First-order Definitions of Rational Functions and S-integers over Holomorphy Rings of Algebraic Functions of Characteristic 0.

Alexandra Shlapentokh*
Department of Mathematics
East Carolina University
Greenville, NC 27858
shlapentokha@mail.ecu.edu

April 4, 2005

Abstract

We consider the problem of constructing first-order definitions in the language of rings of holomorphy rings of one variable function fields of characteristic 0 in their integral closures in finite extensions of their fraction fields and in bigger holomorphy subrings of their fraction fields. This line of questions is motivated by similar existential definability results over global fields and related questions of Diophantine decidability.

1 Introduction.

This paper grew out of attempts to reproduce some existential definability results, obtained for global fields, over one variable function fields of characteristic zero. To refer to fields of both types we will use the term "product formula fields". Product formula fields posses discrete valuations, i.e. homomorphisms from the multiplicative group of the field into $\mathbb{Z}$. These valuations correspond to prime ideals of rings of algebraic integers when K is a number field or to the prime ideals of the integral closure of a polynomial ring, when K is a function field. This correspondence will allow us to use the terms "valuations" and "primes" interchangeably.

If $\mathcal{W}$ is a set of primes of K, we can define a ring

$$O_{K,\mathcal{W}} = \{z \in K | \text{ord}_{\mathfrak{t}} z \geq 0, \forall \mathfrak{t} \notin \mathcal{W}\},$$

where $\text{ord}_{\mathfrak{t}} z$ is the value of the valuation corresponding to the prime $\mathfrak{t}$ on z. If $\mathcal{W}$ is finite, $O_{K,\mathcal{W}}$ is called a ring of $\mathcal{W}$-integers. If $\mathcal{W}$ is arbitrary and K is a function field, then $O_{K,\mathcal{W}}$ is called a holomorphy ring of K. (More information about these rings can be found in Chapter 2 of [12].) Given a finite extension L/K of product formula fields, one could try to give an existential definition in the language of rings of $O_{K,\mathcal{W}}$ in its integral closure in L. (The integral closure of a holomorphy ring or its analog over a number field is also a holomorphy ring or its analog.) Another existential definability question concerns producing an existential definition in the language of rings of $O_{K,\mathcal{W}}$ over K. Both questions grew out of attempts to extend Hilbert's Tenth Problem originally solved over $\mathbb{Z}$ to other domains. (See [9] for an introduction to the subject.)

Existential definitions of $\mathbb{Z}$ have been constructed over rings of integers of some number fields, but the general problem is still open. There are also some results where $\mathbb{Z}$ and rings of integers are existentially defined over some rings $O_{K,\mathcal{W}}$, where K is a number field distinct from $\mathbb{Q}$ and $\mathcal{W}$ is infinite. (These results

*The research for this paper has been partially supported by NSF grants DMS-9988620, DMS-0354907 and ECU Thomas Harriot College of Arts and Sciences Research Award.

can be found in [5], [8], [7], [20], [27], [28], [33], [35], [39], and [21].) However, we have no results concerning existential definability of rings of integers over any number field and there are serious doubts about the existence of such definitions. (See [15], [16], [17], [18], [3], [4], [40] and [22] for more details concerning this issue.)

Similar questions have been investigated over function fields of positive characteristic. There the question of giving an existential definition of rings of $\mathcal{W}$-integers over their integral closure in the extensions has been resolved completely in [30] for the case when the constant field is finite. Further, existential definitions of rings of $\mathcal{S}$-integers have been constructed over holomorphy rings $O_{K,\mathcal{W}}$ for function fields K over finite field of constants and infinite $\mathcal{W}$ of Dirichlet density arbitrarily closed to 1. (See [34] and [37] for more details.) However, the problem of giving an existential definition of a ring of integers over its fraction field remains unsolved.

The questions of the first-order definability over global fields have been resolved completely by J. Robinson for number fields (see [24] and [25]) and R. Rumely for function fields over finite fields of constants (see [26]).

The definability (and (un)decidability) situation turned out to be far more vexing over function fields of characteristic 0. There are existential and first order definability results producing definitions of $\mathbb{Z}$ and Diophantine models over various rings and fields of rational and algebraic functions (e.g. [2], [1], [6], [13], [41], [42], [19], [11], [10], [29] and [38]). The most general Diophantine undecidability results for one-variable case are due to Moret-Bailly ([19]) and Eisenträger ([10]). These results, which are generalizations of results by Denef and Kim and Roush, show Diophantine undecidability of function fields whose constant fields are subfields of p-adics or are formally real. They also show Diophantine undecidability of semilocal subrings of function fields over any field of constants of characteristic 0.

The results which are conspicuously absent from the "known" list concern the fields with algebraically closed fields of constants. The main stumbling block here is an existential or even a first-order definition of order at a function field prime. We should also note here that an undecidability or a definability result for a field usually implies the analogous results for all the holomorphy subrings of the field. On the other hand, results for rings (e. g. semi-local holomorphy subrings) do not in general imply the analogous results for all the other holomorphy sub rings of the field unless we have a definition of order.

Despite a great deal of progress in the study of definability and decidability of function fields of characteristic 0, until now there have been no results asserting first-order or existential definability of any ring of $\mathcal{S}$-integers of a function field of characteristic 0 over a much bigger holomorphy ring. In this paper we produce the first results of this kind. We also will produce some existential undecidability results for holomorphy subrings complementing results of Moret-Bailly and Eisenträger.

Before proceeding further we should describe the languages we will use for our first-order definitions. Let

$$\mathcal{L}_R(a_1, \ldots, a_m) = (0, 1, +, \cdot, a_1, \ldots, a_m)$$

be a language of rings with finitely many additional constant symbols besides "0" and "1". All the first-order and existential definitions in this paper will be done in such a language.

Our main results are contained in the following theorems.

Theorem 5.3.

Let E/K be a finite extension of function fields of characteristic 0 such that the field of constants of E is a number field. Let $\mathcal{S}_K$ be a finite set of primes of K. Let $\mathcal{S}_E$ be the set of all the primes of E lying above $\mathcal{S}_K$. Then $O_{K,\mathcal{S}_K}$ is first-order definable over $O_{E,\mathcal{S}_E}$.

Theorem 5.2.

Let K be a function field of characteristic 0 over a field of constants C. Let M be any number field contained in C, including $\mathbb{Q}$. Let $\mathcal{S}_K$ be a finite set of primes of K. Let $x \in O_{K,\mathcal{S}_K}$. Then $M[x]$ has a first order

definition over $O_{K,\mathcal{S}_K}$.

Theorem 5.5.

