid t^m - t^k \wedge t^m - t^k \mid t^n - 1 \wedge t^k - 1 \mid t^m - t \wedge t^m - t^n - 1 \mid t^k - 1$$

(*clearly $\tau(x, y, z)$ is a formula of L*).

(ii) *If $m, n \neq 0$ and $m \neq n$ then $m = -n$ if and only if*

$$t^m - 1 \mid t^n - 1 \quad \text{and} \quad t^n - 1 \mid t^m - 1.$$

Proof. (i) The "only if" direction is clear.

We prove the "if" direction: By the relations $t^n - 1 \mid t^m - t^k$, $t^m - t^k \mid t^n - 1$ and Lemma 2.2(ii) we find that $n \mid m - k$ and $m - k \mid n$, hence $m - k = \pm n$. Similarly from $t^k - 1 \mid t^m - t^n$ and $t^m - t^n \mid t^k - 1$ we get $m - n = \pm k$. If $m - k = -n$ then substituting into the relation $m - n = \pm k$ we get $k - 2n = \pm k$, which gives either $n = 0$ or $n = k$, both of which contradict the hypothesis. Hence $m = k + n$.

(ii) The "only if" direction is clear. We prove the "if" direction. From the two divisibilities we see that $n \mid m$ and $m \mid n$, hence $m = \pm n$. Thus, since $m \neq n$, we obtain $m = -n$. ∎

LEMMA 2.5. *There are positive-existential formulas $\phi_1(x, y, z)$ and $\phi_2(x, y, z)$ of the language L, with free variables x, y and z, such that for any integral domain A the following holds*:

(a) *Assume that 2 is a unit in A. Then for any $x, y, z \in \{t^n : n \in \mathbb{Z}\} \subset A[t, t^{-1}]$,*

$$\phi_1(x, y, z) \text{ is true in } A[t, t^{-1}] \quad \text{if and only if} \quad z = x \cdot y.$$

(b) *Assume that* 2 *is not a unit in* A. *Then for any* $x, y, z \in \{t^n : n \in \mathbb{Z}\} \subset A[t, t^{-1}]$ *the following is true*:

$$\phi_2(x, y, z) \text{ is true in } A[t, t^{-1}] \quad \text{if and only if} \quad z = x \cdot y.$$

Proof. Define the L-formula $\theta_0(x)$ by

$$\theta_0(x) : \quad x \mid 1 \wedge t - 1 \mid x - 1.$$

By Lemma 2.2(iv), $\theta_0(x)$ is true if and only if $x \in \{t^n : n \in \mathbb{Z}\}$.

In what follows we will be writing formulas indexed by i for $i = 1, 2$. The index $i = 1$ will correspond to the case that 2 is a unit in A, and $i = 2$ to the case that 2 is not a unit in A.

Define the L-formulas

$$\theta_i(x) : \quad \theta_0(x) \wedge \exists w, a, b\ [\theta_0(w) \wedge \psi_i(x, w, a, b)],$$

where ψ_1 and ψ_2 are the formulas of Lemma 2.3. By Lemma 2.3 the formula $\theta_i(x)$ is true if and only if $x \in \{t^n : n \in \mathbb{Z} \setminus \{0\}\}$.

Define the formulas

$$\zeta_i(x, y) : \quad \theta_0(x) \wedge \theta_0(y) \wedge \exists w\ [\theta_i(w) \wedge x - y \mid w - 1].$$

By Lemma 2.3(iii), $\zeta_i(x, y)$ is true if and only if $x, y \in \{t^n : n \in \mathbb{Z}\}$ and $x \neq y$.

Define the formulas

$$\xi_i(x, y, z) : \quad [\theta_i(x) \wedge \theta_i(y) \wedge \theta_i(z) \wedge \zeta(x, y) \wedge \tau(x, y, z)],$$

where $\tau(x, y, z)$ is the formula of Lemma 2.4, and

$$\phi_i(x, y, z) : \quad [\theta_0(x) \wedge \theta_0(y) \wedge \theta_0(z)] \wedge \\ [(x = 1 \wedge y = z) \vee (y = 1 \wedge x = z) \vee \xi_i(x, y, z) \vee \xi_i(x, ty, tz)].$$

