DIOPHANTINE SETS OF POLYNOMIALS
OVER NUMBER FIELDS

JEROEN DEMEYER

(Communicated by Julia Knight)

ABSTRACT. Let $\mathcal{R}$ be a number field or a recursive subring of a number field and consider the polynomial ring $\mathcal{R}[T]$. We show that the set of polynomials with integer coefficients is diophantine over $\mathcal{R}[T]$. Applying a result by Denef, this implies that every recursively enumerable subset of $\mathcal{R}[T]^k$ is diophantine over $\mathcal{R}[T]$.

1. INTRODUCTION

The main result of this paper is

Theorem. *Let $\mathcal{R}$ be a recursive ring contained in a number field and let $\mathcal{S}$ be a recursively enumerable subset of $\mathcal{R}[T]^k$ (for some $k \geq 1$). Then $\mathcal{S}$ is diophantine over $\mathcal{R}[T]$.*

For any recursively stable integral domain, one can easily see that every diophantine set is recursively enumerable (see the end of section 1.1). However, the converse problem — are recursively enumerable sets diophantine? — is much more difficult.

In 1970, Matiyasevich ([10]) showed, building on earlier work by Davis, Putnam and Robinson, that recursively enumerable (r.e.) sets are diophantine for the integers $\mathbb{Z}$. This had as an immediate consequence the negative answer to Hilbert's Tenth Problem: there exists no algorithm which can decide whether a diophantine equation (a polynomial equation in any number of variables) over $\mathbb{Z}$ has a zero over $\mathbb{Z}$. See [1] for a good write-up of the various steps in the proof that r.e. sets are diophantine for $\mathbb{Z}$ and hence the negative answer to Hilbert's Tenth Problem.

The undecidability of diophantine equations has been shown for many other rings and fields; [14] and [15] give an overview of what is known. On the other hand, the equivalence of r.e. and diophantine sets is much stronger and much less is known. Apart from the original result for $\mathbb{Z}$, this equivalence has been shown for $\mathbb{Z}[T]$ by Denef (see [4]), for $\mathcal{O}_K[T_1, \ldots, T_n]$ where K is a totally real number field by Zahidi (see [18] for $n = 1$ and [17] for $n \geq 1$). In characteristic p, it is known for $\mathbb{F}_q[T]$ and for $K[T]$ where K is a recursive algebraic extension of a finite field (see [3]).

The latter ring is not recursively stable, so the equivalence is between diophantine sets and sets which are r.e. for every recursive presentation. All these results use the fact that r.e. sets are diophantine for $\mathbb{Z}$. In this paper, we base our work on Denef's result for $\mathbb{Z}[T]$.

1.1. **Definitions.** We quickly recall the definitions of recursively enumerable sets, recursive rings and diophantine sets. For more background, we refer to the introductory texts [15] and [14].

Definition. Let $\mathcal{S}$ be a subset of $\mathbb{N}^k$. Then $\mathcal{S}$ is called *recursively enumerable* (r.e.) if there exists an algorithm which prints out elements of $\mathcal{S}$ as it runs such that all elements of $\mathcal{S}$ are eventually printed at least once. Since $\mathcal{S}$ can be infinite, this algorithm is allowed to run infinitely long and use an unbounded amount of memory.

Since there are only countably many algorithms but uncountably many subsets of $\mathbb{N}^k$, there certainly exist sets which are not recursively enumerable. There also exist sets which are recursively enumerable but whose complement is not. Finite unions, finite intersections, cartesian products and projections $\mathbb{N}^{k+r} \to \mathbb{N}^k$ of recursively enumerable sets are still recursively enumerable.

Definition. Let $\mathcal{R}$ be a countable ring. Then $\mathcal{R}$ is called a *recursive ring* if there exists a bijection $\theta : \mathcal{R} \to \mathbb{N}$ such that the sets

$$\{(\theta(X), \theta(Y), \theta(X+Y)) \in \mathbb{N}^3 \mid X, Y \in \mathcal{R}\} \text{ and}$$
$$\{(\theta(X), \theta(Y), \theta(XY)) \in \mathbb{N}^3 \mid X, Y \in \mathcal{R}\}$$

are recursively enumerable. In this case, θ is called a *recursive presentation* of $\mathcal{R}$. A recursive ring $\mathcal{R}$ is called *recursively stable* if for any two recursive presentations θ_1 and θ_2, the set $\{(\theta_1(X), \theta_2(X)) \in \mathbb{N}^2 \mid X \in \mathcal{R}\}$ is recursively enumerable.

The intuition of a recursive ring is a ring in which we can effectively compute; it is a ring whose elements can be represented by a computer. The recursive presentation θ gives every element of $\mathcal{R}$ a "code" such that, given the codes of X and Y, we can compute the code of $X + Y$ and of XY. If we have two different recursive presentations θ_1 and θ_2, then an element X of $\mathcal{R}$ has two "codes" $\theta_1(X)$ and $\theta_2(X)$. A ring is recursively stable if and only if $\theta_2(X)$ can be effectively computed from $\theta_1(X)$.

To construct an example of a ring which is not recursive, consider any non-r.e. subset $\mathcal{S}$ of $\mathbb{N}$. Now take the localization of $\mathbb{Z}$ where the n-th prime number is inverted if and only if $n \in \mathcal{S}$. This is a non-recursive subring of $\mathbb{Q}$.

Definition. Let $\mathcal{R}$ be a recursively stable ring with a recursive presentation $\theta : \mathcal{R} \to \mathbb{N}$. Then a subset $\mathcal{S} \subseteq \mathcal{R}^k$ is called *recursively enumerable* if and only if $\theta^{\otimes k}(\mathcal{S})$ is an r.e. subset of $\mathbb{N}^k$.

Intuitively, we can still think of r.e. subsets of $\mathcal{R}^k$ as sets which can be printed by a computer program (possibly running infinitely long). The requirement that $\mathcal{R}$ is recursively stable implies that the definition of r.e. subsets of $\mathcal{R}^k$ does not depend on the choice of θ. One can prove (see [7]) that every field which is finitely generated over its prime field is recursively stable. Furthermore, a recursive integral domain with a recursively stable fraction field is automatically recursively stable. It follows that the polynomial ring $\mathcal{R}[T]$ is recursively stable if $\mathcal{R}$ is a recursive ring contained in a number field.

