ANNALES

DE

L'INSTITUT FOURIER

Laurent MORET-BAILLY & Alexandra SHLAPENTOKH

Diophantine Undecidability of Holomorphy Rings of Function Fields of Characteristic 0

Tome 59, n° 5 (2009), p. 2103-2118.

<http://aif.cedram.org/item?id=AIF_2009___59_5_2103_0>

Ann. Inst. Fourier, Grenoble
59, 5 (2009) 2103-2118

DIOPHANTINE UNDECIDABILITY OF HOLOMORPHY RINGS OF FUNCTION FIELDS OF CHARACTERISTIC 0

by Laurent MORET-BAILLY & Alexandra SHLAPENTOKH (*)

Abstract. — Let K be a one-variable function field over a field of constants of characteristic 0. Let R be a holomorphy subring of K, not equal to K. We prove the following undecidability results for R: if K is recursive, then Hilbert's Tenth Problem is undecidable in R. In general, there exist $x_1, \ldots, x_n \in R$ such that there is no algorithm to tell whether a polynomial equation with coefficients in $\mathbb{Q}(x_1, \ldots, x_n)$ has solutions in R.

Résumé. — Soit K un corps de fonctions d'une variable sur un corps de caractéristique nulle. Soit R un anneau d'holomorphie de K, distinct de K. Si K est récursif, nous démontrons que le dixième problème de Hilbert sur R est indécidable. En général, il existe $x_1, \ldots, x_n$ dans R tels qu'il n'y ait pas d'algorithme décidant si une équation polynomiale à coefficients dans $\mathbb{Q}(x_1, \ldots, x_n)$ a une solution dans R.

1. Introduction

The interest in the questions of existential definability and decidability over rings goes back to a question that was posed by Hilbert: given an arbitrary polynomial equation in several variables over $\mathbb{Z}$, is there a uniform algorithm to determine whether such an equation has solutions in $\mathbb{Z}$? This question, otherwise known as Hilbert's Tenth Problem ("HTP" in the future), has been answered negatively in the work of M. Davis, H. Putnam, J. Robinson and Yu. Matijasevich. (See [4], [5] or [20] for the details of the solution of the original problem.) Since the time when this result was

Keywords: Hilbert's tenth problem, elliptic curves, Diophantine undecidability.
Math. classification: 11U05, 03D35, 11G05.
(*) The second author has been partially supported by NSF grants DMS-0354907 and DMS-0650927.

obtained, similar questions have been raised for other fields and rings. In other words, let R be a ring. Then, given an arbitrary polynomial equation in several variables over a recursive subring R_0 of R, is there a uniform algorithm to determine whether such an equation has solutions in R? (If R is countable and recursive then we can set $R_0 = R$.)

Depending on the nature of the ring the difficulty of answering the question can vary widely. By now, a lot of work has been done to solve the problem over some subrings of number fields and function fields, including the fields themselves in the case of function fields. However there remain quite a few open questions which at the moment seem intractable. Chief among these questions are arguably the Diophantine status of $\mathbb{Q}$ (and number fields in general), the rings of integers of an arbitrary number field, and an arbitrary function field of characteristic 0.

More details on the Diophantine problem over number fields and related issues can be found in [1], [2], [3], [6], [9], [10], [21], [22], [23], [24], [26], [29], [30], [32], [33], [35], [37], [39], [42], [43], and [44]. Results concerning function fields of positive characteristic can be found in [8], [12], [27], [28], [47], [38], [40], and [48]. Also, for a general reference on the subject we suggest [11] and [46].

It turned out that solving HTP over function fields of characteristic 0 was more difficult than over function fields of positive characteristic. However we do know that HTP is undecidable over many function fields and rings of characteristic 0. In particular, we know that HTP is undecidable over fields of functions of finite transcendence degree over constant fields that are formally real or are subfields of finite extensions of $\mathbb{Q}_p$ for some odd rational prime p. (These constant fields include number fields.) Further, we also know that HTP is undecidable over function fields of transcendence degree at least 2 whose field of constants is $\mathbb{C}$. (See [7], [13], [14], [16], [17], [25], [49] for more details on these field results). We also have a few ring results: for rings of $\mathcal{S}$-integers and semi-local rings over any field of constants, and some results for rings "in the middle". (See [25], [36], [41], [50] for more details on ring results.)

One of the problems which was solved over global fields was the construction of an existential definition of order. In other words there exists an existential definition in the language of rings of the set of elements of a given global field whose order at a fixed non-archimedean valuation is non-negative. Over function fields of characteristic 0 this was done successfully over a limited class of fields and the success depended heavily on the nature of the field of constants. As it turned out, an existential definition

of order was one of the two ingredients used for showing the Diophantine undecidability of one variable function fields of characteristic 0. The other ingredient was an elliptic curve of rank 1. This plan was first implemented by Denef for the formally real rational function fields in [7]. As will be described below, the issue of finding the right elliptic curve has been solved in the greatest possible generality by the first author in [25], but the issue of defining the order remains a stumbling block. So we can solve HTP precisely over those function fields in one variable where we can define the order. (See Corollary 10.3.3 of [25].)

To make the matters even more vexing, it is not hard to see that a definition of order together with the Diophantine undecidability of any semilocal subring of a field implies Diophantine undecidability of any ring "in the middle", i.e. any holomorphy ring, pretty much in the same fashion as the Diophantine undecidability of a domain follows from the Diophantine undecidability of its field of fractions. (Both cases also require being able to define the set of non-zero elements. Fortunately, we know how to do it in all cases of interest to us.) And thus the absence of a definition of order in a manner of speaking is responsible for the subject of this paper: the Diophantine undecidability of arbitrary holomorphy rings of characteristic 0 not equal to a field. The main results of this paper are stated below.