It follows from Lemma 2.4 that $\xi_i(x, y, z)$ holds true if and only if $x, y, z \in \{t^n : n \in \mathbb{Z} \setminus \{0\}\}$ and $x \neq y$ and $z = x \cdot y$. Then the ϕ_i have the required properties (the details are left to the reader). ∎

3. The case of zero characteristic

LEMMA 3.1. *There are quantifier-free formulas of the language* L, $\phi_A(x)$, *with free variable* x, *and* $\phi_{\text{mult}}(x, y, z)$, *with free variables* x, y *and* z, *such that for any integral domain* A *of zero characteristic, the following hold*:

(a) *For any* $x \in A[t, t^{-1}]$,

$$\phi_A(x) \text{ is true} \quad \text{if and only if} \quad x \text{ is a unit of } A.$$

(b) *For any* $x, y, z \in A$,

$$\phi_{\text{mult}}(x, y, z) \text{ is true} \quad \text{if and only if} \quad z = x \cdot y.$$

Proof. Define

$$\phi_A(x): \quad x = 1 \vee [x \mid 1 \wedge x - 1 \mid 1].$$

By Lemma 2.1(iv), ϕ_A is a definition of the set of units of A.

Define

$$\phi_{\text{mult}}(x, y, z): \quad [t - x \mid tz - y]. \ \blacksquare$$

Proof of Theorem 1.1 in the case of zero characteristic. (i) For any $f, g \in A[t, t^{-1}]$ we define the relation $f \sim g$ to mean $t - 1 \mid f - g$. Define $y_n = (t^n - 1)/(t - 1)$. By Lemma 2.5 the set

$$D = \{y \in A[t, t^{-1}] : \exists n \in \mathbb{Z}\ [y = y_n]\}$$

and the relation $x = y_n y_k$ (that is, the set $\{(y, w, y \cdot w) : y, w \in D\}$) are positive-existentially definable in L over $(A[t, t^{-1}]; +; |; \{0, 1, t\})$ and those definitions are effective. So, given a polynomial $P(X_1, \ldots, X_s)$ in the variables $X_1, \ldots, X_s$ with rational integer coefficients, the relation $P(Y_1, \ldots, Y_s) \sim 0$ is effectively positive-existentially definable in L over $(A[t, t^{-1}]; +; |; \{0, 1, t\})$.

Given any polynomial $P(X_1, \ldots, X_s)$ with rational integer coefficients, we obviously have

$$\exists X_1, \ldots, X_s \in \mathbb{Z}\ [P(X_1, \ldots, X_s) = 0] \quad \text{if and only if}$$
$$\exists Y_1, \ldots, Y_s \in A[t, t^{-1}]\ [(\wedge_{i=1}^{s} Y_i \in D) \wedge P(Y_1, \ldots, Y_s) \sim 0].$$

This gives an effective interpretation of the positive-existential theory of the structure $(\mathbb{Z}; +, \cdot; 0, 1)$ (the ring-structure of the rational integers) in the positive-existential L-theory of the structure $(A[t, t^{-1}]; +; |; \{0, 1, t\})$, hence if the latter were decidable then the former would be decidable as well. This would contradict Matiyasevich's Theorem (cf. [10]), which implies that the positive-existential ring-theory of $\mathbb{Z}$ is undecidable. This proves Theorem 1.1(i).

(ii) Clearly, using Lemma 2.2(ii), for any $\mu \in A$ the following holds:

$\mu \in \mathbb{Z}$ if and only if

$$\text{there is an } x \in \{t^n : \ n \in \mathbb{Z}\} \text{ such that } \mu \equiv \tfrac{t^n - 1}{t - 1} \bmod (t - 1).$$

It follows that for any $\mu \in A[t, t^{-1}]$,

$\mu \in \mathbb{Z}$ if and only if

$$(\mu \in A) \wedge \exists x \in A[t, t^{-1}]\ [x \mid 1 \wedge t - 1 \mid x - 1 \wedge (t - 1)^2 \mid x - 1 - (t - 1)\mu].$$

In the case that A contains the set $\mathbb{Q}$ of rational numbers, replace in the last formula the subformula $\mu \in A$ by $\mu = 0 \vee \phi_A(\mu)$ (ϕ_A as in Lemma 3.1) to obtain a positive-existential definition of $\mathbb{Z}$ in L over $(A[t, t^{-1}]; +; |; \{0, 1, t\})$. Then ϕ_{mult} of Lemma 3.1 restricted to $\mathbb{Z}$ gives a positive-existential definition of multiplication in $\mathbb{Z}$.