Definition. Let $\mathcal{R}$ be an integral domain and $\mathcal{S}$ be a subset of $\mathcal{R}^k$. Then $\mathcal{S}$ is called *diophantine* over $\mathcal{R}$ if there exists a polynomial $p(a_1, \ldots, a_k, x_1, \ldots, x_n)$ with coefficients in $\mathcal{R}$ such that

$$(1.1) \quad \mathcal{S} = \{(a_1, \ldots, a_k) \in \mathcal{R}^k \mid$$
$$p(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0 \text{ for some } x_1, \ldots, x_n \in \mathcal{R}\}.$$

The polynomial p is called a *diophantine definition* of $\mathcal{S}$. A function $f : \mathcal{R}^m \to \mathcal{R}^n$ is called *diophantine* if the set $\{(\vec{X}, f(\vec{X})) \in \mathcal{R}^{m+n} \mid \vec{X} \in \mathcal{R}^m\}$ is diophantine.

When dealing with decidability questions (analogues of Hilbert's Tenth Problem) it often makes sense to restrict the coefficients of the polynomial p to a subring of $\mathcal{R}$. This is certainly necessary if $\mathcal{R}$ is uncountable. However, if we want to prove that r.e. sets are diophantine, then every singleton in $\mathcal{R}$ needs to be diophantine. Therefore, we might as well assume that we take all of $\mathcal{R}$ as a ring of coefficients.

If $\mathcal{R}$ is a recursively stable ring, then every diophantine set is recursively enumerable. To see this, consider a diophantine set $\mathcal{S}$ defined as in (1.1). Construct an algorithm which tries all possible values $(a_1, \ldots, a_k, x_1, \ldots, x_n) \in \mathcal{R}^{k+n}$ and evaluates $p(a_1, \ldots, a_k, x_1, \ldots, x_n)$. Whenever a zero is found, it prints $(a_1, \ldots, a_k)$. This algorithm will print exactly the set $\mathcal{S}$.

1.2. **Overview.** We introduce the following definition:

Definition 1.1. Let $\mathcal{R}$ be an integral domain. A *degree bounding predicate* on $\mathcal{R}[T]$ is a binary relation δ on $\mathcal{R}[T]$ satisfying:
- For any F in $\mathcal{R}[T]$, there exists a $d \geq 0$ such that $\delta(F, T^d)$ is true.
- Whenever $\delta(F, T^d)$ is true, it follows that $F = 0$ or $\deg(F) \leq d$.

The main result from section 3 is the following:

Theorem. *Let $\mathcal{R}$ be an integral domain of characteristic zero such that $\mathcal{R}[T]$ admits a diophantine degree bounding predicate. Then $\mathbb{Z}[T]$ is diophantine over $\mathcal{R}[T]$.*

To prove this theorem, we first show that the set of polynomials in $\mathcal{R}[T]$ that divide some $T^u - 1$ is diophantine. This is done using a Pell equation, as was done similarly in the definition of powers of T in [2], Section 4. A polynomial F dividing $T^u - 1$, normalised such that $F(0) = -1$, is equal to $T^d - 1$ if and only if $F(2^d + 1) = (2^d + 1)^d - 1$. This gives a diophantine definition of the powers of T over $\mathcal{R}[T]$. Moreover, any polynomial dividing $T^d - 1$ such that $F(2^d + 1)$ is an integer has integer coefficients. In this way, we can give a diophantine definition (over $\mathcal{R}[T]$) of the polynomials in $\mathbb{Z}[T]$ dividing some $T^u - 1$. We call these the *root-of-unity polynomials*. For this, we do not need the assumption about the degree bounding predicate, so it works for all rings $\mathcal{R}[T]$, where $\mathcal{R}$ is an integral domain of characteristic zero.

The set of root-of-unity polynomials is T-adically dense in $\mathbb{Z}[[T]]^*$, which allows us to show that all of $\mathbb{Z}[T]$ is diophantine over $\mathcal{R}[T]$. In this step, we need a diophantine formula for Euclidean division. Here we use the diophantine degree bounding predicate.

In section 4, we show that such a diophantine degree bounding predicate exists for the rings $\mathcal{R}[T]$, where $\mathcal{R}$ is contained in a number field. We apply a result by Kim and Roush, who showed in [9] that diophantine equations over $L(T)$ are undecidable if L is contained in a finite extension of $\mathbb{Q}_p$ for some $p \geq 3$. They

showed undecidability by giving a diophantine definition of some subset of the discrete valuation ring $L[T]_{(T)}$. This subset contains all the rational functions in $L[T]_{(T)}$ whose coefficients are algebraic over $\mathbb{Q}$. Since "negative degree" is a discrete valuation, the same method gives a diophantine definition of "degree" in $\mathcal{R}[T]$.

Once we know that $\mathbb{Z}[T]$ is diophantine over $\mathcal{R}[T]$, Denef's result that r.e. subsets of $\mathbb{Z}[T]^k$ are diophantine over $\mathbb{Z}[T]$ (see [4]) implies:

Corollary. *Let $\mathcal{R}$ be an integral domain of characteristic zero such that $\mathcal{R}[T]$ admits a diophantine degree bounding predicate. Let $\mathcal{S}$ be an r.e. subset of $\mathbb{Z}[T]^k$. Then $\mathcal{S}$ is diophantine over $\mathcal{R}[T]$.*

In section 5 we show how to conclude from this that all r.e. subsets of $\mathcal{R}[T]^k$ are diophantine.

2. Special polynomials

In this section, we state some properties of the Chebyshev polynomials X_n and Y_n and cyclotomic polynomials Φ_n. We also define root-of-unity polynomials. Everything in this section concerns only the ring $\mathbb{Z}[T]$.

2.1. Chebyshev polynomials.

Definition 2.1. Let $n \in \mathbb{Z}$ and define polynomials $X_n, Y_n \in \mathbb{Z}[T]$ using the following equation:

$$(2.1) \qquad (T + \sqrt{T^2 - 1})^n = X_n(T) + \sqrt{T^2 - 1}\, Y_n(T).$$

Since $(T + \sqrt{T^2 - 1})^{-1} = (T - \sqrt{T^2 - 1})$, this definition makes sense for negative n.

The degree of X_n is $|n|$; the degree of Y_n is $|n| - 1$ for $n \neq 0$, while $Y_0 = 0$.

In the literature, X_n is called the n-th Chebyshev polynomial of the first kind and Y_{n+1} is called the n-th Chebyshev polynomial of the second kind (such that the n-th Chebyshev polynomials have degree n for $n \geq 0$).