Let K be a function field of characteristic 0 over a field C satisfying the "high genus equations" condition or a formally real field with Archimedean order. (The "high genus equations" condition is described in Definition 4.8.) Let $\mathcal{S}_K$ be a finite set of primes of K. Then there exists an infinite set of K-primes $\mathcal{W}_K$ (with infinite complement) such that $O_{K,\mathcal{S}_K}$ and $\mathbb{Z}$ have first-order definitions over $O_{K,\mathcal{W}_K}$.

We also prove several other definability and undecidability results over holomorphy rings.

2 Overview of Main Ideas and Some Preliminary Facts.

The main method used in this paper is a version of a "weak vertical method" described in [36]. The obstacle, which arises over function fields of characteristic 0 and which has been overcome over global fields, is the lack of suitable "bound equations" as described in [36]. To construct "bound equations" over global fields one can rely on the fact that the residue fields of all the primes are finite, while this is certainly not the case in the case of characteristic zero function fields. The lack of "bound equations" leads to first-order definability results only, in place of results asserting existential definability.

Given a finite extension of fields L/K, the "weak vertical method" requires an equation with infinitely many solutions over L, all of which are actually in K. In our case L and K will be function fields of characteristic 0 and the requisite equations will be equations defining constants of K. Thus, a significant portion of the paper is devoted to the discussion of first-order or existential definitions of constants over function fields and rings of characteristic 0.

Before we can proceed with the technical core of the paper, we need to note two useful technical facts whose proof can be found in [31].

2.1 Proposition.

Let K be a product formula field, $\mathcal{W}$ any set of non-archimedean primes of K. Then the set of non-zero elements of $O_{K,\mathcal{W}}$ has an existential definition over $O_{K,\mathcal{W}}$.

2.2 Corollary.

Let K be a product formula field, $\mathcal{W}$ any set of non-archimedean primes of K. Let $A \subset K$ be first-order (existentially) definable. Then $A \cap O_{K,\mathcal{W}}$ is first-order (respectively existentially) definable over $O_{K,\mathcal{W}}$.

We conclude this section with a notation list to be used in Section 3 and Section 4 of the paper.

2.3 Notation.

- K will denote a one variable function field of characteristic zero over a field of constants C.
- Let $x \in K \setminus C$ be a fixed element.
- Let $[K : C(x)] = n$.
- Let $\mathfrak{q}_{C(x)}$ be the prime of $C(x)$ which is the pole of x in $C(x)$.
- For $h \in C(x)$, let $\deg(h) = -\mathrm{ord}_{\mathfrak{q}_{C(x)}} h$. (For $h \in C[x]$, $\deg(h)$ will be the degree of the polynomial.)
- Let $\mathfrak{q}_{K,1}, \ldots, \mathfrak{q}_{K,r}, r \leq n$ be all the factors of $\mathfrak{q}_{C(x)}$ in K.

- Let $\mathcal{S}_K = \{\mathfrak{q}_{K,1}, \ldots, \mathfrak{q}_{K,r}\}$.
- Let $\mathcal{P}(K)$ be the set of all the primes of K.
- Let $\mathcal{W}_K \subset \mathcal{P}(K)$ be such that $\mathcal{S}_K \subset \mathcal{W}_K$ and $\mathcal{P}(K) \setminus \mathcal{W}_K$ is infinite.
- For any $\mathcal{U}_K \subseteq \mathcal{P}(K)$, let
$$O_{K,\mathcal{U}_K} = \{z \in K | \mathrm{ord}_{\mathfrak{t}} z \geq 0, \forall \mathfrak{t} \notin \mathcal{U}_K\}.$$
- Let $\mathcal{V}_K \subset \mathcal{P}(K) \setminus \mathcal{W}_K$ be an infinite set.
- Let $C_{\mathcal{V}_K}$ be the set of all constants of K such that all K-primes dividing $x - c$ are in $\mathcal{V}_K$.
- Let G be a subfield of C.
- Let $G_{\mathcal{V}_K} = C_{\mathcal{V}_K} \cap G$ be infinite.
- Let $\gamma \in K \setminus C$ be such that $K = C(x, \gamma)$.
- Let $D = D(\gamma)$ be the discriminant of the power basis of γ.
- Let g be the genus of K.

2.4 Remark.

Before proceeding with the technical core of the paper, we would like to discuss the relationship between the rings of $\mathcal{S}$-integers and the rings of integral functions. The rings of $\mathcal{S}$-integers are holomorphy rings where only finitely many primes are allowed as poles. A ring of integral functions is the integral closure in a function field of a polynomial ring of a rational subfield. It is pretty clear that any ring of integral functions is a ring of $\mathcal{S}$-integers, where the only primes allowed as poles are the poles of the element generating the polynomial ring. However, the converse is also true, i.e. any ring of $\mathcal{S}$-integers is an integral closure in the function field under consideration of a polynomial ring generated by some (non-constant) element of the field. The Strong Approximation Theorem guarantees the existence of a field element with poles at all the valuations in $\mathcal{S}$ and no other poles. Thus the integral closure of the polynomial ring generated by this element will be precisely the given ring of $\mathcal{S}$-integers.

3 Defining Polynomials Using Congruences.

In this section we set up the foundation for the "weak vertical method".

3.1 Lemma.

Let $z \in O_{K,\mathcal{S}_K}$. Then for some $b_0, \ldots, b_{n-1} \in C[x]$, it is the case that

$$D(\gamma)z = \sum_{i=0}^{n-1} b_i \gamma^i.$$

(The proof of this lemma is identical to the proof of Lemma 4.1 of [36].)

3.2 Lemma: Weak Vertical Method.

Let $f, g \in C[x]$. Let $w = \sum_{i=0}^{n-1} a_i \gamma^i \in O_{K,\mathcal{S}_K}$, where $a_0, \ldots, a_{n-1} \in C(x)$ and for $i = 0, \ldots, n-1$, we have that

$$\deg(f) > \deg(a_i) + \deg(D(\gamma)). \tag{3.1}$$

Further, suppose that in $O_{K,\mathcal{S}_K}$, we also have that

$$w \cong g \bmod f. \tag{3.2}$$

Then $w \in C[x]$, or in other words for $i = 1, \ldots, n-1$, it is the case that $a_i = 0$.

Proof.

Equation (3.2) implies

$$\frac{(a_0 - g)}{f} + \sum_{i=1}^{n-1} \frac{a_i}{f} \gamma^i \in O_{K,\mathcal{S}_K}, \tag{3.3}$$

and therefore for $i = 1, \ldots, n-1$, we have that $\frac{Da_i}{f} \in C[x]$. This however implies that either $a_i = 0$ or $\deg(Da_i) \geq \deg(f)$. The second alternative is ruled out by our assumptions. Thus, the lemma holds.