4. The case of nonzero characteristic. In this section we will assume that A is an integral domain of characteristic $p > 0$, where p is a prime number. So the field $\mathbb{F}_p$ with p elements is a subring of A. We denote by E the ring of all elements of A which are algebraic over $\mathbb{F}_p$. It is easy to see that E is a field. We will show that the relation $x \in E[t, t^{-1}]$ is positive-existential in L over $(A[t, t^{-1}]; +; |; \{0, 1, t\})$ and that for $x, y, z \in E[t, t^{-1}]$ the relation $z = x \cdot y$ is also positive-existential. It follows that the decision problem for the positive-existential ring-theory of $E[t, t^{-1}]$ (with constant symbols for 0, 1 and t) can be effectively interpreted in the positive-existential theory of L over $(A[t, t^{-1}]; +; |; \{0, 1, t\})$. In the next section we will show that the positive-existential ring-theory of $E[t, t^{-1}]$ is undecidable by encoding the diophantine theory of $\mathbb{Z}$ into it, hence proving Theorem 1.1 in the case of positive characteristic.

LEMMA 4.1. *If* $x \in A[t, t^{-1}]$ *then* $x \in E[t, t^{-1}] \setminus \{0, 1, t\}$ *if and only if*

$$\exists n \in \mathbb{Z} \setminus \{0\}\ [x \,|\, t^n - 1 \wedge x - 1 \,|\, t^n - 1 \wedge x - t \,|\, t^n - 1].$$

Proof. Recall that all the finite field extensions of $\mathbb{F}_p$ are cyclic, of the form $\mathbb{F}_{p^l}$, the field with p^l elements. It follows that any polynomial with coefficients in a finite extension $\mathbb{F}_{p^l}$ which is monic (i.e. with highest degree coefficient equal to 1) and has only simple zeros, divides (in $\mathbb{F}_{p^l}[t]$) some polynomial of the form $t^{n+1} - t$ with $n \geq 1$. Therefore, any monic polynomial $y \in E[t]$ divides in $E[t]$ some polynomial $(t^n - t)^{p^s} = t^{np^s} - t^{p^s}$ with $n \geq 1$. Conversely, if $y \in A[t]$ is monic and $y \,|\, t^m - t^n$ in $A[t]$ with $m \neq n$, then all the zeros of y are zeros of $t^m - t^n$ and are therefore algebraic, hence $y \in E[t]$.

The "only if" part of the conclusion follows from the above observations and Lemma 2.1(iii). We prove the "if" part. By Lemma 2.1(i) write $x = t^{-r}z$ for some $z \in A[t]$ which is not divisible by t and some $r \in \mathbb{Z}$. We assume without loss of generality that $n > 0$ (replacing n by $-n$ if necessary). It suffices to show that $z \in E[t]$. Let a be the leading coefficient of z. Assume that $r \geq 0$. The divisibilities of the right hand side of the equivalence of the lemma imply $z \,|\, t^n - 1$, $z - t^r \,|\, t^n - 1$ and $z - t^{r+1} \,|\, t^n - 1$. It follows from the observations of the preceding paragraph and the first of the divisibilities that $(1/a)z \in E[t]$. By a similar argument applied to the second divisibility, if $n > r$ we obtain $(1/a)(z - t^r) \in E[t]$ and if $n < r$ we obtain $z - t^r \in E[t]$; in both of these cases it is clear that $1/a, z \in E[t]$. If $n = r$ then the third divisibility gives $z - t^{r+1} \in E[t]$, hence also $z \in E[t]$. If $r < 0$ then the first divisibility implies $(1/a)x \in E[t]$ and the second divisibility implies $(1/a)(x - 1) \in E[t]$, so $1/a \in E$ and $x \in E[t]$. ∎

LEMMA 4.2. (i) *For any* $x, y, z \in A[t, t^{-1}]$ *we have*:

$[x, y, z \in E[t, t^{-1}] \setminus \{0, 1, t\}$ *and* $z = x \cdot y]$ *if and only if*

$$\exists n \in \mathbb{Z} \setminus \{0\}\ [x \,|\, t^n - 1 \wedge x - 1 \,|\, t^n - 1 \wedge x - t \,|\, t^n - 1 \wedge$$

$$y \mid t^n - 1 \wedge y - 1 \mid t^n - 1 \wedge y - t \mid t^n - 1 \wedge$$
$$z \mid t^n - 1 \wedge z - 1 \mid t^n - 1 \wedge z - t \mid t^n - 1 \wedge$$
$$t^{7n} - x \mid yt^{7n} - z].$$

(ii) *The sets* $E[t, t^{-1}]$ *and* $\{(x, y, z) : x, y, z \in E[t, t^{-1}] \wedge z = x \cdot y\}$ *are positive-existential in* L *over* $(A[t, t^{-1}]; +; |; \{0, 1, t\})$.

Proof. (i) The necessity of the right hand side condition follows from Lemmas 2.1(iii) and 4.1. We prove the sufficiency. The fact that $x, y, z \in E[t, t^{-1}] \setminus \{0, 1, t\}$ follows from Lemma 4.1. Let $x = t^m x'$, $y = t^k y'$ and $z = t^r z'$ for some $m, k, r \in \mathbb{Z}$ and some $x', y', z' \in E[t]$ such that the constant terms of x', y' and z' are nonzero. Assume that $n \in \mathbb{Z}$ is such that the conditions of the right hand side formula hold. Let $|n|$ be the absolute value of n. The relations $x \mid t^n - 1$ and $x - 1 \mid t^n - 1$ imply $x \mid t^{|n|} - 1$ and $x - 1 \mid t^{|n|} - 1$ over $E[t, t^{-1}]$.

We claim that $\deg(x'), |m| \leq |n|$ ($\deg(x')$ is the degree of x'). Assume first that $m \geq 0$. Then $x \in E[t]$, the divisibilities $x \mid t^{|n|} - 1$ and $x - 1 \mid t^{|n|} - 1$ imply that $\deg(x) \leq |n|$ (since at least one of x, $x - 1$ has a nonzero constant term and by Lemma 2.1(iii) the corresponding divisibility holds over $E[t]$ as well), hence $m \leq |n|$. Now assume that $m < 0$. The divisibility $x - 1 \mid t^{|n|} - 1$ implies $x' - t^{-m} \mid t^{|n|} - 1$ and $x' - t^{-m}$ has a nonzero constant term, therefore by Lemma 2.1(iii), x' and $x' - t^{-m}$ divide $t^{|n|} - 1$ in $E[t]$. In particular $\deg(x'), \deg(x' - t^{-m}) \leq |n|$, thus $|m| \leq |n|$. So the claim has been proved. Similarly we have $\deg(y'), |k|, \deg(z'), |r| \leq |n|$.

From the relation $t^{7n} - x \mid yt^{7n} - z$ we obtain $t^{7n} - x \mid yx - z$, and hence $t^{7n} - x \mid y'x't^{m+k} - z't^r$. Let

$$v = \begin{cases} t^{7n-m} - x' & \text{if } 7n - m \geq 0, \\ 1 - t^{m-7n}x' & \text{if } 7n - m < 0. \end{cases}$$

Then $v \in E[t]$ and since $\deg(x'), |m| \leq |n|$, in both cases v has nonzero constant term and $\deg(v) \geq 6|n|$. Let

$$w = \begin{cases} y'x't^{m+k-r} - z' & \text{if } m + k - r \geq 0, \\ y'x' - z't^{r-m-k} & \text{if } m + k - r < 0. \end{cases}$$

Then obviously $w \in E[t]$ and $\deg(w) \leq 5|n|$. Clearly v divides w in $E[t]$ (by Lemma 2.1(iii)). Therefore, since $\deg(v) \geq 6|n| > 5|n| \geq \deg(w)$ (we took into account that $n \neq 0$), it follows that $w = 0$. So $y'x't^{m+k-r} - z' = 0$, and thus $z = y \cdot x$.

(ii) First, we recall from Lemma 2.5 that the set $\{t^n : n \in \mathbb{Z} \setminus \{0\}\}$ is positive-existentially definable, say by the formula $\theta(x)$ (the reader may observe that in the terminology of the proof of Lemma 2.5 this is θ_2). Then, by Lemma 4.1, the formula

$$\varepsilon(x): \quad x=0 \vee x=1 \vee x=1 \vee \exists u\,[\theta(u) \wedge x \,|\, u-1 \wedge x-1 \,|\, u-1 \wedge x-t \,|\, u-1]$$

is a definition of $E[t,t^{-1}]$ in $A[t,t^{-1}]$.