THEOREM 1.1. — *Let K be a countable recursive one variable function field of characteristic 0. Then Hilbert's Tenth Problem is not solvable over any holomorphy ring of K not equal to the whole field.*

THEOREM 1.2. — *Let K be a one variable function field of characteristic 0 over a field of constants C. Then for any holomorphy ring of K not equal to the whole field, there exist elements $x_1, \ldots, x_n \in K \setminus C$ such that there is no algorithm to tell whether a polynomial equation with coefficients in $\mathbb{Q}(x_1, \ldots, x_n)$ has solutions in the ring.*

Remark 1.3. — The reason for two separate statements has to do with the possibility that the function field K is not countable. That possibility forces us to examine more carefully what we can allow as coefficients of our polynomial equations. In the case of a countable field it is possible to allow every element of the field as a coefficient, but in the case the field is not countable we have to restrict the set of possible coefficients to a countable set. In our case this set will depend on the ring.

Remark 1.4. — The case of holomorphy rings which are actually rings of $\mathcal{S}$-integers, i.e. rings where only finitely many primes of the field are allowed in the pole divisors of the ring elements, has been treated by the

second author in [34]. While it is not explicitly discussed in the paper, the statement of the Theorem 1.2 follows from the construction of the equations. We should also like to note that the aforementioned paper of the second author, just as the present one, was a generalization of ideas of Denef from [7]. In this paper Denef used a Pell equation to construct a model of integers instead of an elliptic curve. In view of this result we will always assume that the set of primes allowed in the pole divisors is infinite.

In some cases we will be able to prove a stronger result giving an existential definition of $\mathbb{Z}$ over an arbitrary holomorphy subring of the field not equal to the whole field. More specifically the following theorem holds.

THEOREM 1.5. — *Let K be any function field of characteristic 0 over a field of constants C. Assume there exists a subset C_0 of C such that C_0 contains $\mathbb{Z}$ and has a Diophantine definition over K. Then $\mathbb{Z}$ is existentially definable over any holomorphy ring of K not equal to the whole field.*

Remark 1.6. — We know of many function fields of characteristic 0 where constants are existentially definable. They include function fields over ample fields of constants and other large fields, including fields which are algebraically closed. (See [18], [31], and [45] for various examples.)

The main idea behind the proofs of Theorems 1.1 – 1.5 is rather simple. In a ring, where not all primes are inverted, there is a natural way to define the order using divisibility. So even if we cannot do it over a field, we can define the order over a ring (or come pretty close). We are now ready to proceed with the technical details.

2. Basic Diophantine Facts

We start with giving precise definitions to the objects we are going to study, beginning with Diophantine sets.

DEFINITION 2.1. — *Let $R_0 \subset R$ be rings and let $A \subset R^m$. A* Diophantine definition *of A over R, with coefficients in R_0, is a finite collection of polynomials $\{f_{i,j}(t_1, \dots, t_m, x_1, \dots, x_n), i = 1, \dots, r, j = 1, \dots, s\} \subset R_0[t_1, \dots, t_m, x_1, \dots, x_n]$ such that for any $(t_1, \dots, t_m) \in R^m$, we have the equivalence*

$$(t_1, \dots, t_m) \in A \iff \exists\, x_1, \dots, x_n \in R, \bigvee_{j=1}^{s} \bigwedge_{i=1}^{r} f_{i,j}(t_1, \dots, t_m, x_1, \dots, x_n) = 0.$$

We say that A is Diophantine over R *w.r.t. R_0 if it has such a Diophantine definition.*

Remark 2.2. — In general R_0 plays an auxiliary role and is often omitted, the default value being of course R.

Remark 2.3. — Consider a Diophantine set A as in Definition 2.1.

If R is a domain (which is generally the case in applications), then A has a Diophantine definition "with $s = 1$", i.e. consisting of a system of polynomial equations, without the disjunction operation.

If, moreover, the fraction field of R is not algebraically closed, we can even take $r = s = 1$; in other words, A has Diophantine definition consisting of one equation. Most authors take this as the definition of a Diophantine set. (See [5] or [46], Chapter I for more details.)

We will be able to construct such a definition of $\mathbb{Z}$ over holomorphy subrings of our function field K provided a subset of the constant field containing $\mathbb{Z}$ has a Diophantine definition over K.

DEFINITION 2.4. — *Let R be a ring and let R_0 be a recursive subring of R. We say that* Hilbert's tenth problem is solvable *in R, with coefficients in R_0, if there is an algorithm taking as input a finite set of polynomials in $R_0[X_1, \dots, X_m]$ (for some arbitrary $m > 0$) and telling whether they have a common zero in R^m.*
We write H10(R, R_0) *for this property. If R is recursive we take* H10(R) *to mean* H10(R, R).

Remark 2.5. — Assume H10(R, R_0) holds, and let $A \subset R^m$ be Diophantine w.r.t. R_0, with given Diophantine definition $(f_{i,j})_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s}$. Then A is a finite union of projections of sets A_j $(1 \leqslant j \leqslant s)$ defined by polynomial systems (with some extra variables). Since $A = \emptyset$ if and only if each A_j is empty, there is an algorithm (taking $(f_{i,j})$ as input) telling whether A is empty or not. This of course could be taken as a definition for the H10 property.

With the same assumptions, let t be a point in $R_0^m \subset R^m$. Then $\{t\}$ is Diophantine w.r.t. R_0, and we have that $t \in A$ if and only if $\{t\} \cap A \neq \emptyset$. Hence, the above discussion shows that there is an algorithm telling whether t belongs to A.

