# ON EXISTENTIAL DEFINITIONS OF C.E. SUBSETS OF RINGS OF FUNCTIONS OF CHARACTERISTIC 0

RUSSELL MILLER & ALEXANDRA SHLAPENTOKH

ABSTRACT. We extend results of Denef, Zahidi, Demeyer and the second author to show the following.

(1) Every c.e. set of integers has a single-fold Diophantine definition over the ring of integral functions of any function field of characteristic 0.
(2) Every c.e. set of integers has a single-fold Diophantine definition over a polynomial ring over an integral domain $Z$ of characteristic 0.
(3) All c.e. subsets of polynomial rings over rings of totally real integers have finite-fold Diophantine definitions. (These are the first examples of infinite rings with this property.)
(4) Let $K$ be a one-variable function field over a field of constants $k$, and let $\mathfrak{p}$ be any prime of $K$. If $k$ is algebraic over $\mathbb{Q}$ and for some odd prime $p$ embeddable into a finite extension of $\mathbb{Q}_{\mathfrak{p}}$, then the valuation ring of $\mathfrak{p}$ has a Diophantine definition over $K$. If $k$ is embeddable into a real field, then valuation rings are existentially definable for "almost all" primes.
(5) Let $K$ be a one-variable function field over a number field and let $\mathscr{S}$ be a finite non-empty set of its primes. Then all c.e. subsets of $O_{K,\mathscr{S}}$ are Diophantine over $O_{K,\mathscr{S}}$. (Here $O_{K,\mathscr{S}}$ is the ring of $\mathscr{S}$-integers or a ring of integral functions.)

## 1. INTRODUCTION

In 1969, building on earlier work by Martin Davis, Hilary Putnam and Julia Robinson, Yuri Matiyasevich demonstrated the impossibility of solving Hilbert's Tenth Problem. In doing so, he also completed a proof of the theorem asserting that Diophantine (or existentially definable in the language of rings) sets and computably enumerable sets of integers were the same. In other words, it was proved that for every positive integer $n$, every computably enumerable subset of $\mathbb{Z}^n$ had a Diophantine definition over $\mathbb{Z}$. We describe the notions of a Diophantine definition and a Diophantine set in a more general setting.

**Definition 1.1.** Let $R$ be a commutative ring and let $n$ be a positive integer. In this case a set $A \subset R^n$ is called Diophantine over $R$ if for some $m > 0$ and some polynomial

$$f(T_1, \ldots, T_n, X_1, \ldots, X_m) \in R[\bar{T}, \bar{X}]$$

we have that for all $(t_1, \ldots, t_n) \in R^n$ it is the case that

$$(t_1, \ldots, t_n) \in A \text{ if and only if } \exists x_1, \ldots, x_m \in R \text{ such that } f(t_1, \ldots, t_n, x_1, \ldots, x_m) = 0.$$

The first author was partially supported by Grant # DMS – 1362206 from the National Science Foundation, by Grant # 581896 from the Simons Foundation, by the Queens College Research Enhancement Program, and by several grants from The City University of New York PSC-CUNY Research Award Program. The second author was partially supported by Grant # DMS – 1161456 from the National Science Foundation.

The polynomial $f(\bar{T}, \bar{X})$ is called a Diophantine definition of $A$ over $R$.

If a set $A$ is Diophantine over $R$ and for every $\bar{t} \in A$ we have that $\bar{x}$ as above is unique, we say that $f(\bar{T}, \bar{X})$ is a *single-fold* definition of $A$. If for every $\bar{t} \in A$ we have that there are only finitely many $\bar{x}$ as above, we say that $f(\bar{T}, \bar{X})$ is a *finite-fold* definition of $A$.

**Question 1.2.** Does every c.e. set of integers have a finite-fold Diophantine definition over $\mathbb{Z}$?

The answer to this question, raised by Yuri Matiyasevich almost immediately after his solution to Hilbert's Tenth Problem, is unknown to this day. The issue of finite-fold representation is of more than just esoteric interest because of its connection to many other questions. For an extensive survey of these connections we refer the reader to a paper of Matiyasevich ([13]). Here we would like to give just one example that can be considered a generalization of Hilbert's Tenth Problem.

Let $\mathfrak{N} = \{0, 1, \ldots, \aleph_0\}$ and let $\mathfrak{M}$ be any nonempty proper subset of $\mathfrak{N}$. Let $\mathscr{P}(\mathfrak{M})$ be the set of polynomials $P$ with integer coefficients such that the number of solutions to the equation $P = 0$ is in $\mathfrak{M}$. Martin Davis showed in [3] that $\mathscr{P}(\mathfrak{M})$ is undecidable. If we ask whether $\mathscr{P}(\mathfrak{M})$ is c.e, then the answer is currently unknown. At the same time, if we replace polynomials by exponential Diophantine equations, then we can answer the question. Craig Smoryńsky in [23] proved that $\mathscr{E}(\mathfrak{M})$ is c.e. if and only if $\mathfrak{M} = \{\alpha | \alpha \geq \beta\}$ for some finite $\beta$. (Here $\mathscr{E}(\mathfrak{M})$ is a collection of exponential Diophantine polynomials with positive integer coefficients such that if an exponential Diophantine polynomial $E \in \mathscr{E}(\mathfrak{M})$, then the number of solutions to the equation $E = 0$ is in $\mathfrak{M}$.) Smoryńsky's proof relied on a result obtained by Matiyasevich in [14] that every computably enumerable set has a single-fold *exponential* Diophantine definition. One would expect a similar result for (non-exponential) Diophantine equations if the finite-fold question is answered affirmatively.

Matiyasevich also proved that to show that all c.e. sets of integers have single-fold (or finite-fold) Diophantine definitions it is enough to show that the set of pairs $\{(a, b) \in \mathbb{Z}^2_{>0} | b = 2^a\}$ has a single-fold (finite-fold) Diophantine definition. (This will not be surprising to readers familiar with the history of Hilbert's Tenth Problem.)

Unfortunately, the finite-fold question over $\mathbb{Z}$ remains out of reach at the moment, as many other Diophantine questions. In Section 3 of this paper, we take some first timid steps in the investigation of this issue by considering it in a more hospitable environment over function fields of characteristic 0, as described in Section 2. We extend the results of the second author from [20] to show that over any ring of integral functions (otherwise known as a ring of $\mathscr{S}$-integers) any c.e. set of rational integers has a single-fold Diophantine definition (see Theorem 3.9). We also show that over any polynomial ring over an integral domain $Z$ of characteristic 0 it is possible to give a single-fold Diophantine definition for every c.e. set of integers (see Theorem 4.9).

Using these results on single-fold definability of $\mathbb{Z}$ and c.e. sets of integers, following results of Jan Denef from [6] and Karim Zahidi from [26], we show in

Section 5 that all computably enumerable subsets of a polynomial ring over a ring of integers of a totally real number field are finite-fold existentially definable. As far as we know, this is the first example of this kind. (See Theorem 5.2.)

In Section 7 we generalize results of Jeroen Demeyer from [4] to show that all c.e. subsets of rings of integral functions over number fields are Diophantine (see Theorem 7.1). In order to do so, we needed to generalize the earlier treatments (given in the papers [15] of Laurent Moret-Bailly and [7] of Kirsten Eisentraeger) of definability of integrality at a degree $1$ valuation over a function field of characteristic zero where the constant field is a number field. Both of those papers in turn extend results of H. K. Kim and Fred Roush from [10] where the two authors give a Diophantine definition of integrality at a valuation of degree 1 over a rational function field with a constant field embeddable into a $p$-adic field. (Such constant fields include all number fields.) The papers of Moret-Bailly and Eisentraeger are primarily concerned with extending results pertaining to Hilbert's Tenth Problem and so they extend the results of Kim and Roush just enough for their arguments to go through, by showing the following for a function field $K$ over a field of constants $k$ as described above: if $T$ is a non-constant element of $K$ and the pole $\mathfrak{q}$ of $T$ splits completely into distinct primes in the extension $K/k(T)$, then there exists a Diophantine subset of $K$ such that all rational functions in that subset are integral at $\mathfrak{q}$.

In contrast, our proof required a Diophantine definition of the valuation ring of a single factor of $\mathfrak{q}$ in $K$. In order to obtain such a definition we reworked the original construction of Kim and Roush. In this paper we show that the valuation ring of "almost" any prime of a function field $K$ of characteristic 0 is existentially definable over a function field with a constant field algebraic over $\mathbb{Q}$ and embeddable into a finite extension of $\mathbb{Q}_p$ for $p \neq 2$ or $\mathbb{R}$. The "almost" part applies only to the case where we have to use the fact that the constant field under consideration is embeddable into $\mathbb{R}$. If the constant field is embeddable into a finite extension of $\mathbb{Q}_p$, with $p \neq 2$, then we can give an existential definition (with a parameter, of course) of *any* valuation ring. We also should note here that the class of constant fields described above contains an infinite subset of non-finitely generated fields. (See Section 6.)

## 2. Number Fields, Function Fields and Rings

2.1. **Discrete Valuations.** Let $L$ be a field. A discrete valuation $v$ of a field $L$ is a map $v : L \longrightarrow \mathbb{Z} \cup \{\infty\}$ satisfying the following conditions:

(1) $v(0) = \infty$;
(2) $v(xy) = v(x) + v(y)$;
(3) $v(x + y) \geq \min(v(x), v(y))$.

The ring $R_v = \{x \in L | v(x) \geq 0\}$ is called the valuation ring of $v$. For any element $x \in L^*$, either $x \in R_v$ or $\frac{1}{x} \in R_v$. The ring is a local ring, i.e. it has a unique maximal ideal containing all the elements of the ring with positive valuation. By a prime $\mathfrak{p}$ of $L$, we will mean the maximal ideal of the valuation ring $R_v$ corresponding to one of the valuations $v$ defined on $L$. Given $f \in R_v, f \neq 0$, we define $\text{ord}_{\mathfrak{p}} f$ to be the largest non-negative integer $n$ such that $f \in \mathfrak{p}^n$. If $f \not\in R_v$, then $\frac{1}{f} \in R_v$, and we define $\text{ord}_{\mathfrak{p}} f = -\text{ord}_{\mathfrak{p}} \frac{1}{f}$. We define the order of 0 to be infinity. If $f \in L$ is such that $\text{ord}_{\mathfrak{p}} f > 0$, we will say that $f$ has a zero at $\mathfrak{p}$. If $\text{ord}_{\mathfrak{p}} f \geq 0$, then we say that $f$ is integral at $\mathfrak{p}$. If $\text{ord}_{\mathfrak{p}} f < 0$, then we say that $f$ has a pole at $\mathfrak{p}$.

Each valuation defines a metric on the field $L$. The completion of $L$ under this metric is denoted by $L_{\mathfrak{p}}$ or $L_v$.

2.1.1. *Extensions of discrete valuations under finite algebraic extensions.* If $M/L$ is a finite extension of valued fields of characteristic 0, then a valuation $v$ of $L$ can have finitely many extensions to $M$. Let $w_1, \ldots, w_r$ be all extensions of $v$ to $M$ with corresponding valuation rings $R_{w_i}$ and prime ideals $\mathfrak{p}_i$. For each $i$ we have that $R_{w_i} \cap L = R_v$ and $\mathfrak{p}_i \cap L = \mathfrak{p}$ -the maximal ideal of $R_v$. In this situation we will say that $\mathfrak{p}_i$ lies above $\mathfrak{p}$ in $M$. We also have that $R = \bigcap R_{w_i}$ is the integral closure of $R_v$ in $L$ (see Theorem 2, Section 4.2 of [18]).

If $M/L$ is Galois, then all extensions of the same valuation $v$ are conjugate under the action of the Galois group. In other words, the Galois group acts transitively on rings $R_{w_i}$ and prime ideals $\mathfrak{p}_i$ (see Theorem 2, Section 4.2 of [18]). Thus, if $v$ has a unique extension $w$ to $M$, then the Galois group will map $R_w$ and its prime ideal to themselves.

In $M$, the ideal $\mathfrak{p}R = \prod \mathfrak{p}_i^{e_i}$, where $e_i$ is called the ramification degree of $\mathfrak{p}_i$ over $\mathfrak{p}$. We will also refer to each $\mathfrak{p}_i$ as a factor of $\mathfrak{p}$ in $M$, and we will refer to the product $\prod \mathfrak{p}_i^{e_i}$ as the factorization of $\mathfrak{p}$ in $M$. If $e_i > 1$, we say that the prime $\mathfrak{p}_i$ is ramified in the extension $M/L$ or ramified over $\mathfrak{p}$. For any $i$ and any $x \in L$, we have that $\text{ord}_{\mathfrak{p}_i} x = e_i \text{ord}_{\mathfrak{p}} x$. This relation between the orders allows one to determine ramification degree in some extensions.

**Lemma 2.1.** *Let $M/L, \mathfrak{p}, \mathfrak{p}_i$ be as above. Suppose there exists $x \in L$ such that for some $i$ we have that $\text{ord}_{\mathfrak{p}_i} x \neq \text{ord}_{\mathfrak{p}} x$. Then $\text{ord}_{\mathfrak{p}_i} x \equiv 0 \bmod \text{ord}_{\mathfrak{p}} x$, the ramification degree of $\mathfrak{p}_i$ over $\mathfrak{p}$ denoted by $e(\mathfrak{p}_i/\mathfrak{p})$ is equal to $\frac{\text{ord}_{\mathfrak{p}_i} x}{\text{ord}_{\mathfrak{p}} x} > 1$, and $\mathfrak{p}$ is ramified in this extension.*

**Corollary 2.2.** *Suppose $M = L(\gamma)$, $\gamma^2 = c \in L$, and $\text{ord}_{\mathfrak{p}} c$ is odd. Then there exists a factor $\mathfrak{q}$ of $\mathfrak{p}$ in $M$ such that $e(\mathfrak{q}/\mathfrak{p}) \equiv 0 \bmod 2$.*

*Proof.* Let $\mathfrak{q}$ be a factor of $\mathfrak{p}$ in $M$. Then $\text{ord}_{\mathfrak{q}} c = 2\text{ord}_{\mathfrak{q}} \gamma \equiv 0 \bmod 2$. At the same time we have that $\text{ord}_{\mathfrak{q}} c = e(\mathfrak{q}/\mathfrak{p}) \text{ord}_{\mathfrak{p}} c$. Thus $e(\mathfrak{q}/\mathfrak{p}) \equiv 0 \bmod 2$. □

The field $R_v/\mathfrak{p}R_v$ is called the residue field of $v$. If $w_i$ is an extension of $v$ to $M$, as above, then $R_{w_i}/\mathfrak{p}_i R_{w_i}$ is a finite extension of $R_v/\mathfrak{p}R_v$ and $f(\mathfrak{p}_i/\mathfrak{p}) = [R_{w_i}/\mathfrak{p}_i : R_v/\mathfrak{p}R_v]$ is called the relative degree of $\mathfrak{p}_i$ over $\mathfrak{p}$. The following formula relates the ramification and relative degrees to the degree of the extension.

$$\sum_i e_i f_i = [M : L]. \tag{2.1}$$

Here $e_i = e(\mathfrak{p}_i/\mathfrak{p}), f_i = f(\mathfrak{p}_i/\mathfrak{p})$ (see Theorem 3, Section 6.2 of [18]).

We also have the following relation between valuations and norms. Using the same notation as above, we have that

$$\text{(2.2)} \qquad \operatorname{ord}_{\mathfrak{p}}\mathbf{N}_{M/L}(y) = \sum_i f_i \operatorname{ord}_{\mathfrak{p}_i} y.$$

*Proof.* Chapter 4, §5, Corollary 2 (of Theorem 6) of [1]. □

2.1.2. *Discriminant.* Let $U$ be a finite extension of a characteristic 0 field $H$ endowed with a discrete valuation $\mathfrak{p}_H$. Let $\mathfrak{p}_U$ lie above $\mathfrak{p}_H$ in $U$. Let $\Omega = \{\omega_1, \ldots, \omega_n\} \subset R_{\mathfrak{p}_U}$ be a basis of $U$ over $H$. Then the discriminant of the basis $\Omega$ is $\prod_{i \neq j}(\omega_i - \omega_j)^2 \in R_{\mathfrak{p}_H}$. We can use the discriminant of a basis to determine whether some primes are not ramified in the extension $U/H$.

**Proposition 2.3.** *Let $U, H, \Omega, \mathfrak{p}_H$ be as above. If the discriminant of $\Omega$ is prime to the ideal $\mathfrak{p}_H$, then $e(\mathfrak{p}_U/\mathfrak{p}_H)$=1.*

*Proof.* Theorem 7.3, §7, Chapter 1 of [9]. □

2.1.3. *Completions.* First we consider a relationship between a field and its completion.

**Proposition 2.4.** *Suppose $F$ is a field endowed with a discrete valuation $v$. Let $F_v$ be the completion of $F$ under a metric corresponding to $v$. Then $v$ can be extended to $F_v$ so that the following statements are true.*

1. *$v(F) \cong v(F_v)$. In particular, $F_v$ is also a discrete valuation field.*
2. *If $\tilde{R}_v$ is the valuation ring of $v$ extended to $F_v$, then its maximal ideal $\mathfrak{p}_v = \mathfrak{p}\tilde{R}_v$.*
3. *$R_v/\mathfrak{p} \cong \tilde{R}/\mathfrak{p}_v\tilde{R}$.*

*Proof.* See Proposition M, Section 2.2 of [18]. □

Next we address some properties of extensions of complete fields.

**Proposition 2.5.** *A finite extension of a discrete valuation field is a discrete valuation field.*

*Proof.* See Proposition G, Section 4.1 of [18]. □

As we pointed out above, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ under a discrete valuation corresponding to a prime $p$. It follows that any finite extension of $\mathbb{Q}_p$ will also be a discrete valuation field.

Using notation above, we consider the extension of completions $M_{\mathfrak{p}_i}/L_{\mathfrak{p}}$. In this case we have the formula for the local degree in terms of the ramification and relative degrees.

**Proposition 2.6.** $[M_{\mathfrak{p}_i} : L_{\mathfrak{p}}] = e(\mathfrak{p}_i/\mathfrak{p})f(\mathfrak{p}_i/\mathfrak{p})$.

*Proof.* See Proposition 3.8, §4, Chapter II of [9]. □

2.1.4. *Integral closure.* Let $K$ be a field. Let $v_1, \ldots,$ be a collection of discrete valuations on $K$. Let $R_{v_i}$ be the valuation ring of $v_i$. Let $R = \bigcap_{i=1}^{\infty} R_{v_i}$. Note that $R$ is necessarily non-empty, since $0, 1 \in R$ and $R$ is a ring. Let $M/K$ be a finite separable extension. For each $v_i$ let $w_{i,1}, \ldots, w_{i,s_i}$ be all of the extensions of $v_i$ to $M$. Let $\hat{R}$ be the integral closure of $R$ in $M$, i.e. the set of all elements of $M$ satisfying monic polynomials over $R$.

**Proposition 2.7.** *Let $x \in M$ be such that $w_{i,j}(x) \geq 0$. Then $x \in \hat{R}$.*

*Proof.* First assume $M/K$ is Galois. Since the Galois group acts transitively on the set of extensions of each $v_i$, we have that if $w_{i,j}(x) \geq 0$ for all $i, j$ and $\hat{x}$ is a conjugate of $x$ over $K$, then $w_{i,j}(\hat{x}) \geq 0$ for all $i, j$. Therefore the coefficients of the monic irreducible polynomial of $x$ over $K$ have non-negative valuations at all $w_{i,j}$. At the same time, if $a \in R$ and $w_{i,j}(a) \geq 0$ for some $j$, then $v_i(a) \geq 0$. Therefore, the coefficients of the monic irreducible polynomial of $x$ over $K$ are in $R$.

If $M/K$ is not Galois and $x \in M$, then when we consider $x$ in the Galois closure $\hat{M}$ of $M$ over $K$, the element will have non-negative valuations at all extensions of $v_i$'s to $\hat{M}$. Thus, by the argument above, the monic irreducible polynomial of $x$ over $K$ will have all of its coefficients in $R$. □

**Corollary 2.8.** *Let $M/K$ be a finite separable extension. Let $\mathscr{S}$ be a collection of valuations of $K$ and let*

$$O_{K,\mathscr{S}} = \{x \in K | v(x) \geq 0 \text{ for all valuations } v \notin \mathscr{S}\}.$$

*Let $\mathscr{W}$ be the set of all extensions of valuations in $\mathscr{S}$ to $M$. Then the integral closure of $O_{K,\mathscr{S}}$ is $O_{M,\mathscr{W}}$.*

*Proof.* To apply the proposition we just need to note that $O_{K,\mathscr{S}} = \bigcap_{v \notin \mathscr{S}} R_v$ and $O_{M,\mathscr{W}} = \bigcap_{w \notin \mathscr{W}} R_w$. □

2.2. **Number Fields.** A number field $H$ is a finite extension of $\mathbb{Q}$. All discrete valuations of $\mathbb{Q}$ correspond to the prime ideals of $\mathbb{Z}$. The integral closure $O_H$ of $\mathbb{Z}$ in $H$ is called the ring of integers of $H$. All discrete valuations of $H$ correspond to prime ideals of $O_H$. Let $v_H$ be a discrete valuation on $H$. Let $R_{v_H}$ be its valuation ring and let $\mathfrak{p}_H$ be the maximal ideal. Then $O_H \cap \mathfrak{p}_H$ is a maximal ideal of $O_H$ and every maximal ideal of $O_H$ arises this way.

Next we have two corollaries of Proposition 2.3 having to do with ramification of dyadic primes in extensions of degree 2.

**Corollary 2.9.** *Let $H$ be a number field and let $a \in O_H$ be such that $a \equiv 1 \bmod 4$. Then no dyadic prime ramifies in the extension $H(\sqrt{a})/H$). (A dyadic prime is a prime corresponding to a valuation extending the 2-adic valuation on $\mathbb{Q}$.)*

*Proof.* If $a \equiv 1 \bmod 4$ then $\frac{\sqrt{a}-1}{2}$ is an algebraic integer. Now consider a basis $\{1, \frac{\sqrt{a}-1}{2}\}$ for our quadratic extension. The discriminant of this extension is $a$ and therefore not divisible by any dyadic prime. Hence by Proposition 2.3, no dyadic prime ramifies. □

**Corollary 2.10.** *Let $H$ be a number field such that for any dyadic prime $\mathfrak{q}$ of $H$ we have that $H_{\mathfrak{q}}$ contains a root of the polynomial $x^2+1$. Then no prime ramifies in the extension $[H(i):H]$.*

*Proof.* If we choose a basis $\Omega = \{1, i\}$ of $H(i)$ over $H$, then the discriminant of $\Omega$ is 4. Hence, by Proposition 2.3, the only primes that can possibly ramify in this extension are dyadic primes. At the same time, if $\mathfrak{q}$ is a dyadic prime of $H$, and $\mathfrak{t}$ is a prime of $H(i)$ restricting to $\mathfrak{q}$ on $H$, then $[H(i)_{\mathfrak{t}} : H_{\mathfrak{q}}] = 1$. Therefore, by Proposition 2.6, we have that $e(\mathfrak{t}/\mathfrak{q})f(\mathfrak{t}/\mathfrak{q}) = 1$ and $e(\mathfrak{t}/\mathfrak{q}) = f(\mathfrak{t}/\mathfrak{q}) = 1$. Thus, no dyadic prime ramifies in the extension $H(i)/H$, and therefore no prime ramifies in this extension. □

We end this section noting one of the differences between discrete valuations of number fields and function fields of characteristic 0: in the case of number fields, the residue fields of primes are always finite.

2.3. **Function Fields.** Throughout this paper, by a function field $K$ we will mean a finite extension of a rational function field $k(t)$, where $t$ is transcendental over a field $k$ of characteristic 0. By the constant field of $K$ we will mean the algebraic closure of $k$ in $K$. (In our case we will often have a situation where the algebraic closure of $k$ in $K$ is equal to $k$ by construction.)

All discrete valuations $v$ of function fields that we will consider in this paper will be trivial on the field of constants, that is we will assume that for any non-zero constant $c \in k$ we have that $v(c) = 0$. All discrete valuations of a rational function field $k(t)$, trivial on $k$, correspond to irreducible polynomials in $k[t]$ or to the degree valuation. The residue field $R_v/\mathfrak{p}$ is isomorphic to a finite extension of the constant field of $K$. The degree of this extension is referred to as “the degree of the prime $\mathfrak{p}$”.

From the formula (2.1) we derive the following corollary.

**Corollary 2.11.** *Let $M/k(T)$ be a function field extension, where $k(T)$ is a rational function field in $T$ over a constant field $k$. Suppose in $M$ we have that $T$ has a pole at one prime $\mathfrak{q}_\infty$ only. Let $\mathfrak{Q}_\infty$ be the infinite valuation of $k(T)$. Then $\mathfrak{q}_\infty$ is the only prime of $M$ lying above $\mathfrak{Q}_\infty$, and $e(\mathfrak{q}_\infty/\mathfrak{Q}_\infty) =$ ord$_{\mathfrak{q}_\infty} T$.*

*Proof.* Suppose $\mathfrak{t} \neq \mathfrak{q}_\infty$ is another prime of $M$ lying above $\mathfrak{Q}_\infty$. Then $\text{ord}_{\mathfrak{t}} T < 0$ in $M$, contradicting assumptions on $T$. Further, $\text{ord}_{\mathfrak{q}_\infty} T = e(\mathfrak{q}_\infty/\mathfrak{Q}_\infty)\text{ord}_{\mathfrak{Q}_\infty} T$. □

Function field valuations can help us distinguish constant and non-constant elements of the function field. Each non-constant element of the field must have a pole at some valuation and a zero at some valuation. An element of the field without any zeros or poles must be a constant.

For the field of constants we will most often select some algebraic extension of $\mathbb{Q}$. One can also consider all possible embeddings of $k$ into $\widetilde{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$ inside $\mathbb{C}$. If all the embeddings are contained in $\mathbb{R}$, then the field is called totally real. If a field is algebraic over $\mathbb{Q}$ and has an embedding into $\mathbb{R}$, then we will call it formally real.

2.4. **Function Field Primes vs. Number Field Primes.** Throughout the paper it will be important to keep in mind the distinction between the number field and function field primes. For example, consider $K = \mathbb{Q}(t)$. The prime ideal $(3)$ corresponds to a valuation of $\mathbb{Q}$, but not of $\mathbb{Q}(t)$. The valuation ring $R_3$ consists of all rational numbers with denominators not divisible by $3$.

The ideal generated by $t$ in $\mathbb{Q}[t]$ corresponds to a valuation of $K$. Its valuation ring $R_t$ consists of all rational functions with denominators not divisible by $t$. Further, all rational numbers are also included in $R_t$.

## 3. Single-fold Diophantine Representations of C.E. Sets of Integers over Rings of $\mathscr{S}$-integers of Function Fields of Characteristic 0

In this section we describe a finite-fold Diophantine definition of c.e. sets of integers over rings of integral functions. Before we do that, we have to reconsider certain old methods of defining sets to make sure they produce single-fold definitions. We start with the issue of intersection of Diophantine sets.

3.1. **Single-Fold and Finite-Fold Definition of "And".** As long as we consider rings whose fraction fields are not algebraically closed, we can continue to use the "old" method of combining several equations into a single one without introducing extra solutions, as in Lemma 1.2.3 of [20]. More specifically we have the following proposition.

**Proposition 3.1.** *Let $R$ be an integral domain such that its fraction field is not algebraically closed. Let $\ell \in \mathbb{Z}_{>0}$ and $A, B, C \subset R^{\ell}$ be Diophantine subsets of $R^{\ell}$ such that the sets $B$ and $C$ have single (finite) fold definitions, and $A = B \cap C$. Then $A$ has a single (finite) fold definition.*

*More specifically, if we let $h(T) = a_0 + a_1T + \ldots + T^n$ be a polynomial without roots in the fraction field of $R$, let $\bar{x} = (x_1, \ldots, x_\ell), \bar{z} = (z_1, \ldots, z_m)$, let $f(\bar{x}, \bar{z})$ be a single (finite) fold definition of $B$, and let $g(\bar{x}, \bar{z})$ be a single (finite) fold definition of $C$, then*

$$\hat{h}(\bar{x}, \bar{z}) = a_0 f(\bar{x}, \bar{z})^n + a_1 f(\bar{x}, \bar{z})^{n-1} g(\bar{x}, \bar{z}) + \ldots + g(\bar{x}, \bar{z})^n$$

*is a single (finite) fold definition of $A$.*

The proof of this proposition is the same as for Lemma 1.2.3 of [20].

