

# Decision problems in Algebra and analogues of Hilbert's tenth problem

A tutorial presented at American Institute of Mathematics and Newton Institute of Mathematical Sciences

Thanases Pheidas  
*University of Crete*

Karim Zahidi  
*University of Antwerp*

## Contents

---

1	Part A: Decidability results	211
	1.1 Presburger arithmetic	213
	1.2 Addition and divisibility	214
	1.3 Addition and exponentiation	217
	1.4 The analogue of Hilbert's tenth problem for algebraic groups	217
	1.5 The results of Ax for 'almost all primes'	218
	1.6 Model-completeness	218
	1.7 Complete theories	219
	1.8 Power-series and germs of analytic functions: existential decidability and Artin approximation	220
	1.9 Positive-existential versus existential	222
2	Part B: A qualitative analogue of HTP and the Conjectures of S. Lang	224
	2.1 A language for geometric problems	226
	2.2 A geometric problem	227
	2.3 Varieties with an infinite number of points over a ring	228
3	Part C: Hilbert's tenth problem for analytic and meromorphic functions	229
4	Part D: Comments on the analogue of Hilbert's tenth problem for $\mathbb{Q}$	230
	References	232

---

## Introduction

One of the first tasks undertaken by Model Theory was to produce elimination results, for example methods of eliminating quantifiers in formulas of certain structures. In almost all cases those methods have been effective and thus provide algorithms for examining the truth of

possible theorems. On the other hand, Gödel's Incompleteness Theorem and many subsequent results show that in certain structures, constructive elimination is impossible. The current article is a (very incomplete) effort to survey some results of each kind, with a focus on the decidability of existential theories, and ask some questions at the intersection of Logic and Number Theory. It has been written having in mind a mathematician without prior exposition to Model Theory. Our presentation will consist of four parts.

Part A deals with positive (decidability) results for analogues of Hilbert's tenth problem for substructures of the integers and for certain local rings.

Part B focuses on the 'parametric problem' and the relevance of Hilbert's tenth problem to conjectures of Lang.

Part C deals with the analogue of Hilbert's tenth problem for rings of Analytic and Meromorphic functions.

Part D is an informal discussion on the chances of proving a negative (or could it be positive?) answer to the analogue of Hilbert's tenth problem for the field of rational numbers.

A central undecidability result in our presentation will be Hilbert's tenth problem, which asked:

*Give a procedure which, in a finite number of steps, can determine whether a polynomial equation (in several variables) with integer coefficients has or does not have integer solutions.*

The answer by Matiyasevich ([43]), following work of Davis, Putnam and J. Robinson, was negative ('no such algorithm can exist').

Analogous questions can be asked for domains other than the ring of integers. In trying to ask questions "similar" to Hilbert's tenth problem (from now on denoted by HTP) in rings other than the rational integers, one has to specify the kind of 'diophantine equations' one considers. For example, say that we want to ask HTP for the ring of polynomials  $\mathbb{C}[z]$  in one variable,  $z$ , with complex coefficients. Let  $\mathcal{D}$  be a class of 'diophantine equations' over  $\mathbb{C}[z]$ , that is, polynomial equations in many variables, with coefficients in  $\mathbb{C}[z]$ . The analogue of HTP for this class is "does there exist an algorithm to decide, given any equation in  $\mathcal{D}$ , whether that equation has or does not have solutions in  $\mathbb{C}[z]$ ?". It is obvious that if one chooses  $\mathcal{D}$  to be the set of all 'diophantine equations' over  $\mathbb{C}[z]$  then the answer to the question is NO, simply because  $\mathcal{D}$  is uncountable (algorithms, in the classical sense, treat only countable problems). On the other hand, one may take  $\mathcal{D}$  to be the set of 'diophantine equations' which have coefficients in  $\mathbb{Z}[z]$  or in  $\mathbb{Z}[i][z]$  ( $i = \sqrt{-1}$ )