The couples (X_n, Y_n) satisfy the Pell equation $X^2 - (T^2 - 1)Y^2 = 1$. Conversely, we have:

Proposition 2.2. *Let $\mathcal{R}$ be an integral domain of characteristic zero, and let Z be a non-constant polynomial in $\mathcal{R}[T]$. If X and Y in $\mathcal{R}[T]$ satisfy $X^2 - (Z^2 - 1)Y^2 = 1$, then $X = \pm X_n(Z)$ and $Y = Y_n(Z)$ for some $n \in \mathbb{Z}$.*

Proof. See [5], Lemma 2.1. Since $X_{-n} = X_n$ and $Y_{-n} = -Y_n$, we do not need to put $\pm$ in front of $Y_n(Z)$. $\qquad\square$

The Chebyshev polynomials also satisfy the following identity:

Proposition 2.3. *In $\mathbb{Q}(T)$, the following equality holds for all $n \in \mathbb{Z}$:*

$$(2.2) \qquad T^n = X_n\left(\frac{T + T^{-1}}{2}\right) + \frac{T - T^{-1}}{2} Y_n\left(\frac{T + T^{-1}}{2}\right).$$

Proof. Define $W := T + \sqrt{T^2 - 1}$, then $W^{-1} = T - \sqrt{T^2 - 1}$. Now formula (2.1) becomes

$$W^n = X_n\left(\frac{W + W^{-1}}{2}\right) + \frac{W - W^{-1}}{2} Y_n\left(\frac{W + W^{-1}}{2}\right) \qquad\square$$

2.2. **Cyclotomic and root-of-unity polynomials.** Let $\Phi_n \in \mathbb{Z}[T]$ denote the n-th cyclotomic polynomial. This is defined as $\Phi_n(T) = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*}(T - \zeta_n^x)$, where ζ_n is a primitive n-th root of unity. This is an irreducible polynomial in $\mathbb{Z}[T]$. The cyclotomic polynomials satisfy $T^n - 1 = \prod_{a|n} \Phi_a(T)$ (see [8], Ch. 13, §2). By the Möbius Inversion Theorem, this implies

$$(2.3) \qquad \Phi_n(T) = \prod_{a|n}(T^{n/a} - 1)^{\mu(a)},$$

where μ denotes the Möbius function (see [8], Ch. 2, §2).

Proposition 2.4. *Let $n \geq 2$ and let $n = \prod_{i=1}^k p_i^{e_i}$ be its prime decomposition. Let $d := \prod_{i=1}^k p_i^{e_i-1}$. Then*

$$\Phi_n(T) \equiv 1 + (-1)^{k+1}T^d \pmod{T^{2d}}.$$

Proof. Since $n \geq 2$, we have $\sum_{a|n} \mu(a) = 0$ (see [8], Prop. 2.2.3). Therefore, it follows from equation (2.3) that

$$\Phi_n(T) = \prod_{a|n}(1 - T^{n/a})^{\mu(a)}.$$

We compute this product modulo T^{2d}. If $n/a \geq 2d$, then $(1 - T^{n/a})^{\mu(a)}$ is congruent to 1 (mod T^{2d}). Therefore, we only need to consider the factors where $a > n/(2d)$. On the other hand, if a is not squarefree, then $\mu(a) = 0$ and $(1 - T^{n/a})^{\mu(a)} = 1$.

The only squarefree a dividing n such that $a > n/(2d) = (\prod_{i=1}^k p_i)/2$ is $a = n/d$. So we have

$$\Phi_n(T) \equiv (1 - T^d)^{\mu(n/d)} \pmod{T^{2d}}.$$

If k is even, then $\mu(n/d) = 1$ and we have the desired result. If k is odd, then $\mu(n/d) = -1$, and we have $(1 - T^d)^{-1} = (1 + T^d)(1 - T^{2d})^{-1} \equiv 1 + T^d \pmod{T^{2d}}$. □

Corollary 2.5. *Let $d \in \mathbb{N}$ and $s \in \{-1, 1\}$. Then there exist infinitely many $n \in \mathbb{N}$ such that*

$$\Phi_n(T) \equiv 1 + sT^d \pmod{T^{2d}}.$$

Proof. Factor d as $\prod_{i=1}^k p_i^{e_i}$ and let $m := \prod_{i=1}^k p_i^{e_i+1}$. If r is any squarefree number coprime to m, then it follows from Proposition 2.4 that $\Phi_{rm}(T)$ is congruent to $1 \pm T^d \pmod{T^{2d}}$, where the sign of T^d is determined by the parity of the number of factors in r. □

Definition 2.6. We call a polynomial $F \in \mathbb{Z}[T]$ a *root-of-unity polynomial* if it satisfies one of the following three equivalent conditions:

   (1) F is a divisor of $T^u - 1$ for some $u > 0$.
   (2) F or $-F$ is a product of distinct cyclotomic polynomials.
   (3) $F(0) = \pm 1$, F is squarefree and all the zeros of F are roots of unity.

Let $\mathcal{C}$ denote the set of all root-of-unity polynomials.

Proposition 2.7. *Let $F \in \mathbb{Z}[T]$ with $F(0) \in \{-1, 1\}$, and let $d \in \mathbb{N}$. Then there exists a polynomial $M \in \mathcal{C}$ such that $F \equiv M \pmod{T^d}$.*

If we are working in the T-adic topology, then "$F \equiv M \pmod{T^d}$" means that M is an approximation of F with a precision of T^d. Since the units of $\mathbb{Z}[[T]]$ are exactly the power series F with $F(0) = \pm 1$, the proposition can be rephrased as follows: *the set of root-of-unity polynomials is T-adically dense in $\mathbb{Z}[[T]]^*$.*

Proof. Since the set $\mathcal{C}$ is invariant under changing sign, we may assume without loss of generality that $F(0) = 1$.

The proof will be done by induction on d, which means that we will construct better and better approximations of F. For $d = 1$, we can take $M = 1$. Now let $d \geq 1$ and assume that $F \equiv M_0 \pmod{T^d}$, where $M_0 \in \mathcal{C}$. Then $F - M_0 \equiv cT^d \pmod{T^{d+1}}$ for some $c \in \mathbb{Z}$. If c happens to be zero, then we can take $M = M_0$.

First consider the case $c > 0$. By Corollary 2.5, we can find an $n_1 \in \mathbb{N}$ such that $\Phi_{n_1}(T) \equiv 1 + T^d \pmod{T^{2d}}$ and such that $\Phi_{n_1}(T)$ is not a factor of M_0. Let $M_1 := M_0 \Phi_{n_1}(T)$. Since $M_0(0) = 1$, we get

$$F - M_1 \equiv F - M_0(1 + T^d) \equiv (F - M_0) - M_0 T^d \equiv (c-1)T^d \pmod{T^{d+1}}.$$

We can iterate this procedure. Set $M_2 := M_1 \Phi_{n_2}(T)$ for a Φ_{n_2} which is congruent to $1 + T^d \pmod{T^{2d}}$, then $F - M_2 \equiv (c-2)T^d \pmod{T^{d+1}}$. After c steps, we have $F - M_c \equiv 0 \pmod{T^{d+1}}$. So we can take $M := M_c$.