3.2. **Pell Equations over Rings of Functions of Characteristic 0.** Next we take a look at the old workhorse of Diophantine definitions: the Pell equation. It turns out that in the context of defining integers over rings of functions this equation produces "naturally" single-fold definitions.

**Lemma 3.2.** *(Essentially Lemma 2.1 of* [5]*, or Lemma 2.2 of* [21] *) Let $Z$ be an integral domain of characteristic not equal to 2. Let $v \in Z[x], v, x$ transcendental over $Z$. Let $f_n(v), g_n(v) \in Z[x]$ be such that $f_n(v) - (v^2-1)^{1/2} g_n(v) = (v - (v^2-1)^{1/2})^n$. (In* [21] *there is a typographical error in this equation: the "square" is misplaced on the right-hand side.) In this case*

(1) *$deg(f_n) = n \cdot deg(v), deg(g_n) = (n-1) \cdot deg(v)$,*
(2) *$\ell$ dividing $n$ is equivalent to $g_\ell$ dividing $g_n$,*

(3) *The pairs $(\pm f_n, \pm g_n)$ with $n \in \mathbb{Z}$ are all the solutions to $f^2 - (v^2-1)g^2 = 1$ in $Z[x]$.*

Below we use the following notation.

**Notation 3.3.**

- Let $K$ denote a function field of characteristic 0 over the constant field $k$.
- Let $\mathscr{S} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ be a finite non-empty set of primes (or valuations) of $K$.
- Let $O_{K,\mathscr{S}} = \{x \in K \mid (\forall \mathfrak{p} \notin \mathscr{S}) \text{ ord}_{\mathfrak{p}} x \geq 0\}$ be the ring of $\mathscr{S}$-integers of $K$.
- For $D \in O_{K,\mathscr{S}}$ such that $D$ is not a square in $K$, let

$$H_{K,D,\mathscr{S}} = \{u - D^{1/2}v \mid u, v \in O_{K,\mathscr{S}} \;\&\; u^2 - Dv^2 = 1\}.$$

The lemma below explains the nature of invertible elements of $O_{K,\mathscr{S}}$.

**Lemma 3.4.** *Let $z \in O_{K,\mathscr{S}}$ be a unit of the ring. Then for any $\mathfrak{q} \notin \mathscr{S}$ we have that ord$_{\mathfrak{q}} z = 0$.*

*Proof.* Suppose $z$ is a unit of $O_{K,\mathscr{S}}$. Then $\frac{1}{z} \in O_{K,\mathscr{S}}$. Let $\mathfrak{q}$ be a prime of $K$ such that ord$_{\mathfrak{p}} z > 0$. Then ord$_{\mathfrak{p}} \frac{1}{z} < 0$. Consequently, $\mathfrak{q} \in \mathscr{S}$. □

The next proposition explains how to choose a parameter $a$ so that the solutions to the Pell equation satisfy certain conditions.

**Proposition 3.5.** *There exists $a \in O_{K,\mathscr{S}}$ satisfying the following conditions.*

1. *ord$_{\mathfrak{p}_1} a < -2^r$, where $r$ is a positive integer.*
2. *ord$_{\mathfrak{p}_i}(a-1) > 0$ and ord$_{\mathfrak{p}_i}(a-1)$ is odd for $i = 2, \ldots, s$.*
3. *$a - 1$ is not a unit of $O_{K,\mathscr{S}}$.*
4. *In $K(\sqrt{a^2-1})$, the $K$-prime $\mathfrak{p}_1$ factors as a product of two primes of $K(\sqrt{a^2-1})$ denoted by $\mathfrak{q}_\infty$ and $\mathfrak{q}$. In other words, in $K(\sqrt{a^2-1})$ we have that $\mathfrak{p}_1 = \mathfrak{q}_\infty \mathfrak{q}$.*
5. *The element $T = a - \sqrt{a^2-1}$ of $K(\sqrt{a^2-1})$ has a zero at $\mathfrak{q}$, a pole at $\mathfrak{q}_\infty$, and no other zeros or poles.*
6. *For $D = a^2 - 1$, we have that $H_{K,D,\mathscr{S}}$ modulo $\pm 1$ is a cyclic group generated by $a - D^{1/2}$.*
7. *For any non-zero integer $b$ we have that $a - \sqrt{a^2-1} - b$ is not a unit of $O_{K,\mathscr{S}}[\sqrt{a^2-1}]$.*
8. *Let $f_n, g_n$ be as in Lemma 3.2. Then $g_{-n} = -g_n$, $f_{-n} = f_n$, and*

$$g_n \equiv n \mod (a-1)$$

*in the ring $\mathbb{Z}[a]$. (Note that $f_n, g_n \in \mathbb{Z}[a]$.)*

*Proof.* The proof of this proposition is contained in [22], but we reproduce some parts of it here for the convenience of the reader.

Let $\mathfrak{t}$ be a prime of $K$ not in $\mathscr{S}$. Let $\mathscr{T} = \mathscr{S} \cup \{\mathfrak{t}\}$. By Lemma 3.2 of [22], there exists a $w \in O_{K,\mathscr{S}}$ such that ord$_{\mathfrak{p}_1} w = -2^s$ for some positive integer $r$ and ord$_{\mathfrak{a}} w = 1$ for all $\mathfrak{a} \in \mathscr{T} \setminus \{\mathfrak{p}_1\}$. Now let $a = w + 1$ and observe that ord$_{\mathfrak{p}_1} a = $ ord$_{\mathfrak{p}_1} w = -2^s$, and ord$_{\mathfrak{a}}(a-1) = 1$ for all $\mathfrak{a} \in \mathscr{T} \setminus \{\mathfrak{p}_1\}$. Further, $a - 1$ is not a unit of $O_{K,\mathscr{S}}$, by Lemma 6.13, since $a - 1$ has a zero at a prime not in $\mathscr{S}$. Thus (1) –(3) are satisfied.

Observe also, that, since ord$_{\mathfrak{a}} D = $ ord$_{\mathfrak{a}}(a^2-1) = $ ord$_{\mathfrak{a}}(a-1) = 1$ for primes $\mathfrak{a}$ in $\mathscr{T} \setminus \{\mathfrak{p}_1\}$, these primes ramify in the extension $K(D^{1/2})/K$ with ramification degree at least 2 by Corollary 2.2, and therefore there is only one prime in the extended field lying above each prime of $\mathscr{S} \setminus \{\mathfrak{p}_1\}$ by (2.1).

Let $\mathfrak{A}$ be a prime of $K(D^{1/2})$ such that $\text{ord}_{\mathfrak{A}}(x - D^{1/2}y) > 0$. Then $\text{ord}_{\mathfrak{A}}(x + D^{1/2}y) < 0$, and $\text{ord}_{\mathfrak{A}} 2x < 0$. Since $x \in O_{K,\mathscr{S}}$, we must conclude that $\mathfrak{A}$ lies above a prime in $\mathscr{S}$. Further, we note that $\varepsilon^{-1}$ is the conjugate of $\varepsilon$ over $K$. Therefore, $\text{ord}_{\mathfrak{A}}\varepsilon > 0$ implies $\text{ord}_{\bar{\mathfrak{A}}}\varepsilon^{-1} > 0$, where $\bar{\mathfrak{A}}$ is a conjugate ideal of $\mathfrak{A}$ over $K$. The conjugate ideal $\bar{\mathfrak{A}}$ must also be lying above the same $K$-prime $\mathfrak{a} \in \mathscr{S}$. If $\mathfrak{a}$ is ramified in the extension $K(D^{1/2})/K$, as we have discussed above, there is only one ideal above $\mathfrak{a}$ in the extended field. Hence $\bar{\mathfrak{A}} = \mathfrak{A}$, and we have a contradiction due to our assumption that $\text{ord}_{\mathfrak{A}}\varepsilon > 0$. The case of the negative order leads to a similar contradiction. Thus we conclude that for all $\mathfrak{a} \in \mathscr{S} \setminus \{\mathfrak{p}_1\}$ we have that $\text{ord}_{\mathfrak{A}}\varepsilon = 0$ for the prime $\mathfrak{A}$ lying above $\mathfrak{a}$ in the extension.

Since $H_{K,D,\mathscr{S}}$ does contain a non-constant element, e.g. $a - D^{1/2}$, we deduce that $a - D^{1/2}$ must have a zero and a pole at valuations lying above $\mathfrak{p}_1$. So the prime $\mathfrak{p}_1$ factors in $K(D^{1/2})$, i.e. it has at least two factors in the extended field. In the extension of degree 2, a prime of a smaller field can have at most two distinct factors in the bigger field by (2.1). Therefore, $\mathfrak{p}_1$ has exactly two distinct factors $\mathfrak{q}_\infty$ and $\mathfrak{q}$. Thus (4) is satisfied.

Without loss of generality we can assume that $\text{ord}_{\mathfrak{q}_\infty}(a - D^{1/2}) < 0$ and $\text{ord}_{\mathfrak{q}}(a - D^{1/2}) > 0$. As we noted above, the element $(a - D^{1/2})$ can have zeros or poles at primes lying above primes of $\mathscr{S}$ only. So, $(a - D^{1/2})$ has no other zeros or poles and (5) is satisfied.

We now consider a group homomorphism from $H_{K,D,\mathscr{S}}$ to $\mathbb{Z}$ sending an element $\varepsilon \in H_{K,D,\mathscr{S}}$ to its order at $\mathfrak{q}_\infty$. We claim the kernel of this map contains $\pm 1$ only. Indeed, suppose $\text{ord}_{\mathfrak{q}_\infty}\varepsilon = 0$. If $\varepsilon$ is not a constant, it must have a positive order at some valuation and a negative order at a different valuation. But, again by the discussion above, there is only one valuation left as a candidate for a zero and a pole of $\varepsilon$. This valuation is $\mathfrak{q}$. But it cannot be a zero and a pole of $\varepsilon$. Thus, $\varepsilon$ is a constant.

Next we observe that by Lemma 2.2 of [22], the only constants in $H_{K,D,\mathscr{S}}$ are $\pm 1$. So modulo $\pm 1$ it is the case that $H_{K,D,\mathscr{S}}$ is isomorphic to a subgroup of $\mathbb{Z}$. Thus, $H_{K,D,\mathscr{S}}$ modulo $\pm 1$ is cyclic. The fact that $H_{K,D,\mathscr{S}}$ is generated by $a - D^{1/2}$ modulo $\pm 1$ follows from Lemma 2.5 of [22]. Thus (6) is satisfied.

To show that $a - \sqrt{a^2 - 1} - b$ is not a unit of $O_{K,\mathscr{S}}[\sqrt{a^2 - 1}]$ for any non-zero integer $b$, we first rewrite $a - \sqrt{a^2 - 1} - b$ as $a - \sqrt{a^2 - 1} - 1 + c$, where $c$ is an integer not equal to 1. Next let $\mathfrak{A}$ be a prime of $K(D^{1/2})$ lying above some prime in $\mathfrak{a} \in \mathscr{T} \setminus \{\mathfrak{p}_1\}$. Then $\text{ord}_{\mathfrak{A}}(a - \sqrt{a^2 - 1} - 1) = 1$, since $\text{ord}_{\mathfrak{a}}(a - 1) = 1$ by construction and $\text{ord}_{\mathfrak{A}}(a - 1) = e(\mathfrak{A}/\mathfrak{a})\text{ord}_{\mathfrak{a}}(a - 1) = 2$ because $e(\mathfrak{A}/\mathfrak{a})$, the ramification degree of $\mathfrak{A}$ over $\mathfrak{a}$, is equal to 2. At the same time, $\text{ord}_{\mathfrak{a}}(a + 1) = \text{ord}_{\mathfrak{a}}(a - 1 + 2) = 0$ implying that $\text{ord}_{\mathfrak{a}}(a^2 - 1) = 1$, and taking the ramification into account, as above, we deduce that $\text{ord}_{\mathfrak{A}}\sqrt{a^2 - 1} = 1$. Hence $\text{ord}_{\mathfrak{A}}(a - \sqrt{a^2 - 1} - 1) = \min(\text{ord}_{\mathfrak{A}}(a - 1), \text{ord}_{\mathfrak{A}}(\sqrt{a^2 - 1})) = 1$. Note also that $\text{ord}_{\mathfrak{q}_\infty}(a - \sqrt{a^2 - 1} - 1) < 0$, and $\text{ord}_{\mathfrak{q}}(a - \sqrt{a^2 - 1} - 1) = 0$, since $\text{ord}_{\mathfrak{q}}(a - \sqrt{a^2 - 1}) > 0$.

Now let $\delta = a - \sqrt{a^2 - 1} - 1 + c$. If $\delta$ is a unit of $O_{K,\mathscr{S}}[\sqrt{a^2 - 1}]$, then either $\delta$ is a constant or all zeros and poles of $\delta$ are among $K(D^{1/2})$-primes lying above

$K$-primes in $\mathscr{S}$. First we note that $\text{ord}_{\mathfrak{q}_\infty}\delta < 0$, and hence $\delta$ is not a constant. Next we consider the case of $c = 0$. Let $\mathfrak{T}$ be the $K(D^{1/2})$-prime lying above the $K$-prime $\mathfrak{t} \in \mathscr{T} \setminus \mathscr{S}$. As we have discussed above, if $c = 0$, then $\text{ord}_{\mathfrak{T}}\delta = 1$, and $\delta$ is not a unit.

Suppose now that $c \neq 0, 1$ and $\delta$ is a unit. Given our assumptions on $c$, we know that $\text{ord}_{\mathfrak{A}}\delta = 0$ for all $\mathfrak{A}$ lying above a $K$-prime $\mathfrak{a} \in \mathscr{S} \setminus \{\mathfrak{p}_1\}$. Further, $\text{ord}_{\mathfrak{q}_\infty}\delta < 0$. Therefore the only prime that can possibly be a zero of $\delta$ is $\mathfrak{q}$. But $\text{ord}_{\mathfrak{q}}(a - \sqrt{a^2-1}) > 0$, and therefore $\text{ord}_{\mathfrak{q}}(a - \sqrt{a^2-1}) - 1 + c$, where $-1 + c$ is a non-zero constant, must be 0. Hence there is no valuation that can be a zero of $\delta$, and we arrive at a contradiction with our assumption that $\delta$ is a non-constant unit. Hence, (7) is satisfied.

Finally, (8) follows from Lemma 2.3 of [22].

□

**Remark 3.6.** Let $u, w \in O_{K,\mathscr{S}}$, let $a$ be as in Proposition 3.5. Finally assume $u^2 - (a^2-1)w^2 = 1$. Then what can we say about $u - \sqrt{a^2-1}w$? By Proposition 3.5, there exists $n \in \mathbb{Z}$ such that $u = \pm f_n, w = \pm g_n$, where

$$(a - \sqrt{a^2-1})^n = \varepsilon^n = f_n - \sqrt{a^2-1}g_n.$$

Thus, we have four possibilities:

$$\begin{aligned} u - \sqrt{a^2-1}w &= f_n - \sqrt{a^2-1}g_n = \varepsilon^n, n \in \mathbb{Z}_{\geq 0},\\ u - \sqrt{a^2-1}w &= f_n + \sqrt{a^2-1}g_n = \varepsilon^n, n \in \mathbb{Z}_{\leq 0},\\ u - \sqrt{a^2-1}w &= -f_n - \sqrt{a^2-1}g_n = -\varepsilon^n, n \in \mathbb{Z}_{\leq 0},\\ u - \sqrt{a^2-1}w &= -f_n + \sqrt{a^2-1}g_n = -\varepsilon^n, n \in \mathbb{Z}_{\geq 0}. \end{aligned}$$

Alternatively,

$$u - \sqrt{a^2-1}w = \pm\varepsilon^n, n \in \mathbb{Z}.$$

**Lemma 3.7.** *(Essentially Lemma 3.4 of* [22]*.) Let $R$ be any subring of $O_{K,\mathscr{S}}$ containing a local subring of $\mathbb{Q}$. (In particular, $R$ can be equal to $O_{K,\mathscr{S}}$.) Then there exists a subset $C$ of $R$ that contains only constants, includes $\mathbb{Z}$, and is single-fold Diophantine over $R$.*

*Proof.* We remind the reader that the set $\mathscr{S}$ contains $s$ primes. Let $\pi$ be the product of all non-invertible rational primes (or 1, if $R$ contains $\mathbb{Q}$), and let $C \subset R$ be the set of all elements $x \in R$ such that the following equations over $R$ have solutions in unknowns $j_1, \ldots, j_{s+1}$:

$$(3.3) \qquad \begin{cases} j_1(\pi x^2 + \pi + 1) = 1,\\ \ldots\\ j_{s+1}(\pi x^2 + (s+1)\pi + 1) = 1 \end{cases}$$

We claim that System (3.3) has solutions in $R$ only if $x$ is a constant, while conversely, if $x \in \mathbb{Z}$, these equations have solutions in $R$. Indeed, if $x$ is not a constant, neither are $\pi x^2 + \pi + 1, \ldots, \pi x^2 + (s+1)\pi + 1$. Therefore, since these elements are invertible in $O_{K,\mathscr{S}}$, they all must have zeros at valuations of $\mathscr{S}$ only by Lemma 3.4. However, these $s + 1$ elements do not share any zeros since their differences are constants, while there are only $s$ valuations in $\mathscr{S}$, the set of potential zeros for these elements. Thus, we have a contradiction stemming from our assumption that $x$ is not a constant.

The converse is obvious: if $x \in \mathbb{Z}$, then $\pi x^2 + \pi r + 1$ is invertible for each $r \in \mathbb{Z}$. Please note that given $x \in O_{K,\mathscr{S}}$, if System (3.3) has solutions, then these solutions are unique. □

**Notation 3.8.** Let $J(x)$ denote the system of equations (3.3).

We will use this system to give a single-fold Diophantine definition of $\mathbb{Z}$ over $O_{K,\mathscr{S}}$.

**Theorem 3.9.** *$\mathbb{Z}$ has a single-fold Diophantine definition over $O_{K,\mathscr{S}}$.*

*Proof.* There are several ways to state this proof. We choose the way that we will later use to produce a single-fold definition of exponentiation for $\mathbb{Z}$. Let $a \in O_{K,\mathscr{S}}$ be as in Proposition 3.5 and consider the following equations and conditions:

$$u^2 - (a^2-1)w^2 = 1; \tag{3.4}$$

$$c \equiv w \bmod (a-1) \text{ in } O_{K,\mathscr{S}}; \tag{3.5}$$

$$J(c). \tag{3.6}$$

Supposed now that Equations (3.4)–(3.6) are satisfied with variables ranging over $O_{K,\mathscr{S}}$. Then, by Proposition 3.5 and Lemma 3.2, $w = w_n \equiv n \bmod (a-1)$ for some $n \in \mathbb{Z}$. Thus, $c \equiv n \mod (a-1)$ in $O_{K,\mathscr{S}}$. Since $a-1$ is not a unit of $O_{K,\mathscr{S}}$, we have that $c-n$ is a constant with a zero at some valuation of $K$. Hence $c = n$.

Conversely, given $c = n \in \mathbb{Z}$, set $w = w_n$ and observe that all the equations are satisfied. Note also, that this is the only solution to the equations. □

**Notation 3.10.** Let $U(c,u,w)$ denote the system of equations (3.4)–(3.6).

We now give a single-fold Diophantine definition of exponentiation.

**Theorem 3.11.** *The following set has a single-fold Diophantine definition over $O_{K,\mathscr{S}}$:*

$$\{(b,c,d) \mid b,c,d \in \mathbb{Z}_{\neq 0}, d > 0, c = b^d\}.$$

*Proof.* Consider the following system of equations:

$$b \neq 0, b \neq \pm 1, \tag{3.7}$$

$$U(c, u_c, w_c). \tag{3.8}$$

$$U(b, u_b, w_b), \tag{3.9}$$

$$U(d, u_d, w_d), \tag{3.10}$$

(3.11)
$$\exists n \in \mathbb{Z}, x, y \in O_{K,\mathscr{S}}[\sqrt{a^2-1}] : (\varepsilon^n \neq \pm 1) \wedge (\pm\varepsilon^n - c = (\varepsilon - b)x) \wedge (d - \frac{\pm\varepsilon^n - 1}{\varepsilon - 1} = y(\varepsilon - 1)).$$

First of all, from Equations (3.7)– (3.10) we deduce that $b, c, d$ are integers and $b \neq \pm 1, 0$. Next we note that (3.11) implies that $n \neq 0$ and $(\varepsilon - 1)$ divides $\pm\varepsilon^n - 1$ in $O_{K,\mathscr{S}}$. Note that by Proposition 3.5, we also have that $\varepsilon - 1$ is not a unit of $O_{K,\mathscr{S}}$. If we choose the "minus" option in (3.11), then we have that $\varepsilon - 1$ divides $\varepsilon^n + 1$. Since $\varepsilon - 1$ divides $\varepsilon^n - 1$ and $\varepsilon^n + 1$ and $\varepsilon^n \pm 1 \neq 0$, it follows that $\varepsilon - 1$ divides $2$, and thus is a unit of $O_{K,\mathscr{S}}$. Hence the "minus" option cannot occur. Consequently, (3.11) can be rewritten as:

(3.12)

$$\exists n \in \mathbb{Z}, x, y \in O_{K,\mathscr{S}}[\sqrt{a^2-1}] : (\varepsilon^n \neq \pm 1) \wedge (\varepsilon^n - c = (\varepsilon - b)x) \wedge (d - \frac{\varepsilon^n - 1}{\varepsilon - 1} = y(\varepsilon - 1)).$$

From (3.12) we deduce that $\varepsilon^n - c \equiv 0 \bmod (\varepsilon - b)$ in $O_{K,\mathscr{S}}$. At the same time $\varepsilon^n \equiv b^n \bmod (\varepsilon - b)$ in $O_{K,\mathscr{S}}$. Therefore, $c \equiv b^n \bmod (\varepsilon - b)$. By Proposition 3.5 we conclude that $(\varepsilon - b)$ is not a unit, and therefore $b^n - c$ has a zero at a valuation of $K$. Since $b, c$ are constants, we must infer that $b^n = c$. Since $b \in \mathbb{Z}_{\neq 0, \pm 1}, c \in \mathbb{Z}$, we also must have that $n > 0$. At the same time, also from (3.12), we have that $d \equiv n \bmod (\varepsilon - 1)$ in $O_{K,\mathscr{S}}$. By the same argument as above we conclude that $d = n > 0$.

Conversely, assuming $b, c, d \in \mathbb{Z}, b \neq 0, \pm 1, d > 0, c = b^d$, it is easy to see that (3.11) can be satisfied with only one choice for the sign in front of $\varepsilon^n$.

The last equation (3.11) above has coefficients in $O_{K,\mathscr{S}}[\sqrt{a^2-1}]$, and variables $x, y$ ranging over the extended ring also. So to complete the proof we need to rewrite this equation so that the coefficents are in $O_{K,\mathscr{S}}$ and the variables take values in this ring also. Below we rewrite (3.11) as a system of equations over $O_{K,\mathscr{S}}$ with all variables ranging in $O_{K,\mathscr{S}}$. To make it easier to connect (3.11) with (3.13) we indicate in parenthesis the corresponding entry in (3.11).

(3.13)

$$\begin{cases} u^2 - (a^2-1)w^2 = 1 \, \text{(in other words, } \pm\varepsilon^n = u - \sqrt{a^2-1}w), \\ u - \sqrt{a^2-1}w - c = (a - \sqrt{a^2-1} - b)(x_1 - x_2\sqrt{a^2-1}), \\ \text{(in other words, } \pm\varepsilon^n - c = (\varepsilon - b)x), \\ d(a - \sqrt{a^2-1} - 1) - (u - \sqrt{a^2-1}w - 1) = (y_1 - \sqrt{a^2-1}y_2)(a - \sqrt{a^2-1} - 1)^2, \\ \text{(in other words, } d(\varepsilon - 1) - (\pm\varepsilon^n - 1) = y(\varepsilon - 1)^2). \end{cases}$$

Thus System (3.13), with all the variables ranging over $O_{K,\mathscr{S}}$, is equivalent to Conjunction (3.11). This concludes the proof of Theorem 3.11. □

**Notation 3.12.** For future reference we will denote the equations (3.7)–(3.10) together with (3.13) by

$$G(a, b, c, d, u, w, x_1, x_2, y_1, y_2).$$

**Corollary 3.13** (Single-fold definition of positive integers over $O_{K,\mathscr{S}}$)**.** *Let $a$ be as in Proposition 3.5, and let*

$$\textit{Plus} = \{d \in O_{K,\mathscr{S}} | \exists c, u, w, x_1, x_2, y_1, y_2 \in O_{K,\mathscr{S}} : G(a, 2, c, d, u, w, x_1, x_2, y_1, y_2)\}.$$

*Then Plus= $\mathbb{Z}_{>0}$, and this Diophantine definition is single-fold.*

*Proof.* Given Theorem 3.11, the only point that needs a proof is the single-fold property of the definition. Given a $d > 0$, to satisfy the system, we must have that

$$c = 2^d, u = f_d, w = g_d, \text{(in other words } u - \sqrt{a^2-1}w = \varepsilon^d),$$

$$x_1 - x_2\sqrt{a^2-1} = \frac{u - \sqrt{a^2-1}w - 2^d}{a - \sqrt{a^2-1} - 2}, \text{(in other words } \varepsilon^d - 2^d \equiv 0 \bmod (\varepsilon - 2)),$$

$$(y_1 - \sqrt{a^2-1}y_2)(a - \sqrt{a^2-1} - 1)^2 = d(a - \sqrt{a^2-1} - 1) - (u - \sqrt{a^2-1}w - 1),$$

$$\text{( in other words } d \equiv \frac{\varepsilon^d - 1}{\varepsilon - 1} \bmod (\varepsilon - 1)).$$

Thus the values of all variables are uniquely determined by $d$.

□

We also have another corollary to be used in Section 7.

**Corollary 3.14.** *The set* $\{(s, u_s, w_s) | s \in \mathbb{Z}_{>0}\}$ *is single-fold Diophantine over* $O_{K,\mathscr{S}}$*.*

*Proof.* Consider the set

$$\{(s, u, w) \in O^3_{K,\mathscr{S}} | \exists c, x_1, x_2, y_1, y_2 \in O_{K,\mathscr{S}} : G(a, 2, c, s, u, w, x_1, x_2, y_1, y_2)\}.$$

By the same argument as in the proof of Corollary 3.13, the set consists of all the triples in the required form, and given such a triple, the values of all the other variables are determined uniquely. □

Combining Theorem 3.9, Theorem 3.11, Corollary 3.13 with a result of Matiyasevich from [14] we now have the following theorem.

**Theorem 3.15.** *Every c.e. set of integers has a single-fold Diophantine definition over* $O_{K,\mathscr{S}}$*.*

*Proof.* The result of Matiyasevich discussed in the introduction shows that every c.e. set of integers has a single-fold definition using polynomial equations and equations of the form $y = 2^x$ for $x, y \in \mathbb{Z}_{>0}$. In other words, if $A$ is a c.e. subset of $\mathbb{Z}^r$, then $(a_1, \ldots, a_r) \in A$ if and only if the following system of equations and conditions can be satisfied over $\mathbb{Z}$ with a unique set of values for all variables with each $f_i$ being a polynomial with integer coefficients.

$$\begin{gathered} f_i(\bar{a}, z_{i,1}, \ldots, z_{i,r_i}, x_{i,1}, y_{i,1}, \ldots, x_{i,m_i}, y_{i,m_i}) = 0, i = 1, \ldots, s, \\ y_{i,j} > 0, x_{i,j} > 0, i = 1, \ldots, s, j = 1, \ldots, m_i, \\ y_{i,j} = 2^{x_{i,j}}, i = 1, \ldots, s, j = 1, \ldots, m_i. \end{gathered}$$

By Theorem 3.9, Theorem 3.11 and Corollary 3.13 we can add equations of the form $g(Y, X_1, \ldots X_r) = 0$ having solutions in $O_{K,\mathscr{S}}$ if and only if $Y \in \mathbb{Z}$, and for every $Y \in \mathbb{Z}$ there will be only one choice of values for $X_1, \ldots, X_r$ in $O_{K,\mathscr{S}}$. Further, we can add equations of the form $h(U, V, Y_1, \ldots, Y_k)$ having solutions in $O_{K,\mathscr{S}}$ if and only if $U, V \in \mathbb{Z}_{>0}, U = 2^V$ and with a unique set of values for $Y_1, \ldots, Y_K \in O_{K,\mathscr{S}}$. Thus, we can construct a single-fold definition of the set $A$ over $O_{K,\mathscr{S}}$. □

## 4. Single-Fold Diophantine Representations of C.E. Sets of Rational Integers over Polynomial Rings of Characteristic 0.