or in  $\mathbb{Z}$ . Each of these choices gives a different 'analogue of HTP for  $\mathbb{C}[z]$ '. In this paper we will be specifying  $\mathcal{D}$  by specifying the *language* in which we work. Notice that the analogue of HTP for  $\mathbb{C}[z]$  for the class  $\mathcal{D}$ , asked for systems of diophantine equations (rather than single equations), is really the question of decidability of the positive-existential theory of  $\mathbb{C}[z]$  in the language  $L$  which contains symbols for addition, multiplication, equality, and constant symbols for the coefficients of the equations of  $\mathcal{D}$  (or constant symbols whose interpretations generate exactly the set of coefficients of equations of  $\mathcal{D}$ ). For example, the analogue of HTP (for systems of equations) for  $\mathbb{C}[z]$  with  $\mathcal{D}$  the set of equations with coefficients in  $\mathbb{Z}$  is equivalent to the question of decidability of the positive-existential theory of  $\mathbb{C}[z]$  in the language  $L_r = \{+, \cdot; =; 0, 1\}$ , while that with  $\mathcal{D}$  the set of equations with coefficients in  $\mathbb{Z}[z]$  is equivalent to the question of decidability of the positive-existential theory of  $\mathbb{C}[z]$  in the language  $L_z = \{+, \cdot; =; 0, 1, z\}$ .

We will consider structures (models) such as the field  $\mathbb{C}(z)$ . Each structure comes with a language, i.e. a set of symbols for the relations, functions and distinguished elements of the structure. For example we consider  $\mathbb{C}(z)$  as an  $L_z$ -structure, with symbol for the relations  $=$ , the functions  $+$  (addition) and  $\cdot$  (multiplication) and the distinguished elements  $0$ ,  $1$  and  $z$ . The *first order sentences* of the language of the structure are the sentences built using the symbols of the language, variables ranging over the universe of the structure, quantifiers ( $\exists$  and  $\forall$ ) and logical connectives, by the usual rules. The *existential* (resp. *positive-existential*) sentences are those that start with existential quantifiers which are followed by a quantifier-free formula (resp. by a quantifier-free formula which is a disjunction of conjunctions of relations - negations of relations are not allowed in this case). The *(full) theory* (resp. *existential theory*, *positive-existential theory*) of the structure is the set of sentences (resp. existential sentences, positive-existential sentences) which are true in the structure.

We say that the theory (resp. existential theory, positive-existential theory) of a structure is *decidable* if there exists an algorithm which determines whether any given sentence (resp. existential sentence, positive-existential sentence) is true or false in the structure - otherwise we say that the theory is *undecidable*.

We present a list of decidability properties of some structures of common use. The first three lines in the table of the next page contain substructures of the ring of rational integers:  $(\mathbb{Z}, +, n \mapsto 2^n, 0, 1)$  is the structure of  $\mathbb{Z}$  with addition and the partial function  $n \mapsto 2^n$  (with

	ex. th. in $L_T$	ex. th. in $L_z$	full th.
$(\mathbb{Z}, +, 0, 1)$	Y		Y
$(\mathbb{Z}, +, n \mapsto 2^n, 0, 1)$	Y		Y
$(\mathbb{Z}, +,  , 0, 1)$	Y		N
$(\mathcal{O}_K, +,  , 0, 1)$	conj. N		N
$\mathbb{Z}$	N		N
$\mathcal{O}_K$	conj. N		N
$\mathbb{Q}$	?		N
$\mathbb{F}_q[z], \mathbb{R}[z], \mathbb{C}[z]$	N	N	N
$\mathbb{F}_q(z)$	?	N	N
$\mathbb{R}(z)$	?	N	N
$\mathbb{C}(z)$	?	?	?
$\mathcal{H}(\{a\})$	Y	Y	Y
$\mathcal{H}(U)$	Y	?	N
$\mathcal{H}(\mathbb{C})$	?	?	N
$\mathcal{M}(U)$	Y	?	?
$\mathcal{M}(\mathbb{C})$	?	?	?