Remark 2.6. — Just as in Remark 2.3, if R is a domain with non-algebraically closed fraction field, it suffices to check H10 for systems consisting of one polynomial: this is the traditional definition of the H10 property.

PROPOSITION 2.7. — *Let $R_1 \subset R_2 \subset R_3$ be rings, with R_1, R_2 and the inclusion $R_1 \subset R_2$ recursive. Let I be an ideal of R_3 with the following properties:*

- *I is generated by finitely many elements of R_2* (in particular, it is Diophantine w.r.t. R_2).
- *$R_1 \cap I = \{0\}$.*
- *The set $R_1 + I \subset R_3$ is Diophantine w.r.t. R_2.*

Then H10(R_3, R_2) *implies* H10(R_1).

Proof. — Assume H10(R_3, R_2). Let $D \subset R_1^m$ be defined by

$$D := \left\{ t \in R_1^m \mid \forall i \in \{1, \dots, r\},\ f_i(t) = 0 \right\}$$

where the f_i's are polynomials with coefficients in R_1. We are looking for an algorithm telling whether D is empty.

Put $\Delta := R_1 + I$, which is Diophantine in R_3 by assumption, and define $B \subset R_3^m$ by

$$B := \left\{ t \in \Delta^m \mid \forall i \in \{1, \dots, r\},\ f_i(t) \in I \right\}.$$

Clearly, B is Diophantine w.r.t. R_2 since Δ and I are. Hence, by H10(R_3, R_2), there is an algorithm telling whether B is empty, so it suffices to prove that $D = \emptyset$ if and only if $B = \emptyset$. The "if" part is trivial since $D \subset B$. Conversely, assume there exists some $t \in B$. By definition of Δ, there exists $t_1 \in R_1^m$ which is congruent (coordinatewise) to $t \mod I$. Then for each i we still have $f_i(t_1) \in I$, but also $f_i(t_1) \in R_1$ since f_i has coefficients in R_1. Hence $f_i(t_1) = 0$, which means that $t_1 \in D$, hence $D \neq \emptyset$. (In fact it is easy to see that $B = D + IR_3^m$ and $D = R_1^m \cap B$.) □

We will also use the following standard trick:

PROPOSITION 2.8. — *Let $R_0 \subset R \subset R'$ be rings, with R_0 recursive. Assume that, as an R-module, R' has a finite basis $\mathcal{B} = \{b_1, \dots, b_m\}$ such that R_0 contains the following elements:*

- *the coordinates of 1 in $\mathcal{B}$,*
- *the entries of the matrix of multiplication by b_i in R', for each $i \in \{1, \dots, m\}$.*

We identify R' with R^m using $\mathcal{B}$. Let $D \subset R'^d$ be Diophantine over R' w.r.t. R_0. Then:

(1) *D (as a subset of R^{md}) is Diophantine over R (w.r.t. R_0).*
(2) *$D \cap R^d \subset R^d$ is Diophantine over R (w.r.t. R_0).*

Proof. — (1) is immediate from the assumptions. The first assumption also implies that the inclusion $R \subset R' \cong R^m$ identifies R with a Diophantine subset of R^m w.r.t. R_0, so the same property holds for the inclusion $R^d \subset R'^d \cong R^{md}$. Assertion (2) follows. □

3. Basic Facts on Function Fields and Holomorphy Rings

DEFINITION 3.1. — *Let C be a field. Then a (one-variable) function field K over C is a finite extension of the rational function field $C(t)$. (Equivalently, it is a finitely generated extension of C of transcendence degree* 1*). For such a function field K, a* prime *of K is a nontrivial discrete valuation of K which is trivial on C. We denote by $\mathcal{P}_K$ the set of all such primes (abusingly omitting C from the notation). For $\mathfrak{p} \in \mathcal{P}_K$ we adopt the traditional notation $\mathrm{ord}_\mathfrak{p}$ for the corresponding normalized valuation and we denote by $O(\mathfrak{p})$ the associated valuation ring. If $\mathcal{W}$ is a* non-empty *subset of $\mathcal{P}_K$, we put*

$$O_{K,\mathcal{W}} = \bigcap_{\mathfrak{p} \notin \mathcal{W}} O(\mathfrak{p}) = \big\{h \in K \mid \forall \mathfrak{p} \notin \mathcal{W} \text{ we have that } \mathrm{ord}_\mathfrak{p} h \geqslant 0\big\}.$$

$O_{K,\mathcal{W}}$ is called a holomorphy ring *of K.*

Note that, with the above notations, taking $\mathcal{W} = \emptyset$ would lead to the intersection of *all* rings $O(\mathfrak{p})$ ($\mathfrak{p} \in \mathcal{P}_K$). This ring is the algebraic closure C' of C in K, a finite extension of C, and K is a function field over C' with the same set $\mathcal{P}_K$ and rings $O_{K,\mathcal{W}}$ as over C. Therefore, for the purposes of this paper we can always replace C by C', i.e. assume C algebraically closed in K. (In other words, K is a *regular extension* of C).