3.3 Proposition.

$$C(x) \cap O_{K,\mathcal{W}_K} = \{v \in O_{K,\mathcal{W}_K} | (\forall c \in C_{\mathcal{V}_K})(\exists b \in C)(\exists h \in O_{K,\mathcal{W}_K})(v - b = (x - c)h)\} \tag{3.4}$$

Proof.

Let

$$V = \{v \in O_{K,\mathcal{W}_K} | (\forall c \in C_{\mathcal{V}_K})(\exists b \in C)(\exists h \in O_{K,\mathcal{W}_K})(v - b = (x - c)h)\}.$$

First of all we note that any element of $C(x) \cap O_{K,\mathcal{W}_K}$ is in V. Indeed, let $p(x) \in C(x) \cap O_{K,\mathcal{W}_K}$. Then for all $c \in C$,

$$h = \frac{p(x) - p(c)}{x - c} \in C(x) \cap O_{K,\mathcal{W}_K},$$

and we can let $b = p(c)$.

Now let $v \in V$. Then for some $u, z \in O_{K,\mathcal{S}_K}$, we have that

$$v = \frac{u}{z},$$

$$Z = \mathbf{N}_{K/C(x)}(z) \in C[x]$$

and

$$Zv \in O_{K,\mathcal{S}_K}.$$

Further, $v \in C(x)$ if and only if $Zv \in C[x]$. Since Z is a polynomial in x, as above, for all $c \in C$,

$$Z(x) \cong Z(c) \bmod (x - c) \text{ in } C[x] \subset O_{K,\mathcal{W}_K}.$$

Therefore, if for all $c \in C_{\mathcal{V}_K}, \exists b \in C$,

$$v \cong b \bmod (x - c) \text{ in } O_{K,\mathcal{W}_K},$$

then for all $c \in C_{\mathcal{V}_K}, \exists b \in C$,

$$Zv \cong bZ(c) \bmod (x - c) \text{ in } O_{K,\mathcal{W}_K}.$$

Now we can write

$$Zv = \sum_{i=0}^{n-1} a_i \gamma^i, a_i \in C(x).$$

Since $C_{\mathcal{V}_K}$ is infinite, we can choose distinct $c_1, \ldots, c_m \in C_{\mathcal{V}_K}$ with

$$m > \deg(a_i) + \deg(D(\gamma)).$$

Let $b_i \in C$ be such that $v \cong b_i \bmod (x - c_i)$ in $O_{K,\mathcal{W}_K}$. Next let $g \in C[x]$ be such that

$$g \cong Z(c_i)b_i \bmod (x - c_i) \text{ in } C[x].$$

(Such a g exists by the Strong Approximation Theorem (see page 23 of [12]).) Now we conclude that

$$Zv - g = h \prod_{i=1}^{m} (x - c_i), h \in O_{K,\mathcal{W}_K}.$$

Next we note that

$$h = \frac{Zv - g}{\prod_{i=1}^{m}(x - c_i)},$$

and poles of h can come from poles of $Zv - g$ or zeros of $\prod_{i=1}^{m}(x - c_i)$. However, by definition of $C_{\mathcal{V}_K}$, no prime of K which is a zero of $x - c_i$ belongs to $\mathcal{W}_K$. Therefore, all the poles of h come from poles of $Zv - g$. This means that $h \in O_{K,\mathcal{S}_K}$ and

$$Zv \cong g \bmod \prod_{i=1}^{m} (x - c_i) \text{ in } O_{K,\mathcal{S}_K}.$$

In this case, however, using our assumptions and Lemma 3.2 we can conclude that $Zv \in C[x]$ and $v \in C(x)$.

We next prove a refinement of Proposition 3.3.

3.4 Proposition.

$$G(x) \cap O_{K,\mathcal{W}_K} = \{v \in O_{K,\mathcal{W}_K} | (\forall c \in G_{\mathcal{V}_K})(\exists b \in G)(\exists h \in O_{K,\mathcal{W}_K})(v - b = (x - c)h)\} \tag{3.5}$$

Proof.

As in Proposition 3.3, it is easy to verify that

$$G(x) \cap O_{K,\mathcal{W}_K} \subseteq \{v \in O_{K,\mathcal{W}_K} | (\forall c \in G_{\mathcal{V}_K})(\exists b \in G)(\exists h \in O_{K,\mathcal{W}_K})(v - b = (x - c)h)\}$$

Indeed, if $v \in G(x)$, then for all $c \in G, v(c) \in G$. Suppose now that, that

$$z \in \{v \in O_{K,\mathcal{W}_K} | (\forall c \in G_{\mathcal{V}_K})(\exists b \in G)(\exists h \in O_{K,\mathcal{W}_K})(v - b = (x - c)h)\} \tag{3.6}$$

From Proposition 3.3 we know that $z \in C(x)$ and for infinitely many values $a \in G$ we have that $z(a) \in G$. Then by Lemma 2.3 of [32], $z \in G(x)$.

We will next consider an example of definability within the same function field.

3.5 Proposition.

Let C contain an algebraic extension M of $\mathbb{Q}$. Let O_M be the set of algebraic integers of M. Assume all but finitely many elements of O_M belong to $C_{\mathcal{V}_K}$. Then

$$O_M[x] \subset V = \{v \in O_{K,\mathcal{W}_K} | (\forall c \in O_M \cap C_{\mathcal{V}_K})(\exists b \in O_M, h \in O_{K,\mathcal{W}_K}) : v - b = h(x - c)\} \subset M[x]. \tag{3.7}$$

Proof.

First of all, it is clear that $O_M[x] \subset V$. Further, by Proposition 3.4, if $v \in V$, then $v \in M(x)$. Assume $v \notin M[x]$ and let $Q(x)$ be a monic irreducible over M polynomial dividing the reduced denominator of v so that

$$v(x) = \frac{A(x)}{Q(x)^i B(x)},$$

where

$$(A(x), Q(x)) = (B(x), Q(x)) = (A(x), B(x)) = 1$$

as polynomials over M. Let α be a root of $Q(x)$ in the algebraic closure of M. Then

$$B(\alpha)A(\alpha) \neq 0.$$

Let $M_1 \subset M$ be a number field containing all the coefficients of $Q(x)$. Let $\mathfrak{p}$ be a prime of M_1 unramified and splitting completely in the Galois closure of $M_1(\alpha)$ over M_1. By Chebotarev Density Theorem, there are infinitely many such primes and therefore we can pick such a prime $\mathfrak{p}$ satisfying the following conditions

1. α is integral at $\mathfrak{p}$.
2. All the coefficients of $A(x)$ and $B(x)$ are integral at $\mathfrak{p}$.