In this section we prove the analogue of Theorem 3.15, but for polynomial rings over arbitrary commutative integral domains with unity of characteristic 0. If the ring of constants contains $\mathbb{Q}$, then we can set $K$ to be the fraction field of the polynomial ring, let $\mathfrak{p}_1$ be the prime ideal of the valuation ring corresponding to the degree valuation and apply Theorem 3.15. So the only case that we need to consider is the situation where the ring of constants does not contain $\mathbb{Q}$. If the constant ring does not contain $\mathbb{Q}$, it can contain infinitely many non-invertible primes, and therefore we cannot use the definition of a constant set containing all integers from Lemma 3.7. For exactly the same reason, we cannot use multiplicative inverses to define the set of non-zero elements. Thus, we will have to modify some parts of the proof of Theorem 3.15.

First we need the following basic fact.

**Lemma 4.1.** *If $a, b$ are non-zero relatively prime integers, then $\frac{1}{b} \in \mathbb{Z}[\frac{a}{b}]$.*

*Proof.* Since $(a, b) = 1$ we have that for some $x_1, x_2 \in \mathbb{Z}$ it is the case that $ax_1+bx_2 = 1$. Thus $\dfrac{1}{b} = \dfrac{ax_1 + bx_2}{b} = x_1\dfrac{a}{b} + x_2 \in \mathbb{Z}[\dfrac{a}{b}]$.

□

Next we deal with the question of saying that an element is not 0.

**Lemma 4.2.** *Let $R$ be a ring of characteristic $0$ and $p$ a rational prime that does not have an inverse in the ring. In this case, there exists a set $A = A_p$ such that $0 \notin A$, $p\mathbb{Z} + 1 \subset A$, and if $px + 1 \in A \cap \mathbb{Z}$, then $x \in \mathbb{Z}$.*

*Proof.* Let $A = \{px + 1 \mid x \in R\} \subset R$. Then $0 \notin A$. Indeed, if $0 \in A$ then $\frac{1}{p} \in R$, and we have a contradiction. Suppose now that for some $x \in R$ we have that $px + 1 \in \mathbb{Z}$. We claim that $x \in \mathbb{Z}$. Observe that if $px + 1 \in \mathbb{Z}$ then $px = z \in \mathbb{Z}$ and $\frac{z}{p} = x \in R$. If $x \notin \mathbb{Z}$, then $(p, z) = 1$, and $p$ has an inverse in $R$ by Lemma 4.1, in contradiction of our assumptions. Finally, clearly $p\mathbb{Z} + 1 \subset A_p$. □

**Theorem 4.3.** *(Similar to Theorem 5.1 of* [21]*) If $Z$ is an integral domain of characteristic 0 and $x$ is transcendental over $Z$, then $\mathbb{Z}$ is single-fold Diophantine over $R = Z[x]$.*

*Proof.* As we explained above, without loss of generality, we can assume that $\mathbb{Q} \not\subset R$, and therefore, by Lemma 4.1, $R$ contains at least one non-inverted prime. Consider the following set of equations,

$$(f_i - \sqrt{(a^2x^2-1)}g_i) = (ax - \sqrt{(a^2x^2-1)})^i, i = 2, 3 \tag{4.14}$$

$$f^2 - (a^2x^2 - 1)g^2 = 1, \tag{4.15}$$

$$f - \sqrt{a^2x^2-1}g - 1 = (f_3\sqrt{a^2x^2-1}g_3 - 1)(z_1 - \sqrt{a^2x^2-1}z_2) \tag{4.16}$$

$$t|g_3g_2, \tag{4.17}$$

$$t \equiv g \mod g_3^2, \tag{4.18}$$

$$ax|f, \tag{4.19}$$

$$a = t/g_3, \tag{4.20}$$

We show that these equations can be satisfied with some values of variables

$$a \neq 0, f, g, f_2, g_2, f_3, g_3, t, z_1, z_2 \in Z[x]$$

only if we choose $a$ to be an odd integer.

Let $Q$ be the fraction field of $Z$. First, we would like to consider the polynomial ring $Q(x)$ as a ring of $\mathscr{S}$-integers, where $\mathscr{S}$ contains only one element: the prime corresponding to the degree valuation. We do this so that we can utilize some conclusions from Proposition 3.5. If we consider the Pell equation $f^2 - Dg^2 = 1$, where $D = A^2 - 1$ is not a square, in $Q[x]$ and $A \in Q[x] \setminus Q$, then, since $\mathscr{S}$ contains only one prime, we can conclude that by Proposition 3.5, all solutions of the equation will correspond to powers of $A - \sqrt{A^2 - 1}$. So unlike the case of $O_{K,\mathscr{S}}$, where $\mathscr{S}$ had more than one element, we do not need any extra assumptions on $A$.

Further, for any non-constant $A$, there exists a prime $\mathfrak{t}$ of $Q(x)$ corresponding to some irreducible polynomial and distinct from the degree valuation, such that $A - 1$ has a zero at $\mathfrak{t}$. The factor $\mathfrak{T}$ of this prime in $Q(x, \sqrt{A^2 - 1})$ will divide $\varepsilon - 1 = A - \sqrt{A^2 - 1} - 1$ as in the general case. Further, as in the general case, if $\delta$ is a unit of $Q[x, \sqrt{A^2 - 1}]$, then it has a non-zero valuation at primes of $Q(x, \sqrt{A^2 - 1})$ extending the degree valuation only. Thus, $\varepsilon - 1$ is not a unit no matter what non-constant $A$ we choose. Finally, if we choose $A \in Z[x]$, all solutions to the Pell equation will be contained in $Z[x]$.

Next we note that for any choice of $a \in Z[x] \setminus \{0\}$, we have that $a^2x^2 - 1 \notin \mathbb{Z}$. Indeed, if $a \in Z[x]$ and $a \neq 0$, then $\deg(a)$ as a polynomial in $x$ is bigger or equal to 0. Therefore, the degree of $a^2x^2 - 1$ is bigger or equal to 2. Thus, as discussed above, by Lemma 3.2 we have from (4.15) that $f = \pm f_n, g = \pm g_n$ for some $n \in \mathbb{Z}_{\geq 0}$. Alternatively, $g = g_m, m \in \mathbb{Z}$. Let $\varepsilon = ax - \sqrt{a^2x^2 - 1}$. Then $f - \sqrt{a^2x^2 - 1}g = \pm\varepsilon^m$ for some $m \in \mathbb{Z}$. (See Remark 3.6 for the discussion of signs.) Next, since $\varepsilon - 1$ is not a unit, we deduce that $\varepsilon^3 - 1$ is not a unit. So, from (4.16), as in the proof of Theorem 3.11, we conclude that $f - \sqrt{a^2x^2 - 1}g = \varepsilon^m$, $m = 3r, r \in \mathbb{Z}_{\neq 0}$. Further, from (5.33) we obtain that $f_1 | f_m$, implying that $m$ is odd. (From the binomial expansion, it is easy to see that $f_1$ divides $f_m$ in the polynomial ring only if $m$ is odd.) Hence, $r$ is odd. From Lemma 3.2 we also have that

$$(f_{3r} - \sqrt{(a^2x^2 - 1)}g_{3r}) = (ax - \sqrt{(a^2x^2 - 1)})^{3r} = (f_3 - \sqrt{(a^2x^2 - 1)}g_3)^r = (f_3 \pm \sqrt{(a^2x^2 - 1)}g_3)^{|r|}.$$

$$g_{3r} = \pm \sum_{|r|-i \text{ odd}} \binom{|r|}{i} f_3^i((ax)^2 - 1)^{(|r|-i-1)/2} g_3^{|r|-i},$$

where "$-$" corresponds to $r < 0$. Thus $g_{3r} \equiv r f_3^{|r|-1} g_3 \bmod g_3^2$. Additionally, we have that $f_3^2 \equiv 1 \bmod g_3^2$. Since $|r| - 1$ is even, we now deduce $g_{3r} \equiv r g_3 \bmod g_3^2$. Thus, we conclude using (4.18) that $t \equiv rg_3 \bmod g_3^2$ or equivalently

$$g_3^2 | (t - rg_3). \tag{4.21}$$

From (4.17) we have $t|g_3g_2$ so that $\deg(t) < 2\deg(g_3)$, and $\deg(t - rg_3) < \deg(g_3^2)$. Therefore (4.21) implies that $t - rg_3 = 0$, $a = t/g_3 = r$, that is, $a$ is an odd integer.

Conversely, suppose $r$ is an odd integer and let $a = r$. Then $t = ag_3 = rg_3$. To satisfy (4.15) and (4.16) we need to set $(f, g) = (f_m(ax), g_m(ax))$, where $m \neq 0, m \in \mathbb{Z}$. Further, (4.16) requires that $m \equiv 0 \bmod 3$. To satisfy (4.18), we need to arrange for $t \equiv g \bmod g_3^2$, or in other words, we need $ag_3 - g_m \equiv 0 \bmod g_3^2$ to be satisfied. As before, (5.33) implies $m$ is an odd number. So we have to set $m = 3r'$, where $r'$ is odd. Thus, again as above we have that $g_m \equiv r'g_3 \bmod g_3^2$. Therefore, we have to choose $r' \equiv r \bmod g_3$. But since both $r', r \in \mathbb{Z}$, and $g_3 \notin Z$, the only way to satisfy the equivalence is to set $r' = r$. Now (4.14)–(4.16), (4.18) and (5.33) are satisfied. Since $g_2(rx) = 2rx$, and we set $t = rg_3(rx)$, we can conclude that $t \Big| g_3(rx)g_2(rx)$, and (4.17) and (4.20) are satisfied. Observe, that given an odd integer $a$, the remaining variables have to take the values described above.

We now show how to state the assumption that $a \neq 0$. Let $p$ be a rational prime without a multiplicative inverse in $R$. We replace the condition $a \neq 0$ by $a = 2ps + 1, s \in R$. By Lemma 4.2, the added equation will imply that $a \neq 0$.

Now, if Equations (4.14)–(4.20) together with the new equation $a = 2ps + 1$ are satisfied, by Lemma 4.2, we conclude that $a = 2ps + 1$ is an odd integer, i. e. $a = 2u + 1$ for some $u \in \mathbb{Z}$. Therefore $2ps + 1 = 2u + 1$ or $sp = u \in \mathbb{Z}$. Since $ps \in \mathbb{Z}$, the only prime that can divide the denominator of $s$ is $p$. But by Lemma 4.1, we have that $p$ cannot appear in a reduced denominator of an element in $R$. Therefore, we conclude that $s \in \mathbb{Z}$. Hence, Equations (4.14)–(4.20) together with the new equation $a = 2ps + 1$ are satisfiable over $R$ if and only if $s \in \mathbb{Z}$.

□

**Notation 4.4.** We denote Equations (4.14) – (4.20), together with the equation $a = 2ps + 1$ by $F(a, x, f, g, f_2, g_2, f_3, g_3, t, p, s)$. Thus,

$$\mathbb{Z} = \{s \in Z[x] \mid F(a, x, f, g, f_2, g_2, f_3, g_3, t, p, s)\}.$$

In this formula $p$ is a fixed parameter corresponding to a prime not inverted in $R$.

In this section, as in the section concerning rings of $\mathscr{S}$-integers, we will need to know that for any $a \in R, b \in \mathbb{Z}_{\neq 0}$ we have that $\varepsilon^n - b = (ax - \sqrt{a^2x^2 - 1})^n - b$ is not a unit of $R[\sqrt{a^2x^2 - 1}]$. There is a similar statement in Proposition 3.5. The difference between that statement and the statement below is that over $O_{K,\mathscr{S}}$ we fixed $a$, while here $a$ ranges over $R$.

**Lemma 4.5.** *Let $a \in Z[x], b, n \in \mathbb{Z}, abn \neq 0$. Then we have that $\varepsilon^n - b$ is not a unit in $Z[x, \sqrt{a^2x^2 - 1}]$.*

*Proof.* Let $K$ be the fraction field of $R$. Let $f_n(ax) - \sqrt{a^2x^2 - 1}g_n(ax) = \varepsilon^n(ax) = \varepsilon^n$. The minimal polynomial of $\varepsilon^n$ over $Z[x]$ is of the form $X^2 - 2f_nX + 1$. Therefore, for any $b \in \mathbb{Z}$, we have that $\mathbf{N}_{K(\sqrt{a^2x^2-1})/K}(b - \varepsilon^n) = b^2 - 2f_nb + 1$. Here we note that the only units of $Z[x]$ are some elements of $Z$. So, if $b^2 - 2f_nb + 1 \notin Z$, then we conclude that $b^2 - 2f_n b + 1$ is not a unit. Since $f_n \notin Z, b \neq 0$, we conclude that $b^2 - 2f_n b + 1$ is not a unit in $Z[x]$, and, therefore, $\varepsilon - b$ is not a unit in $Z[x, \sqrt{a^2x^2 - 1}]$.

□

Now that we have a single-fold Diophantine definition of integers, we can produce a single-fold definition of non-zero integers, and then positive integers and exponentiation.

**Lemma 4.6.** *If $Z$ is an integral domain of characteristic 0 and $x$ is transcendental over $Z$, then $\mathbb{Z}_{\neq 0}$ is single-fold Diophantine over $R = Z[x]$.*

*Proof.* As above, without loss of generality, we can assume that there exists a prime $p \in \mathbb{Z}$, not invertible in $R$. Let $s \in R$ be given and consider the following sequence of equations:

$$F(a, x, f, g, f_2, g_2, f_3, g_3, t, p, s), \tag{4.22}$$

$$F(\hat{a}, x, \hat{f}, \hat{g}, \hat{f}_2, \hat{g}_2, \hat{f}_3, \hat{g}_3, \hat{t}, p, \hat{s}), \tag{4.23}$$

$$u^2 - (x^2 - 1)w^2 = 1, \tag{4.24}$$

$$u - (x^2 - 1)^{1/2}w - \hat{s} \equiv 0 \bmod (x - (x^2 - 1)^{1/2} - p), \tag{4.25}$$

$$\hat{s} \equiv 0 \bmod p \tag{4.26}$$

$$s - \frac{u - w\sqrt{x^2 - 1} - 1}{x - \sqrt{x^2 - 1} - 1} = (z_1 - z_2\sqrt{x^2 - 1})(x - \sqrt{x^2 - 1} - 1). \tag{4.27}$$

From (4.22) via Notation 4.4, we conclude that $s, \hat{s} \in \mathbb{Z}$. If we set $\varepsilon = \varepsilon(x) = (x - \sqrt{x^2 - 1})$, then by Lemma 3.2 and Remark 3.6 we deduce from (4.24) that $u - \sqrt{x^2 - 1}w = \pm\varepsilon^m, m \in \mathbb{Z}$. By Lemma 4.5 we also know that $\varepsilon - p$ is not a unit of $R$. Suppose $m = 0$. Then $\pm\varepsilon^m = \pm 1$ and consequently $\hat{s} \equiv \mp 1$ to satisfy (4.25). In this case however, we get a contradiction with (4.26). Thus, $m \neq 0$, and $s = m$, while $\hat{s} = p^m$.

To see that this definition is single-fold, let $s \in R$. Then by Theorem 4.3, there is a unique set of values that can be taken by variables

$$a, f, g, f_2, g_2, f_3, g_3, t, \hat{a}, \hat{f}, \hat{g}, \hat{f}_2, \hat{g}_2, \hat{f}_3, \hat{g}_3, \hat{t} \in R$$

for any given value of $s$ and $\hat{s}$. Finally, given $s \in \mathbb{Z}_{\neq 0}$, Equation (4.24) forces $u - w\sqrt{x^2 - 1} = (x - \sqrt{x^2 - 1})^s$, $\hat{s} = p^s$. Thus, $u, w$ are also determined uniquely. □

The next theorem will show existence of single-fold definitions for all c.e. subsets of rational integers in polynomial rings. The proofs will proceed via Diophantine definitions of exponentiation with arguments similar to the ones used in the proof of Theorem 3.11.

**Notation 4.7.** Let $\hat{U}(s, \ldots)$ denote Equations (4.22)-(4.27). So that over $R$

$$\mathbb{Z}_{\neq 0} = \{s | \exists \ldots . \hat{U}(s, \ldots)\},$$

and this definition is single-fold.

**Theorem 4.8.** *Let $Z$ be an integral domain of characteristic 0, and assume $x$ is transcendental over the fraction field of $Z$ and $\mathbb{Q} \not\subset R := Z[x]$. Then every c.e. set of rational integers has a single-fold Diophantine definition over $R$.*

*Proof.* We can now proceed as in the case of the rings of integral functions. Consider the following system of equations:

$$\hat{U}(c, \ldots). \tag{4.28}$$

$$\hat{U}(b, \ldots), \tag{4.29}$$

$$\hat{U}(d, \ldots), \tag{4.30}$$

$$\exists n \in \mathbb{Z}, x, y \in R[\sqrt{a^2-1}] : (\pm\varepsilon^n - c = (\varepsilon - b)x) \ \& \ (d - \frac{\pm\varepsilon^n - 1}{\varepsilon - 1} = y(\varepsilon - 1)). \tag{4.31}$$

By the same argument, as in the case of integral functions, this system gives a single-fold definition of the set

$$\hat{G} = \{(b, c, d) \in \mathbb{Z}^3_{\neq 0}, d > 0, c = b^d\}.$$

Finally, if we set $b = 2$, we get the set $\hat{G} = \{(2, c, d) \in \mathbb{Z}^3_{>0} | c = 2^d\}$. Using Matiyasevich's result, we now conclude that the assertion of the theorem holds by the same argument as in the proof of Theorem 3.15. □

Finally, putting the result above together with our observation about the case when $\mathbb{Q} \subset R$, we obtain the following result.

**Theorem 4.9.** *Let $Z$ be an integral domain of characteristic 0, and assume $x$ is transcendental over the fraction field of $Z$. Then every c.e. set of rational integers has a single-fold Diophantine definition over $R = Z[x]$.*

## 5. Finite-fold Diophantine Definition of C.E. Sets of Polynomial Rings over Totally Real Fields of Constants

So far we have produced single-fold definitions of certain c.e. subsets of a ring. We now construct our first examples of rings where all c.e. sets have finite-fold definitions. To do this we combine the arguments above with the proof of Zahidi from [26] showing that over a polynomial ring with coefficients in a ring of integers of a totally real number field, all c.e. sets were Diophantine. Zahidi's result was in turn an extension of a result of Denef from [6] in which the coefficients of the polynomial ring came from $\mathbb{Z}$.

Any discussion of c.e. sets of a polynomial ring and a ring of integral functions to be discussed later, must of course involve some discussion of indexing of the ring. In other words we will need a bijection from a ring into the positive integers such that given a "usual" presentation of a polynomial (or an integral function in the future) we can effectively compute the image of this polynomial (or this integral function), and conversely, given a positive integer, we can determine what polynomial (or integral function) was mapped to it. For a discussion of an effective indexing map in the case of a rational function field we refer the reader to the paper of Zahidi. A discussion of indexing for function fields can be found in [20].

In this paper we will assume that such an indexing is given and, following Zahidi, will denote it by $\theta$ going from positive integers to polynomials. Below we describe the rest of our notation and assumptions.

**Notation and Assumptions 5.1.**

- Let $k$ be a totally real number field.
- Let $O_k$ be the ring of integers of $k$.
- Let $\alpha_1, \ldots, \alpha_r$ be an integral basis of $O_k$ over $\mathbb{Z}$.
- Let $\theta : \mathbb{Z}_{>0} \longrightarrow O_k[X]$ be the effective bijection discussed above.
- Define $P_n(X) := \theta(n)$.
- For each $n \in \mathbb{Z}$ define $U_n(X)$ and $W_n(X)$ in $O_k[X]$ (uniquely) to satisfy
$$U_n(X) - (X^2-1)^{1/2}W_n(X) = (X-(X^2-1)^{1/2})^n.$$

As we indicated before, our intention is to follow the plan laid out by Zahidi and Denef, just making sure that all the definitions in that plan are finite-fold. This plan entails showing (a) that all c.e. subsets of $\mathbb{Z}$ are (finite-fold) Diophantine over the polynomial ring in question and (b) that the indexing is (finite-fold) Diophantine or, in other words, the set
$$\{(n, P_n(X)) | n \in \mathbb{Z}_{>0}\}$$
is (finite-fold) Diophantine over $O_k[X]$. Zahidi provides a brief argument in his paper that we apply to our situation, given that we have a finite-fold way of combining equations, to see that (a) and (b) imply the following theorem.

**Theorem 5.2.** *Let $Z$ be the ring of integers in a totally real number field $k$. Let $\theta$ be an effective indexing of $Z[X]$; then every $\theta$-computably enumerable relation over $Z[X]$ is a finite-fold Diophantine relation over $Z[X]$.*

Thus we concentrate on proving the following proposition.

**Proposition 5.3.** *The set*
$$\{(n, P_n(X)) | n \in \mathbb{Z}_{>0}\}$$
*is finite-fold Diophantine over $O_k[X]$.*

The lemmas below constitute a proof of the proposition. Like the earlier authors, we will make use of a theorem of Y. Pourchet representing positive-definite polynomials as sums of five squares. We start with an auxiliary lemma.

**Lemma 5.4.** *Fix a positive integer $n$ and $n+1$ algebraic integers $\{a_0, a_1, \ldots, a_n\} \subset O_k$. Then there is exacly one polynomial $G(X) \in O_k[X]$ of degree at most $n$ such that $G(i) = a_i, i = 0, \ldots, n$.*

*Proof.* Let $G(X) = b_0 + b_1X + \ldots + b_nX^n$ and observe that our requirement on the values of $G(X)$ implies that the coefficients of $G$ must be the solutions of a linear system $A\bar{b} = \bar{a}$, where $A = (c_{i,j}), c_{i,j} = i^j, i, j = 0, \ldots, n, (\bar{b})^t = (b_0, \ldots, b_n), (\bar{a})^t = (a_0, \ldots, a_n)$. (Here "$t$" denotes transposition.) Note that $\det(A)$ is a van der Monde determinant, and therefore not equal to 0. Thus, the system has a unique solution. □

**Corollary 5.5.** *Let $h$ be a fixed positive integer, let $F(X) \in O_k[X]$, let $\Omega$ be the set of all embeddings $\sigma$ of $k$ into its algebraic closure, let*

$$B_h = \{G(X) \in O_k[X] | (\textbf{\textit{deg}}(G) \leq \textbf{\textit{deg}}(F)) \wedge (\forall \sigma \in \Omega, \forall i = 0, \ldots, \textbf{\textit{deg}}(F) - 1 : |\sigma(G(i))| \leq h)\}.$$

*Then $B_h$ is finite.*

*Proof.* Let $V$ be the set of elements $v$ of $O_k$ such that for any $\sigma \in \Omega$ we have that $|\sigma(v)| < h$. Let $m = [k : \mathbb{Q}]$, and let $v \in V$. Then any coefficient of the monic irreducible polynomial of $v$ over $\mathbb{Q}$ must be an integer of absolute value less than or equal to $\max(mh, mh^m)$. Thus $V$ is a finite set.

Now let $G(X) \in B_h$. Then $\deg(G) \leq \deg(F) = n$. Next we note that $G(i) \in V$ for $i = 0, \ldots, n-1$. Thus, $(G(0), \ldots, G(n-1)) \in V^n$. So that the set of possible $n$-tuples of values $\{(G(0), \ldots, G(n-1))\}$ is finite. By Lemma 5.4, for each $n$-tuple $(a_0, \ldots, a_n)$, there exists only one polynomial of degree less than or equal to $n$ such that $G(i) = a_i$. Thus we now conclude that the number of polynomials $G$ in $B_h$ is finite. □

**Definition 5.6.**
- If $F$ is a polynomial in $O_k[X]$, then $F$ is *positive-definite* on $k$ (denoted by Pos($F$)) if and only if $\sigma(F(a)) \geq 0$ for all $a \in k$ and for all real embeddings $\sigma$ of $k$ into its algebraic closure.
- If $F$ is a polynomial in $O_k[X]$, then $F$ is *strictly positive-definite* on $k$ if and only if $\sigma(F(t)) > 0$ for all $t \in k$ and for all real embeddings $\sigma$ of $k$ into its algebraic closure.
- Let $\text{Pos}_2(g, F) \subset \mathbb{Z} \times O_k[X]$, contain pairs $(g, F)$ such that $g^2F = F_1^2 + \ldots + F_5^2$ for some $F_1, \ldots, F_5 \in O_k[X]$.

**Lemma 5.7.** *For any $F \in O_k[X]$ we have that Pos($F$) if and only if there exists $g \in \mathbb{Z}$ such that Pos$_2(g, F)$.*

*Proof.* Suppose there exists $g \in \mathbb{Z}$ such that $g^2F = F_1^2 + \ldots + F_5^2$ for some $F_1, \ldots, F_5 \in O_k[X]$. Then, clearly Pos($F$) is true. Conversely, suppose Pos($F$) is true. Then by a theorem of Pourchet (see [16]), we have that $F = G_1^2 + \ldots + G_5^2$, for some $G_1, \ldots, G_5 \in k[X]$. Let $g \in \mathbb{Z}$ be such that for any coefficient $a$ of $G_1, \ldots, G_5$, we have that $ga \in O_k$. Then Pos$_2(g, F)$. □

**Lemma 5.8.** *The relation Pos$_2$ is finite-fold Diophantine over $O_k[X]$.*

*Proof.* By definition of Pos$_2$ we have that Pos$_2(g, F)$ if and only if there exist $F_1, \ldots, F_5 \in O_k[X]$ such that

$$g^2F = F_1^2 + \ldots + F_5^2. \tag{5.32}$$

We now show that for a given $g$ and $F$, there can be only finitely many solutions to (5.32). First of all, the degrees of $F_1, \ldots, F_5$ are bounded by the degree of $F$. Secondly, observe that for $i = 0, \ldots, \deg(F) - 1, j = 1, \ldots, 5$ we have that $|\sigma(F_j(i))|^2 \leq g^2|\sigma(F(i))|$ for all embeddings $\sigma \in \Omega$. (See Corollary 5.5 for definition of $\Omega$.) Let $h = \max\{g\sqrt{|\sigma(F(i))|}\}$, where $\max$ is taken over $i = 0, \ldots, \deg(F) - 1$ and all $\sigma \in \Omega$. Then if (5.32) holds, we have that $F_1, \ldots, F_5 \in B_h$. By Corollary 5.5, we have that $B_h$ is finite. □

**Definition 5.9.** The relation $\text{Par}(n, b, c, d, g, v_1, \ldots, v_r)$ on the rational integers is defined to be the conjunction of the following conditions:

(1) $n \in \mathbb{Z}_{\geq 1}$, ($\theta(n) = P_n \in O_k[T]$);
(2) $b, c, d, g \in \mathbb{Z}_{\geq 0}, v_1, \ldots, v_r \in \mathbb{Z}$;
(3) $d = \deg(P_n)$;
(4) $c$ is the smallest possible non-negative integer such that that $W_{d+2}^2 + c - P_n^2 - 1$ is strictly positive;
(5) $g$ is the smallest possible positive integer such that $\text{Pos}_2(g, W_{d+2}^2 + c - P_n^2 - 1)$.
(6) $\forall x \in \mathbb{Z}:$ if $0 \leq x \leq d$ then $W_{d+2}(x) \leq b$;
(7) $P_n(2b + 2c + d) = v_1\alpha_1 + \ldots + v_r\alpha_r$.