If $\mathcal{W} = \mathcal{P}_K$, then $O_{K,\mathcal{W}} = K$. Otherwise, $O_{K,\mathcal{W}}$ is a Dedekind domain with fraction field K; its maximal ideals correspond bijectively to elements of $\mathcal{P}_K \setminus \mathcal{W}$, via the map

$$\mathfrak{p} \longmapsto I_\mathfrak{p} := \big\{h \in O_{K,\mathcal{W}} \mid \mathrm{ord}_\mathfrak{p} h > 0\big\}.$$

We shall derive Theorems 1.1, 1.2 and 1.5 from the following result:

THEOREM 3.2. — *Let K and $\mathcal{W}$ be as above, with $\emptyset \neq \mathcal{W} \neq \mathcal{P}_K$ and* $\mathrm{char}\, K = 0$. *Let $\mathfrak{p} \notin \mathcal{W}$ be a prime of K, and let $I_\mathfrak{p}$ be the corresponding maximal ideal of $O_{K,\mathcal{W}}$. Then $\mathbb{Z} + I_\mathfrak{p}$ is Diophantine in $O_{K,\mathcal{W}}$.*

Proof of Theorems 1.1, 1.2 and 1.5 (from 3.2). — For Theorems 1.1 and 1.2 we simply apply Proposition 2.7 with $R_1 = \mathbb{Z}$ and $R_3 = O_{K,\mathcal{W}}$. We

take for R_2 the subring of R_3 generated by a finite subset containing a generating set for $I_{\mathfrak{p}}$ and all elements occurring in a Diophantine definition of $\mathbb{Z}+I_{\mathfrak{p}}$. The condition $I_{\mathfrak{p}}\cap\mathbb{Z}=\{0\}$ is obvious since nonzero integers are invertible in $C\subset O_{K,\mathcal{W}}$.

For Theorem 1.5, we have $\mathbb{Z}\subset(\mathbb{Z}+I_{\mathfrak{p}})\cap C_0\subset(\mathbb{Z}+I_{\mathfrak{p}})\cap C=\mathbb{Z}$ (the last equality follows from $C\cap I_{\mathfrak{p}}=\{0\}$). Hence $\mathbb{Z}=(\mathbb{Z}+I_{\mathfrak{p}})\cap C_0$ is Diophantine. □

From now on, we assume that C is algebraically closed in K, and that the characteristic is zero. If $\hat{C}$ is a finite extension of C, then $\hat{K}:=\hat{C}\otimes_C K$ is a finite extension of K, and a function field over $\hat{C}$. Moreover, for $\mathcal{W}$ as above, the following three subrings of $\hat{K}$ are equal:

- $\hat{C}\otimes_C O_{K,\mathcal{W}}$,
- the integral closure of $O_{K,\mathcal{W}}$ in $\hat{K}$,
- the holomorphy ring $O_{\hat{K},\hat{\mathcal{W}}}$ where $\hat{\mathcal{W}}$ is the set of primes of $\hat{K}$ inducing primes in $\mathcal{W}$.

The first description shows in particular that $O_{\hat{K},\hat{\mathcal{W}}}$ is a free module over $O_{K,\mathcal{W}}$, of rank $[\hat{C}:C]$.

In addition, let $\mathfrak{p}\notin\mathcal{W}$ be a prime of K. Then there exists a prime $\hat{\mathfrak{p}}\notin\hat{\mathcal{W}}$ of $\hat{K}$ extending $\mathfrak{p}$, and the corresponding ideals $I_{\mathfrak{p}}\subset O_{K,\mathcal{W}}$ and $I_{\hat{\mathfrak{p}}}\subset O_{\hat{K},\hat{\mathcal{W}}}$ satisfy $I_{\mathfrak{p}}=O_{K,\mathcal{W}}\cap I_{\hat{\mathfrak{p}}}$. It follows that $\mathbb{Z}+I_{\mathfrak{p}}=O_{K,\mathcal{W}}\cap(\mathbb{Z}+I_{\hat{\mathfrak{p}}})$. By Proposition 2.8 (2) we see that if $\mathbb{Z}+I_{\hat{\mathfrak{p}}}$ is Diophantine in $O_{\hat{K},\hat{\mathcal{W}}}$, then $\mathbb{Z}+I_{\mathfrak{p}}$ is Diophantine in $O_{K,\mathcal{W}}$.

In particular, to prove Theorem 3.2 for K, $\mathcal{W}$, $\mathfrak{p}$, we may replace these data by $\hat{K}$, $\hat{\mathcal{W}}$, $\hat{\mathfrak{p}}$, respectively.

We shall use this remark as follows: take for $\hat{C}$ the residue field of $\mathfrak{p}$. We have a surjective morphism $O_{K,\mathcal{W}}\to\hat{C}$ of C-algebras, hence (tensoring with $\hat{C}$) a surjective $\hat{C}$-morphism $O_{\hat{K},\hat{\mathcal{W}}}\to\hat{C}$. Its kernel defines a prime $\hat{\mathfrak{p}}$ of $\hat{K}$ above $\mathfrak{p}$, which has *degree one* in the sense that its residue field is the constant field $\hat{C}$ of $\hat{K}$. To summarize, *we can always assume that the prime $\mathfrak{p}$ of Theorem 3.2 has degree one.*

As we have already mentioned above, our paper has two main inputs. The first one is contained in a paper of Denef (see [7]) which constructs a rank one elliptic curve over any rational function field of characteristic 0 together with a way of generating integers. The second input is a result of the first author that allows the elliptic curve constructed by Denef to retain its nice properties under finite extensions. More specifically we will use the following result which is a consequence of Theorem 1.8 (ii) and Proposition 2.3.1 of [25].