We now produce a positive-existential definition in L of multiplication in $E[t,t^{-1}]$. Recall from Lemma 2.5 that multiplication restricted to the subset $\{t^n : n \in \mathbb{Z}\}$ of $A[t,t^{-1}]$ is positive-existentially definable, say by the formula $\phi(x,y,z)$ (meaning $z = x \cdot y$). So the set $\{(t^n, t^{7n}) : n \in \mathbb{Z} \setminus \{0\}\}$ is positive-existentially definable, say by the formula $\chi(x,y)$.

Let $\omega_0(x,y,z)$ be the formula

$$(x=0) \wedge z=0) \vee (x=1 \wedge z=y) \vee (x=t \wedge z=ty).$$

Define the formula $\omega(x,y,z,u,v,w)$ by

$$\omega(x,y,z,u,v,w): \quad \omega_0(x,y,z) \vee [\varepsilon(x) \wedge \varepsilon(y) \wedge \varepsilon(z) \wedge \theta(u) \wedge \theta(v) \ \wedge \chi(u,v) \wedge x \,|\, u-1 \wedge x-1 \,|\, u-1 \wedge x-t \,|\, u-1 \wedge y \,|\, u-1 \wedge y-1 \,|\, u-1 \wedge y-t \,|\, u-1 \wedge z \,|\, u-1 \wedge z-1 \,|\, u-1 \wedge z-t \,|\, u-1 \wedge v-x \,|\, w-z].$$

Then, by (i), whenever $w = y \cdot v$, the formula $\omega(x,y,z,u,v,w)$ is true if and only if $(x,y,z \in E[t,t^{-1}]$ and $u,v \in \{t^n : \ n \in \mathbb{Z} \setminus \{0\}\}$ and $v = u^7$ and $z = x \cdot y)$. Hence the L-formula

$$\omega_1(x,y,z): \quad \exists u,v,w\ [\theta(y) \wedge \phi(y,v,w) \wedge \omega(x,y,z,u,v,w)]$$

is a definition of the set

$$\{(x,y,z) : x,y,z \in E[t,t^{-1}] \wedge y \in \{t^n : n \in \mathbb{Z}\} \setminus \{0\} \wedge z = x \cdot y\},$$

and

$$\exists u,v,w\ [\omega_1(y,v,w) \wedge \omega(x,y,z,u,v,w)]$$

is a definition of the set $\{(x,y,z) : x,y,z \in E[t,t^{-1}] \wedge z = x \cdot y\}$. ∎

5. The positive-existential theory of $E[t,t^{-1}]$ and the case of positive characteristic. In this section we prove that the positive-existential ring-theory of $E[t,t^{-1}]$ is undecidable. In the light of the results of the previous section this implies the undecidability of the positive-existential L-theory of $(A[t,t^{-1}];+;|;\{0,1,t\})$, that is, Theorem 1.1(i) in the case of positive characteristic.

LEMMA 5.1. (i) *Assume that* $\mathrm{char}(E) = p \neq 2$. *Then for any* $m,n \in \mathbb{Z}$ *with* $m,n \neq 0$ *we have*:

$$\exists y \in E[t,t^{-1}]\ \left[\frac{t^{2mn}-1}{t^{2n}-1} = \pm y^2\right]$$

if and only if

$$\exists s \in \mathbb{N}_0\ [m = \pm p^s].$$

(ii) *If* $\mathrm{char}(E) = 2$ *then for any* $m, n \in \mathbb{Z}$ *with* $m, n \neq 0$ *we have*:

$$\exists y \in E[t, t^{-1}] \left[\frac{t^{3mn} - 1}{t^{3n} - 1} = y^3 \vee (t^{3mn} - 1)(t^{3n} - 1) = y^3 \right]$$

if and only if

$$\exists s \in \mathbb{N}_0 \ [m = \pm 2^s].$$

(iii) *For any* $t^m, t^n \in E[t, t^{-1}]$, *the relation* $\exists s \in \mathbb{N}_0 \ [m = \pm p^s n]$ *is positive-existential in* L *over* $(A[t, t^{-1}]; +; |; \{0, 1, t\})$.