domain  $\mathbb{N}$ ), and  $(\mathbb{Z}, +, |, 0, 1)$  the structure of  $\mathbb{Z}$  with addition and divisibility. On the fourth line is the structure of addition and divisibility in a ring  $\mathcal{O}_K$  of integers of the number field  $K$  - which is assumed not to be imaginary quadratic. The positive-existential theories of those structures have been shown to be of the same hardness as the positive-existential theories of the corresponding ring structures, but it is an open problem whether the latter are undecidable for arbitrary  $K$  (see the comment below). In the first four lines the columns ‘ex. th.’ and ‘full th.’ show the decidability properties of the existential and the full theory of the structure, respectively. The remaining structures are ring structures:  $\mathbb{Q}$  is the field of rational numbers,  $\mathbb{R}$  the field of real numbers,  $\mathbb{C}$  the field of complex numbers,  $\mathbb{F}_q$  is the finite field with  $q$  elements,  $B[z]$  the ring of polynomials in the variable  $z$  with coefficients in the ring  $B$ ,  $B(z)$  the corresponding field of rational functions in  $z$ ,  $\mathcal{H}(\mathcal{D})$  the ring of analytic functions of the variable  $z$  as that ranges in an open superset of the subset  $\mathcal{D}$  in the complex plane,  $\mathcal{M}(\mathcal{D})$  is the corresponding field of meromorphic functions,  $U$  is the open unit disk.  $L_T$  is the language  $\{+, \cdot; =; 0, 1\}$  which, for rings of functions is augmented by the predicate  $T$  which is interpreted as ‘ $x$  is not a constant function’.

For rings of functions of the variable  $z$  the language  $L_z$  is as above. The first column shows whether the positive existential theory of the ring in the language  $L_T$  is decidable or not ('Y' means decidable, 'N' means undecidable, 'conj. N' means 'conjectured to be undecidable', '?' denotes an open problem), the second column corresponds to the similar properties in the language  $L_z$  and the third column to that of the full theory in the language  $L_T$  for the rings  $\mathbb{Z}$ ,  $\mathcal{O}_K$  and  $\mathbb{Q}$  and the language  $L_z$  for the remaining rings.

Note that it is known that the theories of many rings  $\mathcal{O}_K$  are undecidable (e.g. for abelian  $K$ ) and it has been conjectured that all of them are, but the question for arbitrary  $K$  remains open.

For a fast introduction to applications of Model Theory to Algebra the reader may consult [9] and [66]. The solution of HTP can be found in [15], and is explained very nicely to the non-expert in [14]. Surveys of questions similar to the present paper's are [47], [51], [52] and [59]. Surveys of elimination ('decidability') techniques and results can be found in [60] (and many later more specialized articles, from the Algebraist's point of view).

We are indebted to F. Campana, J. Demeyer and T. Scanlon for various comments towards improvements of this paper.

## 1 Part A: Decidability results

For a quick introduction to a basic elimination technique, whose origin lies in the early days of Model Theory, solve the following Exercise.

Say that we work in a language  $L$ . A theory  $T$  (i.e. a subset of the set of formulas) of  $L$  admits *elimination of quantifiers* if any  $L$ -formula  $\phi(x)$  is equivalent in  $T$  to an existential formula.

**Exercise 1.1** (a) Let  $T$  be an  $L$ -theory. Assume that any formula of the form  $\exists x \psi(x, y)$ , where  $x$  is one variable,  $y$  is a tuple of variables and  $\psi$  is quantifier-free, is equivalent in  $T$  to a quantifier-free formula. Prove that  $T$  admits elimination of quantifiers.

[Hint: Recall that any formula is equivalent to one in *prenex normal form* (i.e. a sequence of quantified variables, followed by a quantifier-free formula). Thus it suffices to consider only formulas of that form. You may then use induction on the number of quantifiers. Also note that to prove that  $\forall x \phi(x, y)$  (with  $\phi$  quantifier-free) is quantifier-free, it suffices to prove that its negation (which is an existential formula) is quantifier-free.]