The case $c < 0$ is analogous; the only difference is that we need to multiply with polynomials which are congruent to $1 - T^d \pmod{T^{d+1}}$. $\square$

3. Defining polynomials with integer coefficients

In this section, we will prove the following theorem:

Theorem 3.1. *Let $\mathcal{R}$ be an integral domain of characteristic zero such that $\mathcal{R}[T]$ admits a diophantine degree bounding predicate (see Definition 1.1). Then $\mathbb{Z}[T]$ is diophantine over $\mathcal{R}[T]$.*

For $\mathcal{R}$ a subring of a number field, we will prove in section 4 that the assumption of Theorem 3.1 is satisfied. In section 5, we will show how Theorem 3.1 implies the main theorem.

In this section, we prove Theorem 3.1 in three steps: First, we give a diophantine definition of all divisors of some $T^u - 1$ in $\mathcal{R}[T]$. Second, we restrict these to the polynomials which have integer coefficients, i.e. the root-of-unity polynomials. We also give a diophantine definition of the powers of T in $\mathcal{R}[T]$. Finally, we use Proposition 2.7 to give a diophantine definition of $\mathbb{Z}[T]$ over $\mathcal{R}[T]$.

3.1. **Divisors of $T^u - 1$.** We give a diophantine definition of the elements in $\mathcal{R}[T]$ which divide $T^u - 1$ for some $u > 0$ without requiring that they have coefficients in $\mathbb{Z}$.

Proposition 3.2. *In $\mathcal{R}[T]$, the set of all polynomials dividing $T^u - 1$ for some $u > 0$ is diophantine.*

Proof. Let G be in $\mathcal{R}[T]$. We claim that G divides some $T^u - 1$ if and only if there exist H, S, X, Y and m in $\mathcal{R}[T]$ such that the following formula is satisfied:

$$(3.1) \qquad X^2 - \left(\left(\tfrac{T+T^2S^3}{2}\right)^2 - 1\right)Y^2 = 1$$

$$(3.2) \qquad \wedge\ X \equiv 1 \pmod{T + T^2 S^3 - 2}$$

$$(3.3) \qquad \wedge\ Y \equiv m \pmod{T + T^2 S^3 - 2}\ \wedge\ m \in \mathbb{Z}\setminus\{0\}$$

$$(3.4) \qquad \wedge\ GH = 1 - TS\ \wedge\ X + \left(\tfrac{T-S}{2}\right)Y \equiv 1 \pmod{G}.$$

This is a diophantine formula because a congruence $A \equiv B \pmod{C}$ can be written as $(\exists X)(A - B = CX)$ and the set $\mathbb{Z}\setminus\{0\}$ is diophantine because $\mathbb{Z}$ is diophantine over $\mathcal{R}[T]$ (see [16], Theorem 5.1).

The polynomial $T + T^2 S^3$ is never constant, so Proposition 2.2 says that formula (3.1) is equivalent to

$$(3.5) \qquad X = \pm \mathrm{X}_n\left(\tfrac{T+T^2S^3}{2}\right)\ \text{and}\ Y = \mathrm{Y}_n\left(\tfrac{T+T^2S^3}{2}\right)\ \text{for some } n \in \mathbb{Z}.$$

Since $\mathrm{X}_n(1) = 1$, the condition (3.2) forces the "$\pm$" sign in (3.5) to be positive. Since $\mathrm{Y}_n(1) = n$, it follows from (3.3) that $n = m$; hence, $n \neq 0$.

The formula $(\exists H, S)(GH = 1 - TS)$ is equivalent to saying that $G(0)$ is a unit. This is certainly satisfied if G divides $T^u - 1$.

Since $GH = 1 - TS$, we have $S \equiv T^{-1} \pmod{G}$. So, the last part of formula (3.4) becomes equivalent to

$$\mathrm{X}_n\left(\tfrac{T+T^{-1}}{2}\right) + \left(\tfrac{T-T^{-1}}{2}\right)\mathrm{Y}_n\left(\tfrac{T+T^{-1}}{2}\right) \equiv 1 \pmod{G}.$$

Using Proposition 2.3, this is equivalent to $T^n \equiv 1 \pmod{G}$. Without loss of generality, we may assume that $n > 0$ (otherwise multiply both sides by T^{-n}). Then $T^n \equiv 1 \pmod{G}$ is equivalent to $G \mid T^n - 1$. $\qquad\square$

3.2. **Powers of T and root-of-unity polynomials.** In this section, we show that the set of powers of T and the set of root-of-unity polynomials are diophantine over $\mathcal{R}[T]$. Here $\mathcal{R}[T]$ is any integral domain of characteristic zero. Some of the arguments in this section were inspired by [4] and [18].

We need to work with absolute values on a number field K. We refer to [13], Ch. III, §1. There are "finite" (non-archimedean) absolute values coming from discrete valuations on K, and there are "infinite" (archimedean) absolute values of the form $|x|_\sigma = |\sigma(x)|$, where $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding. Usually, absolute values are normalized in a different way: $|\sigma(x)|$ for real embeddings and $|\sigma(x)|^2$ for complex embeddings. With the usual normalization, we have the product formula for all $x \in K^*$ (see [13], Ch. III, Prop. (1.3)):

$$(3.6) \qquad\qquad \prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = 1,$$

where the product ranges over all absolute values (finite and infinite). A consequence of this is the following: if $x \in K^*$ and $|x|_{\mathfrak{p}} < 1$ for some prime $\mathfrak{p}$, then there must be a prime $\mathfrak{q}$ such that $|x|_{\mathfrak{q}} > 1$. This consequence remains true even if one uses a different normalization for the absolute values.

Definition 3.3. Let $d \geq 1$ be an integer. Define the set $\mathcal{G}_d$ as the set of all polynomials $G \in \bar{\mathbb{Q}}[T]$ such that

(1) The coefficients of G are algebraic integers.
(2) The degree of G is at most d.
(3) For every coefficient γ_i of G, we have $|\sigma(\gamma_i)| \leq 2^{d-1}$ for all embeddings $\sigma : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$.
(4) $G(2^d + 1)$ is an integer.

For every such polynomial, its coefficients generate a certain number field K. Therefore we only need to consider the finitely many embeddings $K \hookrightarrow \mathbb{C}$ in the third condition.

Some obvious elements of $\mathcal{G}_d$ are the polynomials with integer coefficients of degree at most d with coefficients in the interval $[-2^{d-1}, 2^{d-1}]$. We will show that these are the only elements of $\mathcal{G}_d$.