Proof. (i) Observe that for $l \in \mathbb{Z}$,

$$\frac{t^{p^s l} - 1}{t^l - 1} = ((t^l - 1)^{(p^s - 1)/2})^2.$$

Assume that $m = p^s h$ and $n = p^r j$ with $h, j \in \mathbb{Z}$ not divisible by p, and $s, r \in \mathbb{N}_0$. Then $(t^{2mn} - 1)/(t^{2hj} - 1)$ and $(t^{2n} - 1)/(t^{2j} - 1)$ are squares in $E[t, t^{-1}]$. Therefore $(t^{2mn} - 1)/(t^{2n} - 1)$ is a square in $E[t, t^{-1}]$ if and only if $(t^{2hj} - 1)/(t^{2j} - 1)$ is a square. Since $t^{2hj} - 1 = -t^{2hj}(t^{-2hj} - 1)$ we find that $(t^{2mn} - 1)/(t^{2n} - 1)$ is of the form $\pm y^2$ for some $y \in E[t, t^{-1}]$ if and only if $(t^{2|hj|} - 1)/(t^{2|j|} - 1)$ is of the same form. Now observe that the polynomials $t^{|2hj|} - 1$ and $t^{|2j|} - 1$ have only simple zeros (they have no common zeros with their derivatives), hence $(t^{2|hj|} - 1)/(t^{2|j|} - 1)$ is of the form $\pm y^2$ if and only if $|h| = 1$.

(ii) For $l \in \mathbb{Z}$,

$$\frac{t^{4^s l} - 1}{t^l - 1} = ((t^l - 1)^{(4^s - 1)/3})^3, \qquad (t^{2 \cdot 4^s l} - 1)(t^l - 1) = ((t^l - 1)^{(2 \cdot 4^s + 1)/3})^3$$

and $(4^s - 1)/3$, $(2 \cdot 4^s + 1)/3 \in \mathbb{Z}$. We distinguish cases according to whether the order of m at the prime 2 is even or odd. The rest is similar to (i) and is left to the reader.

(iii) follows from (i), (ii) and Lemma 4.2 (to express $\exists y \in E[t, t^{-1}]$ $[x = y^2]$). ∎

Proof of Theorem 1.1 in the case of characteristic $p > 0$. We will prove first (iv), and then (iii) and (i). Let $|_{\mathbb{Z}}$ denote divisibility in the integers and define $|_p$ as follows: For $m, n \in \mathbb{Z}$,

$$m \,|_p\, n \quad \text{if and only if} \quad \exists s \in \mathbb{Z}^+ \ [m = \pm p^s n].$$

We will interpret effectively the positive-existential theory of the model $(\mathbb{Z}; +; |_{\mathbb{Z}}; |_p; \{0, 1\})$ in the positive-existential ring-theory of $E[t, t^{-1}]$. We consider the powers of t in $E[t, t^{-1}]$ as representing the rational integers, i.e. for $m \in \mathbb{Z}$, t^m represents m. Under this correspondence we want to show that for $m, n, k \in \mathbb{Z}$, the relations $m = n + k$, $m \,|_{\mathbb{Z}}\, n$ and $m \,|_p\, n$ are positive-existential in the ring $E[t, t^{-1}]$. Hence, if the positive-existential ring-theory of $E[t, t^{-1}]$ were decidable, the positive-existential theory of

$(\mathbb{Z}; +; |_{\mathbb{Z}}; |_p; \{0,1\})$ would be decidable as well. But the latter is undecidable as is proved in [4]. The fact that the relation $m\,|_{\mathbb{Z}}\,n$ is positive-existential in the ring-theory of $E[t,t^{-1}]$ under the stated correspondence is given by Lemma 2.2(i); the analogous facts for $+$ and $|_p$ are given by Lemmas 2.5 and 5.1, respectively. This proves Theorem 1.1(iv).

Lemmas 4.1 and 4.2 show that the set $E[t,t^{-1}]$ and the graph of multiplication in it are positive-existential in L over $(A[t,t^{-1}]; +; |; \{0,1,t\})$, hence (iii) and (i) follow.