**Lemma 5.10.** *Par is a recursive relation on integers.*

*Proof.* Given our assumption that $\theta(n)$ is effective, that is we can effectively determine the degree and coefficients of $P_n$, the first three conditions can be checked algorithmically over $\mathbb{Z}$. So, we may start with describing an algorithm for computing $c$ and $g$.

We start by calculating $c$. For every $\sigma : k \to \mathbb{R}$ we will determine the smallest non-negative integer $c_\sigma$ such that $\sigma(W_{d+2}^2 - P_n^2 - 1) + c_\sigma > 0$ for all values of the variable. Then we will set $c = \max_\sigma\{c_\sigma\}$.

We compute $c_{\text{id}}$ first. The degree of $P_n$ is $d$, and the degree of $W_{d+2}$ is $d + 1$ by Lemma 3.2. (We can compute $W_{d+2}$ algorithmically, since $(U_{d+2} - \sqrt{x^2 - 1}W_{d+2}) = (x - \sqrt{x^2 - 1})^{d+2}$). Thus the polynomial $W_{d+2}^2 - P_n^2 - 1$ is of degree $2(d + 1)$ with a leading coefficient equal to the square of an element of $k \subset \mathbb{R}$, and therefore has an absolute minimum. By Corollary 8.4, there is an algorithm to verify whether this minimum is positive. If the answer is "yes", then we set $c_{\text{id}} = 0$. If the answer is "no", then we consider $W_{d+2}^2 - P_n^2 - 1 + 1 = W_{d+2}^2 - P_n^2$ and check whether $W_{d+2}^2 - P_n^2$ is strictly positive for all values of the variable. If the answer is "yes", we set $c_{\text{id}} = 1$. If the answer is "no", we consider $W_{d+2}^2 - P_n^2 + 1$, etc. If $\mu < 0$ is the minimum value of $W_{d+2}^2 - P_n^2 - 1$, then the process will terminate in at most $[\mu] + 1$ steps.

We now calculate $c_\sigma$ for some $\sigma \neq \text{id}$. We note that since the leading coefficient of $W_{d+2}^2 - P_n^2 - 1$ is a square, the leading coefficient of $\sigma(W_{d+2}^2 - P_n^2 - 1)$ is positive. Thus, we can proceed as in the case of $\sigma = \text{id}$.

We can now determine $g$. By a result of Pourchet cited above, we can write the polynomial

$$W_{d+2}^2 - P_n^2 + c - 1 = G_1^2 + \ldots + G_5^2, \tag{5.33}$$

where $G_i \in k[T]$ and $\deg(G_i) \leq \frac{d+1}{2}$. Since $k$ is a finite extension of $\mathbb{Q}$ and we can assume without loss of generality that we are given the minimal irreducible polynomial of the generator over $\mathbb{Q}$, we can construct a computable presentation of the field $k$. Therefore, we can also produce an effective listing of all polynomials over $k$ of degree less or equal to $\frac{d+1}{2}$. Since we have a computable presentation of $k$, given a quintuple of polynomials $G_1, \ldots, G_5$ we can effectively determine whether (5.33) holds. Hence we have an effective way of searching for polynomials over $k$ of degree less than or equal to $\frac{d+1}{2}$ to satisfy (5.33).

By examining coefficients of these polynomials, we can determine an integer $g_{\max}$ such that $g_{\max}G_i \in O_k[T]$. The value $g_{\max}$ is an upper bound on the set of $g$'s we have to search to find $g_{\min}$. The number $g_{\min}$ will satisfy the following equation for some $F_1, \ldots, F_5 \in O_k[x]$:

$$g_{\min}^2(W_{d+2}^2 - P_n^2 + c - 1) = F_1^2 + \ldots + F_5^2.$$

Then $\deg(F_s) \leq \frac{1}{2}\deg(W_{d+2}^2 - P_n^2 + c - 1)$, and for $i = 0, \ldots, d+1$ and all embeddings $\sigma$ of $k$ into $\mathbb{R}$, we have that

$$|\sigma(F_s(i))| \leq g_{\min}^2(W_{d+2}^2(i) - \sigma(P_n^2(i)) + c - 1) \leq g_{\max}^2(W_{d+2}^2(i) - \sigma(P_n^2(i)) + c - 1),$$

where $s = 1, \ldots, 5$. By Corollary 5.5, there are only finitely many polynomials $F$ satisfying these inequalities, and we can determine them all. Once we determine all possible $F_1, \ldots, F_5$, starting with $g = 1$ and continuing through $g_{\max}$, we can check if any quintuple of possible polynomials works with any particular $g$, and thus determine $g_{\min}$.

We now consider Condition (6). By checking all values of $W_{d+2}(x)$ for $x \in \mathbb{Z}, x \in \{1, \ldots, d\}$, we can determine the maximum value of the set. Finally, to determine $v_1, \ldots, v_r$, we can start running through all linear combinations with integer coefficents of the basis vectors until we hit $P_n(2b + 2c + d)$.

□

The final piece of proof comes from the lemma below, taken almost verbatim from Zahidi's paper.

**Lemma 5.11.** *For any $n \in \mathbb{Z}_{>0}$ we have that $F \in O_k[x] \wedge F = P_n$ if and only if $\exists b, c, d, g, v_1, \ldots, v_r \in O_k[x]$ :*

(1) *Par$(n, b, c, d, g, v_1, \ldots, v_r)$;*

(2) *Pos$_2(g, (W_{d+2}^2 + c - F^2 - 1))$;*

(3) *$F(2b + 2c + d) = v_1\alpha_1 + \ldots + v_r\alpha_r$.*

*Proof.* Suppose $F = P_n$ for some natural number $n$. Then one can easily find natural numbers $b, c, d, g$ and rational integers $v_1, \ldots, v_r$ such that the relation (1) is satisfied. Part (2) of the lemma can be satisfied because $\deg(P_n) < \deg(W_{d+2})$. Further, (3) will be satisfied by satisfying Par$(n, b, c, d, g, v_1, \ldots, v_r)$, because $F = P_n$.

Conversely suppose Conditions (1)-(3) are satisfied for some natural numbers $c, d, n, b, g$ and integers $v_1, \ldots, v_r$. In this case we have to prove that $F = P_n$. From conditions (1) and (3) it follows that

$$(F - P_n)(2b + 2c + d) = 0.$$

Thus, if $F \neq P_n$, there is some $S \in O_k[x] \neq 0$ such that

$$F - P_n = (x - 2b - 2c - d)S.$$

Now by Condition (2), it is the case that $F$ has degree at most $d + 1$, while $P_n$ has degree $d$ (by Condition (1)), and hence, $S$ has degree at most $d$. So for some integer $u$ with $0 \leq u \leq d$, we have $S(u) \neq 0$. Now for at least one real embedding $\sigma$ we have

$$|\sigma((F - P_n)(u))| = |(2b + 2c + d - u)||\sigma(S(u))| \geq 2b + 2c,$$

(since $u \leq d$ and the fact that given an algebraic integer $a$ in a totally real number field, $a \neq 0$, there is at least one real embedding such that $|\sigma(a)| \geq 1$). At the same time, again by Condition (2) of the lemma and by Part (6) of the definition of the relation Par, for any real embedding $\sigma$ we have, for all integers $x$ with $0 \leq x \leq d$ :

$$|\sigma(F(x))| \leq |\sigma(F(x)^2 + 1)| \leq W_{d+2}^2(x) + c < b + c,$$

and

$$|\sigma(P_n(x))| \leq |\sigma(P_n^2(x) + 1)| \leq W_{d+2}^2(x) + c < b + c,$$

and hence

$$|\sigma((F - P_n)(x))| < 2b + 2c,$$

leading to a contradiction. □

The last lemma completes the proof of Proposition 5.3 and Theorem 5.2.

One reason for our emphasis on finite-fold Diophantine definitions is that they allow us to determine the difficulty of deciding whether a polynomial has infinitely many solutions in a given ring $S$, an infinite version of Hilbert's Tenth Problem:

$$HTP^{\infty}(S) = \bigcup_n \{f \in S[X_1, \ldots, X_n] \ : \ (\exists^{\infty}(x_1, \ldots, x_n) \in S^n) \ f(x_1, \ldots, x_n) = 0\}.$$

The following corollary is a good example of the connection between these topics: Theorem 5.2 actually proves that for the rings involved, $HTP^{\infty}$ has the greatest complexity possible.

**Corollary 5.12.** *Let $R$ be the ring of integers in a totally real number field $k$. Assume $R[T]$ has an effective indexing $\theta$ with domain $\mathbb{N}$ for which $\theta^{-1}(0)$ is decidable. Then, for some fixed $n \in \mathbb{N}$, the set of polynomials in $n$ variables over $R[T]$ with infinitely many solutions there,*

$$HTP_n^{\infty}(R[T]) = \{f \in R[T][X_1, \ldots, X_n] \ : \ (\exists^{\infty}(x_1, \ldots, x_n) \in (R[T])^n) \ f(x_1, \ldots, x_n) = 0\},$$

*is $\Pi_2^0$-complete, and thus computably isomorphic to $\overline{\emptyset''}$, the complement of the Turing jump of the Halting Problem.*

*Proof.* The assumption that $\theta^{-1}(0)$ is decidable allows us to build an effective injective index, so assume that $\theta$ itself is injective. By Theorem 5.2, there is a polynomial $g(E, Y, Z_1, \ldots, Z_m)$ over $R[T]$ such that, for all $(e, y) \in \mathbb{N}^2$, if $\varphi_e(y)$ fails to halt, then $g(e, \theta(y), \vec{Z})$ has no solution in $R[T]$; whereas if $\varphi_e(y)$ does halt, then $g(e, \theta(y), \vec{Z})$ has at least one solution in $R[T]$, but only finitely many. It follows that, for each fixed $e$, $g(e, Y, \vec{Z})$ has infinitely many solutions in $R[T]$ if dom$(\varphi_e)$ is infinite, but only finitely many if dom$(\varphi_e)$ is finite. It is well known that the set **Inf** of indices $e$ for which $\varphi_e$ has infinite domain is a $\Pi_2^0$-complete set ([24], Theorem IV.3.2), computably isomorphic to $\overline{\emptyset''}$, and we have just described a $1$-reduction from **Inf** to $HTP_n^{\infty}(R[T])$, by $e \mapsto g(e, Y, \vec{Z})$. On the other hand, $HTP_n^{\infty}(R[T])$ itself is $\Pi_2^0$, hence $1$-reducible to **Inf**, so by Myhill's Theorem (see [24, I.5.4]), the two are computably isomorphic. □

The computability-theoretic notation used here is standard; e.g. see [24]. Computable isomorphism is the strongest equivalence in general use in computability, so the corollary gives a very precise measurement of the complexity of $HTP_n^\infty(R[T])$. The value of $n$ is simply one greater than the least number $m$ of variables required for a polynomial $g$ giving a finite-fold Diophantine definition of the Halting Problem in $R[T]$. Notice that we not only have proven the $\Pi_2^0$-completeness of $HTP^\infty(R[T])$, the general question of whether a polynomial has infinitely many solutions in $R[T]$, but in fact have established $\Pi_2^0$-completeness for its restriction $HTP_n^\infty(R[T])$ to polynomials with at most $n$ variables.

## 6. Defining Valuation Rings over Function Fields of Characteristic 0

In this section we give an existential definition of valuation rings for function fields of characteristic 0 over some classes of fields of constants including all number fields. More specifically, we will assume the constant field $k$ to be a field algebraic over $\mathbb{Q}$ with an embedding into a finite extension $M$ of $\mathbb{Q}_p$ for some odd rational prime $p$ or into $\mathbb{R}$ (making $k$ formally real). Note that number fields satisfy these assumptions on $k$.

The method we use below is extendible to a much larger class of fields of characteristic 0 and to higher transcendence degree fields of positive characteristic. We intend to describe these extensions in future papers.

We now state the two main theorems of the section.

**Theorem 6.1.** *Let $k$ be a field algebraic over $\mathbb{Q}$ and such that $k$ has an embedding into a field $M$, a finite extension of $\mathbb{Q}_p$ for some odd prime $p$. Let $K$ be a function field over $k$, and let $\mathfrak{u}$ be a (function field) prime of $K$. Then the set $\{f \in K : \text{ord}_{\mathfrak{u}} f \geq 0\}$ is Diophantine over $K$.*

**Theorem 6.2.** *Let $k$ be a field algebraic over $\mathbb{Q}$ and such that $k$ has an embedding into $\mathbb{R}$. Let $K$ be a function field over $k$, and let $\mathfrak{u}$ be a prime of $K$ such that its residue field is embeddable into $\mathbb{R}$. (For example, $\mathfrak{u}$ can be a prime of odd degree.) Then the set $\{f \in K : \text{ord}_{\mathfrak{u}} f \geq 0\}$ is Diophantine over $K$.*

### 6.1. Replacing a given field by its finite extension.

For technical reasons that will become clear below it is often convenient to work in a finite extension of the given field. The following lemmas explain why replacing a field by its finite extension does not materially change the nature of definable sets. That is, if a certain kind of a set is definable in a finite extension, then this type of sets is definable over the original field. The first lemma describes a general property of Diophantine definitions under finite extensions.

**Lemma 6.3.** *Let $F_2/F_1$ be a finite field extension. Let $A \subset F_2$ and assume $A$ is Diophantine over $F_2$. Then $A \cap F_1$ is Diophantine over $F_1$.*

*Proof.* The proof follows from Lemma 2.1.17 of [20] and the fact that $F_2 \leq_{Dioph} F_1$. (See Definition 2.1.5 of [20]). □

The next lemma describes a relation between the order of an element of a function field at a prime and the order of this element at a factor of the prime in a finite extension. (We remind the reader that prime factorization in finite extensions and ramification degree are discussed in Section 2.)

**Lemma 6.4.** *Let $\hat{K}$ be a finite extension of a function field $K$, let $\hat{\mathfrak{q}}$ be a prime of $\hat{K}$ above a prime $\mathfrak{q}$ of $K$, and let $A$ be the set of all elements of $\hat{K}$ with non-negative order at $\hat{\mathfrak{q}}$. Assume further that $A$ is Diophantine over $\hat{K}$. Then $A \cap K$ is Diophantine over $K$ and consists of all elements of $K$ with non-negative order at $\mathfrak{q}$.*

*Proof.* Let $f \in K$. Then $\text{ord}_{\hat{\mathfrak{q}}} f = \dfrac{1}{e}\text{ord}_{\mathfrak{q}} f$, where $e = e(\hat{\mathfrak{q}}/\mathfrak{q})$ is the ramification degree of $\hat{\mathfrak{q}}$ over $\mathfrak{q}$. Therefore, $\text{ord}_{\hat{\mathfrak{q}}} f \geq 0$ if and only if $\text{ord}_{\mathfrak{q}} f \geq 0$. Thus, $f \in A \cap K$ if and only if $\text{ord}_{\mathfrak{q}} f \geq 0$. Finally, by Lemma 6.3, we have that $A \cap K$ is Diophantine over $K$. □

**Remark 6.5.** If the constant field $k$ has an embedding into a finite extension of $\mathbb{Q}_p$, the same is true of any finite extension of $k$.

In view of Lemma 6.4 and Remark 6.5, we can assume that if $k$ has an embedding into a finite extension of $\mathbb{Q}_p, p > 2$, then $k$ has no real embeddings. (For example, we can adjoin $i$ to the original field.)

6.2. **Using quadratic forms to pick out elements of $K$ of even order at a degree 1 prime.** The next lemma will be a key to distinguishing elements with an even order at a given prime $\mathfrak{T}$ of the function field $K$ from elements with an odd order at $\mathfrak{T}$. The prime $\mathfrak{T}$ in question will be assumed to be of degree 1, so that its residue field is isomorphic to the field of constants $k$ of our function field $K$. The degree 1 assumption also implies that for every $x \in K$ with $\text{ord}_{\mathfrak{T}} x \geq 0$ there exists a constant $c \in k$ such that $\text{ord}_{\mathfrak{T}}(x - c) > 0$. The quadratic form that will do the job will have its coefficients in the constant field and will be anisotropic over the constant field. An anisotropic form does not have any non-trivial zeros.

**Proposition 6.6.** *Let $k$ be any field of characteristic 0 such that the following form:*

$$X^2 - aY^2 - bZ^2 + abW^2 \tag{6.1}$$

*is anisotropic over $k$ for some values $a, b \in k$. If $K$ is a function field over $k$, $\mathfrak{T}$ is a prime (or a valuation) of $K$ of degree 1 and $h \in K$ is such that $\text{ord}_{\mathfrak{T}} h$ is odd, then the equation*

$$X^2 - aY^2 - bZ^2 + abW^2 = h \tag{6.2}$$

*has no solution $(X, Y, Z, W)$ in $K$.*

*Proof.* Assume the opposite and observe that due to the fact that function field valuations are non-archimedean and $\text{ord}_{\mathfrak{T}} h$ is odd,

$$2\min(\text{ord}_{\mathfrak{T}} X, \text{ord}_{\mathfrak{T}} Y, \text{ord}_{\mathfrak{T}} Z, \text{ord}_{\mathfrak{T}} W) < \text{ord}_{\mathfrak{T}} h.$$

Next let $U \in \{X, Y, Z, W\}$ be such that $\text{ord}_{\mathfrak{T}} U = \min\{\text{ord}_{\mathfrak{T}} X, \text{ord}_{\mathfrak{T}} Y, \text{ord}_{\mathfrak{T}} Z, \text{ord}_{\mathfrak{T}} W\}$ and divide every variable in (6.2) by $U^2$

$$\left(\frac{X}{U}\right)^2 - a\left(\frac{Y}{U}\right)^2 - b\left(\frac{Z}{U}\right)^2 + ab\left(\frac{W}{U}\right)^2 = \frac{h}{U^2}. \tag{6.3}$$

Observe that $\frac{h}{U^2}$ has a zero at $\mathfrak{T}$, while at least one of $\left\{\frac{X}{U}, \frac{Y}{U}, \frac{Z}{U}, \frac{W}{U}\right\}$ is equal to 1. Thus considering (6.3) mod $\mathfrak{T}$, taking into account that $\mathfrak{T}$ is a degree 1 prime, we conclude that the form (6.1) is isotropic over $k$ in contradiction of our assumption. □

6.2.1. *Replacing the field $M$ by the completion of $k$ under the $p$-adic valuation.* Since $k$ is embeddable into a finite extension $M$ of $\mathbb{Q}_p$, we can identify $k$ with a subfield of $M$. Since $M$ is a finite extension of $\mathbb{Q}_p$, there is a unique extension of the $p$-adic valuation to $M$ and $M$ is complete under this extended valuation. Let $v$ be the extension of the $p$-adic valuation to $M$. Let $R_v$ be the valuation ring of $v$. Let $\mathfrak{p}$ be the prime ideal of $R_v$ containing all $M$-elements with positive valuation. Let $F_{\mathfrak{p}} \cong R_v/\mathfrak{p}R_v$ be the residue field of $\mathfrak{p}$. Since $M$ is complete under $v$, we must have $\mathbb{Q}_p \subseteq k_{\mathfrak{p}} = k_v \subseteq M$, where $k_{\mathfrak{p}} = k_v$ is the completion of $k$ in the $\mathfrak{p}$-adic or, alternatively, $v$-adic metric. Thus, we can assume, without loss of generality, that $M = k_{\mathfrak{p}}$.

6.3. **Constructing a form anisotropic over $k$.** First of all, we note that if our quadratic form is anisotropic over $k_{\mathfrak{p}}$, then it is anisotropic over $k$. We also know that a form (6.1) is anisotropic over $k_{\mathfrak{p}}$ precisely when $\text{ord}_{\mathfrak{p}}a = 0$, $a$ is not a square in $k_{\mathfrak{p}}$, and $\text{ord}_{\mathfrak{p}}b$ is odd or $\text{ord}_{\mathfrak{p}}b = 0$, $b$ is not a square in $k_{\mathfrak{p}}$, and $\text{ord}_{\mathfrak{p}}a$ is odd. This will be shown in Lemmas 6.11 and 6.12. So our first task is to show that such a pair $(a, b)$ exists in $k^2$.

Since we don't know much about $k$ besides the fact that it is algebraic over $\mathbb{Q}$ and $[k_{\mathfrak{p}} : \mathbb{Q}_p]$ is finite, it would help us in the future, if we could find a pair $(a, b) \in H^2$, where $H$ is a specific *number field* contained in $k$. Obviously, any number field containing $H$ will work too.

First, we note that we can find a number field inside $k$ such that its completion under the restriction of $v$ to this number field is as large as possible.

**Lemma 6.7.** *As above, let $v$ be the extension of the $p$-adic valuation on $\mathbb{Q}_p$ to $k$, $R_v$ the valuation ring of $v$ and $\mathfrak{p}$ the maximal ideal of the valuation ring. Then there exist a number field $H \subset k$ such that the completion of $H$ under $\mathfrak{p}_H = \mathfrak{p} \cap H$ is equal to $k_{\mathfrak{p}}$.*

*Proof.* First we note that for any number field $H \subset k$, we have that $\mathbb{Q}_p \subseteq H_{\mathfrak{p}_H} \subseteq k_{\mathfrak{p}}$, and the assumption that $[k_{\mathfrak{p}} : \mathbb{Q}_p] < \infty$ implies that $[k_{\mathfrak{p}} : H_{\mathfrak{p}_H}] < \infty$.

We now proceed in two steps. First, we will show that there exists a number field $U_f \subset k$ such that $f(\mathfrak{p}/\mathfrak{p}_{U_f}) = 1$, where $\mathfrak{p}_{U_f} = \mathfrak{p} \cap U_f$. Next we will show that there exists a number field $U_e$ such that $e(\mathfrak{p}/\mathfrak{p}_{U_e}) = 1$, where $\mathfrak{p}_{U_e} = \mathfrak{p} \cap U_e$. Finally, we will set $H$ to be any number field containing $U_fU_e$.

Let $U$ be a field contained in $k$. Then $R_v \cap U$ is the valuation ring of the valuation $v_U$ corresponding to the restriction of $v$ to $U$. Similarly, if $\mathfrak{p}$ is the maximal ideal of $R_v$, then $\mathfrak{p}_U = U \cap \mathfrak{p}$ is the maximal ideal of $R_{v_U}$. Finally, the residue field $F_{\mathfrak{p}}$ of $\mathfrak{p}$ is an extension of $F_{\mathfrak{p}_U}$, the residue field of $\mathfrak{p}_U$.

Let $F_{\mathfrak{p}_{k_{\mathfrak{p}}}}$ be the residue field of the extension of $v$ to $k_{\mathfrak{p}}$. By assumption, $[k_{\mathfrak{p}} : \mathbb{Q}_p] < \infty$. So, by Proposition 2.6 the degree $[F_{\mathfrak{p}_{k_{\mathfrak{p}}}} : \mathbb{F}_p]$, where $\mathbb{F}_p$ is a field of $p$ elements, is finite, and thus $F_{\mathfrak{p}_{k_\mathfrak{p}}}$ is a finite field also. Since $k_\mathfrak{p}$ is the completion of $k$ under the metric induced by $v$, we have that $F_{\mathfrak{p}_{k_\mathfrak{p}}} \cong F_\mathfrak{p}$, by Proposition 2.4. Hence $F_\mathfrak{p}$ is also finite. Thus, $[F_\mathfrak{p} : F_{\mathfrak{p}_U}] < \infty$.

Suppose now that $U$ is a number field contained in $k$. By the arguments above $F_\mathfrak{p}/F_{\mathfrak{p}_U}$ is a finite field extension of a finite degree. Thus, it is simple. Let $\alpha$ generate $F_\mathfrak{p}$ over $F_{\mathfrak{p}_U}$. Since $\alpha \in F_\mathfrak{p}$, there exists $x \in k$ such that the residue class of $x$ is $\alpha$. We can now set $U_f = U(x)$.

Since $[k_\mathfrak{p} : \mathbb{Q}_p] < \infty$, by Proposition 2.6, we have that $e(\mathfrak{p}/p)$ is finite. Further, $k_\mathfrak{p}$ is a discrete valuation field and therefore contains an element $\beta$ with $v(\beta) = 1$. Since $k_\mathfrak{p}$ is a completion of $k$ under $v$, there exists an element $\gamma \in k$ such that $\text{ord}_{\mathfrak{p}_{k_\mathfrak{p}}}(\gamma - \beta) > 1$. Then

$$\text{ord}_{\mathfrak{p}_{k_\mathfrak{p}}}(\gamma) = \text{ord}_{\mathfrak{p}_{k_\mathfrak{p}}}(\gamma - \beta + \beta) = \min(\text{ord}_{\mathfrak{p}_{k_\mathfrak{p}}}(\gamma - \beta), \text{ord}_{\mathfrak{p}_{k_\mathfrak{p}}}(\beta)) = \text{ord}_{\mathfrak{p}_{k_\mathfrak{p}}}\beta = 1.$$

Let $U_e = Q_p(\gamma)$ and let $H = U_f(\gamma)$. We claim that $k_\mathfrak{p}$ is not ramified over $H_{\mathfrak{p}_H}$. Indeed, we have that

$$1 = \text{ord}_\mathfrak{p}\gamma = e(\mathfrak{p}/\mathfrak{p}_H)\text{ord}_{\mathfrak{p}_H}(\gamma).$$

Thus, $e(\mathfrak{p}/\mathfrak{p}_H) = 1$. Also, by construction $F_\mathfrak{p} \cong F_{\mathfrak{p}_H}$. Thus, $f(\mathfrak{p}/\mathfrak{p}_H) = 1$. By Proposition 2.6, we can now conclude that $[k_\mathfrak{p} : k_{\mathfrak{p}_H}] = 1$. □

Next we show that the elements $a, b$ needed to construct an anisotropic quadratic form can be found in the number field $H$ discussed above.

**Lemma 6.8.** *There exists a number field $H \subseteq k$ containing algebraic integers $a, b$ such that $a$ is not a square in $k_\mathfrak{p}$, ord$_\mathfrak{p}a = 0$, and ord$_\mathfrak{p}b$ is odd.*

*Proof.* Let $H \subseteq k$ be a number field such that, using the same notation as above, we have $H_{\mathfrak{p}_H} \cong k_\mathfrak{p}$. This congruence implies the residue fields of $\mathfrak{p}_{k_\mathfrak{p}}$ and $\mathfrak{p}_H$ are the same and are both finite. Now let $\gamma \in H$ be such that $\text{ord}_\mathfrak{p}(\gamma) = 0$, and $\gamma$ is not a square modulo $\mathfrak{p}$ in $k$. Such an element $\gamma$ exists in $H$, because not all elements of a finite field $F_\mathfrak{p} \cong F_{\mathfrak{p}_H}$ are squares of other elements of the field. By construction, the number field $H$ contains an element $a$ such that $a \equiv \gamma \mod \mathfrak{p}$. Further, by the Strong Approximation Theorem (see page 239 of [8]) any residue class of the prime $\mathfrak{p}_H$ contains algebraic integers. Therefore, we can assume $a \in O_H$, the ring of integers of $H$.

To show the existence of $b \in O_H$ such that ord$_\mathfrak{p}b$ is odd, it is enough to find an element in $O_H$ such that $\text{ord}_{\mathfrak{p}_H}b = \text{ord}_\mathfrak{p}b = 1$. The existence of such an element follows from the fact that the $\mathfrak{p}_H$ corresponds to a discrete valauation. □

**Remark 6.9.** We note here that once we found a number field $H$ with requisite $a$ and $b$, any extension of $H$ will also work. In the future $H$ will be any number field contained in $k$ and containing $a, b$ and the coefficients of a polynomial under consideration.

**Remark 6.10.** In what follows we will need one more requirement to impose on $a$. We will need $a \equiv 1 \mod 4$. This requirement is compatible with the requirement of $a$ not being a square in $F_\mathfrak{p}$ by the Strong Approximation Theorem (see page 239 of [8]).