Lemma 3.4. *Fix an integer $d \geq 1$ and take two distinct elements A and B in $\mathcal{G}_d$. Then $A(2^d + 1) \neq B(2^d + 1)$.*

Proof. Let K be a number field containing the coefficients of A and B and let $\mathcal{O}$ be its ring of integers.

Let $D := A - B$ and write $D(T) = \sum_{i=0}^{e} \delta_i T^i$ with $\delta_e \neq 0$. To ease notation, write $h := 2^d + 1$. We want to prove that $D(h) \neq 0$, so assume that $D(h) = 0$. Then

$$(3.7) \qquad \delta_e h^e = -\sum_{i=0}^{e-1} \delta_i h^i.$$

Take an infinite absolute value $|\cdot|$ on K (coming from an embedding $K \hookrightarrow \mathbb{C}$). The coefficients of A and B have absolute value at most 2^{d-1}; therefore $|\delta_i| \leq 2^d$. Since $\delta_e \in \mathcal{O}$ is integral over $\mathbb{Z}$, we have $|\delta_e|_{\mathfrak{p}} \leq 1$ for every finite absolute value on K. As explained in the beginning of this section, this implies that $|\delta_e| \geq 1$ for some infinite absolute value on K. If we take an absolute value $|\cdot|$ such that $|\delta_e| \geq 1$, then (3.7) implies the following contradiction:

$$h^e \leq |\delta_e h^e| \leq \sum_{i=0}^{e-1} |\delta_i| h^i \leq 2^d \frac{h^e - 1}{h - 1} = h^e - 1. \qquad \square$$

Proposition 3.5. *All elements of $\mathcal{G}_d$ have integer coefficients.*

Proof. Take any $G \in \mathcal{G}_d$ and write $G = \sum_{i=0}^{d} \gamma_i T^i$ (where we allow $\gamma_d = 0$). Let $h := 2^d + 1$. We have the following bound for any infinite absolute value:

$$|G(h)| \leq \sum_{i=0}^{d} |\gamma_i| h^i \leq 2^{d-1} \frac{h^{d+1} - 1}{h - 1} = \frac{h^{d+1} - 1}{2}.$$

In Lemma 3.4, we showed that $G(h)$ cannot take the same value for two different elements G of $\mathcal{G}_d$. Since $G(h) \in \mathbb{Z}$ by definition of $\mathcal{G}_d$ and $|G(h)| \leq (h^{d+1} - 1)/2$, it follows that $\mathcal{G}_d$ has at most h^{d+1} elements. But we already know h^{d+1} elements in $\mathcal{G}_d$, namely the polynomials of degree $\leq d$ with integer coefficients in $[-2^{d-1}, 2^{d-1}]$. It follows that these are the only elements of $\mathcal{G}_d$. $\qquad \square$

We have a diophantine definition of the divisors of $T^u - 1$ in $\mathcal{R}[T]$, but we only want those divisors with integer coefficients. We take care of this using the following proposition.

Proposition 3.6. *Let K be a number field. Let $F \in K[T]$ be a non-constant polynomial satisfying $F(0) \in \{-1, 1\}$ whose zeros (over an algebraic closure) are all roots of unity. Let d be an integer greater than or equal to the degree of F. Then $F \in \mathcal{G}_d$ if and only if $F(2^d + 1) \in \mathbb{Z}$.*

Proof. The "only if" direction is immediate; it remains to prove the "if" direction. Conditions 2 and 4 in the definition of $\mathcal{G}_d$ are trivially satisfied. Let e be the degree of F (then $e \leq d$) and write

$$(3.8) \qquad F(T) = \sum_{i=0}^{e} \alpha_i T^i.$$

Over an algebraic closure, F can be factored as

$$(3.9) \qquad F(T) = \alpha_e (T - \zeta_1) \cdots (T - \zeta_e),$$

where every ζ_i is a root of unity. We see that $F(0) = \alpha_e (-1)^e \prod_{i=1}^{e} \zeta_i$. This must be equal to 1 or -1; therefore α_e is also a root of unity. Since roots of unity are algebraic integers, all coefficients of F are algebraic integers.

Write $\sigma_{e,i}$ for the i-th elementary symmetric polynomial in e variables. Since $\sigma_{e,i}$ has $\binom{e}{i}$ terms, it follows that $\alpha_i = \alpha_e \cdot \sigma_{e,i}(\zeta_1, \ldots, \zeta_e)$ is the sum of $\binom{e}{i}$ roots of unity. Let $|\cdot|$ be an infinite absolute value on K. Then we have $|\alpha_i| \leq \binom{e}{i}$. Since $\binom{e}{i} \leq 2^{e-1}$ for all $e \geq 1$, we have $|\alpha_i| \leq 2^{e-1} \leq 2^{d-1}$. $\qquad \square$

Proposition 3.7. *Let K be a number field and let $F \in K[T]$ be a polynomial whose zeros (over an algebraic closure) are all roots of unity. Assume that $F(0) = -1$ and that there exists an integer $d \geq 1$ such that $F(2^d + 1) = (2^d + 1)^d - 1$. Then $F(T) = T^d - 1$.*

Proof. We claim that the degree of F is at most d. Indeed, let e be the degree of F and suppose that $e \geq d + 1$. We have $F = \alpha_e (T - \zeta_1) \cdots (T - \zeta_e)$ with α_e and all ζ_i roots of unity. For any infinite absolute value $|\cdot|$ on K we have $|F(2^d + 1)| = \prod_{i=1}^{e} |2^d + 1 - \zeta_i| \geq (2^d)^e = (2^e)^d > (2^d + 1)^d - 1$, a contradiction.

So F has degree at most d, and we can apply Proposition 3.6. This gives $F \in \mathcal{G}_d$. Since the polynomials F and $T^d - 1$ are both elements of $\mathcal{G}_d$ and they have the same value at $2^d + 1$, Lemma 3.4 implies that they must be equal. $\qquad \square$

Using the preceding propositions, we can now prove:

Theorem 3.8. *Let $\mathcal{R}$ be any integral domain of characteristic zero. Then the sets $\{T^n \mid n \geq 0\}$ and $\mathcal{C}$ are diophantine over $\mathcal{R}[T]$.*

Proof. First of all, $\mathbb{Z}$ is diophantine over $\mathcal{R}[T]$ (see [16], Theorem 5.1). Since the set $\{(d, (2^d + 1), (2^d + 1)^d - 1) \in \mathbb{Z}^3 \mid d \geq 1\}$ is recursive, it must be diophantine over $\mathbb{Z}$, hence diophantine over $\mathcal{R}[T]$. Propositions 3.2 and 3.7 imply that the set $\{T^d - 1 \mid d \geq 1\}$ is also diophantine over $\mathcal{R}[T]$: this set consists exactly of the polynomials dividing some $T^u - 1$ in $\mathcal{R}[T]$ such that $F(0) = -1$ and $F(2^d + 1) = (2^d + 1)^d - 1$ for some $d \geq 1$. Remark that $F(a) = b$ is indeed a diophantine condition; it is equivalent to $(T - a) | (F - b)$. Then also the set $\{T^n \mid n \geq 0\}$ is diophantine over $\mathcal{R}[T]$.