(b) Consider the field  $\mathbb{C}$  of complex numbers as an  $L_r$ -structure. Consider a system of polynomial equations and inequations

$$S(x, y) : \bigwedge_i f_i(x, y) = 0 \wedge \bigwedge_j g_j(x, y) \neq 0$$

where  $x$  is one variable,  $y = (y_1, \dots, y_m)$  and each  $y_k$  is a variable, the indices  $i$  and  $j$  range over some finite sets  $I$  and  $J$  respectively, and each  $f_i$  and  $g_j$  is a polynomial in  $\mathbb{Z}[x, y_1, \dots, y_m]$ . Prove that the formula  $\exists x S(x, y)$  is equivalent to a quantifier-free formula,

[Hint: First notice that the existential quantifier distributes over  $\vee$  ('or'). In the next few lines a 'polynomial' is an element of  $\mathbb{Z}[x, y]$ . Note that we may assume that  $J$  is empty or a singleton, i.e. there is no inequation or a single inequation in the system. First assume that  $J$  is empty and use the theory of *resultants* (see any graduate book in Algebra) to eliminate the existential quantifier (but the resulting equivalent existential formula contains, in general, inequations). In case  $J$  is a singleton, show that one can reduce to the previous case, generalizing to many variables the following observations about two variables:

Say that  $y$  is one variable. Consider the system

$$T(x, y) : f(x, y) = 0 \wedge g(x, y) \neq 0.$$

(i) Show that a system  $T_1 : T(x, y) \wedge h(x, y) = 0$ , with  $h$  a nontrivial polynomial in  $x$  and  $y$  and with degree in  $x$  lower than that of  $f$ , is equivalent to a system like  $T$  (possibly with some relations involving only the variable  $y$ ) but with degree of  $f$  in  $x$  lower than the original one. Achieve this by euclidean division of  $f$  by  $h$ : there is a polynomial  $a$  in  $y$  and polynomials  $h_1$  and  $q$  in  $(x, y)$  and with degree of  $h_1$  in  $x$  lower than that of  $h$  such that  $af = qh + h_1$  ( $a$  is the highest degree coefficient of  $h$  as a polynomial in  $x$ ); then the system  $T_1$  is equivalent to the disjunction of the systems  $T(x, y) \wedge h - ax^r = 0 \wedge a = 0$ , where  $r$  is the degree in  $x$  of  $h$ , and  $h = 0 \wedge h_1 = 0 \wedge ag \neq 0$ . Observe that both the latter systems have sum of degrees in  $x$  of the polynomial equations lower than that of  $T_1$ . Iterate.

(ii) Using the euclidean algorithm for polynomials, find a polynomial  $d$  which is a greatest common divisor in  $\mathbb{Q}(y)[x]$  of  $f$  and  $g$  with respect to  $x$  and for which the following holds formally:  $bd = uf + vg$  for some polynomials  $u, v, b$ , with  $v$  having degree in  $x$  lower than that of  $f$  and with  $b$  being a no-zero polynomial of the variable  $y$  only. Then  $T$  is equivalent to the disjunction of systems  $f = 0 \wedge bd \neq 0$  and  $f = 0 \wedge v = 0 \wedge g \neq 0$ . The second of the latter leads to 'simpler' systems, by the

previous paragraph. The first one has degree in  $x$  of the polynomial inequation less than the original one.

(iii) Iterating the results of the last paragraph, observe that  $T$  is equivalent to a disjunction of systems which have the form  $f = 0$  together with some relations involving only the variable  $y$ . Then observe that for any value of  $y$ ,  $f(x, y) = 0$  is satisfiable if  $f$  is non-trivial as a polynomial in  $x$  (since  $\mathbb{C}$  is algebraically closed). Hence the satisfiability of each of the latter systems is equivalent to the satisfiability of a disjunction of systems of the variable  $y$  only. Hence the existential quantifier  $\exists x$  has been eliminated.

Use (a) to conclude that the theory of  $\mathbb{C}$  in  $L_r$  admits elimination of quantifiers. Observe that the procedure of finding a quantifier-free formula equivalent to a given formula, is effective. Conclude that the theory of  $\mathbb{C}$  in  $L_r$  is decidable, that is, there is an algorithm to determine whether any given sentence of  $L_r$  is true or false in  $\mathbb{C}$ .