6.3.1. *Taking a closer look at the quadratic form $X^2 - aY^2 - bZ^2 + abW^2$ over $k$ and over $K$.*

**Lemma 6.11.** *If $a$ is not a square in $k$, then the form* (6.1) *is isotropic over $k$ if and only if there exists $y \in k(\sqrt{a})$ such that $\mathrm{N}_{k(\sqrt{a})/k}(y) = b$.*

*Proof.* Suppose we have a non-trivial representation of 0 by the form (6.1). Then without loss of generality, we can assume that $Z$ and $W$ are not simultaneously 0. Otherwise, we are looking at the equation

$$X^2 - aY^2 = 0, \tag{6.4}$$

while $a$ is not a square in $k$. The only solution to (6.4) is $X = Y = 0$. So we get a trivial representation of 0.

Assuming that $Z$ and $W$ are not simultaneously 0 and we have a non-trivial representation of 0 by the form (6.1), we note that $Z^2 - aW^2 \neq 0$, and we can rewrite the equation as

$$\frac{X^2 - aY^2}{Z^2 - aW^2} = b$$

or

$$\exists y \in k(\sqrt{a}) : b = N_{k(\sqrt{a})/k}(y). \tag{6.5}$$

Conversely, suppose (6.5) is true. Then $b = U^2 - aV^2$, where either $U \neq 0$, or $V \neq 0$. Thus we have that $U^2 - aV^2 - b = 0$. Let $X = U, Y = V, Z = 1, W = 0$, and we have a non-trivial representation of 0 by the form (6.1) over $k$.

□

**Lemma 6.12.** *Let $H \subset k$ be a number field. Let $a, b \in O_H$ be such that ord$_{\mathfrak{p}}a = 0$, $a$ is not a square in $k_{\mathfrak{p}}$ and ord$_{\mathfrak{p}}b$ is odd. (Such a number field $H$ and elements $a, b \in H$ exist by Lemma 6.8.) Then* (6.1) *is anisotropic over $k$ and $k_{\mathfrak{p}}$.*

*Proof.* Suppose (6.1) is isotropic. Then by Lemma 6.11, we have that (6.5) is true. Since $a$ is not a square in $k_{\mathfrak{p}}$, $\mathrm{ord}_{\mathfrak{p}}a = 0$ and $\mathfrak{p}$ is not a dyadic prime, we have that by Proposition 2.3, the extension $k_{\mathfrak{p}}(\sqrt{a})/k_{\mathfrak{p}}$ is an unramified extension of degree 2 of $\mathfrak{p}$-adically complete fields. If $\mathfrak{t}$ is the prime of $k_{\mathfrak{p}}(\sqrt{a})$ above $\mathfrak{p}$, then by Proposition 2.6, the relative degree $f(\mathfrak{t}/\mathfrak{p})$ of $\mathfrak{t}$ over $\mathfrak{p}$ is 2. Thus, by Proposition 2.1

$$\mathrm{ord}_{\mathfrak{p}} N_{k(\sqrt{a})/k}(y) = f(\mathfrak{t}/\mathfrak{p}) \mathrm{ord}_{\mathfrak{t}} y \equiv 0 \bmod 2.$$

But ord$_{\mathfrak{p}}b$ is odd. So (6.5) cannot hold, and the form (6.1) is anisotropic. □

6.4. **How to make a quadratic form isotropic.** In this section we discuss the sufficient conditions for making a quadratic form isotropic over a number field.

**Lemma 6.13.** *Let $H$ be a number field. Let $\mathfrak{q}$ be any prime of $H$ (not necessarily equal to $\mathfrak{p}$, a prime lying above $p$ in $H$ and the prime lying above $p$ in $k_{\mathfrak{p}}$). Let $a, b \in H$ be units at $\mathfrak{q}$ (ord$_{\mathfrak{q}}a$ = ord$_{\mathfrak{q}}b = 0$). Assume further that $a \equiv 1 \bmod 4$. Then in $H_{\mathfrak{q}}$, the completion of $H$ under a $\mathfrak{q}$-adic metric, the form* (6.1) *is isotropic.*

*Proof.* If $\mathfrak{q}$ is not dyadic, and $a$ is a unit at $\mathfrak{q}$, then $\mathfrak{q}$ is unramified in the extensions $H(\sqrt{a})/H$ and $H_{\mathfrak{q}}(\sqrt{a})/H_{\mathfrak{q}}$, by Proposition 2.3. If $\mathfrak{q}$ is a dyadic prime, then given our assumption that $a \equiv 1 \bmod 4$, we also have that $\mathfrak{q}$ is unramified in the extensions

$H(\sqrt{a})/H$ and $H_{\mathfrak{q}}(\sqrt{a})/H_{\mathfrak{q}}$ by Corollary 2.9. Further, since $b$ is a unit at $\mathfrak{q}$ also, it is a norm in the extension of $H_{\mathfrak{q}}(\sqrt{a})/H_{\mathfrak{q}}$, by Proposition 3.11 of [9]. Hence (6.5) can be solved in $H_{\mathfrak{q}}$. □

Next we observe that $b$ does not have to be a unit at $\mathfrak{q}$ to be an $H_{\mathfrak{q}}(\sqrt{a})$ norm. It is enough for $b$ to have an even order.

**Corollary 6.14.** *Let $\mathfrak{q}, a, b, H$ be as above, but assume $a$ is a unit at $\mathfrak{q}$ while $\text{ord}_{\mathfrak{q}}b$ is even. Then in $H_{\mathfrak{q}}$ the form* (6.2) *is isotropic.*

*Proof.* Let $\pi$ be a local uniformizing parameter with respect to $\mathfrak{q}$ in $H$ (i.e. $\text{ord}_{\mathfrak{q}}\pi = 1$). If $\text{ord}_{\mathfrak{q}}b$ is even, then we can replace $b$ in the quadratic form by $\hat{b} = \pi^{2s}b$, where $s \in \mathbb{Z}$ and $\text{ord}_{\mathfrak{q}}\pi^{2s} = -\text{ord}_{\mathfrak{p}}b$, without changing the status of the form with respect to being isotropic or anisotropic. Observe that $\hat{b}$ is a unit at $\mathfrak{q}$, and the corollary now follows from Lemma 6.13. □

To explain how we will make use of the conditions for isotropy described above, we prove the following proposition.

**Proposition 6.15.** *Let $H$ be a number field without any real embeddings. Assume that for some $a, b \in H$, $a \equiv 1 \bmod 4$ we have that the form* (6.1) *is anisotropic. Then the following statements are true.*

(1) *There exist finitely many non-dyadic $H$-primes $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ such that the form is anisotropic over $H_{\mathfrak{a}_i}$.*
(2) *For each $\mathfrak{a}_i$ such that the form is anisotropic over $H_{\mathfrak{a}_i}$ we have that either $a$ is not a square in $H_{\mathfrak{a}_i}$ and $\text{ord}_{\mathfrak{a}_i}b$ is odd, or vice versa.*
(3) *Let $F$ be a finite extension of $H$ where each $\mathfrak{a}_i$ ramifies with even ramification degree. Then* (6.1) *is isotropic over $F$.*

*Proof.* Since $H$ does not have any real embeddings, if the form (6.1) is isotropic in $H_{\mathfrak{t}}$ for every prime $\mathfrak{t}$ of $H$, then by the Hasse-Minkowski Theorem (Theorem 27.2 of [19]) the form would be isotropic over $H$.

Further, for all but finitely many primes $\mathfrak{a}$ we have that both $a$ and $b$ are units, and therefore $\mathfrak{a}$ is not ramified in the extension $H(\sqrt{a})/H$ by Proposition 2.3 when the prime $\mathfrak{a}$ is not dyadic. If $\mathfrak{a}$ is dyadic then given that $a \equiv 1 \bmod 4$, we have that $\mathfrak{a}$ does not ramify in the extension $H(\sqrt{a})/H$ by Corollary 2.2. Hence $b$ is an $H(\sqrt{a})$-norm by Proposition 3.11 of [9]. Therefore, there are only finitely many completions where the form can be anisotropic.

Let $\mathfrak{A}_i$ be a prime above $\mathfrak{a}$ in $F$. Then $\text{ord}_{\mathfrak{A}_i}a$ is even and $\text{ord}_{\mathfrak{A}_i}b$ is even. So by the Corollary 6.14, the form is isotropic over $F_{\mathfrak{A}_i}$. Now if $\mathfrak{B}$ lies above a prime $\mathfrak{b}$ such that the form was isotropic over $H_{\mathfrak{b}}$, then, since $F_{\mathfrak{B}}$ is an extension of $H_{\mathfrak{b}}$, the form is isotropic over $F_{\mathfrak{B}}$. Hence, in $F$ the form is isotropic locally at all primes and therefore is isotropic over $F$. □

6.5. **Representing polynomials of even degree by quadratic forms: the $p$-adic case.** Before tackling all functions in $K$ of even order at a given *function field* prime $\mathfrak{T}$, we learn how to represent polynomials of even degree, where the degree valuation is the restriction of the function field valuation associated to $\mathfrak{T}$ to a rational function field. As we will see later, that will be enough to represent all other functions of $K$ of even order at $\mathfrak{T}$.

The key to representing polynomials by quadratic forms is the following proposition due to Y. Pourchet (see [16], Proposition 3) concerning representation of polynomials by quadratic forms over rational function fields.

**Proposition 6.16.** *Let $k$ be a field of characteristic $\neq 2$. Let $a, b \in k, f \in k[T]$, where $T$ is transcendental over $k$. Then there exist $X, Y, W, Z \in k[T]$ such that $f = X^2 - aY^2 - bZ^2 + abW^2$ if and only if the following conditions are satisfied*

- *For every prime factor $p(T)$ of $f(T)$ over $k$ of odd multiplicity, we have that the form is isotropic in the residue field of $k(T)$ modulo $p(T)$.*
- *The form represents the leading coefficient of $f(T)$ over $k$.*

Since the form (6.1) is anisotropic over $k$, it is clear that it will not represent all polynomials of even degree. For example, if the polynomial is a product of an even number of linear factors, it will not be represented by the form. So, given a polynomial of even degree we have to modify it without changing its degree, so that the modified polynomial is irreducible and adjoining a root of this polynomial to $k$ will generate an even degree extension of $k$ where the quadratic form becomes isotropic. Pourchet's proposition implies the quadratic form will represent every such polynomial.

At the same time, since our modification does not change the degree, the modified odd degree polynomial will not be represented by our quadratic form by Proposition 6.6. Our first step is to describe a type of polynomial producing the extensions we need.

**Lemma 6.17** (Essentially Eisenstein Irreducibility Criteria). *Let $H, \mathfrak{q}$ be as above. Let $a_0, \dots, a_m \in H$ be such that*

1. *$\text{ord}_{\mathfrak{q}} a_m = 0$,*
2. *$\text{ord}_{\mathfrak{q}} a_i \geq r > 1$, for $i = 1, \dots, m-1$,*
3. *$\text{ord}_{\mathfrak{q}} a_0 = r - 1 > 0$ with $(m, r-1) = 1$.*

*Let*

$$f(T) = a_m T^m + a_{m-1} T^{m-1} + \dots + a_0 \in H[T]$$

*In this case $f(T)$ is irreducible over $H_{\mathfrak{q}}$ and adjoining a root of $f(T)$ produces a totally ramified extension of $H_{\mathfrak{q}}$.*

*Proof.* Let $\alpha$ be a root of $f(T)$ in the algebraic closure of $H_{\mathfrak{q}}$. Let $\mathfrak{Q}$ be a prime above $\mathfrak{q}$ in $H_{\mathfrak{q}}(\alpha)$. If $\text{ord}_{\mathfrak{Q}} \alpha \geq 0$, then, since $\text{ord}_{\mathfrak{q}} a_m = \text{ord}_{\mathfrak{Q}} a_m = 0$, we have that

$$\text{ord}_{\mathfrak{Q}} \alpha^m = \text{ord}_{\mathfrak{Q}}(-a_{m-1}\alpha^{m-1} - \dots - a_1\alpha - a_0).$$

Let $e = e(\mathfrak{Q}/\mathfrak{q})$ be the ramification degree of $\mathfrak{Q}$ over $\mathfrak{q}$, and note that for $i = m-1, \dots, 1$ we have that

$$\text{ord}_{\mathfrak{Q}}(a_i\alpha^i) \geq e \cdot \text{ord}_{\mathfrak{q}} a_i \geq er > e(r-1) = e \cdot \text{ord}_{\mathfrak{q}} a_0.$$

Thus,

$$\text{ord}_{\mathfrak{Q}} \alpha^m = \text{ord}_{\mathfrak{Q}}(-a_{m-1}\alpha^{m-1} - \dots - a_1\alpha - a_0) = \min_{i=0,\dots,m-1}(\text{ord}_{\mathfrak{Q}} a_i\alpha^i) = e \cdot \text{ord}_{\mathfrak{q}} a_0 = e(r-1)$$

Since $(r-1, m) = 1$, we conclude that $e = m$, and the polynomial is irreducible.

Suppose now $\text{ord}_{\mathfrak{Q}}\alpha < 0$. Then for any $i = 1, \ldots, m-1$ we have

$$\text{ord}_{\mathfrak{Q}}(a_m\alpha^m) = \text{ord}_{\mathfrak{Q}}(\alpha^m) < \text{ord}_{\mathfrak{Q}}(\alpha^i) < \text{ord}_{\mathfrak{Q}}a_i\alpha^i.$$

Therefore,

$$e(r-1) = \text{ord}_{\mathfrak{Q}}a_0 = \text{ord}_{\mathfrak{Q}}(-a_m\alpha^m - a_{m-1}\alpha^{m-1} - \ldots - a_1\alpha) = m \cdot \text{ord}_{\mathfrak{Q}}(\alpha),$$

so that once again we have that $e = m$, and $f(T)$ is irreducible.

Finally we also note that the polynomial produces a totally ramified extension for $\mathfrak{q}$, since the ramification degree of $\mathfrak{Q}$ over $\mathfrak{q}$ is equal to the degree of the extension.

□

6.5.1. *Finding a convenient rational subfield.* Our next goal is to find a suitable rational function field contained in $K$ to make a transition from polynomials of even degree to functions of even order at $\mathfrak{T}$ easier. Essentially we need to decide what element $T \in K$ will generate a good rational function field $k(T)$.

One of the issues to consider is the ramification degree of $\mathfrak{T}$ over $k(T)$. If the ramification is even, then a polynomial of odd degree in $k(T)$ can have even order at $\mathfrak{T}$. Fortunately, such a situation is not difficult to avoid. All we need is an element $T$ with an odd degree pole at $\mathfrak{T}$. Additionally, to isolate the order at $\mathfrak{T}$ we do not want the degree valuation of $k(T)$ to have more than one extension to $K$. So what we need is an element $T$ of $K$ such it has an odd degree pole at $\mathfrak{T}$ and no other poles. The next lemma establishes existence of such an element of $K$.

**Lemma 6.18.** *For any valuation $\mathfrak{T}$ of $K$, for all sufficiently large $s > 0$, there exists $T \in K$ such that $\mathfrak{T}$ is the only valuation where $T$ has a pole, and $\text{ord}_{\mathfrak{T}}T = -3^s$.*

*Proof.* One can use the same proof as in Lemma 3.6 of [22], except that one should replace $2$ by $3$. □

**Lemma 6.19.** *Let $\mathfrak{T}$ and $T$ be as above. Then for any $f \in k[T]$ we have that $\text{ord}_{\mathfrak{T}}f$ is even if and only the degree of $f$ is even in $k(T)$.*

*Proof.* Observe that the degree valuation in $k(T)$ is the only valuation where $T$ has a pole in $k(T)$. Thus, if a valuation $\mathfrak{T}$ is an extension of the degree valuation to $K$, then $\text{ord}_{\mathfrak{T}}T < 0$ in $K$. But $T$ has only one pole in $K$. Therefore, $\mathfrak{T}$ is the only valuation of $K$ extending the degree valuation of $k(T)$ to $K$. Further, $\text{ord}_{\mathfrak{T}}T = e \cdot \deg(T)$, where $e$ is the ramification degree of $\mathfrak{T}$ over the degree valuation. By (2.1), we have that $e(\mathfrak{T}/\deg)f(\mathfrak{T}/\deg) = 3^{-s}$. Since $\mathfrak{T}$ is of degree 1, its residue field is $k$. The same is true of the degree valuation of $k(T)$. Hence $f(\mathfrak{T}/\deg) = 1$ and $3^s = e$. In particular the ramification degree is odd. Since for any $f \in k[T]$, we have that $\text{ord}_{\mathfrak{T}}f = 3^s\deg(f)$, the lemma holds.

□

We are now ready for the first of the two main technical propositions of this section. First, we recap our notation, since we are going to use it in the propositions.

**Notation 6.20.**

- $p \neq 2$ is a prime number
- $k$ is an algebraic extension of $\mathbb{Q}$.

- $K$ is a function field over $k$.
- There exists a non-archimedean valuation $v$ of $k$ such that $v$ restricts to the $p$-adic valuation of $\mathbb{Q}$ and $[k_v : \mathbb{Q}_p] < \infty$. We denote by $\mathfrak{p}$ the maximal ideal of the valuation ring $R_v$.
- $H \subset k$ is a number field, i.e. $[H : \mathbb{Q}] < \infty$. We let $\mathfrak{p}_H$ be the maximal ideal of $R_{v_H} = R_v \cap H$.
- $a, b \in O_H$, $a$ is not a square mod $\mathfrak{p}$, $a \equiv 1 \bmod 4$, $\text{ord}_{\mathfrak{p}} b$ is odd.
- $\mathfrak{T}$ is a prime of $K$ of degree one.
- $T \in K$ is such that $\text{ord}_{\mathfrak{T}} T = -3^s, s \in \mathbb{Z}_{>0}$, and $T$ has no other poles in $K$.

**Remark 6.21.** In the proof below, the number field $H$ can be replaced by any finite extension of it inside $k$. We will extend $H$ as needed to make sure the coefficients of a polynomial under consideration are in $H$.

**Proposition 6.22.** *Let $f \in K$.*

(1) *If $\text{ord}_{\mathfrak{T}} f < 0$ and $\text{ord}_{\mathfrak{T}} f$ is odd, then for any $\xi \neq 0, \mu \in k$, the equation*

$$X^2 - aY^2 - bZ^2 + abW^2 = \xi f + \mu \tag{6.6}$$

*has no solution in $K$.*

(2) *If $f \in H[T]$, and $\text{ord}_{\mathfrak{T}} f$ is even (or in other words $\deg(f)$ is even), then there exist $\xi \neq 0, \mu \in H$ such that* (6.6) *has a solution in $H(T) \subset K$.*

(3) *For each $f$ and each choice of $\xi \neq 0, \mu \in H$ such that* (6.6) *has a solution in $H(T) \subset K$, there exists a finite set $\mathscr{Q}$ of primes of $H$ and a positive constant $N$ such that if $\xi_1, \mu_1 \in H$ and are such that $\text{ord}_{\mathfrak{q}}(\xi - \xi_1) > N, \text{ord}_{\mathfrak{q}}(\mu - \mu_1) > N$ for all $\mathfrak{q} \in \mathscr{Q}$, then*

$$X^2 - aY^2 - bZ^2 + abW^2 = \xi_1 f + \mu_1 \tag{6.7}$$

*has a solution $(X, Y, Z, W) \in K^4$.*

*Proof.* Suppose $f \in K$ and $\text{ord}_{\mathfrak{T}} f$ is odd. In this case, for any $\xi \neq 0, \mu \in k$ we know that $\text{ord}_{\mathfrak{T}}(\xi f + \mu) = \text{ord}_{\mathfrak{T}} f < 0$ and it is odd. So, by Proposition 6.6 applied to $h = \xi f + \mu$ we conclude that (6.6) has no solutions in $K$.

If we consider the form $X^2 - aY^2 - bZ^2 + abW^2$ over $H$, then we note that any four dimensional form is universal locally at any non-archimedean prime $\mathfrak{q}$, i.e. it represents every element of the completion $H_{\mathfrak{q}}$. Without loss of generality, by Lemma 6.3 we can assume that $k$ and $H$ have no real embeddings. By the Hasse-Minkowski local-global principle, we can then conclude that the form is universal over $H$. (See Corollary 27.5, Chapter V of [19].) Thus, if $f \in H$ (and therefore $\text{ord}_{\mathfrak{T}} f = 0$), the equation (6.6) can be satisfied.

Now assume that $f \in H[T] \setminus H$, and $\text{ord}_{\mathfrak{T}} f$ is even (or in other words $\deg(f)$ is even). We now show that for some constants $\xi \neq 0, \mu \in H$, the quadratic form equation (6.6) has solutions in $H(T)$.

We start with examining the isotropic/anisotropic status of (6.1) over $H$. If the form is isotropic in $H$, then by Proposition 6.16, we are done, since the form can represent any constant in $H$. Suppose the form is anisotropic over $H$. Then, by Proposition 6.15, there is a finite set $\mathscr{Q}$ of $H$-primes such that the form is anisotropic over $H_{\mathfrak{q}}$ for all $\mathfrak{q} \in \mathscr{Q}$ and is isotropic in all other completions of $H$. Further, for each $\mathfrak{q} \in \mathscr{Q}$, either $\text{ord}_{\mathfrak{q}} a$ is odd, or $\text{ord}_{\mathfrak{q}} b$ is odd.

We now describe the set of conditions on $\xi$ and $\mu$ making sure that

(1) $\xi f + \mu$ is irreducible over $H(T)$, and
(2) if $\mathfrak{t}$ is the prime of $H(T)$ corresponding to $\xi f + \mu$, then in the residue field of $\mathfrak{t}$, the norm (6.1) becomes isotropic.

Let $\pi \in O_H$ be such that $\text{ord}_{\mathfrak{q}}\pi = 1$ for every $\mathfrak{q} \in \mathscr{Q}$ . (Such an element exists by the Strong Approximation Theorem, (see page 239 of [8]).) Let $a_0, \ldots, a_n \in O_H$ and assume

$$f(T) = a_nT^n + \ldots + a_0 = a_n\left(\frac{\pi^rT}{\pi^r}\right)^n + a_{n-1}\left(\frac{\pi^rT}{\pi^r}\right)^{n-1} + \ldots + a_0 =$$
$$a_n\left(\frac{U}{\pi^r}\right)^n + a_{n-1}\left(\frac{U}{\pi^r}\right)^{n-1} + \ldots + a_0,$$

where $r$ is a non-negative integer such that $\text{ord}_{\mathfrak{q}}\pi^r\dfrac{a_i}{a_n} > 2$ for all $\mathfrak{q} \in \mathscr{Q}$ and for any coefficient $a_i, i = 0, \ldots, n-1$, and $U = \pi^rT$. Now set $\xi = \dfrac{\pi^{nr}}{a_n}$ and let $g(U) = \xi f(T)$. (Observe that $\xi \neq 0$ as required.) Then

$$g(U) = U^n + c_{n-1}U^{n-1} + \ldots + c_0,$$

where

$$c_i = \xi\frac{a_i}{\pi^{ri}} = \frac{\pi^{nr}}{a_n}\frac{a_i}{\pi^{ri}} = \pi^{nr-ri}\frac{a_i}{a_n} = \pi^{nr-ri-r}\frac{\pi^ra_i}{a_n}, i = 0, \ldots, n-1.$$

Thus,

$$\forall \mathfrak{q} \in \mathscr{Q} : \text{ord}_{\mathfrak{q}}c_i > 2 + (nr - ri - r) = 2 + r(n - i - 1) \geq 2$$

for $i = 0, \ldots, n-1$.

Next let $\mu \in O_H$ be such that $\forall \mathfrak{q} \in \mathscr{Q} : \text{ord}_{\mathfrak{q}}\mu = 1$ and observe that $h(U) = g(U) + \mu$ is irreducible by Lemma 6.17, and adjoining a root $\alpha$ of $h(U)$ to $H$ will ramify $\mathfrak{q}$ with even ramification degree. This will make the quadratic form in (6.2) isotropic at the factors above $\mathfrak{q}$ in $H(\alpha)$ by Corollary 6.14.

Now let $\xi_1, \mu_1 \in H$, $U = \pi^rT$, and let $\hat{g}(U) = \xi_1 f(T) = \hat{c}_nU^n + \hat{c}_{n-1}U^{n-1} + \ldots + \hat{c}_0$. Then $\hat{c}_i = \xi_1\frac{a_i}{\pi^{ri}}$. Let $\mathfrak{q} \in \mathscr{Q}$ and note that $\text{ord}_{\mathfrak{q}}(c_i - \hat{c}_i) = \text{ord}_{\mathfrak{q}}(\xi - \xi_1) + \text{ord}_{\mathfrak{q}}\frac{a_i}{\pi^{ri}}$. Let $N > 0$ be large enough so that for all $\mathfrak{q} \in \mathscr{Q}, j = 0, \ldots, n-1$

$$N + \min_{i,\mathfrak{q}}(\text{ord}_{\mathfrak{q}}\frac{a_i}{\pi^{ri}}) > \text{ord}_{\mathfrak{q}}(\xi\frac{a_j}{\pi^{rj}}) = \text{ord}_{\mathfrak{q}}c_j.$$

Pick $\xi_1$ such that $\text{ord}_{\mathfrak{q}}(\xi - \xi_1) > N$ and observe that for all $\mathfrak{q} \in \mathscr{Q}$, for all $i = 0, \ldots, n-1$ we now have that $\text{ord}_{\mathfrak{q}}(\hat{c}_i - c_i) > \text{ord}_{\mathfrak{q}}c_i$. Then for all $\mathfrak{q} \in \mathscr{Q}$, for all $i$, we get that

$$\text{ord}_{\mathfrak{q}}\hat{c}_i = \text{ord}_{\mathfrak{q}}((\hat{c}_i - c_i) + c_i) = \text{ord}_{\mathfrak{q}}c_i \geq 2.$$

Now let $\mu_1$ be such that for all $\mathfrak{q}$ we have that

$$\text{ord}_{\mathfrak{q}}(\mu - \mu_1) > 2.$$

Then $\text{ord}_{\mathfrak{q}}\mu_1 = \text{ord}_{\mathfrak{q}}\mu$ by the same argument as for $\xi_1$. Thus, $\text{ord}_{\mathfrak{q}}\mu_1 = 1$. We now can apply Lemma 6.17 to the polynomial $\hat{h} = \xi_1 f(T) + \mu_1$ to conclude that all primes in $\mathscr{Q}$ ramify in the residue field of the extension generated by $\hat{h}$ with ramification degree divisible by $2$ and then proceed in the same manner as we did for the polynomial $h$. □

6.6. **Representing polynomials by quadratic forms: the real embedding case.** We now consider the case of $k$ with a real embedding. First we prove the following lemma.

**Lemma 6.23.** *Let $H$ be a number field. Suppose $H$ contains an element $\alpha$ such that $\alpha^2 = -1 + 2^r, r \in \mathbb{Z}_{>2}$. Let $\mathfrak{q}$ be a dyadic prime (i.e a prime dividing 2). Then $i \in H_{\mathfrak{q}}$ and the extension $H(i)/H$ is unramified at all primes of $H$.*

*Proof.* Let $g(x) = x^2 + 1$, then $g(\alpha) = 2^r \equiv 0 \mod 2^r$. At the same time $g'(\alpha) = 2\alpha \equiv 0 \bmod 2$, and $g'(\alpha) \not\equiv 0 \bmod 2\mathfrak{q}$. Therefore, $\text{ord}_{\mathfrak{q}} g(\alpha) = e(\mathfrak{q}/2)r > 2e(\mathfrak{q}/2) = e(\mathfrak{q}/2)\text{ord}_{\mathfrak{q}} g'(\alpha)$. Thus, by Hensel's Lemma (Chapter XII, §7, Proposition 7.6 of [12]), $g(x)$ has a root in $H_{\mathfrak{q}}$. Now by Corollary 2.10, we can conclude that no prime ramifies in this extension. □

As before, without loss of generality, by Lemma 6.3, we can assume that $\sqrt{7} \in k$. (Adjoining $\sqrt{7}$ will not change the existence of a real embedding.) In what follows, we use the same notation as above with the following modifications.