For the second assertion, take any $F \in \mathcal{R}[T]$. Proposition 3.6 shows that $F \in \mathcal{C}$ if and only if there exists a $d \geq 1$ such that $F | T^d - 1$, $F(0) \in \{-1, 1\}$ and $F(2^d + 1) \in \mathbb{Z}$. Since $\mathbb{Z}$ and $\{T^d - 1 \mid d \geq 1\}$ are diophantine over $\mathcal{R}[T]$, this is a diophantine condition. $\qquad \square$

3.3. **All polynomials with integer coefficients.** Theorem 3.8 gives us a diophantine definition of $\mathcal{C}$, a subset of $\mathbb{Z}[T]$, over $\mathcal{R}[T]$. To see that all of $\mathbb{Z}[T]$ is diophantine over $\mathcal{R}[T]$, we use Proposition 2.7. By taking remainders of the elements of $\mathcal{C}$ after Euclidean division by T^d, we get all elements of $\mathbb{Z}[T]$ with constant coefficient 1 or -1. In order for Euclidean division to be diophantine, we need a diophantine degree bouding predicate. To get all elements of $\mathbb{Z}[T]$, we just need to add an integer to the polynomials we get as remainders.

Proof of Theorem 3.1. We have to show that $\mathbb{Z}[T]$ is a diophantine subset of $\mathcal{R}[T]$, assuming that $\mathcal{R}[T]$ has a diophantine degree bounding predicate δ. Let X be an element of $\mathcal{R}[T]$. We claim that X is in $\mathbb{Z}[T]$ if and only if

$$(3.10) \quad (\exists M, Q, R, D, c)(X = R + c \ \wedge \ c \in \mathbb{Z} \ \wedge \ M \in \mathcal{C}$$

$$(3.11) \qquad\qquad \wedge \ (\exists d \geq 1)(D = T^d) \ \wedge \ M = QD + R \ \wedge \ \delta(TR + 1, D)).$$

Assume that X is indeed in $\mathbb{Z}[T]$. Then set $c := X(0) - 1$ and $R := X - c$ such that $R(0) = 1$. Let d be such that $\delta(TR + 1, T^d)$ is true and set $D := T^d$. Apply Proposition 2.7 to find an $M \in \mathcal{C}$ such that $R \equiv M \pmod{T^d}$ and let $Q := (M - R)/T^d$. Now it is clear that (3.10) and (3.11) are satisfied.

Conversely, assume that (3.10) and (3.11) are satisfied. We have to show that $X \in \mathbb{Z}[T]$. Since $\mathcal{C} \subseteq \mathbb{Z}[T]$, we know that M is in $\mathbb{Z}[T]$. Formula (3.11) implies that $\deg(TR + 1) \leq d$; hence $R = 0$ or $\deg(R) < d$. It follows that R is the remainder of the Euclidean division of M by $D = T^d$; therefore $R \in \mathbb{Z}[T]$. Since $c \in \mathbb{Z}$, it also follows that $X \in \mathbb{Z}[T]$. $\qquad\qquad\Box$

4. Diophantine definition of degree

As in the Introducion, let K be a number field and let $\mathcal{R}$ be a subring of K with fraction field K. We will show that the relation "$\deg(X) \leq \deg(Y)$" (where we assume $X \neq 0$ and $Y \neq 0$) is diophantine over $\mathcal{R}[T]$. This relation is clearly a degree bounding predicate.

To give a diophantine definition of "$\deg(X) \leq \deg(Y)$", we use the fact that "negative degree" is a discrete valuation on $K(T)$. More precisely, if $F, G \in \mathcal{R}[T]$, then $v_{T^{-1}}(F/G) := \deg(G) - \deg(F)$ defines a discrete valuation on $K(T)$. Therefore, the problem reduces to showing that the discrete valuation ring at T^{-1} in $K(T)$ is diophantine. For this, we need certain quadratic forms used by Kim and Roush (see [9]) to prove undecidability for rational function fields over so-called p-adic fields with p odd. This undecidability has been generalised to arbitrary function fields over p-adic fields with p odd (see [11] or [6]).

Definition 4.1. Let p be a prime number. A field K is called *p-adic* if K can be embedded in a finite extension of $\mathbb{Q}_p$.

It is clear from this definition that every number field is p-adic for every p. For the rest of this section, we fix any odd prime p.

We introduce some notations and definitions concerning quadratic forms:

Definition 4.2. $\langle a_1, \ldots, a_n \rangle$ stands for the quadratic form $a_1 X_1^2 + \ldots a_n X_n^2$. If we have two quadratic forms $\langle a_1, \ldots, a_n \rangle$ and $\langle b_1, \ldots, b_m \rangle$, then we define a product

$$\langle a_1, \ldots, a_n \rangle \langle b_1, \ldots, b_m \rangle =$$
$$\langle a_1 b_1, \ldots, a_n b_1, a_1 b_2, \ldots, a_n b_2, \ldots, a_1 b_m, \ldots, a_n b_m \rangle.$$

A quadratic form $\langle a_1, \ldots, a_n \rangle$ is called *isotropic* over a field K if there exists a non-zero vector $(x_1, \ldots, x_n) \in K^n$ such that $a_1 x_1^2 + \ldots + a_n x_n^2 = 0$. It is called *anisotropic* otherwise.

Following the method by Kim and Roush, we need to work over a field satisfying Hypothesis $(\mathcal{H})$:

Definition 4.3. Let L be a p-adic field with p odd and let $v_{\mathfrak{p}}$ be a discrete valuation on L extending the p-adic valuation on $\mathbb{Q}$. We say that L satisfies Hypothesis $(\mathcal{H})$ if and only if L contains elements α and π such that

  (1) $v_{\mathfrak{p}}(\pi)$ is odd and π is algebraic over $\mathbb{Q}$.
  (2) α is a root of unity.
  (3) L contains a square root of -1.
  (4) The quadratic form $\langle 1, \alpha \rangle \langle 1, \pi \rangle$ is anisotropic (i.e. has no non-trivial zeros) in the completion $L_{\mathfrak{p}}$.
  (5) The quadratic form $\langle 1, \alpha \rangle \langle 1, \pi \rangle$ is isotropic in all 2-adic completions of $\mathbb{Q}(\alpha, \pi, \sqrt{-1})$.