THEOREM 3.3. — *Let K be a function field of characteristic 0 over a field of constants C. Let $\mathfrak{p}$ be a degree one prime of K. Let $\mathfrak{D}$ be a divisor of K such that $\mathrm{ord}_{\mathfrak{q}}\mathfrak{D} \in \{0,1\}$ for any prime $\mathfrak{q}$ of K, $\mathrm{ord}_{\mathfrak{p}}\mathfrak{D} = 0$, and the degree of $\mathfrak{D}$ is at least $2g_K + 2$, where g_K is the genus of K. Let $F(T)$ be a nonsingular cubic polynomial over $\mathbb{Q}$ such that the elliptic curve $Y^2 = F(X)$ has no complex multiplication. Then there exists an $x \in K$ such that its pole divisor is $\mathfrak{D}$, $\mathrm{ord}_{\mathfrak{p}}x > 0$, and the elliptic curve E_x defined by the equation*

$$F\Big(\frac{1}{x}\Big)\,Y^2 = F(X) \tag{3.1}$$

has the property that $E_x(C(x)) = E_x(K)$. Also $E_x(C(x))$ is of rank 1 generated by the point with affine coordinates $(\frac{1}{x}, 1) \in E(C(x)) \setminus E(C)$ modulo 2-torsion.

Proof. — We need a slight refinement of Proposition 2.3.1 of [25]:

LEMMA 3.4. — *With the assumptions of Theorem 3.3, there exists a nonzero $g \in K$ with the following properties:*

- *the divisor of zeros of g is $\mathfrak{D}$,*
- *g has only simple poles, and $\mathfrak{p}$ is one of them,*
- *g has simple ramification (i.e. in the extension $K/C(g)$ no prime has ramification degree greater than 2).*

Proof. — The argument is classical and entirely similar to [25], 2.3.1. Put $d := \deg \mathfrak{D}$. The linear system $|\mathfrak{D}|$ is a projective space of dimension $d - g_k$, and we identify $\mathfrak{D}$ with a (C-rational) point in it. Inside $|\mathfrak{D}|$ we consider the following subvarieties, where Q (resp. Δ) denotes a variable point (resp. effective divisor):

- $H = \{\text{divisors of the form } \mathfrak{p} + \Delta\}$,
- $Z_1 = \{\text{divisors of the form } 2\mathfrak{p} + \Delta\}$,
- $Z_2 = \{\text{divisors of the form } \mathfrak{p} + 2Q + \Delta\}$,
- $Z_3 = \{\text{divisors of the form } 3Q + \Delta\}$.

Clearly, none of these contains $\mathfrak{D}$, and H is a hyperplane because $\mathfrak{p}$ has degree 1. It is proved in [25] that Z_3 has codimension $\geqslant 2$ in $|\mathfrak{D}|$, and similar arguments easily show that the same holds for Z_1 and Z_2. Hence we can find a line in $|\mathfrak{D}|$ through the point $\mathfrak{D}$, defined over C and disjoint from $Z_1 \cup Z_2 \cup Z_3$. This line meets H at a point $\mathfrak{D}'$. There is an element g of K with divisor $\mathfrak{D} - \mathfrak{D}'$, and this g has the required properties. □

Let us return to the proof of Theorem 3.3. Clearly, by multiplying g by some nonzero constant c (in $\mathbb{Q}$, if we wish) we may also choose g with

branch locus disjoint from the inverse roots of F. This makes g *admissible* for $\mathfrak{D}$ in the sense of [25], Definition 1.5.2. Further, it follows from Theorem 1.8 (ii) of [25] that by choosing c appropriately we may assume in addition that g is *good*, i.e. $E_{g^{-1}}(C(g)) = E_{g^{-1}}(K)$.

Now let $x = g^{-1}$: we now have that $E_x(C(x)) = E_x(K)$, and the rest of the theorem follows from the assumption on F and from [7] which describes $E_x(C(x))$. □

4. Diophantine Undecidability of Holomorphy Rings

Notation and Assumptions 4.1. — We start with a first notation set.

- Let K be a function field of characteristic 0 over a field of constants C.
- Let $\mathcal{P}_K$ be the set of all primes of K.
- Let $\emptyset \neq \mathcal{W} \subset \mathcal{P}$, $\mathcal{W} \neq \mathcal{P}$.
- Let $\mathfrak{p} \in \mathcal{P} \setminus \mathcal{W}$ be a prime of degree 1. (By assumption, $\mathcal{P} \setminus \mathcal{W}$ is not empty, and as explained in the previous section we may assume that it contains a prime of degree 1 by extending K).
- Let g_K be the genus of K.
- Assume that $\mathcal{W}$ contains infinitely many primes (in fact the present proof works whenever $\sum_{\mathfrak{q}\in\mathcal{W}} \deg \mathfrak{q} \geqslant 2g_K + 2$). As noted in Remark 1.4 of the introduction, the case where $\mathcal{W}$ is finite is settled in [34]; more precisely, in that case, $\mathbb{Z}$ is Diophantine in $O_{K,\mathcal{W}}$ (Theorem 3.1 of [34]), hence our Theorem 3.2 also holds.
- Let $\mathcal{D} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_{2g_K+2}\}$ be a set of distinct elements of $\mathcal{W}$. (We only need the total degree of $\mathcal{D}$ to be at least $2g_K + 2$, in order to apply Theorem 3.3.)
- Let $x \in K$ be such that its pole divisor is $\prod_i \mathfrak{q}_i$, $\mathrm{ord}_{\mathfrak{p}} x > 0$, and $E(K) = E(C(x))$, where $E = E_x$ is the elliptic curve defined in (3.1). (Such an x exists by Theorem 3.3).

Observe that $x \in O_{K,\mathcal{W}}$ and therefore $O_{K,\mathcal{W}}$ contains the polynomial ring $C[x]$. Moreover, the condition $\mathrm{ord}_{\mathfrak{p}} x > 0$ means that $\mathfrak{p}$ lies above the ideal (x) of $C[x]$. In other words, for any $z \in C(x)$ we have

$$\mathrm{ord}_{\mathfrak{p}} z = (\mathrm{ord}_{\mathfrak{p}} x)(\mathrm{ord}_0 z) \tag{4.1}$$

where, in the right-hand side, z is viewed as a rational function of x.