**Notation 6.24.**
- $\sqrt{7} \in H \subset k$
- $k$ has a real enbedding.

As above, $H$ is any number field contained in $k$ containing $\sqrt{7}$ and the coefficients of the polynomial $f$ under consideration. We now prove an analogue of Proposition 6.22 for fields with a real embedding.

**Proposition 6.25.** *Let $f \in K$.*

(1) *If $\text{ord}_{\mathfrak{T}} f < 0$ and is odd, then for any $\xi \neq 0, \mu \in k$, the equation*

$$X^2 + Y^2 + Z^2 + W^2 = \xi f + \mu \tag{6.8}$$

*has no solution in $K$.*

(2) *If $f \in H[T]$ and $\text{ord}_{\mathfrak{T}} f$ is even (or in other words deg$(f)$ is even), then there exist $\xi \neq 0, \mu \in k$ such that* (6.8) *has a solution $(X, Y, Z, W) \in K^4$.*

(3) *If $\xi, \mu \in k$ are as above, then there exists $\delta > 0$ such that for all $\xi_1, \mu_1$ with $|\xi - \xi_1| < \delta, |\mu - \mu_1| < \delta$ for all archimedean absolute values $|...|$ of $k$, we have that*

$$X^2 + Y^2 + Z^2 + W^2 = \xi_1 f + \mu_1 \tag{6.9}$$

*has a solution $(X, Y, Z, W) \in K^4$.*

*Proof.* We first note that the quadratic form in 6.8 is anisotropic over $\mathbb{R}$, and therefore anisotropic over $k$. Thus, if $\text{ord}_{\mathfrak{T}} f$ is odd, then the proposition holds by the same argument as in Proposition 6.22. The same is true if $f \in H$. (By the Strong Approximation Theorem (see page 239 of [8]), we can always pick $\xi, \mu \in H$ so that the image of $f$ under any real embedding is positive.)

So, assume now that deg$(f)$ is even and $f$ is not a constant. It is enough to show that (6.8) can be satisfied in $H(T)$. We again start by examining anisotropic/isotropic status of the form in question over $H$. As in Lemma 6.3, it is easy to see that the quadratic form in (6.8) is isotropic if and only if $-1$ is a norm in the extension $H(i)/H$. By Hasse Norm Principle, it is enough to show that $-1$ is a norm in all completions of $H$. (See page 103, [2].) Since $H$ contains $\sqrt{7}$, by Lemma 6.23, we have that the extension $H_{\mathfrak{q}}(i)/H_{\mathfrak{q}}$ is unramified for all primes $\mathfrak{q}$ of $H$, and therefore $-1$ is a norm at all primes $\mathfrak{q}$ of $H$ by Proposition 3.11 of [9]. Thus, the only completions where $-1$ is not a norm are the real ones.

We choose $\xi$ so that the leading coefficient of $\xi f$ is positive under all real embeddings. Such a $\xi$ exists by the Strong Approximation Theorem, once again. This step will also make sure that the leading coefficient of $\xi f + \mu$ is representable by the form over $H$. We also choose $\mu > 0$ large enough so that $\xi f + \mu$ has no roots in $\mathbb{R}$ under all real embeddings. Let $h(T) = \xi f(T) + \mu$, and let $g(T)$ be an irreducible factor of $h(T)$. Then $g(T)$ has no roots in $\mathbb{R}$ under any real embedding of $H$, and therefore must be of even degree. Further, if we adjoin a root $\alpha$ of $g(T)$ to $H$, the extended field $H(\alpha)$ will have no real embeddings, and the left side of (6.8) will become isotropic. Thus we can apply Proposition 6.16 again to reach the desired conclusion.

If $\xi_1$ is sufficiently close to $\xi$ under all archimedean absolute values of $k$, then the leading coefficient of $\xi_1 f$ is also positive under all real embeddings. Similarly, if $\mu_1$ is sufficiently close to $\mu$ under all archimedean valuations of $k$, then $h_1(T) = \xi_1 f(T) + \mu_1$ has no real roots under all real embeddings of $k$. □

6.7. **A subset of $k$ Diophantine over $K$.** We now address the issue of giving a Diophantine definition of a set of constants guaranteed to contain constants $\xi_1, \mu_1$ we used in Propositions 6.22 and 6.25.

**Proposition 6.26.** *The following statements are true.*

1. *There exists a Diophantine over $K$ set of constants $A$ such that for any number field $H \subseteq k$ and any finite collection $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of primes of $H$, the set $\{(b, \ldots, b) : b \in A \cap H\} \subset A^r$ is dense in $H_{\mathfrak{q}_1} \times \ldots \times H_{\mathfrak{q}_r}$ under the product topology.*
2. *There exists a Diophantine over $K$ set of constants $A$ such that for any number field $H \subseteq k$ and all real embeddings $\sigma_1, \ldots, \sigma_r$ of $H$, the set $\{(b, \ldots, b) : b \in A \cap H\} \subset A^r$ is dense in $\sigma_1(H) \times \ldots \times \sigma_r(H)$ under the product topology.*

*Proof.* For the $p$-adic case the proof follows from Theorem 5.5 of [7]. For the Archimedean case, we use Lemma 3.6 and Section 3.6 of [17] together with Proposition 5.1 of [7]. □

6.8. **Constructing extensions of $K$ so that a given prime has a factor of degree 1.** So far we have assumed that the prime $\mathfrak{T}$ of $K$ is a degree $1$ prime. If $\mathfrak{T}$ is not of degree $1$, in all but one case we can remedy the situation by taking a finite extension of $k$.

**Lemma 6.27.** *Let $\mathfrak{q}$ be a prime divisor of $K$ of degree greater than 1. Then there exists a finite constant field extension $\hat{k}$ of $k$ such that in $\hat{k}K$ the divisor $\mathfrak{q}$ has at least one factor of degree 1.*

*Proof.* Let $R_{\mathfrak{q}}$ be the residue field of $\mathfrak{q}$. Then $R_{\mathfrak{q}}$ is isomorphic to a finite extension of $k$, and we can identify $R_{\mathfrak{q}}$ with this extension. Let $s(T) \in k[T]$ be the monic irreducible polynomial of a generator $\alpha$ of $R_{\mathfrak{q}}$ over $k$. Let $\mathfrak{q}_i$ be a factor of $\mathfrak{q}$ in $K(\alpha)$. Let $R_i$ be the residue field of $\mathfrak{q}_i$. Since the power basis of $\alpha$ is an integral basis with respect to $\mathfrak{q}$, we can determine the factorization of $\mathfrak{q}$ in $K(\alpha)$ by considering the factorization of $s(T)$ over $R_{\mathfrak{q}}$ (see [11], Chapter I, Section 8, Proposition 25). By assumption on $s(T)$ we have that over $R_{\mathfrak{q}}$ it has at least one factor of degree 1. □

6.9. **The connection between an even order at a prime and being integral at a prime.** The lemmas below show how to use information about multiplicity of the order at a valuation to determine whether a function is integral at the valuation.

**Lemma 6.28.** *Let $K$ and $\mathfrak{T}$ be as in Notation 6.20 and let $h \in K$ be such that ord$_{\mathfrak{T}}(h^{3^{s+1}} + T)$ is even, Then, ord$_{\mathfrak{T}}h < 0$, and ord$_{\mathfrak{T}}h \equiv 0 \bmod 2$. Conversely, if ord$_{\mathfrak{T}}h < 0$, and ord$_{\mathfrak{T}}h \equiv 0 \bmod 2$, we have that ord$_{\mathfrak{T}}(h^{3^{s+1}} + T)$ is even.*

*Proof.* First assume that ord$_{\mathfrak{T}}h \geq 0$. Then ord$_{\mathfrak{T}}(h^{3^{s+1}} + T) =$ ord$_{\mathfrak{T}}T = -3^s$, contradicting our assumptions. Thus ord$_{\mathfrak{T}}h < 0$, and since ord$_{\mathfrak{T}}T = -3^s$ we have that ord$_{\mathfrak{T}}h^{3^{s+1}} <$ ord$_{\mathfrak{T}}T$. Consequently, ord$_{\mathfrak{T}}(h^{3^{s+1}} + T) =$ ord$_{\mathfrak{T}}h^{3^{s+1}} \equiv 0 \bmod 2$. Conversely, if ord$_{\mathfrak{T}}h < 0$, and ord$_{\mathfrak{T}}h \equiv 0 \bmod 2$, we have that ord$_{\mathfrak{T}}(h^{3^{s+1}} + T) =$ ord$_{\mathfrak{T}}h^{3^{s+1}} \equiv 0 \bmod 2$. □

**Lemma 6.29.** *Let $f \in K$. Then ord$_{\mathfrak{T}}(f^{2\cdot 3^{s+1}}T + T^2) \equiv 0 \bmod 2$ if and only if ord$_{\mathfrak{T}}f \geq 0$.*

*Proof.* Suppose ord$_{\mathfrak{T}}f < 0$. Since ord$_{\mathfrak{T}}T = -3^s$, we have that

$$\text{ord}_{\mathfrak{T}}(f^{2\cdot 3^{s+1}}T) < \text{ord}_{\mathfrak{T}}T^2,$$

and

$$\text{ord}_{\mathfrak{T}}(f^{2\cdot 3^{s+1}}T + T^2) = \text{ord}_{\mathfrak{T}}(f^{2\cdot 3^{s+1}}T) = 2\text{ord}_{\mathfrak{T}}(f^{3^{s+1}}) - 3^s \equiv 1 \bmod 2.$$

Conversely, assume that ord$_{\mathfrak{T}}f \geq 0$. Then ord$_{\mathfrak{T}}(f^{2\cdot 3^{s+1}}T) >$ ord$_{\mathfrak{T}}T^2$, and

$$\text{ord}_{\mathfrak{T}}(f^{2\cdot 3^{s+1}}T + T^2) = \text{ord}_{\mathfrak{T}}T^2 = 2 \equiv 0 \bmod 2.$$

□

We now complete the proof of Theorem 6.1.

6.10. **Proof of Theorem 6.1.** We again review our notation and assumptions. We start with an odd prime $p$ and a field $k$ algebraic over $\mathbb{Q}$. Next we assume the existence of a valuation $v$ on $k$ such that $v$ restricts to a $p$-adic valuation on $\mathbb{Q}$, and $[k_v : \mathbb{Q}_p] < \infty$. If necessary, we replace $k$ by its finite extension to make sure $k$ does not have any finite embeddings. We now consider a function field $K$ with the field of constants equal to $k$ and a function field prime $\mathfrak{T}$. If $\mathfrak{T}$ is not of degree 1, then we once again replace $k$ by its finite extension chosen to be isomorphic to the residue field of $\mathfrak{T}$, and we replace $\mathfrak{T}$ by a prime above it in the extended field of degree 1. Replacing the original field $K$ by its finite extension, and the original prime $\mathfrak{T}$ by a prime above it in this finite extension is justified by Lemmas 6.3,6.4 and 6.27.

6.10.1. *A special element $T$.* For all sufficiently large $s \in \mathbb{Z}_{>0}$, by Lemma 6.18, we can find a $T \in K$ with a pole at $\mathfrak{T}$ of order $3^s$, and no other poles. In other words, $\mathrm{ord}_{\mathfrak{T}}T = -3^s$ and for any other prime $\mathfrak{a}$ of $K$, we have that $\mathrm{ord}_{\mathfrak{a}}T \geq 0$. We fix such an element. Note that, by Proposition 2.1, $\mathfrak{T}$ is totally ramified over $k(T)$ with the ramification degree $3^s$. Hence, for any $h \in k(T)$ we have that $3^s \cdot \deg(h) = -\mathrm{ord}_{\mathfrak{T}}h$, and $\deg(h) \equiv 0 \bmod 2$ if and only if $\mathrm{ord}_{\mathfrak{T}}h \equiv 0 \bmod 2$. (For a rational function we define the degree to be the difference of the degrees of the numerator and the denominator.)

6.10.2. *Defining a subset of $K$ containing all polynomials in $T$ of even degree, and no element of $K$ with an odd degree pole at $\mathfrak{T}$.* Let $h \in k[T]$. Then by Proposition 6.22 and Proposition 6.26, Part 1, we have that $\mathrm{ord}_{\mathfrak{T}}h \equiv 0 \bmod 2$ or equivalently $\deg(h) \equiv 0 \bmod 2$ if and only if there exists $\xi, \mu, X, Y, Z, W \in K$ such that

$$X^2 - aY^2 - bZ^2 + abW^2 = \xi h + \mu, \tag{6.10}$$

$$\xi \in A \setminus \{0\}, \mu \in A. \tag{6.11}$$

We remind the reader that $A \subset k$ is Diophantine over $K$. At the same time, if $h \in K$ satisfies (6.10), then $\mathrm{ord}_{\mathfrak{T}}h \equiv 0 \bmod 2$.

6.10.3. *Defining a subset of $K$ containing all rational functions in $T$ of even degree and no element of $K$ of odd order at $\mathfrak{T}$.* Please note that for any $h \in k(T)$, we have that $\mathrm{ord}_{\mathfrak{T}}h \equiv 0 \bmod 2$ if and only if $h = \dfrac{h_1}{h_2}$, where $h_1, h_2 \in k[T] \setminus k$, $h_2(T) \neq 0$ and $\deg(h_1) \equiv \deg(h_2) \equiv 0 \bmod 2$. Indeed, suppose $h = \dfrac{g_1}{g_2}$, $g_2 \neq 0, g_1, g_2 \in k[T] \setminus k$. If $\deg(h)$ is even, then $\deg(g_1) - \deg(g_2)$ is even. Suppose $\deg(g_1) = 2r + 1, r \in \mathbb{Z}_{>0}$. Then note that $h = \dfrac{Tg_1}{Tg_2}$, where we can set $h_1 = Tg_1, h_2 = Tg_2$ to reach the desired conclusion. If either $g_1$ or $g_2$ is a constant, then let $h_1 = T^2g_1, h_2 = T^2g_2$ to reach the desired conclusion once again.

Let $h \in K$ be such that $r = 1, 2$ there exists $\xi_r, \mu_r, X_r, Y_r, Z_r, W_r \in K$ such that

$$X_r^2 - aY_r^2 - bZ_r^2 + abW_r^2 = \xi_r(h_r^{3^{s+1}} + T) + \mu_r, \tag{6.12}$$

$$\xi_r \in A \setminus \{0\}, \mu_r \in A. \tag{6.13}$$

where $h_2 \neq 0$ and $h = \dfrac{h_1}{h_2}$. By Proposition 6.6, we have that $\mathrm{ord}(h_r^{3^{s+1}} + T)$ is even for $r = 1, 2$. By Lemma 6.28, we then conclude that $\mathrm{ord}_{\mathfrak{T}}(h_r)$ is even. Consequently, $\mathrm{ord}_{\mathfrak{T}}h$ is even.

Conversely, if $h \in k(T)$ and $\deg(h)$ is even, we can write $h$ as a ratio of two polynomials $h_1, h_2$ of positive even degrees. If $\deg(h_r)$ is positive and even, then $\deg(h_r^{3^{s+1}} + T)$ is also positive and even, and therefore we can satisfy (6.12) over $K$ by Proposition 6.22.

6.10.4. *Defining a subset of $K$ containing all rational functions of $T$ integral at $\mathfrak{T}$ (or of non-positive degree) and no functions of $K$ with a pole at $\mathfrak{T}$.* Consider now the set of $f \in K$ satisfying the following equations.

$$f^{2\cdot 3^{s+1}}T + T^2 = \frac{h_1}{h_2} \tag{6.14}$$

$$X_{j,r}^2 - aY_{j,r}^2 - bZ_{j,r}^2 + abW_{j,r}^2 = \xi_{j,r}(h_r^{3^{s+1}} + T) + \mu_{j,r}, \quad \text{for } j = 1,2 \text{ and } r = 1,2 \tag{6.15}$$

$$\xi_{j,r} \in A \setminus \{0\}, \mu_{j,r} \in A. \tag{6.16}$$

By Proposition 6.6 and Lemma 6.28, we have that $\text{ord}_{\mathfrak{T}} h_r \equiv 0 \bmod 2$. Therefore,

$$\text{ord}_{\mathfrak{T}}(f^{2\cdot 3^{s+1}}T + T^2) \equiv 0 \bmod 2, \tag{6.17}$$

and thus $\text{ord}_{\mathfrak{T}} f \geq 0$ by Lemma 6.29.

Conversely, if $f \in k(T)$ and $\deg(f)$ is even, then (6.17) holds and we can choose $h_1, h_2 \in k[T]$ of even positive degrees such that (6.14) holds. By Lemma 6.28, we also have that $h_r^{3^{s+1}} + T$ will be a polynomial of even degree, and by Proposition 6.22, we can satisfy (6.14)–(6.16).

6.10.5. *Defining the valuation ring* $R_{\mathfrak{T}}$ *of* $\mathfrak{T}$ *in* $K$. Let $n := [K : k(T)] = 3^s$. We claim that $R_{\mathfrak{T}}$ can be defined as follows: $w \in R_{\mathfrak{T}}$ if and only if there exist

$$\xi_{i,r}, \mu_{i,r}, U_i, h_{i,r}, X_{i,r}, Y_{i,r}, Z_{i,r}, W_{i,r} \in K$$

with $r \in \{1,2\}, i \in \{0, \dots, n-1\}$ such that

$$w^n + U_{n-1}w^{n-1} + \ldots + U_0 = 0 \ \& \tag{6.18}$$

$$\bigwedge_{i=0}^{n-1}((TU_i^{2\cdot 3^{s+1}} + T^2) = \frac{h_{i,1}}{h_{i,2}}) \ \& \tag{6.19}$$

$$\bigwedge_{i=0}^{n-1}\bigwedge_{r=1}^{2} X_{i,r}^2 - aY_{i,r}^2 - bZ_{i,r}^2 + abW_{i,r}^2 = \xi_{i,r}(h_{i,r}^{3^{s+1}} + T) + \mu_{i,r} \ \& \tag{6.20}$$

$$\forall i \in \{0, \dots, n-1\}, r \in \{1,2\} \ (\xi_{i,r} \in A \setminus \{0\} \ \& \ \mu_{i,r} \in A). \tag{6.21}$$

First suppose that Equations (6.18)–(6.21) are satisfied. Then, since $A \subset k$, and $\xi_{i,r} \neq 0$, by Proposition 6.2, we have that $\text{ord}_{\mathfrak{T}}(h_{i,r}^{3^{s+1}} + T)$ is even, and therefore, by Lemma 6.28, $\text{ord}_{\mathfrak{T}} h_{i,r}$ is even and so is $\text{ord}_{\mathfrak{T}}(TU_i^{2\cdot 3^{s+1}} + T^2)$. Hence, by Lemma 6.29, $\forall i \in \{0, \dots. n-1\}$ $\text{ord}_{\mathfrak{T}} U_i \geq 0$.

Suppose now that $\text{ord}_{\mathfrak{T}} w < 0$. In this case,

$$\text{ord}_{\mathfrak{T}}(w^n + U_{n-1}w^{n-1} + \ldots + U_0) = n \cdot \text{ord}_{\mathfrak{T}} w < 0,$$

contradicting the fact that

$$\text{ord}_{\mathfrak{T}}(w^n + U_{n-1}w^{n-1} + \ldots + U_0) = \text{ord}_{\mathfrak{T}} 0 = \infty.$$

Therefore, if for some $w \in K$ we have that Equations (6.18)–(6.21) can be satisfied over $K$, then $\text{ord}_{\mathfrak{T}} w \geq 0$.

Conversely, suppose $w \in K, \text{ord}_{\mathfrak{T}} w \geq 0$. Then, by Corollary 2.8 we have that $w$ is integral over the local subring $R_{1/T}$ of $k(T)$ containing all functions $U \in k(T)$ without a pole at the valuation that is the pole of $T$ in $k(T)$. In other words, $R_{1/T}$ consists of all rational functions $U \in K(T)$ with $\deg(U) \leq 0$, or, equivalently

$\mathrm{ord}_{\mathfrak{T}} U \geq 0$. Hence, $w$ will be a root of a monic polynomial (6.18) with $U_i \in R_{1/T}$. If $\mathrm{ord}_{\mathfrak{T}} U_i \geq 0$, then, by Lemma 6.29, $\mathrm{ord}_{\mathfrak{T}}(T \cdot U_i^{2\cdot 3^{s+1}} + T^2)$ is even, or in other words, $(T \cdot U_i^{2\cdot 3^{s+1}} + T^2)$ is a rational function in $T$ of even degree. Consequently, we can write each $U_i = \dfrac{h_{i,1}}{h_{i,2}}$, where $h_{i,r}$ are polynomials in $T$ of even degrees. Thus, $h_{i,r}^{3^{s+1}} + T$ is a polynomial in $T$ of even degree, and we can find constants in $A$ so that (6.20) can be satisfied over $K$. This concludes the proof of Theorem 6.1.

We now proceed to prove Theorem 6.2.

6.11. **Proof of Theorem 6.2.** In almost every way the proof of Theorem 6.2 is the same as the proof of Theorem 6.1. So we confine ourselves to discussing only those parts where there are differences. We will consider every part of the proof of Theorem 6.1 and indicate what changes, if any, are required.

We start with examining Subsection 6.10.1. In this part of the proof we consider a prime $\mathfrak{T}$ and determine whether we can assume that $\mathfrak{T}$ is of degree 1. For Theorem 6.2, we consider only primes $\mathfrak{T}$ with residue fields embeddable into $\mathbb{R}$. If $\mathfrak{T}$ is not of degree 1, then its residue field is isomorphic to a finite extension $\hat{k}$ of $k$. By Lemma 6.27, in the extension $\hat{k}K$ of $K$ the prime $\mathfrak{T}$ will have a factor of degree 1. As in Subsection 6.10.1, we can extend our field of constants $k$, but the extended field must still be embeddable into $\mathbb{R}$. This condition will be satisfied for $\hat{k}$, given our assumptions on $\mathfrak{T}$. Thus, as in the proof of Theorem 6.1, we can assume that $\mathfrak{T}$ is of degree 1. We can again produce an element $T \in K$ such that $\mathfrak{T}$ is the only pole of $T$ and $\mathrm{ord}_{\mathfrak{T}} T = -3^s$.

From this point on, the proof of Theorem 6.2 is exactly the same as the proof of Theorem 6.1 with (6.10) replaced by (6.8), and the set $A$ defined to satisfy the conditions of Proposition 6.25. The existence of such a set $A$ follows from Proposition 6.26(4).

## 7. Diophantine Definition of C.E. Sets over Rings of Integral Functions

In this section we extend results of J. Demeyer to show that c.e. sets are definable over any ring of integral functions, assuming the constant field is a number field. Since Demeyer showed that such a result holds over polynomial rings over number fields, and since rings of integral functions are finitely generated modules over polynomial rings, it is enough to show that we can give a Diophantine definition of polynomial rings over the rings of integral functions to achieve the desired result. Below we state the main theorem of the section.

**Theorem 7.1.** *Let $K$ be a function field over a field of constants that is a finite extension of $\mathbb{Q}$, and let $\mathscr{S}$ be a finite non-empty collection of its valuations. Then every c.e. subset of $O_{K,\mathscr{S}}$ is Diophantine over $O_{K,\mathscr{S}}$.*

**Remark 7.2.** We remind the reader that the discussion of c.e. subsets of function fields can be found at the beginning of Section 5.

7.1. **Arbitrary powers of a ring element.** In this section we again turn our attention to the rings of $\mathscr{S}$-integers of function fields, discussed in Sections 2 and 3, and consider the case where the field is not necessarily rational. We recall the notation and assumptions we used in these sections and add new ones.

**Notation and Assumptions 7.3.**

- Let $K, k$, $\mathscr{S}$, $a, \mathfrak{q}, \mathfrak{q}_\infty, T = a - \sqrt{a^2 - 1}$, be as in Proposition 3.5.
- Let $R = O_{K,\mathscr{S}}, R' = R[T], R'' = R[T] \cap O_{K(T),\{\mathfrak{q}_\infty\}}$. Since $T$ satisfies a monic polynomial of degree 2 over $R$, every element of $R[T]$ is of the form $a + bT$, where $a, b \in R$.
- Let $\mathscr{S}'$ be the set of primes of $K(T)$ lying above primes of $\mathscr{S}$.
- Let $\mathfrak{Q}_\infty$ be the prime below $\mathfrak{q}_\infty$ in $\mathbb{Q}(T)$. In other words $\mathfrak{Q}_\infty$ corresponds to the infinite valuation of $\mathbb{Q}(T)$. Observe that $\mathfrak{q}_\infty$ is the only prime above $\mathfrak{Q}_\infty$ in $K(T)$.
- Let $d = [K(T) : \mathbb{Q}(T)]$.
- Let $L$ be the Galois closure of $K(T)$ over $\mathbb{Q}(T)$.
- Let $m = [L : \mathbb{Q}(T)]$.
- Let $\beta \in O_{K(T),\{\mathfrak{q}_\infty\}}$ generate $K(T)$ over $\mathbb{Q}(T)$. Since $\beta \in K(T)$, we have that $\beta = a_\beta + b_\beta T, \alpha_\beta, b_\beta \in K$.
- Let $\mathfrak{t}_1, \ldots, \mathfrak{t}_s$ be all of the factors of $\mathfrak{q}_\infty$ and $\mathfrak{Q}_\infty$ in $L$.
- For each positive integer $m$ let $\xi_m$ be a primitive $m$-th root of unity.
- For each positive integer $m$ let $\Phi_m$ be the monic irreducible polynomial of $\xi_m$ over $\mathbb{Q}$. We refer to polynomials of this form as “cyclotomic” polynomials.
- Let $u_m = \deg(\Phi_m) = \varphi(m)$.

7.2. **Outline of the proof.** For the main result of the section we need to construct a Diophantine definition of arbitrary powers of a non-constant element of the ring. It turns out that it is more convenient to construct this definition for an element $T$ of a quadratic extension $R'$ of the ring $R$. We will proceed as follows.

(1) Observe that since $T^2 = 2aT - 1$, for any positive $m$ we have that

$$T^m = a_m + b_m T, a_m, b_m \in R.$$

It also follows that any polynomial $P(T) \in R[T]$ can be written in the form $a_P + b_P T$ with $a_P, b_P \in R$.

(2) We can assume that $\beta \in O_{K(T),\{\mathfrak{q}_\infty\}}$ generating $K(T)$ over $\mathbb{Q}(T)$ is in fact in $R''$ and $a_\beta, b_\beta \in R$. Let $\gamma \in R[T]$ generate $K(T)$ over $\mathbb{Q}(T)$. Such a $\gamma$ always exists since the fraction field of $R[T]$ is $K(T)$. Then $\gamma = a_\gamma + b_\gamma T$, where $a_\gamma, b_\gamma \in R$. Let $D$ be a common denominator of the coefficients of the monic irreducible polynomial of $\gamma$ over $\mathbb{Q}(T)$. Then $D\gamma$ satisfies a monic irreducible polynomial over $\mathbb{Q}[T]$ and therefore is in $O_{K(T),\{\mathfrak{q}_\infty\}}$. At the same time $D\gamma = Da_\gamma + Db_\gamma T$ also generates $K(T)$ over $\mathbb{Q}(T)$. It remains to show that $Da_\gamma + Db_\gamma T \in R[T]$. Since $D \in \mathbb{Q}[T]$, we have that $D = a_D + b_D T$, where $a_D, b_D \in R$ and therefore $D \in R[T]$. Since $R[T]$ is a ring, we have that $Da_\gamma + Db_\gamma T \in R[T]$.

(3) Using Proposition 3.5 we show that the set

$$\text{Pow}(T) = \{(a, b) \in R^2 | \exists m \in \mathbb{Z}_{\geq 0} : a + bT = T^m\}$$

is Diophantine over $R$.

(4) Next we use the set Pow($T$) to show that the set

$$Z(T) = \{(a,b) \in R^2 | a + bT \in \mathbb{Z}[T]\}$$

is Diophantine over $R$. This is the main technical result of the section.