Let $\mathfrak{p}_1$ be a factor of $\mathfrak{p}$ in $M_1(\alpha)$. By Lemmas 6.1 and 6.2, for any $l > 0$, there exists $a \in O_{M_1} \cap C_{\mathcal{V}_K}$ such that

$$l = \mathrm{ord}_{\mathfrak{p}_1}(a - \alpha) > \max(\mathrm{ord}_{\mathfrak{p}_1} A(\alpha) + \mathrm{ord}_{\mathfrak{p}_1} B(\alpha), \mathrm{ord}_{\mathfrak{p}_1} \alpha)$$

and

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}_1} Q(a) &= l, \\ \mathrm{ord}_{\mathfrak{p}_1} A(a) &= \mathrm{ord}_{\mathfrak{p}_1} A(\alpha), \\ \mathrm{ord}_{\mathfrak{p}_1} B(a) &= \mathrm{ord}_{\mathfrak{p}_1} B(\alpha). \end{aligned}$$

Then

$$\mathrm{ord}_{\mathfrak{p}} v(a) = \mathrm{ord}_{\mathfrak{p}_1} v(a) = \mathrm{ord}_{\mathfrak{p}_1} A(a) - \mathrm{ord}_{\mathfrak{p}_1} B(a) - i\mathrm{ord}_{\mathfrak{p}_1} Q(a) < 0.$$

Thus $v(x)$ cannot have a pole at any valuation different from the valuation which is the pole of x. Therefore, $v(x) \in C[x]$.

The results above can be reformulated as the following theorems.

3.6 Theorem.

If C is first-order definable over $O_{K,\mathcal{W}_K}$, then $O_{K,\mathcal{W}_K} \cap C(x)$ is first-order definable over $O_{K,\mathcal{W}_K}$.

Proof.

It is sufficient to replace "$C_{\mathcal{V}_K}$" in Equation (3.4) by "C" to obtain a first order formula defining $O_{K,\mathcal{W}_K} \cap C(x)$ over $O_{K,\mathcal{W}_K}$.

3.7 Theorem.

If G is first-order definable over $O_{K,\mathcal{W}_K}$, then $O_{K,\mathcal{W}_K} \cap G(x)$ is first order definable over $O_{K,\mathcal{W}_K}$.

Proof.

As above, it is sufficient to replace "$G_{\mathcal{V}_K}$" in Equation (3.5) by "G" to obtain a first order formula defining $O_{K,\mathcal{W}_K} \cap G(x)$ over $O_{K,\mathcal{W}_K}$.

3.8 Theorem.

If M is a number field contained in C and O_M is first-order definable over $O_{K,\mathcal{W}_K}$, then $M[x]$ is first order definable over $O_{K,\mathcal{W}_K}$.

Proof.

Here we note the following. As above, we can replace "$O_M \cap C_{\mathcal{V}_K}$" by O_M to obtain

$$O_M[x] \subset V = \{v \in O_{K,\mathcal{W}_K} : \forall c \in O_M, \exists b \in O_M, \exists h \in O_{K,\mathcal{W}_K} : v - b = h(x - c)\} \subset M[x].$$

Next we can observe that $z \in M[x]$ if and only if $\exists c \in O_M : cz \in V$.

4 Defining Constants.

From the preceding section we can conclude that definability of the polynomials and S-integers follows from the definability of the constant field and its subfields. In this section we review some old and provide some new existential and first order definitions of constants. We will start with rings of $\mathcal{S}$-integers and review the existential definition of constants from [29].

4.1 Proposition: Defining Constants over the Rings of $\mathcal{S}$-integers.

Let $x \in O_{K,\mathcal{S}_K}$. Then $x \in C$ if and only if for all $i = 0, \ldots, r$, it is the case that

$$x = -i \vee \exists y_i \in O_{K,\mathcal{S}_K} \text{ such that } y_i(x + i) = 1. \tag{4.1}$$

Proof.

If x is a constant, then for any $i \in \mathbb{N}$, we have that $x + i$ is a constant and, unless $x + i = 0$, a unit of $O_{K,\mathcal{S}_K}$. Further, if $x + i$ is a unit but not a constant, all the zeros of $x + i$ are at some or all of $\mathfrak{q}_{K,1}, \ldots, \mathfrak{q}_{K,r}$. On the other hand, for $i, j \in \mathbb{N}, i \neq j$, the zeros of $x + i$ and $x + j$ are distinct. Thus if (4.1) holds, for at least one $i = 0, \ldots, r$, it is the case that $x + i$ does not have a zero at any $\mathfrak{q}_{K,i}$, but is a unit of $O_{K,\mathcal{S}_K}$. Therefore, for some i, we have that $x + i$ is a constant and therefore x is a constant.

The following proposition was also proved in [29].

4.2 Proposition.

$\mathbb{Z}$ is existentially definable over $O_{K,\mathcal{S}_K}$.

We next proceed to results where we will restrict the possible fields of constants. The proof of the following result can be found in [38].

4.3 Proposition.

Let C be finitely generated over $\mathbb{Q}$. Let E/K be a finite extension and let $\mathcal{W}$ be a set of primes of K such that all but finitely many primes of $\mathcal{W}$ do not split in the extension E/K and the degree of all the primes in $\mathcal{W}$ is bounded by $b \in \mathbb{N}$. Then for some set of K-primes $\mathcal{W}'$, it is the case that $\mathbb{Z}$ has an existential definition over $O_{K,\mathcal{W}'}$, and $\mathcal{W}'$ and $\mathcal{W}$ differ by at most finitely many primes.

In [41] and in [42], Karim Zahidi gave an existential definition of $\mathbb{Z}$ over hyperelliptic fields over real closed fields of constants and over semi-local and local rings of rational functions over algebraically closed fields of constants. In [1], Luc Belair proved the following first-order definability result which we will use later.

4.4 Theorem.

Let C be a formally real field with an Archimedean order. Then $\mathbb{Z}$ is first-order definable over K.

In [14], Königman introduced several ideas leading to a fairly general method of defining constants existentially. Unfortunately, Königman's method and our elaboration of it require the constant fields to be rather large, as we will explain below. (Using similar ideas, Pop defined constants when the field of constants is algebraically closed in [23].)

4.5 Proposition.

Let $f(X,Y) \in C[X,Y]$ be an absolutely irreducible polynomial of genus $g_f > g$. Then for all $a, b \in K$, $f(a,b) = 0 \Rightarrow a, b \in C$.

Proof.

Suppose $f(a,b) = 0$ for some $a, b \in K$. Since C is algebraically closed in K, $a \in C$ if and only if $b \in C$. So suppose $a, b \notin C$. Let $K_0 = C(a,b)$ and note that K/K_0 is a finite separable extension where the genus of K_0 is equal to the the genus of $f(X,Y)$ and therefore is greater than the genus of K. However, by the Riemann-Hurwitz formula (see, for example, [12], page 24) this cannot happen.