### 1.1 Presburger arithmetic

A basic, old result is the decidability of Presburger arithmetic, i.e. the theory of the ordered additive group of integers. Presburger showed that  $\mathbf{Z}$  admits elimination of quantifiers in a language which extends the language  $L_P = \{+, \geq; 0, 1\}$  with predicates for  $a \equiv b \pmod{m}$  for every integer  $m$  (actually Presburger considered the theory of natural numbers, not the integers, and in a language slightly different from  $L_P$  but with the same expressive power).

**Exercise 1.2** Show that the theory of  $\mathbb{Z}$  in the language  $L_P$  is 'model-complete' in the following way:

(a) For each  $k \in \mathbb{N}$  with  $k \geq 2$  define the one-place predicate  $M_k$  to mean ' $M_k(x) \leftrightarrow x$  is a multiple of  $k$ '. Extend the language  $L_P$  by the predicates  $M_k$  to obtain the language  $L_P^M$ .

(b) Observe that each quantifier-free formula of  $L_P^M$  is equivalent to a finite disjunction of formulas of the form

$$\bigwedge_i (f_i(\bar{x}) = 0) \wedge \bigwedge_j (M_{k_j}(g_j(\bar{x}))) \wedge \bigwedge_i (h_i(\bar{x}) \geq 0)$$

where each  $f_i$  and  $g_j$  is a polynomial of degree 1 in the variables of the tuple  $\bar{x}$ .

(c) Prove that each existential  $L_P^M$ -formula, i.e. of the form  $\exists \bar{x} \phi(\bar{x}, \bar{y})$  where  $\phi(\bar{x}, \bar{y})$  is quantifier free, is equivalent to a quantifier-free  $L_P^M$ -

formula. You can do this by eliminating the existential quantifiers, one at a time. For example, to eliminate the quantifier  $\exists x$  from

$$\exists x[a - x \geq 0 \wedge x \geq b \wedge M_2(x + c)]$$

( $a$ ,  $b$  and  $c$  can be linear polynomials in some variables and  $x$  does not occur in any of them) observe that it is equivalent to the disjunction of the formulas that correspond to the cases (A)  $a \geq b + 1$ , (B)  $a = b$  and  $b$  is even and  $c$  is even, and (C)  $a = b$  and  $a$  is odd and  $c$  is odd.

(d) Fix a language and a theory. Assume that each existential formula is equivalent (in the theory) to some quantifier-free formula. Then show that each formula of the language has the same property (i.e. is equivalent to a quantifier-free formula).

One can ask how one can enrich the Presburger language  $L_P$  and still retain decidability for the existential theory of  $\mathbb{Z}$  in this enriched language. Of course, as soon as multiplication is definable from the functions and predicates in the language, one gets undecidability. The bibliography on this subject is quite extensive. For some information see [10] and the bibliography of [51]. Below we will see some results of this kind, as well.

## 1.2 Addition and divisibility

The results we present are from [38] (similar results were obtained in [6]), [39] and [40].

A natural extension of  $L_P$  consists of adding a binary predicate for the divisibility relation  $|$  (that is,  $a|b$  if and only if  $\exists c : b = ac$ ). J. Robinson showed in [53] that multiplication can be defined from addition and divisibility by a first-order formula and hence, the first-order theory of  $\mathbb{Z}$  in this language is undecidable. In contrast, Lipshitz, in [38] (and, independently, Bel'tyukov in [6]) showed that the existential theory of  $\mathbb{Z}$  in the language  $L_{|} = L_P \cup \{| \}$  is decidable. The same is true for any ring of integers of an imaginary quadratic extension of the rationals (in this case the predicate  $>$  has to be excluded from the language). This result is optimal in several ways: multiplication is positive-existential in the  $L_{|}$ -theory of any ring of algebraic integers in a number field other than the rationals and imaginary quadratic ([39] and [40]); hence the  $L_{|}$ -existential-theory of those rings has the same decidability property as the ring theory which has been conjectured – by Denef and Lipshitz, but not yet proved – to be undecidable. These results were later generalized

to polynomial rings over fields: the existential theory of addition and divisibility in a polynomial ring  $k[t]$  over a field  $k$  (in the language  $L = L_P \cup \{t, |\}$ ), is decidable if and only if the existential theory of  $k$  is decidable; the positive existential theory of  $A[t_1, t_2]$  in the language  $L = L_P \cup \{t_1, t_2, |\}$  is undecidable for any commutative domain  $A$ .