(5) At this point, using results of J. Denef, we deduce that for any c.e. set $A \subset \mathbb{Z}[T]^r$, the set of the form

$$B = \{(a_1, b_1, \ldots, a_r, b_r) | a_i, b_i \in R, (a_1 + b_1T, \ldots, a_r + b_rT) \in A\}$$

is Diophantine over $R$. Indeed, using results of Denef we have that every c.e. subset of $\mathbb{Z}[T]^r$ for any positive integer $r$ is Diophantine over $\mathbb{Z}[T]$. Therefore, there exists a polynomial $P(x_1, \ldots, x_r, z_1, \ldots, z_\ell)$ with coefficients in $\mathbb{Z}[T]$ such that $(x_1, \ldots, x_r) \in A$ if and only if $\exists z_1, \ldots, z_\ell \in \mathbb{Z}[T] : P(x_1, \ldots, x_r, z_1, \ldots, z_\ell) = 0$. Rewriting $x_i = a_i + b_iT$ with $(a_i, b_i) \in Z(T)$ and $z_j = c_j + d_jT$ with $(c_j, d_j) \in Z(T)$, we now have that $(a_1, b_1, \ldots, a_r, b_r) \in B$ if and only if

$$\begin{gathered}(a_i, b_i) \in Z(T), \\ \exists (c_j, d_j) \in Z(T) : P(a_1 + b_1T, \ldots, a_r + b_rT, c_1 + d_1T, \ldots, a_\ell + b_\ell T) = 0.\end{gathered}$$

We can also rewrite the coefficients of $P$ in the form $C + DT$, where $C, D$ are fixed elements of $R$. Next, multiplying out all the terms in

$$P(a_1 + b_1T, \ldots, a_r + b_rT, c_1 + d_1T, \ldots, a_\ell + b_\ell T),$$

using the fact that $T^2 = 2aT - 1$ and that $\{1, T\}$ are linearly independent over $R$, we can replace the equation $P(a_1 + b_1T, \ldots, a_r + b_rT, c_1 + d_1T, \ldots, a_\ell + b_\ell T) = 0$ first by an equivalent equation

$$P_1(a_1, b_1, \ldots, a_r, b_r, c_1, d_1, \ldots, c_\ell, d_\ell) + TP_2(a_1, b_1, \ldots, a_r, b_r, c_1, d_1, \ldots, c_\ell, d_\ell) = 0,$$

where $P_1, P_2$ are polynomials with coefficients in $R$, and then by a system

$$\left\{\begin{array}{l} P_1(a_1, b_1, \ldots, a_r, b_r, c_1, d_1, \ldots, c_\ell, d_\ell) = 0, \\ P_2(a_1, b_1, \ldots, a_r, b_r, c_1, d_1, \ldots, c_\ell, d_\ell) = 0 \end{array}\right. \tag{7.22}$$

Thus $(a_1, b_1, \ldots, a_r, b_r) \in B$ if and only if $(a_i, b_i) \in Z(T)$ and

$$\exists (c_1, d_1, \ldots, c_\ell, d_\ell) \in R^{2\ell}$$

such that $(c_j, d_j) \in Z(T)$ and the system (7.22) is satisfied.

(6) We now revisit the issue of effective enumeration of the algebraic objects under consideration we initiated in Section 5. By assumption we have that $K$ is a function field over the field of constants $k$. Therefore, there exists $Y \in R \setminus k$ such that $K/k(Y)$ is a finite extension. Since by assumption $k$ is a number field, we can enumerate $k$ effectively or, in other words, $k$ has a computable presentation where $k$ is represented as a set of linear combinations of powers of some element $\delta$ generating $k$ over $\mathbb{Q}$. Further, $\mathbb{Z}$ is a computable subset of $k$ under this presentation. Similarly, we have computable presentations of $\mathbb{Z}[Y]$, $k[Y]$ and $k(Y)$ such that both $\mathbb{Z}[Y]$ and $k[Y]$ are computable subsets of $k(Y)$. Without loss of generality, we can assume that $K$ is generated by an element $\alpha \in R$ with an explicitly given minimal polynomial over $k[Y]$. Hence, we have a computable presentation of $K$ such that $k(Y)$, $\mathbb{Z}[Y]$ and $k[Y]$ are computable subsets of $K$. Further,

since $a$ is a fixed element of $R$, we can assume it is given to us by its coordinates with respect to the power basis of $\alpha$. Consequently, $T = a - \sqrt{a^2-1}$ satisfies the monic irreducible polynomial $S(t)$ over $K$ of the form $t^2 - 2at + 1$ and the coefficients of this polynomial are given explicitly in terms of the power basis of $\alpha$. Thus, $K(T)$ has a computable presentation such that $K, k(Y), k[Y], \mathbb{Z}[Y]$ are computable subsets of $K(T)$ under this presentation.

We also have a fixed $\beta \in R''$ generating $K(T)$ over $\mathbb{Q}(T)$ and we can assume it is given to us via its coordinates with respect to the power basis of $\alpha$. Given an element $x \in K(T)$ we can find a $2d$-tuple

$$(x_0(T), y_0(T), \dots, x_{d-1}(t), y_{d-1}(T)) \in \mathbb{Z}[T]^{2d}$$

such that $x = \sum_{i=0}^{d-1} \frac{x_i(T)}{y_i(T)}\beta^i$ simply by effectively listing all such linear combinations of the first $d$ powers of $\beta$ and looking for equality with the given element $x$. Hence, $\mathbb{Z}[T]$ is a computable subset of $K(T)$.

Now observe that the set of $2d$-tuples

$$A_Y = (c_0(T), u_0(T), \dots, c_{d-1}(T), u_{d-1}(T)) \subset \mathbb{Z}[T]^{2d}$$

such that $u_0(T)\dots u_{d-1}(T) \neq 0$ and $\sum_{i=0}^{d-1} \frac{c_i(T)}{u_i(T)}\beta^i \in \mathbb{Z}[Y]$ is computable since $\mathbb{Z}[Y]$ is computable in $K(T)$, and therefore $A_Y$ is c.e. Consequently, $A_Y$ is Diophantine over $\mathbb{Z}[T]$. Hence by (5), the set

$$B_Y = \{(a_0, b_0, \dots, a_{2d-1}, b_{2d-1}) \in R^{4d}, (a_0 + b_0T, a_1 + b_1T, \dots, a_{2d-1} + Tb_{2d-1}) \in A_Y\}$$

is Diophantine over $R$. We can rewrite $B_Y$ as

$$B_Y = \{(a_0, b_0, \dots, a_{2d-1}, b_{2d-1}) \in R^{4d}, c := \sum_{i=1}^{d} \frac{a_{2i-2} + b_{2i-2}T}{a_{2i-1} + b_{2i-1}T}\beta^{i-1} \in \mathbb{Z}[Y]\}.$$

Observe that $c$ will take every value in $\mathbb{Z}[Y]$. We can replace $\beta^i$ by $a_{\beta,i} + b_{\beta,i}T$ with $a_{\beta,i}, b_{\beta,i} \in R$, since $\beta^i \in R''$. Further, using the fact that the conjugate of $T$ over $K$ is $T^{-1}$, and $T + T^{-1} = 2a \in R$, we can rewrite

$$\begin{aligned}
\frac{a_{2i-2} + b_{2i-2}T}{a_{2i-1} + b_{2i-1}T} &= \frac{(a_{2i-2} + b_{2i-2}T)(a_{2i-1} + b_{2i-1}T^{-1})}{a_{2i-1}^2 + b_{2i-1}^2 + 2aa_{2i-1}b_{2i-1}} \\
&= \frac{(a_{2i-2} + b_{2i-2}T)(a_{2i-1} + b_{2i-1}(2a - T))}{a_{2i-1}^2 + b_{2i-1}^2 + 2aa_{2i-1}b_{2i-1}} \\
&= \frac{(a_{2i-2} + b_{2i-2}T)(a_{2i-1} + 2ab_{2i-1} - Tb_{2i-1})}{a_{2i-1}^2 + b_{2i-1}^2 + 2aa_{2i-1}b_{2i-1}} = \frac{\hat{a}_{2i-2} + \hat{b}_{2i-2}T}{\hat{a}_{2i-1}},
\end{aligned}$$

where

$$\begin{aligned}
\hat{a}_{2i-2} &= a_{2i-2}(a_{2i-1} + 2ab_{2i-1}) + b_{2i-2}b_{2i-1}, \\
\hat{b}_{2i-1} &= b_{2i-2}(a_{2i-1} + 2ab_{2i-1}) - b_{2i-1}a_{2i-2} - 2ab_{2i-2}b_{2i-1} = b_{2i-2}a_{2i-1} - b_{2i-1}a_{2i-2}, \\
\hat{a}_{2i-1} &= a_{2i-1}^2 + b_{2i-1}^2 + 2aa_{2i-1}b_{2i-1}.
\end{aligned}$$

So we now have that

$$\sum_{i=1}^{d}\frac{a_{2i-2}+b_{2i-2}T}{a_{2i-1}+b_{2i-1}T}\beta^i = \sum_{i=1}^{d}\frac{\hat{a}_{2i-2}+\hat{b}_{2i-2}T}{\hat{a}_{2i-1}}(a_{\beta,i}+b_{\beta,i}T) =$$

$$\sum_{i=1}^{d}\frac{\hat{a}_{2i-2}a_{\beta,i}+\hat{b}_{2i-2}b_{\beta,i}T^2+(\hat{a}_{2i-2}b_{\beta,i}+\hat{b}_{2i-2}a_{\beta,i})T}{\hat{a}_{2i-1}}.$$

Since $T^2 = 2aT - 1$ we have that

$$\sum_{i=1}^{d}\frac{a_{2i-2}+b_{2i-2}T}{a_{2i-1}+b_{2i-1}T}\beta^i =$$

$$\sum_{i=1}^{d}\frac{\hat{a}_{2i-2}a_{\beta,i}-\hat{b}_{2i-2}b_{\beta,i}+(2a\hat{b}_{2i-2}b_{\beta,i}+\hat{a}_{2i-2}b_{\beta,i}+\hat{b}_{2i-2}a_{\beta,i})T}{\hat{a}_{2i-1}} \in \mathbb{Z}[Y] \subset R.$$

Hence,

$$\sum_{i=1}^{d}\frac{2a\hat{b}_{2i-2}b_{\beta,i}+\hat{a}_{2i-2}b_{\beta,i}+\hat{b}_{2i-2}a_{\beta,i}}{\hat{a}_{2i-1}} = 0$$

and

$$\sum_{i=1}^{d}\frac{\hat{a}_{2i-2}a_{\beta,i}-\hat{b}_{2i-2}b_{\beta,i}}{\hat{a}_{2i-1}} = c \in Z[Y].$$

Let $\hat{A} = \prod_{i=1}^{d}\hat{a}_{2i-1}, \hat{A}_i = \frac{\hat{A}}{\hat{a}_{2i-1}}$. Then

$$\sum_{i=1}^{d}\hat{A}_i(\hat{a}_{2i-2}a_{\beta,i}-\hat{b}_{2i-2}b_{\beta,i}) = \hat{A}c.$$

Thus,

$$\mathbb{Z}[Y] = \{c \in R|\exists a_0, b_0, \ldots, a_{2d-1}, b_{2d-1} \in B_Y : \sum_{i=1}^{d}\hat{A}_i(\hat{a}_{2i-2}a_{\beta,i}-\hat{b}_{2i-2}b_{\beta,i}) = \hat{A}c\},$$

where $\hat{A}, \hat{A}_i, \hat{a}_{2i-2}, \hat{b}_{2i-2}$ are fixed polynomials in $a_0, b_0, \ldots, a_{2d-1}, b_{2d-1}$. Hence $\mathbb{Z}[Y]$ is Diophantine over $R$. Now using the result of Denef one more time, we can assert that all c.e. subsets of $R$ are Diophantine.

7.3. **Defining $R''$ over $R$.** To simplify the proof, we will have $K(T)$-variables range not over $R' = R[T]$ but over a subring $R''$ of $R'$, where only one valuation $\mathfrak{q}_\infty$ is allowed as a pole of non-constant elements of the ring. The following lemma shows that this restriction is a Diophantine condition relative to $R$.

**Lemma 7.4.** *The set* $\{(a,b) \in R^2|a + Tb \in R''\}$ *has a Diophantine definition over* $R$.

*Proof.* Observe that once we fix an element $a \in O_{K,\mathscr{S}}$, the field $K(T)$ is fixed. The constant field of $K$ is a number field. Therefore, by Theorem 6.1, for each $\mathfrak{t} \in \mathscr{S}'$

we have that the valuation ring $R_\mathfrak{t}$ of $\mathfrak{t}$ has a Diophantine definition over $K(T)$. Hence, $R_\mathfrak{t} \cap R'$ has a Diophantine definition over $R'$. Thus,

$$R'' = \bigcap_{\mathfrak{t} \in \mathscr{S}' \setminus \{\mathfrak{q}_\infty\}} (R_\mathfrak{t} \cap R')$$

is existentially definable over $R'$. Consequently, there exists a polynomial $P(a + bT, z_1, \dots, z_m)$ with coefficients in $R'$ such that for any $a, b \in R$ the equation $P(a + bT, \bar{z}) = 0$ has solutions $z_1, \dots, z_m \in R'$ if and only if $a + bT \in R''$. Using the fact that $1$ and $T$ are linearly independent over $K$, and $T^2 - 2a + 1 = 0$, we can replace $P(a + bT, z_1, \dots, z_m)$ by a polynomial $Q(a, b, v_1, \dots, v_r)$ such that for any pair $(a, b) \in R^2$ the equation $Q(a, b, v_1, \dots, v_r) = 0$ has solutions $v_1, \dots, v_r \in O_{K,\mathscr{S}}$ if and only if $a + bT \in R''$. □

7.4. **A Diophantine definition of root-of-unity polynomials.** In ([4]), J. Demeyer defined a set $\mathscr{C}$ of *root-of-unity polynomials* to be the set of polynomials $F \in \mathbb{Z}[T]$ satisfying 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.

Observe that the constant polynomials $F(T) = \pm 1$ satisfy the conditions above.

The polynomials in $\mathscr{C}$ have a property that will help us to construct a Diophantine definition of arbitrary polynomials in $T$ over $R''$ using the so-called "weak vertical method" (see [20]). This property is described in the proposition below taken from J. Demeyer's paper.

**Proposition 7.5.** *Let $F \in \mathbb{Z}[T]$ with $F(0) \in \{-1, 1\}$, and let $\ell \in \mathbb{Z}_{>0}$. In this case there exists a polynomial $M \in \mathscr{C}$ such that $F \equiv M \mod T^\ell$ in $\mathbb{Z}[T]$.*

*Proof.* Proposition 2.7 of [4]. □

Before we can use polynomials in $\mathscr{C}$ to construct a Diophantine definition of $\mathbb{Z}[T]$ over $R''$, we need to construct a Diophantine definition of $\mathscr{C}$ over $R''$. The construction of this definition is the main result of this section. We start with a technical lemma to be used in determining the value of polynomials for some values of variables.

**Lemma 7.6.** *Let $\gamma \in R''$ and assume that $\gamma \equiv b \mod (T - c)$ in $R''$ with $b, c \in \mathbb{Z}$. Then $N_{K(T)/\mathbb{Q}(T)}(\gamma) = G(T) \in \mathbb{Q}[T]$, and $G(c) = \pm b^d$.*

*Proof.* First, by Corollary 2.8 we have that $R''$ is contained in the integral closure of $\mathbb{Q}[T]$ in $K(T)$. Therefore, all coefficients of the monic irreducible polynomial of $\beta$ over $\mathbb{Q}(T)$ are polynomials in $\mathbb{Q}[T]$. Hence,

$$G(T) = N_{K(T)/\mathbb{Q}(T)}(\gamma) \in \mathbb{Q}[T].$$

Let $R_L$ be the integral closure of $R''$ in $L$ (the Galois closure of $K(T)$ over $\mathbb{Q}(T)$). Next consider the congruence $\gamma \equiv b \mod (T - c)$ in $R_L$. Let $\gamma_1 = \gamma, \dots, \gamma_m$ be all of the conjugates of $\gamma$ over $\mathbb{Q}(T)$. Since $T, c, b \in \mathbb{Q}(T)$, we have that $\gamma_i \equiv b \bmod (T-c)$ in $R_L$. Thus,

$$N_{L/\mathbb{Q}(T)}(\gamma) = \prod_{i=1}^{m} \gamma_i \equiv b^m \bmod (T-c)$$

in $R_L \cap \mathbb{Q}(T) = \mathbb{Q}[T]$. Further,

$$N_{L/\mathbb{Q}(T)}(\gamma) = (N_{K(T)/\mathbb{Q}(T)}(\gamma))^{[L:K(T)]} = G(T)^{m/d}.$$

Therefore, $G(T)^{m/d} \equiv b^m \bmod (T-c)$, and $G(c)^{m/d} = b^m$. Consequently, $G(c) = \xi \cdot b^d$, where $\xi$ is a root of unity. Since $G(c) \in \mathbb{Q}$, we conclude that $G(c) = \pm b^d$. □

The next lemma begins the construction of a Diophantine definition of $\mathscr{C}$ over $R''$.

**Lemma 7.7.** *Suppose $\alpha \in R''$, and let $m_1, \dots, m_r, p_1, \dots, p_r, c \in \mathbb{Z}_{>0}$ be defined as in Lemma 8.2. Let $n_1, \dots, n_r \in \mathbb{Z}_{>0}$ be such that ord$_{p_i}\Phi_{m_i}(c) = n_i$. Suppose there exists $b \in \mathbb{Z}$ be such that ord$_{p_i} b = n_i$ and Equations (1)–(4) below hold with variables ranging over $R''$.*

(1) $\alpha | (T^\ell - 1)$ *in* $R''$,
(2) $\alpha \equiv \pm 1 \bmod T$.
(3) *ord*$_{\mathfrak{q}_\infty}\alpha =$ *ord*$_{\mathfrak{q}_\infty} T^{\sum_{i=1}^{r} u_{m_i}}$.
(4) $\alpha \equiv b \mod (T-c)$ *in* $R''$.

*In this case $N_{K(T)/\mathbb{Q}(T)}(\alpha) = \prod_{i=1}^{r} \Phi_{m_i}(T)^d$, and $\alpha \in \mathbb{Q}(T)$. Conversely, if $\alpha = \prod_{i=1}^{r} \Phi_{m_i}(T)$, then there exists $b \in \mathbb{Z}$ be such that ord$_{p_i} b = n_i$ and (1) – (4) can be satisfied in the remaining variables over $R''$.*

*Proof.* Let $\mathfrak{Q}_\infty$ be the prime below $\mathfrak{q}_\infty$ in $\mathbb{Q}[T]$. By Corollary 2.11, the prime $\mathfrak{q}_\infty$ is the only prime above $\mathfrak{Q}_\infty$ in $K(T)$, and the ramification degree $e$ of $\mathfrak{q}_\infty$ over $\mathfrak{Q}_\infty$ is equal to $-\text{ord}_{\mathfrak{q}_\infty} T$. Therefore, by Proposition 2.1, we have that

$$f(\mathfrak{q}_\infty/\mathfrak{Q}_\infty) = -d/\text{ord}_{\mathfrak{q}_\infty} T,$$

where $f(\mathfrak{q}_\infty/\mathfrak{Q}_\infty)$ is the relative degree of $\mathfrak{q}_\infty$ over $\mathfrak{Q}_\infty$. Next observe that since $\alpha$ has a pole at $\mathfrak{q}_\infty$ only, $\alpha$ is integral with respect to $\mathbb{Q}[T]$, and therefore $N_{K(T)/\mathbb{Q}(T)}(\alpha)$ is a polynomial over $\mathbb{Q}$ in $T$. Further, using the assumption that $\text{ord}_{\mathfrak{q}_\infty}\alpha = \text{ord}_{\mathfrak{q}_\infty} T^{\sum_{i=1}^{r} u_{m_i}}$ and by Proposition 2.1 again, we have that

$$\begin{aligned} \deg(N_{K(T)/\mathbb{Q}(T)}(\alpha)) &= -\text{ord}_{\mathfrak{Q}_\infty} N_{K(T)/\mathbb{Q}(T)}(\alpha) = -f(\mathfrak{q}_\infty/\mathfrak{Q}_\infty) \cdot \text{ord}_{\mathfrak{q}_\infty}(\alpha) \\ &= \frac{d}{\text{ord}_{\mathfrak{q}_\infty} T} \text{ord}_{\mathfrak{q}_\infty}(\alpha) = \frac{d}{\text{ord}_{\mathfrak{q}_\infty} T} (\text{ord}_{\mathfrak{q}_\infty} T) \sum_{i=1}^{r} u_{m_i} = d \sum_{i=1}^{r} u_{m_i}. \end{aligned}$$

Second, since $\alpha | (T^\ell - 1)$ in $R''$, we have that $N_{K(T)/\mathbb{Q}(T)}(\alpha) \big| (T^\ell - 1)^d$ in $\mathbb{Q}[T]$. The polynomial $T^\ell - 1$ does not have any multiple roots in $\bar{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. Thus, the roots of $N_{K/\mathbb{Q}(T)}(\alpha)$ in $\bar{\mathbb{Q}}$ are of multiplicity at most $d$ and are $\ell$-th roots of unity.

Let $G(T) := N_{K(T)/\mathbb{Q}(T)}(\alpha) \in \mathbb{Q}[T]$. Then

$$G(T) = u \prod_{j | \ell} \Phi_j(T)^{a_j},$$

where $a_j \in \{0, 1, \dots, d\}$ and $u \in \mathbb{Q}$. By Lemma 7.6 and Assumption (2), we have that $G(0) = \pm 1$. By Lemma 8.1 we also have that $\prod_{j|\ell} \Phi_j(0)^{a_j} = \pm 1$. Thus, we conclude that $u = \pm 1$. We now note that $\text{ord}_{p_i} G(c) = \sum_{j|\ell} a_j \cdot \text{ord}_{p_i} \Phi_j(c_i) = a_i n_i$ by the assumption on $c$.

From Assumption (4) and Lemma 7.6, we have that $G(c) = \pm b^d$. Consequently, for all $i = 1, \dots, r$, we have that $\text{ord}_{p_i} G(c) = \text{ord}_{p_i} b^d = d \cdot \text{ord}_{p_i} b = n_i d$ by assumption on $b$. Hence, $a_i = d$ and

$$G(T) = \pm \prod \Phi_{m_i}(T)^d,$$

since $\deg(G(T)) = d \sum u_{m_i} = d \sum \deg(\Phi_{m_i}(T))$. Consequently,

$$N_{K(T)/\mathbb{Q}(T)} \left( \frac{\alpha}{\prod_{i=1}^r \Phi_{m_i}(T)} \right) = \pm 1,$$

implying that

$$\frac{\alpha}{\prod_{i=1}^r \Phi_{m_i}(T)}$$

is a unit of $R''$. But the only units of this ring are elements of the constant field $k$. Hence $\alpha = \mu \prod_{i=1}^r \Phi_{m_i}(T)$ for some $\mu \in k$. But by Assumption 2, we have that $\alpha \equiv \pm 1 \mod T$, and thus $\mu \prod_{i=1}^r \Phi_{m_i}(0) = \pm 1$, implying as before that $\mu = \pm 1$.

Conversely, suppose that $\alpha = \prod_{i=1}^r \Phi_{m_i}(T)$. We show that conditions (1) – (4) are now satisfied. Since $\ell \equiv 0 \mod m_i$, all roots of $\alpha$ are $\ell$-th roots of unity. So (1) is satisfied. Next we note (2) is satisfied by Lemma 8.1. The degree of $\alpha$ is $\sum_{i=1}^r u_{m_i}$. Hence, (3) is satisfied. Finally, by the Strong Approximation Theorem (see page 239 of [8]) we can find $b \in \mathbb{Z}$ such that $\text{ord}_{p_i} b = n_i = \text{ord}_{p_i} \Phi_{m_i}(c) = \text{ord}_{p_i} \alpha$. □

We now show that all conditions in Lemma 7.7 are Diophantine over $R$, and therefore the set $\mathscr{C}$ has a Diophantine description over $R$.

**Lemma 7.8.** $\{(a, b) \in R | a + bT \in \mathscr{C}\}$ *is Diophantine over* $R$.

*Proof.* We need to convert our assumptions on $\ell, m, c, b$ and Conditions (1) – (4) of Lemma 7.7 into a Diophantine definition of the set $\mathscr{C}$. First consider a recursive subset $Z$ of $\mathbb{Z}^4$ satisfying the following condition.

$$(\ell, c, b, n) \in Z$$

if and only if

(1) there exist $r, m_1, \dots, m_r \in \mathbb{Z}_{>1}$ such that $\ell = m_1 \dots m_r$, $(m_i, m_j) = 1$,
(2) there exist distinct $p_1, \dots, p_r$, where for each $i = 1, \dots, r$ we have that $p_i$ is a prime number, and $p_i - 1 \equiv 0 \mod \ell$.
(3) $n_i := \text{ord}_{p_i} \Phi_{m_i}(c) > 0$,
(4) For all $i = 1, \dots, r$, for all $j$ such that $\ell \equiv 0 \mod j$, it is the case that $j \neq m_i$ implies $\text{ord}_{p_i} \Phi_j(c) = 0$.
(5) $n = \sum_{i=1}^r n_i$,
(6) For all $i = 1, \dots, r$, we have that $\text{ord}_{p_i} b = n_i$.

By the MDRP theorem $Z$ is Diophantine over $\mathbb{Z}$ and therefore over $R$. Further, as we noted above, the set $\{(s, u_s, w_s), s \in \mathbb{Z}_{>0}\}$, where $u_s - \sqrt{a^2-1}w_s = T^s$, is Diophantine over $R$ by Corollary 3.14. Thus Condition (1) is Diophantine. Next we note that $\alpha \in R''$, and we can replace Condition (2) with

$$\frac{\alpha - 1}{T} \in R'' \vee \frac{\alpha + 1}{T} \in R''.$$

Further, Condition (3) can be replaced with

$$\text{ord}_{\mathfrak{q}_\infty} \frac{\alpha}{T^n} = 0.$$

The order condition is Diophantine over $R'$ as explained in Section 6. We replace Condition (4) with the following Diophantine condition: $\frac{\alpha - b}{T - c} \in R''$. □

7.5. **A Diophantine definition of $\mathbb{Z}[T]$ over $R''$.** We will now use Proposition 7.5 to give an existential definition of all polynomials in $\mathbb{Z}(T)$ over $R''$ using the "Weak Vertical Method". The idea of this method can be summarized as follows. Let $R_1 \subset R_2$. Suppose $x \in R_2, y \in R_1, w \in R_1$ and by some measure of ”size”, to be made precise below, we have that $w$ is much larger than $x$. Assume additionally, that $x \equiv y \bmod w$ in $R_2$. Then $x \in R_1$.

7.5.1. *A bound on "size".* In our case the "size" of an element $X \in R''$ is its order at $\mathfrak{q}_\infty$. Since $\mathfrak{q}_\infty$ is the only pole allowed for elements of $R''$, the order at $\mathfrak{q}_\infty$ is in fact the degree of the pole divisor of $X$ or the height of $X$. We consider elements of $R''$ in terms of their coordinates with respect to the power basis of $\beta$. We want to bound the order at $\mathfrak{Q}_\infty$ of the coordinates of an element $X \in R''$ with respect to the power basis of $\beta$ in terms of the order at $\mathfrak{q}_\infty$ of the element itself. Before we start, we make the following observation:

**Lemma 7.9.** *Let* $Z \in O_{K(T),q_\infty}$, *and let* $Z = g_0 + g_1\beta + \ldots + g_{d-1}\beta^{d-1}, g_i \in \mathbb{Q}(T)$. *Let*

$$A = (\sigma_j(\beta^i)), j = 1, \ldots, d, i = 0, \ldots, d-1.$$

*Then* $(\det A)^2 g_i \in \mathbb{Q}[T]$.