Two elements $a,\ b \in O_{K,\mathcal{W}}$ will be called *coprime* if they generate the unit ideal, i.e. there exist $A, B \in O_{K,\mathcal{W}}$ such that

$$Aa + Bb = 1. \tag{4.2}$$

Note that we have "Gauss' Lemma": if a and b are coprime and a divides bc in $O_{K,\mathcal{W}}$, then a divides c.

PROPOSITION 4.2. — *The set* $\{h \in O_{K,\mathcal{W}} \mid h \neq 0\}$ *is Diophantine over* $O_{K,\mathcal{W}}$.

Proof. — The proof is essentially a consequence of the Strong Approximation Theorem and can be found in [35]. □

Notation and Assumptions 4.3. — We now add the following notation and assumptions to our list.

- Let $P \in E(K)$ be the point whose affine coordinates derived from (3.1) are $(\frac{1}{x}, 1)$.
- For nonzero $n \in \mathbb{Z}$, let (x_n, y_n) be the affine coordinates of $[n]P$ derived from (3.1). Since $P \in E(C(x))$ we have that x_n and y_n are rational functions of x.
- Since $[n]P$ is not a torsion point, we have $y_n \neq 0$ and we can write
$$\frac{xx_n}{y_n} = \frac{\alpha_n}{\beta_n},$$
where $\alpha_n, \beta_n \in C[x]$ are relatively prime polynomials in x (in particular, since they satisfy relation (4.2) in $C[x] \subset O_{K,\mathcal{W}}$, they are also coprime in $O_{K,\mathcal{W}}$).

The following lemma shows how we will generate integers to show undecidability. Its proof can be found in Lemma 3.2 of [7].

LEMMA 4.4. — *For any* $n \in \mathbb{Z}_{>0}$ *we have that* $\operatorname{ord}_{\mathfrak{p}}\left(x\frac{x_n}{y_n} - n\right) > 0$.

Using Lemma 4.4 and the definition of being coprime, one easily deduces the following lemma.

LEMMA 4.5. — *Let* n *be a nonzero integer. Assume that*

$$\frac{xx_n}{y_n} = \frac{a_n}{b_n}$$

where $a_n,\ b_n \in O_{K,\mathcal{W}}$ *are coprime. Then:*

$$a_n = \varepsilon\alpha_n \quad \text{and} \quad b_n = \varepsilon\beta_n \qquad \text{for some } \varepsilon \in O_{K,\mathcal{W}}^{\times}, \tag{4.3}$$

$$a_n - n\,b_n = xw \qquad \text{for some } w \in O_{K,\mathcal{W}}, \tag{4.4}$$

$$\operatorname{ord}_{\mathfrak{p}}(b_n) = 0. \tag{4.5}$$

Proof. — To prove (4.3) we note that $a_n\beta_n = b_n\alpha_n$, hence (by Gauss' lemma) a_n and α_n divide each other in $O_{K,\mathcal{W}}$. In other words, $\varepsilon := a_n/\alpha_n$ is a unit.

To prove (4.4) and (4.5) we may and will assume, in view of (4.3), that $a_n = \alpha_n$ and $b_n = \beta_n$. Let $w \in K$ be defined by (4.4). Let us prove that $w \in C[x]$. Since a_n and b_n are in $C[x]$ it suffices to prove that $a_n - n\,b_n$ (as a polynomial in x) vanishes at 0, which by (4.1) is equivalent to $\mathrm{ord}_{\mathfrak{p}}(a_n - n\,b_n) > 0$. This is clear from Lemma 4.4 since $a_n - n\,b_n = b_n(x\frac{x_n}{y_n} - n)$ and $b_n \in C[x]$.

Let us now prove (4.5). Since $a_n - n\,b_n$ vanishes at 0 it follows that if b_n vanishes at 0, so does a_n. Since they are relatively prime polynomials, this cannot happen. □

We also have a converse of sorts to (4.4) above.

Lemma 4.6. — *With the assumptions of 4.5, suppose for some $c \in K$ we have that $\mathrm{ord}_{\mathfrak{p}}(a_n - b_n c) > 0$. Then $\mathrm{ord}_{\mathfrak{p}}(c - n) > 0$.*

Proof. — The equation $a_n - b_n c = xw$ implies that $\mathrm{ord}_{\mathfrak{p}}(a_n - b_n c) > 0$ as $\mathrm{ord}_{\mathfrak{p}} x > 0$ and $\mathfrak{p} \notin \mathcal{W}$. Since $\mathrm{ord}_{\mathfrak{p}}(a_n - b_n n) > 0$ by Lemma 4.5, we conclude that $\mathrm{ord}_{\mathfrak{p}}(b_n(c-n)) > 0$. This proves the result by (4.5). □

Next we prove an easy lemma.

Lemma 4.7. — *The set*

$$\mathtt{E} = \left\{(u,v,w,z) \in (O_{K,\mathcal{W}})^4 \;\middle|\; vw \neq 0,\ \exists n \in \mathbb{Z}\setminus\{0\} : x_n = \frac{u}{v}, y_n = \frac{z}{w}\right\}$$

is Diophantine.