We give a short account of the proof of [38]:

Let  $L_\mid = L_P \cup \{|\}$  where  $|$  will be interpreted by ' $a|b \leftrightarrow \exists c[b = ac]$ '.

(a) Show that every existential sentence of  $L_\mid$  is equivalent to a disjunction of formulas of the form  $\exists x\phi(x)$  where

$$(1) \quad \phi(x) : \bigwedge_i (f_i(x)|g_i(x)) \bigwedge_j (h_j(x) \geq 0)$$

where each  $f_i$ ,  $g_i$  and  $h_j$  is a polynomial of degree at most 1 in the variables of the tuple of variables  $x = (x_1, \dots, x_m)$ . To do this one has to

(a1) Eliminate non-divisibilities: observe that  $\neg a|b$  is equivalent to 'a greatest common divisor of  $a$  and  $b$  is different from  $a$  and  $-a$ ' which is equivalent to

$$\exists s, x, y [s|a \wedge s|b \wedge a|x \wedge b|y \wedge s = x - y \wedge \neg(s + a = 0) \wedge \neg(s - a = 0)].$$

(a2) Eliminate equations, e.g. if the equation  $2x - y = 0$  occurs then one can substitute all occurrences of the variable  $x$  by  $\frac{y}{2}$ , clear denominators by multiplying all terms by 2, and add the divisibility  $2|y$ .

In the rest work with notation as in (1).

(b) Impose all possible relative orderings on the variables of  $x$ , e.g.  $x_1 \geq \dots \geq x_m$ , and all possible orderings on the terms  $f_i$ ,  $g_i$  and  $h_i$ . Each one of these cases gives a sentence (the disjunction of all these is equivalent to the initial sentence). So assume that (1) corresponds to such a sentence.

Draw conclusions that eliminate some variables, for example, if a divisibility  $x + f(y)|x + g(y)$  occurs and  $x, x + f(y), x + g(y) \geq 0$  and the variable  $x$  is  $\geq$  to all the variables of the tuple  $y$ , then draw the conclusion that  $\frac{x+g(y)}{x+f(y)}$  is an integer  $\leq M + 1$  where  $M$  is the maximum absolute value of the coefficients of  $f - g$  (**Exercise:** Why?); Consider the cases and eliminate the variable  $x$  (conclude with fewer variables).

(c) Impose certain 'implied' divisibilities, for example, from  $f_1|f_2$  and  $f_2|f_3$  conclude that  $f_1|f_3$  (and add it to the given list of divisibilities).

(d) Iterate (b) and (c). Show that a finite number of iterations concludes with systems which are 'diagonal', in the sense that in each divisibility  $f|g$  there is a variable that occurs in  $g$ , which is 'bigger' than all

variables of  $f$ ; in addition these systems are closed under the operations mentioned in (c).

(e) Show that diagonal systems satisfy the following 'local-to-global' principle: Let  $\phi(x) : \bigwedge_i (f_i(x) | g_i(x)) \bigwedge_j (h_j(x) \geq 0)$  be a diagonal system and let  $\phi'(x)$  be the system obtained from  $\phi$  by deleting all inequalities (so  $\phi'$  contains only divisibilities). Then one can effectively find a natural number  $N$ , such that  $\phi(x)$  has a solution in  $\mathbb{Z}$  if and only if for each prime number  $p \leq N$   $\phi'(x)$  has a solution  $x$  in  $\mathbb{Z}_p$  such that  $f_i(x) \not\equiv 0 \pmod{p^N}$ . Use the decidability of the theory of each  $\mathbb{Z}_p$  to conclude.