Actually we can easily push this proposition a little bit further. In order to do this we need to make a definition.

4.6 Definition.

Let U be finitely generated over C of transcendence degree m. Let $\mathbf{C}$ be the set of all chains $\mathbf{c} = (K_0 \subset \ldots \subset U = K_m)$ such that for $i = 0, \ldots, m-1$, it is the case that K_i is algebraically closed in K_{i+1}, and for $i = 1, \ldots, m$, we have that K_i is of transcendence degree 1 over K_{i-1}. Given a chain $\mathbf{c} = (C \subset K_1 \ldots \subset U)$, let the genus $g(\mathbf{c})$ of $\mathbf{c}$ be the maximum of the set $\{g_1, \ldots, g_m\}$, where for $i = 1, \ldots, m$, we have that g_i is the genus of K_i as a one-variable function field over K_{i-1}. Finally, let $g_U = \min\{g(\mathbf{c}), \mathbf{c} \in \mathbf{C}\}$.

Now we can state an obvious but useful corollary of Proposition 4.5.

4.7 Corollary.

Let U be as in Definition 4.6. Let $f(X,Y) \in C[X,Y]$ be absolutely irreducible with the genus $g_f > g_U$. Then for all $a, b \in U$, we have that $f(a,b) = 0 \Rightarrow a, b \in C$.

Now, in order to make Proposition 4.5 and Corollary 4.7 useful we need to make sure $f(a,b)$ has enough solutions in C. It will certainly be true if C is algebraically closed, but we can also make do with smaller fields. To describe the fields we have in mind we need another definition.

4.8 Definition.

A field C will be called a *high genus equations* field if for any $g > 0$ there exists a polynomial $f(X,Y) \in C[X,Y]$ absolutely irreducible over C, of genus greater than g, such that the following conditions are satisfied.

- There exists a finite family of polynomials $\{h_i(x_1, \ldots, x_k)\} \subset C[x_1, \ldots, x_k]$ such that $h_i(a_1, \ldots, a_k) \in C$ for all i implies $a_1, \ldots, a_k \in C$.
- For any $c \in C$, for some $a_2, \ldots, a_k \in C$, for all i, we have that polynomial $f(h_i(c, a_2, \ldots, a_k), Y) = 0$ has a root in C.

Given this definition, it is trivial to show that the following proposition holds.

4.9 Proposition.

Let C be a high genus equations field. Let U be a function field in several variables over C. Then C is existentially definable over U.

Koenigman provided several interesting examples of high genus equations fields in [14] (though he did not use this terminology). In particular, he showed that ample/large fields and fields F with $(F^n/F)^*$ finite are high genus equations fields. (In case of positive characteristic n has to be prime to the characteristic.) However, one can easily generate additional examples as shown below.

4.10 More Examples of High Genus Equations Fields.

Let

$$f_{n,m}(X,Y) = Y^n - \prod_{i=1}^{m}(X - c_i),$$

where $c_1, \ldots, c_m \in C$ are distinct. Assume $(m,n) = 1$ and consider the extension $C(X,Y)/C(X)$, where $f_{n,m}(X,Y) = 0$. It is clear that in this extension the infinite prime of $C(X)$ as well as the primes corresponding to $(X - c_1), \ldots, (X - c_m)$ are completely ramified. It is also clear that no other prime of $C(X)$ is ramified in the extension $C(X,Y)/C(X)$. Furthermore, the $C(X,Y)$-factor of $(X - c_i)$ is of relative degree 1 and also of degree 1 in $C(X,Y)$. Let $g_X = 0$ be the genus of $C(X)$, and let g_f be the genus of $C(X,Y)$ (and the genus of f). Then by the Riemann-Hurwitz formula,

$$2g_f - 2 = n(g_X - 2) + \deg \sum_{i=0}^{m}(n-1)\mathfrak{P}_i,$$

where $\mathfrak{P}_0$ is the prime above the infinite valuation in $C(X,Y)$, and for $i = 1, \ldots, m$, we let $\mathfrak{P}_i$ denote the prime above $X - c_i$. Thus,

$$g_f = \frac{1}{2}((m+1)(n-1) - 2n + 2) = \frac{1}{2}(mn - n - m + 1) = \frac{(m-1)(n-1)}{2}.$$

If we fix n and consider arbitrarily large m's, we get another proof of the fact that fields where "almost" every element is an n-th power are high genus equations fields. On the other hand we can fix m and let $n = p^k, k \in \mathbb{N}$. A field such that for all $k \in \mathbb{N}$, $\forall c \in C, \exists b \in C : f_{p^k,m}(b,c) = 0$ will also be a high genus equations field.

4.11 Remark.

In many applications we don't need an existential definition of the set of all constants but of a constant set containing $\mathbb{Q}$. In these cases the constant field C can be smaller than in the examples above. For example, we would not need almost every element of C to be an n^k-th power for all $k \in \mathbb{N}$, just elements of $\mathbb{Q}$. Similarly, it would be enough to require that for all $k \in \mathbb{N}$, $\forall c \in \mathbb{Q}, \exists b \in C : f_{p^k,m}(b,c) = 0$.

We can now prove a new version of Proposition 4.3

4.12 Proposition.

Let C contain a high genus equations field, but assume that C is not algebraically closed. Let E/K be a finite extension and let $\mathcal{W}$ be a set of primes of K such that all but finitely many primes of $\mathcal{W}$ do not split

in the extension E/K. Then for some set of K-primes $\mathcal{W}'$, $\mathbb{Z}$ has an existential definition over $O_{K,\mathcal{W}'}$, and $\mathcal{W}'$ and $\mathcal{W}$ differ by at most finitely many primes.

Proof.

From the proof of Theorem 5.1 of [38], it follows that for some $\mathcal{W}'$ as described in the statement of the proposition and some prime $\mathfrak{P} \notin \mathcal{W}'$ there exists a polynomial $p(t, z_1, \ldots, z_k) \in O_{K,\mathcal{W}'}[t, z_1, \ldots, z_k]$ such that if for some $t, z_1, \ldots, z_k \in O_{K,\mathcal{W}'}$, we have that

$$p(t, z_1, \ldots, z_k) = 0, \tag{4.2}$$

then there exists $n \in \mathbb{N}$ such that

$$(t - n) = wv, \tag{4.3}$$

where $w, v \in O_{K,\mathcal{W}'}$ and $\mathrm{ord}_{\mathfrak{P}} w > 0$. Further for any $n \in \mathbb{N}$, there exist $t, z_1, \ldots, z_k \in O_{K,\mathcal{W}'}$ such that (4.2) and (4.3) are satisfied. We now combine (4.2) and the following conditions:

$$c \in C \wedge t - c = wu, \tag{4.4}$$

Then (4.2) and (4.4) together will imply that $c - n$ has a zero at $\mathfrak{P}$, implying that the difference is 0. Conversely, for any $n \in \mathbb{N}$, we can satisfy (4.2) and (4.4).