Proposition 4.4 ([9], Proposition 8)**.** *Let K be a p-adic field for an odd prime p and let $v_{\mathfrak{p}}$ be a discrete valuation on K extending the p-adic valuation on $\mathbb{Q}$. Then there exists a finite extension L of K which satisfies Hypothesis $(\mathcal{H})$.*

The next two propositions deal with certain quadratic forms. Our variable T is the inverse of the variable t that Kim and Roush use.

Proposition 4.5 ([9], Proposition 7)**.** *Let L be any field of characteristic 0 and suppose that $\langle 1, -\alpha \rangle \langle 1, \pi \rangle$ is an anisotropic quadratic form over L. Let $F \in L(T)$ be such that $v_{T^{-1}}(F)$ is non-negative and even. Then one of the following two is anisotropic over $L(T)$:*

$$(4.1) \qquad\qquad \langle T, -\alpha T, -1, -F \rangle \langle 1, \pi \rangle,$$

$$(4.2) \qquad\qquad \langle T, -\alpha T, -1, -\alpha F \rangle \langle 1, \pi \rangle.$$

The following proposition follows from [9]. However, here we use a reformulation by Eisenträger (see [6], Theorem 8.1).

Proposition 4.6. *Let L be a p-adic field satisfying Hypothesis $(\mathcal{H})$ for elements α and π in L. Let $\mathcal{U} \subseteq L(T)$ be such that $\mathcal{U} \cap \mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_m}$ for every finite set of rational primes $\{p_1, \ldots, p_m\}$. Let $G \in L(T)$ be such that $v_T(G) = -2$ and $v_{T^{-1}}(G) = 1$. Assume that the coefficients of G are algebraic over $\mathbb{Q}$. Then there exist $\gamma_3, \gamma_5 \in \mathcal{U}$ such that, if we let*

$$(4.3) \qquad\qquad F := (1 + T^{-1})^3 G(T) + \gamma_3 T^{-3} + \gamma_5 T^{-5},$$

then the following quadratic forms are both isotropic over $L(T)$:

$$(4.4) \qquad\qquad \langle T, \alpha T, -1, -F \rangle \langle 1, \pi \rangle,$$

$$(4.5) \qquad\qquad \langle T, \alpha T, -1, -\alpha F \rangle \langle 1, \pi \rangle.$$

The most natural choice for $\mathcal{U}$ would be $\mathcal{U} = L$. However, for our applications, $\mathcal{U}$ needs to be diophantine in $L(T)$. In the article by Kim and Roush, $\mathcal{U}$ is a subset of L. However, since enlarging the set $\mathcal{U}$ only weakens the proposition, we can even take $\mathcal{U}$ in $L(T)$.

Taking these last two propositions together, we can prove the following:

Proposition 4.7. *Let L and $\mathcal{U}$ be as in Proposition 4.6 with the additional condition that every element $A \in \mathcal{U}$ satisfies $v_{T^{-1}}(A) \geq 0$. Let $X \in L(T)$ with algebraic coefficients and define*

$$G(T) := \frac{(T + T^2) + X^3}{T^3 + T^2 X^3}.$$

Then $v_{T^{-1}}(X) \geq 0$ if and only if there exist $\gamma_3, \gamma_5 \in \mathcal{U}$ such that the quadratic forms (4.4) and (4.5) are both isotropic with F as in (4.3).

Proof. Write $G_N := (T + T^2) + X^3$ and $G_D := T^3 + T^2 X^3$ such that $G = G_N/G_D$. Assume that $v_{T^{-1}}(X) \geq 0$. Then $v_{T^{-1}}(G_N) = -2$ and $v_{T^{-1}}(G_D) = -3$ such that $v_{T^{-1}}(G) = 1$. If $v_T(X) \geq 1$, then $v_T(G_N) = 1$ and $v_T(G_D) = 3$ such that $v_T(G) = -2$. If $v_T(X) \leq 0$, then $v_T(G_N) = 3v_T(X)$ and $v_T(G_D) = 2 + 3v_T(X)$ such that $v_T(G) = -2$. In short, if $v_{T^{-1}}(X) \geq 0$, then we have $v_{T^{-1}}(G) = 1$ and $v_T(G) = -2$. Proposition 4.6 gives us that (4.4) and (4.5) are indeed isotropic for some choice of γ_3 and γ_5 in $\mathcal{U}$.

Conversely, assume that $v_{T^{-1}}(X) < 0$. We must show that one of the forms (4.4) or (4.5) is anisotropic for every γ_3, γ_5 with non-negative valuation at T^{-1}. Since $v_{T^{-1}}(X) \leq -1$, we have $v_{T^{-1}}(G_N) = 3v_{T^{-1}}(X)$ and $v_{T^{-1}}(G_D) = -2 + 3v_{T^{-1}}(X)$. Therefore $v_{T^{-1}}(G) = 2$. Since $v_{T^{-1}}(\gamma_i) \geq 0$, it follows from (4.3) that $v_{T^{-1}}(F) = 2$. Hypothesis $(\mathcal{H})$ says that $\langle 1, \alpha \rangle \langle 1, \pi \rangle$ is locally anisotropic at $\mathfrak{p}$; hence it is also globally anisotropic over L. Since L contains $\sqrt{-1}$, signs in quadratic forms do not matter. Therefore, we can apply Proposition 4.5. $\qquad\square$

Theorem 4.8. *Let $\mathcal{R}$ be a subring of a number field. In the ring $\mathcal{R}[T]$, the relation "$\deg(X) \leq \deg(Y)$" with X and Y being non-zero elements of $\mathcal{R}[T]$ is diophantine over $\mathcal{R}[T]$.*

Proof. Since the non-zero elements of $\mathcal{R}[T]$ form a diophantine subset of $\mathcal{R}[T]$ (see [12, Théorème 3.1]), we can construct a diophantine interpretation of the fraction field $K(T)$ over $\mathcal{R}[T]$. Let L be a finite extension of K which satisfies Hypothesis $(\mathcal{H})$. Using a basis of L as a K-vector space, there is a diophantine model of $L(T)$ over $K(T)$.