6. The universal-existential theory. We will investigate the universal-existential theory of $A[t]$, where A is an integral domain and t a variable. Observe that for any $x \in A[t]$ we have:

x is a power of t different from 1 if and only if

$$t \,|\, x \wedge t-1 \,|\, x-1 \wedge \forall z\ [z \nmid 1 \wedge z \,|\, x \to t \,|\, z].$$

So we have a universal definition of the relation

$$P(x): \quad \text{'}x \text{ is a power of } t\text{'}.$$

We intend to show that, under the assumption of Theorem 1.2, the positive-existential theory of $A[t]$ with the structure $(A[t]; +; |; P; \{0,1,t\})$ of addition, divisibility and the relation P (i.e. as a model of the language $L \cup \{P\}$) is undecidable.

Assume first that $\mathrm{char}(A) = 0$ and $\mathbb{Q} \subset A$. Then the set U of invertible elements of A is existentially definable by

$$u \in U \quad \text{if and only if} \quad u \,|\, 1 \text{ in } A[t].$$

The following lemmas follow easily from the considerations of Section 2.

LEMMA 6.1. *For any $x \in A[t]$ we have*:

$x \in \mathbb{Z}$ *if and only if*

$$x = 0 \vee (x \,|\, 1 \wedge \exists z, w \in A[t]\ [P(z) \wedge (t-1)x = z - 1 - (t-1)^2 w]).$$

LEMMA 6.2. *If $x, y, z \in A$ then*

$$z = x \cdot y \quad \textit{if and only if} \quad t - x \,|\, ty - z.$$

Proof of Theorem 1.2 in the case of characteristic zero. It follows from the previous two lemmas that $\mathbb{Z}$ and multiplication in $\mathbb{Z}$ are existentially definable in $A[t]$ with the structure of addition, divisibility and P. Thus we can effectively interpret the positive-existential ring-theory of $\mathbb{Z}$ in the universal-existential theory of $(A[t]; +; |; \{0,1,t\}$. Hence, since the former is undecidable (a consequence of the negative answer to Hilbert's tenth problem, cf. [10]) the latter is undecidable as well.

Assume now that $\mathrm{char}(A) > 0$.

The following lemmas are analogous to Lemmas 2.4, 4.1 and 4.2, respectively; their proofs are very similar and are left to the reader.

LEMMA 6.3. *If* $\mathrm{char}(A) > 0$, *the following holds in* $A[t]$:

$t^m = t^n t^k$ *if and only if*

$$\forall z\ [\neg t \mid z \wedge z \mid t^m - t^k \to z \mid t^n - 1] \wedge [t^n - 1 \mid t^m - t^k].$$

LEMMA 6.4. *Assume that* $\mathrm{char}(A) > 0$. *Let* E *denote the field of elements of* A, *algebraic over the prime subfield. Then for any* $x \in A[t]$ *we have*:

$x \in E[t]$ *if and only if* $[x = 0 \vee x = 1 \vee x = t] \vee$

$$\exists n, m \in \mathbb{N}\ [t^n \neq t^m \wedge x \mid t^n - t^m \wedge x - 1 \mid t^n - t^m \wedge x - t \mid t^n - t^m].$$

LEMMA 6.5. *Assume that* $\mathrm{char}(A) > 0$ *and let* E *be as in the previous lemma. If* $x, y, z \in E[t]$ *and* $x, y, z \neq 0, 1, t$ *then*

$z = x \cdot y$ *if and only if*

$$\begin{aligned}\exists n, m, k \in \mathbb{N}\ [&x \mid t^n - t^m \wedge x - 1 \mid t^n - t^m \wedge x - t \mid t^n - t^m\ \wedge\\ &y \mid t^n - t^m \wedge y - 1 \mid t^n - t^m \wedge y - t \mid t^n - t^m\ \wedge\\ &z | t^n - t^m \wedge z - 1 \mid t^n - t^m \wedge z - t \mid t^n - t^m\ \wedge\\ &x - t^{7k} \mid y t^{7k} - z \wedge t^{m+n} = t^k \wedge t^m \neq t^n].\end{aligned}$$