5 First Order Definitions Using Constants.

Using the results of the preceding sections we can now construct several first-order definitions. We will start with the first-order definability zero characteristic function field analogs of existential definability results in [5], [8], [7], [20], [27], [28], [21] (these results cover number fields), and [30] (this paper deals with function fields of positive characteristic).

5.1 Theorem.

Let E/K be a finite extension of function fields of characteristic 0 over the same field of constants C. Let $\mathcal{S}_K$ be a finite set of primes of K. Let $\mathcal{S}_E$ be the set of all the primes of E lying above $\mathcal{S}_K$. Then $O_{K,\mathcal{S}_K}$ is first order definable in the language of rings over $O_{E,\mathcal{S}_E}$.

Proof.

By Proposition 4.1, C is first order definable in $O_{E,\mathcal{S}_E}$. Let $x \in O_{K,\mathcal{S}_K}$ be such that x has a pole at every prime of $\mathcal{S}_K$ and no other poles. Such an x exists by Strong Approximation Theorem (see [12], page 21). Then $C[x] \subseteq O_{K,\mathcal{S}_K}$, and $C[x] = O_{E,\mathcal{S}_E} \cap C(x)$ (see Proposition 2.12, page 22 of [12]). By Theorem 3.6, $C[x]$ has a first-order definition over $O_{E,\mathcal{S}_E}$. Let $\alpha \in O_{K,\mathcal{S}_K}$ be a generator of K over $C(x)$. Then $y \in O_{K,\mathcal{S}_K}$ if and only if $y = \sum_{i=0}^{[K:C(x)]-1} \frac{a_i(x)}{b_i(x)} \alpha^i$, where $a_i(x), b_i(x) \in C[x], b_i \neq 0$ and $y \in O_{E,\mathcal{S}_E}$.

Next we use Proposition 4.2 to obtain two definability results. The first theorem follows immediately from Proposition 4.2 and Theorem 3.8. The proof of the second theorem is almost identical to the proof of Theorem 5.1.

5.2 Theorem.

Let K be a function field of characteristic 0 over a field of constants C. Let M be any number field contained in C, including $\mathbb{Q}$. Let $\mathcal{S}_K$ be a finite set of primes of K. Let $x \in O_{K,\mathcal{S}_K}$ be such that it has a pole at every valuation of $\mathcal{S}_K$. Then $M[x]$ has a first-order definition over $O_{K,\mathcal{S}_K}$.

5.3 Theorem.

Let E/K be a finite extension of function fields of characteristic 0 such that the field of constants of E is a number field. Let $\mathcal{S}_K$ be a finite set of primes of K. Let $\mathcal{S}_E$ be the set of all the primes of E lying above $\mathcal{S}_K$. Then $O_{K,\mathcal{S}_K}$ is first order definable over $O_{E,\mathcal{S}_E}$.

We will now make use of definitions of constants over holomorphy rings and fields. Here we will prove results which are the first-order definability analogs of the results in [33], [35], [39] (number field case) and [34], [37] (function fields of positive characteristic). We should note here that dealing with function fields of characteristic 0 we are missing an essential tool to measure the "size" of the holomorphy rings – Dirichlet density. Thus we cannot estimate how close we are to the fraction field of the ring under consideration.

5.4 Theorem.

Let K be a function field over a high genus equations field C or a formally real field with Archimedean order. Let $\mathcal{W}_K$ be a set of primes of K. Let $x \in O_{K,\mathcal{W}_K}$. Assume that for infinitely many $a \in C$, the primes which are zeros of $x - a$ are not in $\mathcal{W}_K$. Then $C(x) \cap O_{K,\mathcal{W}_K}$ is first-order definable over $O_{K,\mathcal{W}_K}$. (This theorem follows immediately from Proposition 4.9 and Theorems 4.4 and 3.6.)

5.5 Theorem.

Let K be a function field over a high genus equations field C or a formally real field with Archimedean order. Let $\mathcal{S}_K$ be a finite set of primes of K. Then there exists an infinite set of primes $\mathcal{W}_K$ such that its complement in the set of all primes of K is also infinite, and $O_{K,\mathcal{S}_K}$ and $\mathbb{Z}$ have a first-order definition over $O_{K,\mathcal{W}_K}$.

Proof.

By Lemma 6.3, there exists $z \in O_{K,\mathcal{S}_K}$ such that the integral closure of $C[z]$ in K is $O_{K,\mathcal{S}_K}$, and infinitely many primes of K have a conjugate distinct from itself over $C(z)$. We describe the steps leading to a construction of a set $\mathcal{W}_K$ with required properties. Let $\mathcal{U}_K$ contain $\mathcal{S}_K$ and all the primes with a distinct conjugate over $C(z)$. Next consider all the primes of $\mathcal{U}_K$ outside $\mathcal{S}_K$ lying above primes occurring in the numerator of $z - a$ for some $a \in C$. If this set is finite, set $\mathcal{W}_K = \mathcal{U}_K$. If this set is infinite then divide all $a \in C$ such that a zero of $z - a$ is in $\mathcal{U}_K \setminus \mathcal{S}_K$ into two infinite subsets, and remove all the zeros of $z - a$ with a in the first subset from $\mathcal{U}_K$. Call the resulting set $\mathcal{V}_K$. Finally consider all the full sets of $C(z)$-conjugates in $\mathcal{V}_K \setminus \mathcal{S}_K$. From each full set of conjugates remove one prime. Then call the resulting set $\mathcal{W}_K$. Now by Theorem 5.4, $C[z] = C(z) \cap O_{K,\mathcal{W}_K}$ is first-order definable over $O_{K,\mathcal{W}_K}$. Further, if $y \in O_{K,\mathcal{W}_K}$, then $y \in O_{K,\mathcal{S}_K}$ if and only if y satisfies a monic polynomial of degree $[K : C(z)]$ over $C[z]$. Finally, by Proposition 4.2, $\mathbb{Z}$ is existentially definable over $O_{K,\mathcal{S}_K}$.

5.6 Remark.

As in all the other cases, the first-order definability of $\mathbb{Z}$ leads to the first order undecidability of the ring in question. We must note here that not all the rings to which the theorem above applies are covered by the previously known results. In particular, if C is algebraically closed, the resulting first-order undecidability result is new.