Proof. — Since we know how to define non-zero elements over any holomorphy ring and all the points of $E(K)$ are in fact of the form $[n]P + T$ where T is a 2-torsion point, we can easily define the set

$$\mathtt{E}_{\mathrm{even}} = \left\{(u',v',w',z') \in (O_{K,\mathcal{W}})^4 \;\middle|\; \exists k \in \mathbb{Z}\setminus\{0\} : x_{2k} = \frac{u'}{v'}, y_{2k} = \frac{z'}{w'}\right\}$$

using Theorem 3.3. Then $(u,v,w,z) \in \mathtt{E}$ if and only if either $(u,v,w,z) \in \mathtt{E}_{\mathrm{even}}$ or $\left(\frac{u}{v}, \frac{z}{w}\right) = \left(\frac{u'}{v'}, \frac{z'}{w'}\right) +_E \left(\frac{1}{x}, 1\right)$, where $(u',v',w',z') \in \mathtt{E}_{\mathrm{even}}$. □

Proof of Theorem 3.2. — Put $I = I_{\mathfrak{p}} = \{t \in O_{K,\mathcal{W}} \mid \mathrm{ord}_{\mathfrak{p}}(t) > 0\}$, and let us prove that $\mathbb{Z} + I$ is Diophantine in $O_{K,\mathcal{W}}$.

Let ξ be an element of $O_{K,\mathcal{W}}$. We claim that the following are equivalent:

(1) $\xi \in \mathbb{Z} + I$,

(2) either $\xi \in I$, or the following system has a solution (u, v, w, z, a, b, A, B) in $O_{K,\mathcal{W}}^8$:

$$\begin{cases} (u, v, w, z) \in \mathtt{E} \\ \dfrac{a}{b} = \dfrac{xuw}{vz} \\ Aa + Bb = 1 \\ a - b\xi \in I. \end{cases} \tag{4.6}$$

This clearly implies the result since both $\mathtt{E}$ and I are Diophantine (the former by 4.7, and the latter because it is a finitely generated ideal).

First, assume (1). If $\xi \in I$ we are done. Otherwise, we may assume that $\xi =: n$ is a nonzero integer since both (1) and (2) are invariant under adding an element of I to ξ. We construct a solution of (4.6) as follows. First, choose u, v, w, z so that $\frac{u}{v} = x_n$, $\frac{z}{w} = y_n$ (first relation). Put $a = \alpha_n$ and $b = \beta_n$ (as defined in 4.3): the second relation is satisified and we can find A and B satisfying the third. Finally by (4.4) the fourth relation holds since $x \in I$.

Now assume that (2) holds. As before, (1) is trivial if $\xi \in I$. Otherwise, fix a solution (u, v, w, z, a, b, A, B) of (4.6). By definition of $\mathtt{E}$ there is a nonzero integer n such that $x_n = \frac{u}{v}$ and $y_n = \frac{z}{w}$. We can then apply Lemmas 4.5 and 4.6 with $a_n = a$, $b_n = b$ and $c = \xi$ to conclude that $\mathrm{ord}_{\mathfrak{p}}(\xi - n) > 0$. In other words, $\xi \in \mathbb{Z} + I$. □

BIBLIOGRAPHY

[1] J.-L. Colliot-Thélène, A. Skorobogatov & P. Swinnerton-Dyer, "Double fibres and double covers: Paucity of rational points", *Acta Arithmetica* **79** (1997), p. 113-135.

[2] G. Cornelissen, T. Pheidas & K. Zahidi, "Division-ample sets and diophantine problem for rings of integers", *Journal de Théorie des Nombres Bordeaux* **17** (2005), p. 727-735.

[3] G. Cornelissen & K. Zahidi, "Topology of diophantine sets: Remarks on Mazur's conjectures", in 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*, American Mathematical Society, 2000, p. 253-260.

[4] M. Davis, "Hilbert's tenth problem is unsolvable", *American Mathematical Monthly* **80** (1973), p. 233-269.

[5] M. Davis, Y. Matiyasevich & J. Robinson, "Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution", *Proc. Sympos. Pure Math.* **28** (1976), p. 323- 378, Amer. Math. Soc.

[6] J. Denef, "Hilbert's tenth problem for quadratic rings", *Proc. Amer. Math. Soc.* **48** (1975), p. 214-220.

[7] ———, "The diophantine problem for polynomial rings and fields of rational functions", *Transactions of American Mathematical Society* **242** (1978), p. 391-399.

[8] ———, "The diophantine problem for polynomial rings of positive characteristic", Logic Colloquium 78, p. 131-145, Logic Colloquium 78, In M. Boffa, D. van Dalen, and K. MacAloon, editors, North Holland, 1979.

[9] ———, "Diophantine sets of algebraic integers, II", *Transactions of American Mathematical Society* **257** (1980), no. 1, p. 227-236.

[10] J. Denef & L. Lipshitz, "Diophantine sets over some rings of algebraic integers", *Journal of London Mathematical Society* **18** (1978), no. 2, p. 385-391.

[11] J. Denef, L. Lipshitz & T. Pheidas, editors, *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, Contemporary Mathematics, vol. 270, American Mathematical Society, Providence, RI, 2000, Papers from the workshop held at Ghent University, Ghent, November 2-5, 1999 .

[12] K. Eisenträger, "Hilbert's tenth problem for algebraic function fields of characteristic 2", *Pacific J. Math.* **210** (2003), no. 2, p. 261-281.

[13] ———, "Hilbert's tenth problem for function fields of varieties over $\mathbb{C}$", *Int. Math. Res. Not.* (2004), no. 59, p. 3191-3205.

[14] ———, "Hilbert's Tenth Problem for function fields of varieties over number fields and p-adic fields", *Journal of Algebra* **310** (2007), p. 775-792.

[15] M. Fried & M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer Verlag, Berlin, second edition, 2005.