*Proof.* We proceed via a "Linear Algebra" proof of the sort described in Chapter 9 of [20]. Let $L$, as above, be the Galois closure of $K(T)$ over $\mathbb{Q}(T)$. Let $\mathscr{T} = \{\mathfrak{t}_1, \ldots, \mathfrak{t}_s\}$ be the set of all distinct factors of $\mathfrak{q}_\infty$ in $L$. Since $\mathfrak{q}_\infty$ is the only factor of the infinite prime $\mathfrak{Q}_\infty$ of $\mathbb{Q}(T)$ in $K(T)$, we have that $\mathscr{T}$ also contains all factors of $\mathfrak{Q}_\infty$ in $L$. Let $\sigma_1 = \text{id}, \ldots, \sigma_d \in \text{Gal}(L/\mathbb{Q}(T))$ be such that the set $\{\sigma_1(\beta), \ldots, \sigma_d(\beta)\}$ contains all distinct conjugates of $\beta$ over $\mathbb{Q}(T)$.

Now consider the following system of linear equations.

$$A\bar{a} = \bar{Z},$$

where

$$A = (\sigma_j(\beta^i)), j = 1, \ldots, d, i = 0, \ldots, d-1,$$
$$\bar{a} = (g_0, \ldots, g_{d-1})^t, \bar{Z} = (\sigma_1(Z), \ldots, \sigma_d(Z))^t.$$

(Here "$t$" denotes transpose.) Since $\sigma_j(\beta) \neq \sigma_r(\beta)$ for all $j \neq r \in \{1, \ldots, d\}$, we have that $\det(A) \neq 0$ as a Vandermonde determinant. Using Kramer's Rule, we can solve for $g_0, \ldots, g_{d-1}$ in terms of $\det(A), \sigma_r(X)$ with $r = 1, \ldots, d$. We obtain that

$$g_j = \frac{\det A_j}{\det A},$$

where $A_j$ is the matrix obtained from $A$ by replacing its $j$-th column by the column $(\sigma_1(Z), \ldots, \sigma_d(Z))^t$. Since $Z, \beta \in R''$, all entries of $A_j$ and $A$ have poles at all factors of $\mathfrak{q}_\infty$ in $L$, and no other poles. (This is so because $\mathfrak{q}_\infty$ and $\sigma(\mathfrak{q}_\infty)$ have the same factorization in $L$. ) Therefore, if we set $D = \det^2(A) \in \mathbb{Q}[T]$, then $u_j = Dg_j = \det A \det A_j \in \mathbb{Q}(T) \cap O_{L,\{\mathfrak{t}_1,\ldots,\mathfrak{t}_s\}} = \mathbb{Q}[T]$, by Corollary 2.8.

□

Given $X \in O_{K(T),\mathfrak{q}_\infty}$ written as $X = \sum_{i=0}^{d-1} c_i\beta^i, c_i \in \mathbb{Q}(T)$, we know $a_i = \det(A)c_i \in \mathbb{Q}[T]$. What we want now is a bound on the degree of $a_i$ in terms of $\mathbf{ord}_{\mathfrak{q}_\infty} X$. The next proposition gives us this bound.

**Proposition 7.10.** *Let $X \in R'', X \notin k$, and let $X = \sum_{i=0}^{d-1} c_i\beta^i, c_i \in \mathbb{Q}(T)$. Let $D = \det A, a_i = Dc_i$ as above. Then there exist $C = C(\beta) \in \mathbb{R}_{>0}$ dependent on $\beta$ only, such that for all $i = 0, \ldots, d-1$ we have that*

$$\textit{deg}(a_i) < C|\textit{ord}_{\mathfrak{q}_\infty} X|.$$

*Proof.* We start with a claim concerning the order of conjugates of $X$ over $\mathbb{Q}(T)$ at the factors of $\mathfrak{q}_\infty$ in $L$.

*Claim:* For any $i = 1, \ldots, s$ and any $\sigma \in \mathrm{Gal}(L/\mathbb{Q}(T))$, it is the case that

$$\mathbf{ord}_{\mathfrak{t}_i}\sigma(X) = \mathbf{ord}_{\mathfrak{t}_1} X.$$

*Proof of the claim:* Since $\mathfrak{t}_1, \ldots, \mathfrak{t}_s$ are conjugates over $K(T)$ and $\mathbb{Q}(T)$, the Galois group $\mathrm{Gal}(L/K(T))$ acts transitively on the set $\mathscr{T}$, and all elements of $\mathrm{Gal}(L/\mathbb{Q}(T))$ permute $\mathscr{T}$. So, fix $i \in \{1, \ldots, s\}$ and $\sigma \in \mathrm{Gal}(L/\mathbb{Q}(T))$. For some $r \in \{1, \ldots, s\}$, we have that $\sigma(\mathfrak{t}_r) = \mathfrak{t}_i$. Let $\mu \in \mathrm{Gal}(L/K(T))$ be such that $\mu(\mathfrak{t}_1) = \mathfrak{t}_r$. Then

$$\mathbf{ord}_{\mathfrak{t}_1} X = \mathbf{ord}_{\sigma\mu(\mathfrak{t}_1)}\sigma\mu(X) = \mathbf{ord}_{\mathfrak{t}_i}\sigma(X).$$

Similarly, $\mathbf{ord}_{\mathfrak{t}_1}\beta = \mathbf{ord}_{\mathfrak{t}_i}\sigma(\beta)$ for all $i = 1, \ldots, s, \sigma \in \mathrm{Gal}(L/\mathbb{Q}(T))$. □

Since $a_i \in \mathbb{Q}[T]$, we have that $\mathbf{ord}_{\mathfrak{t}_1} a_j < 0$. Let $A_{i,j}$ be the $i, j$-th minor of $A$, as above. Then $\mathbf{ord}_{\mathfrak{t}_1} \det A < 0, \mathbf{ord}_{\mathfrak{t}_1} \det A_{i,j} < 0$ and these orders depend on $\beta$ only. Let $C_1 = \max_{i,j}(|\mathbf{ord}_{\mathfrak{t}_1} \det A|, |\mathbf{ord}_{\mathfrak{t}_1} \det A_{i,j}|)$.

We now make the following observation we will use in our calculations below. Let $Y = \sum_r Y_r \in L$. Assume $\mathbf{ord}_{\mathfrak{t}_1} Y < 0$, and for all $r$ we have that $\mathbf{ord}_{\mathfrak{t}_1} Y_r < 0$. Let $Y^*$ be such that $\mathbf{ord}_{\mathfrak{t}_1} Y^* = \min_r\{\mathbf{ord}_{\mathfrak{t}_1} Y_r\}$. Then $\mathbf{ord}_{\mathfrak{t}_1} Y \geq \mathbf{ord}_{\mathfrak{t}_1} Y^*$ by a property of non-archimedean valuations, and $-\mathbf{ord}_{\mathfrak{t}_1} Y \leq -\mathbf{ord}_{\mathfrak{t}_1} Y^*$. Since $\mathbf{ord}_{\mathfrak{t}_1} Y < 0, \mathbf{ord}_{\mathfrak{t}_1} Y^* < 0$, it follows that $|\mathbf{ord}_{\mathfrak{t}_1} Y| \leq |\mathbf{ord}_{\mathfrak{t}_1} Y^*|$.

Using co-factors along the $j$-th column, we see that $\det A_j = \sum_{i=0}^{d-1} \pm\sigma_{i+1}(X) \det A_{i,j}$. Further, using the observation above and the fact $\mathbf{ord}_{\mathfrak{t}_1}\sigma_j(X) = \mathbf{ord}_{\mathfrak{t}_1} X$, we also conclude that

$$|\mathbf{ord}_{\mathfrak{t}_1} \det A_j| = |\mathbf{ord}_{\mathfrak{t}_1}(\sum_{i=0}^{d-1} \pm\sigma_{i+1}(X) \det A_{i,j})| \leq |\mathbf{ord}_{\mathfrak{t}_1} X| + C_1 < 2C_1|\mathbf{ord}_{\mathfrak{t}_1} X|.$$

Thus,

$$|\mathbf{ord}_{\mathfrak{t}_1} a_j| = |\mathbf{ord}_{\mathfrak{t}_1} \det A + \mathbf{ord}_{\mathfrak{t}_1} \det A_j| < C_1 + 2C_1|\mathbf{ord}_{\mathfrak{t}_1} X| < 3C_1|\mathbf{ord}_{\mathfrak{t}_1} X| = C|\mathbf{ord}_{\mathfrak{t}_1} X|,$$

where $C := 3C_1$. Therefore,

$$\mathbf{deg}(a_j) = |\mathbf{ord}_{\mathfrak{Q}_\infty} a_i| \leq |\mathbf{ord}_{\mathfrak{q}_\infty} a_i| < C|\mathbf{ord}_{\mathfrak{q}_\infty} X|,$$

where $C = C(\beta)$ depends on $\beta$ only. □

7.5.2. *Diophantine generation of* $\mathbb{Z}[T]$ *over* $R = O_{K,\mathscr{S}}$. The main proposition of this section is the following one.

**Proposition 7.11.** *The set* $\{(a,b) \in O_{K,\mathscr{S}} | a + bT \in \mathbb{Z}[T]\}$ *is Diophantine over* $R$.

*Proof.* Let $z = z(\beta)$ be a fixed positive integer such that $z(\beta) > C(\beta)$. We start with the following claim.

*Claim:* Given $Y \in R'' \setminus k$, the following system of equations and conditions can be satisfied over $R''$ if only if $Y \in \mathbb{Z}[T]$, and $Y(0) = \pm 1$.

$$M \in \mathscr{C} \subset \mathbb{Z}[T], \tag{7.23}$$

$$\mathbf{ord}_{\mathfrak{q}_\infty} \frac{T^\ell}{Y^z} < 0, \tag{7.24}$$

$$Y \equiv M \bmod T^\ell \text{ in } R''. \tag{7.25}$$

*Proof of the claim:*

First we assume that the Equations (7.23)–(7.25) are satisfied. By Lemma 6.3, we can write $Y = \sum_{i=0}^{d-1} c_i \beta^i$, where $c_i \in \mathbb{Q}(T)$, $Dc_i \in \mathbb{Q}[T], D = (\det A)^2$. Further, by Proposition 7.10, we know that $\mathbf{deg}(Dc_i) < C(\beta)\mathbf{ord}_{\mathfrak{q}_\infty} Y$, Next, we observe that

$$Y - M = (c_0 - M) + c_1(T)\beta + \ldots + c_{d-1}(T)\beta^{d-1},$$

and

$$\frac{Y - M}{T^\ell} \in O_{K(T),\{\mathfrak{q}_\infty\}},$$

by Equation 7.25. Further, by Lemma 7.9

$$\frac{Y - M}{T^\ell} = f_0 + f_1\beta + \ldots + f_{d-1}\beta^{d-1},$$

where $Df_i \in \mathbb{Q}[T]$. We can represent $Y$ as a linear combination of powers of $\beta$ using $f_i$'s as

$$Y = (T^\ell f_0 + M) + T^\ell f_1 \beta + \ldots + T^\ell f_{d-1}\beta^{d-1}.$$

Since $\mathbb{Q}(T)$-coordinates of elements of $K(T)$ with respect to the power basis of $\beta$ are unique, we conclude that for $i = 1, \ldots, d-1$, $f_i = \frac{c_i}{T^\ell}$, and $Df_i = \frac{Dc_i}{T^\ell} \in \mathbb{Q}[T]$. Thus,

$$|\mathbf{ord}_{\mathfrak{q}_\infty} T^\ell| < |\mathbf{ord}_{\mathfrak{q}_\infty} Dc_i| < C(\beta)|\mathbf{ord}_{\mathfrak{q}_\infty} Y|, \tag{7.26}$$

or $c_i = 0$ for $i > 0$. If Inequality (7.26) holds, then by Inequality (7.24) we have that

$$|\mathbf{ord}_{\mathfrak{q}_\infty} Y^z| = |z\mathbf{ord}_{\mathfrak{q}_\infty} Y| < |\ell\mathbf{ord}_{\mathfrak{q}_\infty} T| < C(\beta)|\mathbf{ord}_{\mathfrak{q}_\infty} Y|,$$

so that $z < C(\beta)$. The last inequality contradicts our assumptions on $z$. Consequently, we have to conclude that $c_i = 0$ for $i = 1, \dots, d-1$, and $Y \in \mathbb{Q}[T]$.

We now return to Inequality (7.24) and use the fact that we now know that $Y \in \mathbb{Q}[T]$. We can therefore restate this inequality as saying

$$\deg(T^\ell) > \deg(Y^z) > \deg(Y).$$

Thus from Equation (7.25) we conclude that all coefficients of $Y$ are the same as the first $\deg(Y)$ coefficients of $M$. However, $M \in \mathbb{Z}[T]$, and $M(0) = \pm 1$. Hence the same must be true of $Y$.

We now assume that $Y \in \mathbb{Z}[T]$ and $Y(0) = \pm 1$. Let $\ell > z \cdot \deg(Y)$. Then $\text{ord}_{\mathfrak{q}_\infty} \frac{T^\ell}{Y^z} < 0$, and Inequality (7.24) will be satisfied. By Proposition 7.5, we can find $M \in \mathscr{C}$ to satisfy Equation (7.25). This completes the proof of the Claim.

A few quick observations now complete the proof of the proposition. First, we note that if a polynomial $R \in \mathbb{Z}[T]$, then there exists $c \in \mathbb{Z}$ such that $Y = R + c$ has its constant term equal to 1. Second, we remind the reader that we have a Diophantine definition of elements of $\mathbb{Z}$ from Theorem 3.9. We also have a definition of non-constant elements of $R''$. The non-constant elements must have a negative order at $\mathfrak{q}_\infty$. Third, we remind the reader that by Lemma 7.4, the set $\{a, b \in R | a + bT \in R''\}$ is Diophantine over $R$. Finally, we remind the reader that the set $\mathscr{C}$ is Diophantine over $R''$ by Lemma 7.8. □

From this point on, to complete the proof of Theorem 7.1, we proceed as in the proof outline starting with Part 5.

## 8. Appendix

This section contains some facts about roots of unity and real roots of polynomial equations collected here for the convenience of the reader.

8.1. **Roots of Unity.** Below, for $r \in \mathbb{Z}_{>0}$, the polynomial $\Phi_r(X) \in \mathbb{Z}[X]$ denotes the monic irreducible polynomial of a primitive $r$-th root of unity $\xi_r$.

**Lemma 8.1.** *For every positive integer $t > 1$, it is the case that $\Phi_t(0) = \pm 1$.*

*Proof.* Observe that $\Phi_t(X)\Big|(1 + X + \dots + X^{t-1})$ in $\mathbb{Z}[X]$, and therefore for some $U(X) \in \mathbb{Z}[X]$ we have that $\Phi_t(X)U(X) = 1 + X + \dots + X^{t-1}$. Hence, $\Phi_t(0)U(0) = 1$, where $\Phi_t(0), U(0) \in \mathbb{Z}$. So, $\Phi_t(0) = \pm 1$. □

**Lemma 8.2.** *Let $r \in \mathbb{Z}_{>0}$. Let $\ell = m_1 \dots m_r$, where $m_1, \dots, m_r$ are pairwise relatively prime positive integers. Then there exists a set $\{p_1, \dots, p_r\}$ of distinct prime numbers satisfying the following conditions:*

1. *For all $i = 1, \dots, r$ we have that $p_i \equiv 1 \bmod \ell$.*
2. *For any $i, j \in \mathbb{Z}_{>0}$ such that $\ell \equiv 0 \bmod j, \ell \equiv 0 \bmod i$ and $j \neq i$ it is the case that $(\Phi_j(\xi_i), p_i) = 1$ in the ring of algebraic integers of $\mathbb{Q}(\xi_\ell)$.*

*Further, there exists $c \in \mathbb{Z}_{>0}$ such that $\text{ord}_{p_i}(\Phi_{m_i}(c)) > 0$, and for all $j|\ell, j \neq m_i$ we have that $\text{ord}_{p_i}\Phi_j(c) = 0$.*

*Proof.* First of all, we note that the arithmetic sequence $(t\ell+1)_{t\in\mathbb{Z}_{>0}}$ contains infinitely many primes by the Dirichlet Density Theorem (see Chapter VIII, §4 of [11]). Therefore, we can pick distinct primes $p_1,\ldots,p_r$ so that all of the primes are odd and none of these prime divides $\mathrm{N}_{\mathbb{Q}(\xi_i)/\mathbb{Q}}(\Phi_j(\xi_i))$ for all $i\neq j$ dividing $\ell$.

Now consider $\mathbb{F}_{p_i}$, a field of $p_i$ elements for some $i=1,\ldots,r$. The group of units of this field is cyclic. Let $t$ be a generator of the unit group. Let $s\in\mathbb{Z}_{>0}$ be a divisor of $\ell$. Then $s$ divides $p_i-1$. Let $r=(p_i-1)/s$. Then, $t^r$ is an $s$-th primitive root of unity in $\mathbb{F}_{p_i}$ and the polynomial

$$X^s-1 \tag{8.27}$$

factors completely in $\mathbb{F}_{p_i}$. By Hensel's Lemma (Chapter II, §3, Proposition 3.5 of [9]), we have that the polynomial (8.27) factors completely in $\mathbb{Q}_{p_i}$- the field of $p_i$-adic numbers, or in other words, the $s$-th primitive root of unity $\xi_s\in\mathbb{Q}_{p_i}$ for all positive integers $s$ dividing $\ell$. Let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\xi_s)$ lying above $p_i$. Then $(\mathbb{Q}(\xi_s))_{\mathfrak{p}}\cong\mathbb{Q}_{p_i}(\xi_s)\cong\mathbb{Q}_{p_i}$.

Thus, there is an embedding of $\mathbb{Q}(\xi_s)$ into $\mathbb{Q}_{p_i}$ that maps the ideal generated by a factor of $p_i$ in the ring of integers of $\mathbb{Q}(\xi_s)$ into the ideal generated by $p_i$ in the ring of integers of $\mathbb{Q}_{p_i}$. If $j\neq s$ for some positive integers $j,s$ dividing $\ell$, then by assumption $\Phi_j(\xi_s)$ is not contained in any ideal generated by a factor of $p_i$ in the ring of integers of $\mathbb{Q}(\xi_s)$. Thus, in $\mathbb{Q}_{p_i}$, we have that $\mathrm{ord}_{p_i}(\Phi_j(\xi_s))=0$.

For each $i=1,\ldots,r$ we pick $c_i\in\mathbb{Z}_{>0}$ such that $\mathrm{ord}_{p_i}(c_i-\xi_{m_i})>0$, where we consider $\xi_{m_i}$ as an element of $\mathbb{Q}_{p_i}$. Observe that this choice of $c_i$ implies that

$$\mathrm{ord}_{p_i}\Phi_{m_i}(c_i)=\mathrm{ord}_{p_i}(\Phi_{m_i}(c_i)-\Phi_{m_i}(\xi_{m_i}))\geq\mathrm{ord}_{p_i}(c_i-\xi_{m_i})>0.$$

At the same time, if $j$ is a positive integer dividing $\ell$ and $j\neq m_i$, then by assumption on $p_i$ we have that

$$\mathrm{ord}_{p_i}\Phi_j(c_i)=\min(\mathrm{ord}_{p_i}(\Phi_j(c_i)-\Phi_j(\xi_{m_i})),\mathrm{ord}_{p_i}(\Phi_j(\xi_{m_i})))=\mathrm{ord}_{p_i}(\Phi_j(\xi_{m_i}))=0.$$

By the Strong Approximation Theorem (see page 239 of [8]), we can find $c\in\mathbb{Z}$ such that

$$\mathrm{ord}_{p_i}(c-c_i)>\mathrm{ord}_{p_i}(\Phi_{m_i}(c_i))>0.$$

Then $\mathrm{ord}_{p_i}\Phi_{m_i}(c)=\min(\mathrm{ord}_{p_i}(\Phi_{m_i}(c)-\Phi_{m_i}(c_i)),\mathrm{ord}_{p_i}(\Phi_{m_i}(c_i)))=\mathrm{ord}_{p_i}(\Phi_{m_i}(c_i))$. Finally, if $j$ divides $\ell$ and $j\neq m_i$, then we have

$$\mathrm{ord}_{p_i}(\Phi_j(c))=\min(\mathrm{ord}_{p_i}(\Phi_j(c)-\Phi_j(c_i)),\mathrm{ord}_{p_i}(\Phi_j(c_i)))=\mathrm{ord}_{p_i}(\Phi_j(c_i))=0.$$

□

### 8.2. **Real Roots.**

**Proposition 8.3.** *Let $f(t)\in\mathbb{Q}[t]$ be a polynomial of degree $d$ irreducible over $\mathbb{Q}$ such that all of its roots are real. Let $\alpha_1<\ldots<\alpha_d$ be all of the roots of $f(t)$ in $\mathbb{R}$. Let $P_r(t)\in\mathbb{Q}(\alpha_r)[t]$. Then there is an algorithm to determine whether $P_r(t)$ has any real roots for any $r\in\{1,\ldots,d\}$.*

*Proof.* We can write $P_r(t) = \sum_{i=0}^{\deg(P_r(t))-1} A_{r,i}t^i$, where $A_{r,i} \in \mathbb{Q}(\alpha_r)$. Since $A_{r,i} = \sum_{i=0}^{d-1} a_{r,i,j}\alpha_r^j$, where $a_{r,i,j} \in \mathbb{Q}$, we can now rewrite

$$P_r(t) = \sum_{i=0}^{\deg(P_r(t))-1} \left( \sum_{j=0}^{d-1} a_{r,i,j}\alpha_r^j t^i \right) = Q_r(t, \alpha_r) \in \mathbb{Q}[t, \alpha_r].$$

Fix $r \in \{1, \ldots, d\}$ and consider the following system

$$(8.28) \qquad \left\{ \begin{array}{c} f(x_1) = 0, \\ \vdots \\ f(x_d) = 0, \\ x_1 - x_2 = u_{1,2}^2 + v_{1,2}^2 + w_{1,2}^2 + z_{1,2}^2, \\ x_2 - x_3 = u_{2,3}^2 + v_{2,3}^2 + w_{2,3}^2 + z_{2,3}^2, \\ \vdots \\ x_{d-1} - x_d = u_{d-1,d}^2 + v_{d-1,d}^2 + w_{d-1,d}^2 + z_{d-1,d}^2, \\ w_1(x_1 - x_2) = 1 \\ \vdots \\ w_d(x_d - x_{d-1}) = 1 \\ Q_r(t, x_r) = 0. \end{array} \right.$$

We claim that System 8.28 has a solution $(\beta_1, \ldots, \beta_d, \mu) \in \mathbb{R}^{d+1}$ if and only if $P_r(t)$ has a root in $\mathbb{R}$. Indeed, suppose the system has solutions in $\mathbb{R}$. Then $x_i = \alpha_i, i = 1, \ldots, d$, and $Q_r(t, x_r) = P_r(t)$ has a real root. Conversely, suppose $P_r(t)$ has a real root $\beta_r$. Then we can set $x_i = \alpha_i$, and $t = \beta_r$ to obtain a solution for the system.

By a result of A. Tarski ([25]) there is an algorithm to decide whether System (8.28) has real solutions. □

**Corollary 8.4.** *Let $f(t) \in \mathbb{Q}(t), \alpha_1, \ldots, \alpha_d$ be as in Proposition 8.3. Let $P_r(t) \in \mathbb{Q}(\alpha_r)$. Assume further that deg($P_r(t)$) is even and the leading coefficient is positive. Then there is an algorithm to determine whether there exists $\gamma_r \in \mathbb{R}$ such that $P_r(\gamma_r) \leq 0$.*

*Proof.* Since $\lim_{t \to \pm\infty} P_r(t) = \infty$, if there exists $\gamma_r \in \mathbb{R}$ such that $P_r(\gamma_r) \leq 0$, then $P_r(t)$ has real roots. Conversely, if $P_r(t)$ has real roots, then for some $\gamma_r \in \mathbb{R}$ we have that $P_r(\gamma_r) \leq 0$. □

## References

[1] Chevalley, C., *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, AMS, Providence, RI, 1951, vol. 6.

[2] Childress, N., *Class Field Theory*, Springer, 2009.

[3] Davis, M., On the number of solutions of Diophantine equations, Proc. Amer. Math. Soc. 35, 1972, 562-564

[4] Demeyer, J., “Diophantine sets of polynomials over number fields”, Proc. Amer. Math. Soc. 138 (2010), no. 8, 2715-2728.

[5] Denef, J., “The diophantine problem for polynomial rings of positive characteristic”, 1979, Logic colloquium 78, Boffa, M., van Dalen, D., MacAloon, K. editors, North Holland, 131 - 145.

[6] Denef, J., Diophantine sets over $\mathbf{Z}[T]$, Proc. Amer. Math. Soc., 69(1), 1978, 148-150

[7] Eisenträger, K., “Hilbert’s Tenth Problem for function fields of varieties over number fields and p-adic fields”, 2007, Journal of Algebra, 2007, volume 310, 775- 792.

[8] Fried, M. and Jarden, M., *Field Arithmetic*, Springer 2008, Third edition

[9] Janusz, G,. Algebraic Number Fields, Academic Press, 1973.

[10] Kim, H.,Roush, F. W.,“Diophantine unsolvability over $p$-adic function fields” 1995, Journal of Algebra,176, 83 - 110.

[11] Lang, S., *Algebraic number theory*, Addison Wesley, Reading, MA, 1970.

[12] Lang S., *Algebra*, Springer, 2002, Third edition.

[13] Matiyasevich, Y., “Towards finite-fold Diophantine representations”, 2010, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI), 377, Issledovaniya po Teorii Chisel. 10, 78-90.

[14] Matiyasevich, Y., “Existence of non-effectivizable estimates in the theory of exponential diophantine equations”, 1977, Journal of Soviet Mathematics, 8(3), 299- 311,

[15] Moret-Bailly, L., “Elliptic curves and Hilbert’s Tenth Problem for algebraic function fields over real and $p$-adic fields”, 2006, Journal für Reine und Angewandte Mathematic, 587, 77- 143.

[16] Pourchet, Y., “Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques”, 1971, Acta Arith., 9, 89-104

[17] Poonen, B. and Shlapentokh, A., “Diophantine definability of infinite discrete non-archimedean sets and diophantine models for large subrings of number fields”, 2005, Journal für die Reine und Angewandte Mathematik, 588, 27-48.

[18] Ribenboim, P. *The Theory of Classical Valuations*, Springer, 1998.

[19] Shimura, G., *Arithmetic of Quadratic Forms*, Springer, 2010.

[20] Shlapentokh, A., *Hilbert’s tenth problem: Diophantine classes and extensions to global fields*, Cambridge University Press, 2006.

[21] Shlapentokh, A., “Diophantine definitions for some polynomial rings”, 1990, Comm. Pure Appl. Math., 43(8), 1055-1066.

[22] Shlapentokh, A., “Hilbert’s tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic”, Trans. Amer. Math. Soc. 333 (1992), no. 1, 275-298.

[23] Smoryński, C., A note on the number of zeros of polynomials and exponential polynomials, J. Symbolic Logic, 42(1), 1977, 99-106.

[24] Soare, R. I., Recursively enumerable sets and degrees, Perspectives in Mathematical Logic, A study of computable functions and computably generated sets, Springer-Verlag, Berlin,1987

[25] Tarski, A., A decision method for elementary algebra and geometry. Quantifier elimination and cylindrical algebraic decomposition (Linz, 1993), Texts Monogr. Symbol. Comput., Springer, Vienna, 1998, 24-84.

[26] Zahidi, K., On Diophantine sets over polynomial rings, Proc. Amer. Math. Soc. 128(3), 2000, 877-884.

DEPARTMENT OF MATHEMATICS
QUEENS COLLEGE – C.U.N.Y.
65-30 KISSENA BLVD.
QUEENS, NEW YORK 11367 U.S.A.
PH.D. PROGRAMS IN MATHEMATICS & COMPUTER SCIENCE
C.U.N.Y. GRADUATE CENTER
365 FIFTH AVENUE
NEW YORK, NEW YORK 10016 U.S.A.
*E-mail:* Russell.Miller@qc.cuny.edu
*Web page:* qcpages.qc.cuny.edu/~rmiller

DEPARTMENT OF MATHEMATICS
EAST CAROLINA UNIVERSITY
GREENVILLE, NC 27858 U.S.A.
*E-mail:* shlapentokha@ecu.edu
*Web page:* myweb.ecu.edu/shlapentokha