5.7 Theorem.

Let K be a function field in one variable over a field of constants C finitely generated over a subfield of $\mathbb{C}$. Let $\mathcal{W}_K$ be a set of primes of K such that

1. for some finite extension E of K all but finitely many primes of $\mathcal{W}_K$ do not split in the extension E/K;

2. either C contains a high genus equations field, or C is formally real with Archimedean order, or C is finitely generated over $\mathbb{Q}$ and for some positive integer b all the primes of $\mathcal{W}_K$ are of degree b or less;

3. for some $z \in O_{K,\mathcal{W}_K}$, for all but possibly finitely many $a \in \mathbb{Z}$, the primes dividing $z-a$ are not in $\mathcal{W}_K$.

Then $\mathbb{Q}[z]$ is first-order definable over $O_{K,\mathcal{W}'_K}$, where $\mathcal{W}'_K$ is a set of K-primes differing from $\mathcal{W}_K$ by finitely many elements only.

Proof.

By Proposition 4.3 and Proposition 4.12, $\mathbb{Z}$ is existentially definable over $O_{K,\mathcal{W}'_K}$, where $\mathcal{W}'_K$ is a set of K-primes differing from $\mathcal{W}_K$ by finitely many elements. Now the result follows by Theorem 3.8.

Finally we remark that examples of rings $O_{K,\mathcal{W}_K}$ satisfying the requirements of Theorem 5.7 can be found in [38].

5.8 Remark.

The author was recently informed by Bjorn Poonen that he has constructed a uniform first-order definition of $\mathbb{Q}$ and $\mathbb{Z}$ over any finitely generated function field of characteristic 0. Taking this result into account, one can obtain results analogous to Theorems 5.4 and 5.5 for these fields also. Further in Theorem 5.7 we can drop the assumption that the degrees of primes are bounded in the finitely generated case.

6 Appendix.

6.1 Lemma.

Let F/L be a Galois number field extension of degree m. Let $\alpha \in F$ and let $Q(x)$ the monic irreducible polynomial of α over L. Let $\mathfrak{p}$ be a prime of L such that all the coefficients of $Q(x)$ are integral at $\mathfrak{p}$, and $\mathfrak{p}$ splits completely in the extension F/L. Then for any positive integer l there exists $a_l \in L$ such that for some prime factor $\mathfrak{p}_1$ of $\mathfrak{p}$ in F we have that $\mathrm{ord}_{\mathfrak{p}_1}(a_l - \alpha) \geq l$ and $\mathrm{ord}_{\mathfrak{p}} Q(a_l) \geq l$.

Proof.

Let $\prod_{i=1}^{m} \mathfrak{p}_i$ be the factorization of $\mathfrak{p}$ in F. Then for all i the relative degree of $\mathfrak{p}_i$ over $\mathfrak{p}$ is 1. Further, let $\{\sigma_1, \ldots, \sigma_m\} = \mathrm{Gal}(F/L)$. Without loss of generality, since $\mathfrak{p}$ splits completely and the Galois group of the extension acts transitively on all the factors of $\mathfrak{p}$, we can assume that $\sigma_i(\mathfrak{p}_1) = \mathfrak{p}_i$. Also we can let $\alpha_i = \sigma_i(\alpha)$. (Note that while by assumption $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are all distinct, $\alpha_1 = \alpha, \ldots, \alpha_m$ are not necessarily all distinct.) Let $\pi \in O_L$ be such that such that $\mathrm{ord}_{\mathfrak{p}} \pi = 1$. Then in $F_{\mathfrak{p}_1}$ – the completion of F under $\mathfrak{p}_1$, $\alpha = \sum_{i=0}^{\infty} b_j \pi^j, b_j \in O_L$. Let $a_l = \sum_{i=0}^{l} b_j \pi^j \in O_L$. Then $a_l \cong \alpha \bmod \mathfrak{p}_1^l$, and using the transitive action of the Galois group on the factors of $\mathfrak{p}$ we conclude that for all $i = 1, \ldots, m$ we have that $a_l \cong \alpha_i \bmod \mathfrak{p}_i^l$. Thus, $Q(a_l) = \prod_{\text{distinct } \alpha_i} (a - \alpha_i) \cong 0 \bmod \mathfrak{p}^l$.

6.2 Lemma.

Let F/L be a Galois number field extension of degree m. Let $\alpha \in F$. Let $P(X) \in L[X]$ be such that $P(\alpha) \neq 0$. Let $\mathfrak{q}$ be a prime of F of relative degree 1 over L such that α is integral at $\mathfrak{q}$. Then there exists a positive integer l such that for all $a \in L$ with $\mathrm{ord}_{\mathfrak{q}}(a - \alpha) > l$ we have that $\mathrm{ord}_{\mathfrak{q}} P(a) = \mathrm{ord}_{\mathfrak{q}} P(\alpha)$.

Proof.

Let $P(X) = \sum_{i=0}^{m} A_i X^i, A_i \in L$. Let $b = \min\{\mathrm{ord}_{\mathfrak{q}} A_i, i = 0, \ldots, m\}$. Next let $a \in L$ with

$$\mathrm{ord}_{\mathfrak{q}}(a - \alpha) = l > \max(-b + \mathrm{ord}_{\mathfrak{q}} P(\alpha), \mathrm{ord}_{\mathfrak{q}} \alpha)$$

and consider

$$\mathrm{ord}_{\mathfrak{q}} P(a) = \mathrm{ord}_{\mathfrak{q}}(P(a) - P(\alpha) + P(\alpha)) = \min(\mathrm{ord}_{\mathfrak{q}}(P(a) - P(\alpha)), \mathrm{ord}_{\mathfrak{q}} P(\alpha)) =$$

$$\min(\mathrm{ord}_{\mathfrak{q}}(\sum_{i=1}^{m} A_i(a^i - \alpha^i)), \mathrm{ord}_{\mathfrak{q}} P(\alpha)) = \mathrm{ord}_{\mathfrak{q}} P(\alpha),$$

since $\mathrm{ord}_{\mathfrak{q}} a = \mathrm{ord}_{\mathfrak{q}}(a - \alpha + \alpha) = \min(\mathrm{ord}_{\mathfrak{q}}(a - \alpha), \mathrm{ord}_{\mathfrak{q}} \alpha) = \mathrm{ord}_{\mathfrak{q}} \alpha \geq 0$ and

$$\mathrm{ord}_{\mathfrak{q}}(\sum_{i=1}^{m} A_i(a^i - \alpha^i)) \geq \mathrm{ord}_{\mathfrak{q}}(a - \alpha) + b > \mathrm{ord}_{\mathfrak{q}} P(\alpha).$$

6.3 Lemma.

Let K be a function field over a field of constants C. Then there exists an infinite set of primes $\mathcal{U}_K$ and a finite rational sub-extension $C(z), z \in K$ of K over the same field of constants C such that every prime of $\mathcal{U}_K$ has an $C(z)$-conjugate distinct from itself.