Proof of Theorem 1.2 in the case of positive characteristic. From the last three lemmas we obtain a positive-existential definition of $E[t]$ and of the graph of multiplication in $E[t]$, in the structure $(A[t]; +; |; P; \{0, 1, t\})$, hence also a universal-existential definition in the structure $(A[t]; +; |; \{0, 1, t\})$ of addition and divisibility in $A[t]$. Therefore we obtain an effective interpretation of the positive-existential ring-theory of $E[t]$ in both the positive-existential theory of $(A[t]; +; |; P; \{0, 1, t\})$ and the universal-existential theory of $(A[t]; +; |; \{0, 1, t\})$. By the results of [4], the positive-existential ring-theory of $E[t]$ is undecidable. It follows that both the positive-existential theory of $(A[t]; +; |; P; \{0, 1, t\})$ and the universal-existential theory of $(A[t]; +; |; \{0, 1, t\})$ are undecidable. ∎

Notice that the existential definition of $t^m = t^n t^k$ which was given in Lemma 2.5 does not work in $A[t]$ because t is not a unit; we substituted it by the universal-existential definition of Lemma 6.3. As we commented in the introduction this has a consequence that we cannot prove undecidability of the positive-existential theory of $A[t]$ with the structure of addition, divisibility and the relation P. So we ask:

QUESTION 6.1. *Is the positive-existential theory of the structure* $(\mathbb{F}_p[t]; +; |; P; \{0, 1, t\})$ *decidable* (*also with* $\mathbb{F}_p$ *replaced by any integral domain* A *of positive characteristic which has a decidable existential theory*)*?*

References

[1] A. P. Bel'tyukov, *Decidability of the universal theory of natural numbers with addition and divisibility*, Zap. Nauchn. Sem. LOMI 60 (1976), 15–28 (in Russian).

[2] P. Cegielski, Yu. Matiyasevich and D. Richard, *Definability and decidability issues in extensions of the integers with the divisibility predicate*, J. Symbolic Logic 61 (1996), 515–540.

[3] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. 242 (1978), 391–399.

[4] —, *The Diophantine problem for polynomial rings of positive characteristic*, in: Logic Colloquium '78, North-Holland, 1979, 131–145.

[5] M. Koppel, *Some decidable Diophantine problems: positive solution to a problem of Davis, Matijasevič and Robinson*, Proc. Amer. Math. Soc. 77 (1979), 319–323.

[6] L. Lipshitz, *Undecidable existential problems for addition and divisibility in algebraic number rings II*, ibid. 64 (1977), 122–128.

[7] —, *The Diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc. 235 (1978), 271–283.

[8] —, *Undecidable existential problems for addition and divisibility in algebraic number rings*, ibid. 241 (1978), 121–128.

[9] —, *Some remarks on the Diophantine problem for addition and divisibility*, in: Proceedings of the Model Theory Meeting (Brussels and Mons, 1980), Bull. Soc. Math. Belg. Sér. B 33 (1981), 41–52.

[10] Yu. V. Matijasevich, *Enumerable sets are Diophantine*, Dokl. Akad. Nauk SSSR 191 (1970), 279–282 (in Russian).

[11] P. Pappas, *A Diophantine problem for Laurent polynomial rings*, Proc. Amer. Math. Soc. 93 (1985), 713–718.

[12] T. Pheidas, *The diophantine problem for addition and divisibility in polynomial rings*, thesis, Purdue Univ., 1985.

[13] —, *Extensions of Hilbert's Tenth Problem*, J. Symbolic Logic 59 (1994), 372–397.

[14] T. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, in: Contemp. Math. 270, Amer. Math. Soc., 2000, 49–106.

[15] D. Richard, *Answer to a problem raised by J. Robinson: The arithmetic of positive or negative integers is definable from successor and divisibility*, J. Symbolic Logic 50 (1985), 927–935.

[16] —, *Definissabilité de l'arithmétique par coprimarité et restrictions de l'addition ou de la multiplication*, C. R. Acad. Sci. Paris Sér. I 305 (1987), 665–668.

[17] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic 14 (1949), 98–114.

[18] A. Shlapentokh, *Hilbert's tenth problem over number fields, a survey*, in: Contemp. Math. 270, Amer. Math. Soc., 2000, 107–137.

[19] V. Terrier, *Decidability of the existential theory of the set of natural numbers with order, divisibility, power functions, power predicates, and constants*, Proc. Amer. Math. Soc. 114 (1992), 809–816.

Department of Mathematics
University of Crete
71409 Heraklion, Greece
E-mail: pheidas@math.uoc.gr

Received 27 May 2003;
in revised form 12 July 2004