Since $\deg(X) \leq \deg(Y)$ is equivalent to $v_{T^{-1}}(X/Y) \geq 0$, it suffices to give a diophantine definition of the predicate "$v_{T^{-1}}(X) \geq 0$" with $X \in L(T)$. Let

$$\mathcal{U} = \{n/P \mid n \in \mathbb{Z} \ \wedge \ P \in \mathcal{R}[T] \setminus \{0\}\} \subseteq K(T).$$

By construction, every element $A \in \mathcal{U}$ has $v_{T^{-1}}(A) \geq 0$. The set $\mathcal{U}$ contains $\mathbb{Q}$, which is clearly dense in every $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_m}$. Since quadratic forms being isotropic is a diophantine condition and $\mathcal{U}$ is diophantine, it follows by Proposition 4.7 that "$v_{T^{-1}}(X) \geq 0$" is diophantine. $\qquad\square$

5. Recursively enumerable sets

In this final section we discuss how having a diophantine definition of $\mathbb{Z}[T]$ in $\mathcal{R}[T]$ gives us that r.e. subsets of $\mathcal{R}[T]^k$ are diophantine.

Theorem 5.1. *Let $\mathcal{R}$ be a recursive ring contained in a number field and let $\mathcal{S}$ be a recursively enumerable subset of $\mathcal{R}[T]^k$ (for some $k \geq 1$). Then $\mathcal{S}$ is diophantine over $\mathcal{R}[T]$.*

Proof. Denef showed (see [4]) that r.e. subsets of $\mathbb{Z}[T]^k$ are diophantine over $\mathbb{Z}[T]$. Since $\mathbb{Z}[T]$ is diophantine over $\mathcal{R}[T]$, it follows that r.e. subsets of $\mathbb{Z}[T]^k$ are diophantine over $\mathcal{R}[T]$.

Let K denote the fraction field of $\mathcal{R}$; this is a number field. Let $\alpha \in \mathcal{R}$ be such that $K = \mathbb{Q}(\alpha)$ and let $d := [K : \mathbb{Q}]$. Now any element X of $\mathcal{R}[T]$ can be written as

$$(5.1) \qquad X = \frac{X_0 + X_1\alpha + \cdots + X_{d-1}\alpha^{d-1}}{y}$$

with X_i in $\mathbb{Z}[T]$ and y in $\mathbb{Z} \setminus \{0\}$.

Let $\mathcal{S} \subseteq \mathcal{R}[T]$ be an r.e. set. We have to show that $\mathcal{S}$ is diophantine. To $\mathcal{S}$ we associate a set $\mathcal{T} \subseteq \mathbb{Z}[T]^{d+1}$ using (5.1): the set $\mathcal{T}$ has one tuple $(X_0, X_1, \ldots, X_{d-1}, y)$ $\in \mathbb{Z}[T]^{d+1}$ for every $X \in \mathcal{S}$. This tuple $(X_0, X_1, \ldots, X_{d-1}, y)$ is not unique, but that is not a problem: we can algorithmically try all possible tuples and take the first one which works for a given X. This way, we have a bijection between $\mathcal{S}$ and $\mathcal{T}$. Moreover, the set $\mathcal{T}$ will also be r.e., since we can construct $\mathcal{T}$ from $\mathcal{S}$ using a recursive procedure. Since $\mathcal{T}$ is a subset of $\mathbb{Z}[T]^{d+1}$, it will be diophantine over $\mathcal{R}[T]$. Now it immediately follows that $\mathcal{S}$ is diophantine:

$$X \in \mathcal{S} \iff \big(\exists (X_0, X_1, \ldots, X_{d-1}, y) \in \mathcal{T}\big)\big(Xy = X_0 + X_1\alpha + \cdots + X_{d-1}\alpha^{d-1}\big).$$

The argument for sets $\mathcal{S} \subseteq \mathcal{R}[T]^k$ is very similar, using a set $\mathcal{T} \subseteq \mathbb{Z}[T]^{(d+1)k}$. $\square$

References

[1] Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), no. 3, 233–269. MR0317916 (47:6465)

[2] Jeroen Demeyer, *Recursively enumerable sets of polynomials over a finite field*, J. Algebra **310** (2007), no. 2, 801–828. MR2308181 (2008b:11127)

[3] ———, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Invent. Math. **170** (2007), no. 3, 655–670. MR2357505 (2009f:03053)

[4] Jan Denef, *Diophantine sets over $\mathbb{Z}[T]$*, Proc. Amer. Math. Soc. **69** (1978), no. 1, 148–150. MR0462934 (57:2899)

[5] ———, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78 (M. Boffa, D. van Dalen, and K. Mcaloon, eds.), Studies in logic and the foundations of mathematics, no. 97, North-Holland, 1979, pp. 131–145. MR567668 (81h:03090)

[6] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over number fields and p-adic fields*, J. Algebra **310** (2007), no. 2, 775–792. MR2308179 (2008c:11163)

[7] Albrecht Fröhlich and John C. Shepherdson, *Effective procedures in field theory*, Phil. Trans. Roy. Soc. London **248** (1956), 407–432. MR0074349 (17:570d)

[8] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory (second edition)*, Graduate Texts in Mathematics, no. 84, Springer-Verlag, 1990. MR1070716 (92e:11001)

[9] Ki Hang Kim and Fred Roush, *Diophantine unsolvability over p-adic function fields*, J. Algebra **176** (1995), no. 1, 83–110. MR1345295 (96f:11165)

[10] Yuri Matiyasevich, *Enumerable sets are Diophantine*, Soviet Math. Dokl. **11** (1970), 354–358.

[11] Laurent Moret-Bailly, *Elliptic curves and Hilbert's tenth problem for algebraic function fields over real and p-adic fields*, J. Reine Angew. Math. **587** (2005), 77–143. MR2186976 (2007c:11129)

[12] ———, *Sur la définissabilité existentielle de la non-nullité dans les anneaux*, Algebra & Number Theory **1** (2007), no. 3, 331–346. MR2361937 (2008k:13012)

[13] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original, with a note by Norbert Schappacher and a foreword by G. Harder. MR1697859 (2000m:11104)

[14] Thanases Pheidas and Karim Zahidi, *Undecidability of existential theories of rings and fields: a survey*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (Denef et al., eds.), Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 49–105. MR1802009 (2002a:03085)

[15] Bjorn Poonen, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350. MR2382821 (2008m:11238)

[16] Alexandra Shlapentokh, *Diophantine definitions for some polynomial rings*, Commun. Pure Appl. Math. **43** (1990), 1055–1066. MR1075078 (92c:11150)

[17] Karim Zahidi, *Existential undecidability for rings of algebraic functions*, Ph.D. thesis, Ghent University, 1999.

[18] ———, *On diophantine sets over polynomial rings*, Proc. Amer. Math. Soc. **128** (2000), no. 3, 877–884. MR1641141 (2000e:03120)

Department of Mathematics, Ghent University, Krijgslaan 281, 9000 Gent, Belgium
E-mail address: `jdemeyer@cage.ugent.be`