Proof.

Let $x \in K$. Let $z = x^n, n > 1$. Then, we can let $\mathcal{U}_K$ consist of all the K-primes lying above $C(x)$-primes of the form $x - a$, where $a \in C$.

References

[1] Luc Bélair. La définissabilité des entiers dans les corps de courbes réelles archimédiens. *C. R. Math. Acad. Sci. Paris*, 336(6):459–462, 2003.

[2] Luc Bélair and Jean-Louis Duret. Indécidabilité des corps de courbe réelle. *J. Symbolic Logic*, 59(1):87–91, 1994.

[3] Jean-Louis Colliot-Thélène, Alexei Skorobogatov, and Peter Swinnerton-Dyer. Double fibres and double covers: Paucity of rational points. *Acta Arithmetica*, 79:113–135, 1997.

[4] Gunther Cornelissen and Karim Zahidi. Topology of diophantine sets: Remarks on Mazur's conjectures. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 253–260. American Mathematical Society, 2000.

[5] Jan Denef. Hilbert's tenth problem for quadratic rings. *Proc. Amer. Math. Soc.*, 48:214–220, 1975.

[6] Jan Denef. The diophantine problem for polynomial rings and fields of rational functions. *Transactions of American Mathematical Society*, 242:391–399, 1978.

[7] Jan Denef. Diophantine sets of algebraic integers, II. *Transactions of American Mathematical Society*, 257(1):227– 236, 1980.

[8] Jan Denef and Leonard Lipshitz. Diophantine sets over some rings of algebraic integers. *Journal of London Mathematical Society*, 18(2):385–391, 1978.

[9] Jan Denef, Leonard Lipshitz, and Thanases Pheidas, editors. *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, volume 270 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 2000. Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999.

[10] Kirsten Eisenträger. Hilbert's tenth problem for function fields of varieties over number fields and p-adic fields. Pre-print.

[11] Kirsten Eisenträger. Hilbert's tenth problem for function fields of varieties over $\mathbb{C}$. *Int. Math. Res. Not.*, (59):3191–3205, 2004.

[12] M. Fried and M. Jarden. *Field Arithmetic*. Springer Verlag, New York, 1986.

[13] H. K. Kim and F. W. Roush. Diophantine unsolvability over p-adic function fields. *Journal of Algebra*, 176:83–110, 1995.

[14] Jochen Koenigsmann. Defining transcendentals in function fields. *J. Symbolic Logic*, 67(3):947–956, 2002.

[15] Barry Mazur. The topology of rational points. *Experimental Mathematics*, 1(1):35–45, 1992.

[16] Barry Mazur. Questions of decidability and undecidability in number theory. *Journal of Symbolic Logic*, 59(2):353–371, June 1994.

[17] Barry Mazur. Speculation about the topology of rational points: An up-date. *Asterisque*, 228:165–181, 1995.

[18] Barry Mazur. Open problems regarding rational points on curves and varieties. In A. J. Scholl and R. L. Taylor, editors, *Galois Representations in Arithmetic Algebraic Geometry*. Cambridge University Press, 1998.

[19] Laurent Moret-Bailly. Elliptic curves and Hilbert's Tenth Problem for algebraic function fields over real and p-adic fields. to appear in Journal für Reaine und Angewandte Mathematic.

[20] Thanases Pheidas. Hilbert's tenth problem for a class of rings of algebraic integers. *Proceedings of American Mathematical Society*, 104(2):611–620, 1988.

[21] Bjorn Poonen. Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers. In C. Fieker and D. Kohel, editors, *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Computer Science*, pages 33–42. Springer Verlag, 2002.

[22] Bjorn Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *Journal of AMS*, 16(4):981–990, 2003.

[23] Florian Pop. Elementary equivalence versus isomorphism. *Invent. Math.*, 150(2):385–408, 2002.

[24] Julia Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949.

[25] Julia Robinson. The undecidability of algebraic fields and rings. *Proceedings of the American Mathematical Society*, 10:950–957, 1959.

[26] Robert Rumely. Undecidability and definability for the theory of global fields. *Transactions of the American Mathematical Society*, 262(1):195–217, November 1980.

[27] Harold Shapiro and Alexandra Shlapentokh. Diophantine relations between algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:1113–1122, 1989.

[28] Alexandra Shlapentokh. Extension of Hilbert's tenth problem to some algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:939–962, 1989.

[29] Alexandra Shlapentokh. Hilbert's tenth problem for rings of algebraic functions of characteristic 0. *Journal of Number Theory*, 40(2):218–236, 1992.

[30] Alexandra Shlapentokh. Diophantine relations between rings of S-integers of fields of algebraic functions in one variable over constant fields of positive characteristic. *J. Symbolic Logic*, 58(1):158–192, 1993.

[31] Alexandra Shlapentokh. Diophantine classes of holomorphy rings of global fields. *Journal of Algebra*, 169(1):139–175, October 1994.

[32] Alexandra Shlapentokh. Algebraic and Turing separability of rings. *Journal of Algebra*, 185:229–257, 1996.

[33] Alexandra Shlapentokh. Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator. *Inventiones Mathematicae*, 129:489–507, 1997.

[34] Alexandra Shlapentokh. Diophantine definability over holomorphy rings of algebraic function fields with infinite number of primes allowed as poles. *International Journal of Mathematics*, 9(8):1041–1066, 1998.

[35] Alexandra Shlapentokh. Defining integrality at prime sets of high density in number fields. *Duke Mathematical Journal*, 101(1):117–134, 2000.

[36] Alexandra Shlapentokh. Hilbert's tenth problem over number fields, a survey. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 107–137. American Mathematical Society, 2000.

[37] Alexandra Shlapentokh. Defining integrality at prime sets of high density over function fields. *Monatshefte fuer Mathematik*, 135:59–67, 2002.

[38] Alexandra Shlapentokh. On diophantine decidability and definability in some rings of algebraic functions of characteristic 0. *Journal of Symbolic Logic*, 67(2):759–786, 2002.

[39] Alexandra Shlapentokh. On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2. *Journal of Number Theory*, 95:227–252, 2002.

[40] Alexandra Shlapentokh. A ring version of Mazur's conjecture on topology of rational points. *International Mathematics Research Notices*, 2003:7:411–423, 2003.

[41] Karim Zahidi. The existential theory of real hyperelliptic fields. *Journal of Algebra*, 233(1):65–86, 2000.

[42] Karim Zahidi. Hilbert's tenth problem for rings of rational functions. *Notre Dame Journal of Formal Logic*, 43:181–192, 2003.