[16] H. Kim & F. Roush, "Diophantine undecidability of $\mathbb{C}(t_1, t_2)$", *Journal of Algebra* **150** (1992), no. 1, p. 35-44.

[17] ———, "Diophantine unsolvability over p-adic function fields", *Journal of Algebra* **176** (1995), p. 83-110.

[18] J. Koenigsmann, "Defining transcendentals in function fields", *J. Symbolic Logic* **67** (2002), no. 3, p. 947-956.

[19] S. Lang, *Algebraic Number Theory*, Addison Wesley, Reading, MA, 1970.

[20] Y. Matiyasevich, *Hilbert's Tenth Problem*, The MIT Press, Cambridge, Massachusetts, 1993.

[21] B. Mazur, "The topology of rational points", *Experimental Mathematics* **1** (1992), no. 1, p. 35-45.

[22] ———, "Questions of decidability and undecidability in number theory", *Journal of Symbolic Logic* **59** (1994), no. 2, p. 353-371.

[23] ———, "Speculation about the topology of rational points: An up-date", *Asterisque* **228** (1995), p. 165-181.

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

[25] L. Moret-Bailly, "Elliptic curves and Hilbert's Tenth Problem for algebraic function fields over real and p-adic fields", *Journal für die reine und angewandte Mathematik* **587** (2006), p. 77-143.

[26] T. Pheidas, "Hilbert's tenth problem for a class of rings of algebraic integers", *Proceedings of American Mathematical Society* **104** (1988), no. 2, p. 611-620.

[27] ———, "Hilbert's tenth problem for fields of rational functions over finite fields", *Inventiones Mathematicae* **103** (1991), p. 1-8.

[28] ———, "Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic", *J. Algebra* **273** (2004), no. 1, p. 395-411.

[29] B. Poonen, "Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$", *Journal of AMS* **16** (2003), no. 4, p. 981-990.

[30] B. Poonen & A. Shlapentokh, "Diophantine definability of infinite discrete non-archimedean sets and diophantine models for large subrings of number fields", *Journal für die Reine und Angewandte Mathematik* (2005), p. 27-48.

[31] F. Pop, "Elementary equivalence versus isomorphism", *Invent. Math.* **150** (2002), no. 2, p. 385-408.

[32] H. Shapiro & A. Shlapentokh, "Diophantine relations between algebraic number fields", *Communications on Pure and Applied Mathematics* **XLII** (1989), p. 1113-1122.

[33] A. Shlapentokh, "Extension of Hilbert's tenth problem to some algebraic number fields", *Communications on Pure and Applied Mathematics* **XLII** (1989), p. 939-962.

[34] ———, "Hilbert's tenth problem for rings of algebraic functions of characteristic 0", *J. Number Theory* **40** (1992), no. 2, p. 218-236.

[35] ———, "Diophantine classes of holomorphy rings of global fields", *Journal of Algebra* **169** (1994), no. 1, p. 39-175.

[36] ———, "Diophantine undecidability for some holomorphy rings of algebraic functions of characteristic 0", *Communications in Algebra* **22** (1994), no. 11, p. 4379-4404.

[37] ———, "Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of $\mathbb{Q}$", *Annals of Pure and Applied Logic* **68** (1994), p. 299-325.

[38] ———, "Diophantine undecidability of algebraic function fields over finite fields of constants", *Journal of Number Theory* **58** (1996), no. 2, p. 317-342.

[39] ———, "Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator", *Inventiones Mathematicae* **129** (1997), p. 489-507.

[40] ———, "Diophantine undecidability of function fields of characteristic greater than 2 finitely generated over a field algebraic over a finite field", *Compositio Mathematica* **132** (2002), no. 1, p. 99-120.

[41] ———, "On diophantine decidability and definability in some rings of algebraic functions of characteristic 0", *Journal of Symbolic Logic* **67** (2002), no. 2, p. 759-786.

[42] ———, "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** (2002), p. 227-252.

[43] ———, "A ring version of Mazur's conjecture on topology of rational points", *International Mathematics Research Notices* **7** (2003), p. 411-423.

[44] ———, "On diophantine definability and decidability in some infinite totally real extensions of $\mathbb{Q}$", *Transactions of AMS* **356** (2004), no. 8, p. 3189-3207.

[45] ———, "First-order definitions of rational functions and $\mathcal{S}$-integers over holomorphy rings of algebraic functions of characteristic 0", *Ann. Pure Appl. Logic* **136** (2005), no. 3, p. 267-283.

[46] ———, *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*, Cambridge University Press, 2006.

[47] A. Shlyapentokh, "Diophantine undecidability for some function fields of infinite transcendence degree and positive characteristic", *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)* **304** (2003), no. Teor. Slozhn. Vychisl. 8, p. 141-167, 171.

[48] C. Videla, "Hilbert's tenth problem for rational function fields in characteristic 2", *Proceedings of the American Mathematical Society* **120** (1994), no. 1, p. 249-253.

[49] K. Zahidi, "The existential theory of real hyperelliptic fields", *Journal of Algebra* **233** (2000), no. 1, p. 65-86.

[50] ———, "Hilbert's tenth problem for rings of rational functions", *Notre Dame Journal of Formal Logic* **43** (2003), p. 181-192.

Manuscrit reçu le 23 mai 2008,
révisé le 18 novembre 2008,
accepté le 12 décembre 2008.

Laurent MORET-BAILLY
IRMAR
Université de Rennes 1
Campus de Beaulieu
35042 Rennes Cedex (France)
Laurent.Moret-Bailly@univ-rennes1.fr

Alexandra SHLAPENTOKH
East Carolina University
Department of Mathematics
Greenville, NC 27858 (U.S.A.)
shlapentokha@ecu.edu