**Remark** The local-to-global principle mentioned in (e) fails for systems in general, e.g.  $x + 2 | 2x + 3$  is satisfiable in each  $\mathbb{Z}_p$  but the system  $x + 2 | 2x + 3 \wedge x \geq 0$  is not satisfiable in  $\mathbb{Z}$ .

**Exercise 1.3** The following give some of the main ideas in [39].

Consider the ring of integers  $\mathcal{O}$  of a real quadratic number field  $K$  (e.g.  $K = \mathbb{Q}(\sqrt{5})$ ). Consider known the following fact: There is a unit  $\epsilon_0$  which is 'fundamental' i.e. all units of  $\mathcal{O}$  are of the form  $\pm \epsilon_0^n$  with  $n \in \mathbb{Z}$ .

(a) Show that if  $n|m$  in  $\mathbb{Z}$  then  $\epsilon_0^n - 1 | \epsilon_0^m - 1$  in  $\mathcal{O}$ .

It can be shown that a sort of converse is also true: There is a  $d \in \mathbb{Z}$  such that setting  $\epsilon = \epsilon_0^d$  we have that  $n|m$  in  $\mathbb{Z}$  if and only if  $\epsilon^n - 1 | \epsilon^m - 1$  in  $\mathcal{O}$ . For the rest assume that one has in the language a name (constant symbol) for a unit  $\epsilon$  with these properties and assume that the set  $\{\epsilon^n : n \in \mathbb{Z}\}$  is positive existential in the language  $L \cup \{\epsilon\}$  (all the mentioned facts are true).

(b) Assume that  $m, n \neq 0$  and  $m \neq n$ . Show that  $\epsilon^m = \epsilon^{2n}$  if and only if

$$\epsilon^n - 1 | \epsilon^m - \epsilon^n \wedge \epsilon^m - \epsilon^n | \epsilon^n - 1.$$

(c) Show: If  $x \in \mathcal{O} \setminus \{0\}$  then there is an  $n \neq 0$  such that  $x | \epsilon^n - 1$  (hint: if  $x$  is not a unit then the ring  $\mathcal{O}/(x)$  is finite, hence the natural image of  $\epsilon$  has finite multiplicative order).

(d) Let  $\phi(x)$  denote the formula

$$x \neq 0 \wedge x \neq 1 \wedge x \neq -1 \wedge x | \epsilon^n - 1 \wedge x - 1 | \epsilon^n - 1 \wedge x + 1 | \epsilon^n - 1.$$

Assume that if  $n \neq 0$  and  $\phi(x)$  is true then  $2|x^2| < \epsilon^n$  ( $|w|$  is the absolute value of  $w$ ).

Show: For  $x, y \in \mathcal{O} \setminus \{0, 1, -1\}$  the following is true:  $y = x^2$  if and only if for some  $n \in \mathbb{Z} \setminus \{0\}$  we have

$$\phi(x) \wedge \phi(y) \wedge \epsilon^n - x | \epsilon^{2n} - y.$$

(e) Consider known the following: The relation  $x \neq 0$  is positive-existential in  $L_{\mid} \cup \{\epsilon\}$ .

Use (a)-(d) to produce a formula  $\psi(x, y)$  of  $L_{\mid} \cup \{\epsilon\}$  such that for any  $x, y \in \mathcal{O}$  the following is true in  $\mathcal{O}$ :

$$\psi(x, y) \leftrightarrow y = x^2.$$

Thus squaring over  $\mathcal{O}$  is positive-existential in  $L_{\mid} \cup \{\epsilon\}$ . Prove that this implies that multiplication over  $\mathcal{O}$  is positive-existential in  $L_{\mid} \cup \{\epsilon\}$ . Conclude that the positive-existential theory of  $L_{\mid} \cup \{\epsilon\}$  is undecidable.

### 1.3 Addition and exponentiation

The following are results from [58].

The first-order theory of  $\mathbb{N}$  in the language  $L = L_P \cup \{\text{exp}_2\}$ , where  $\text{exp}_2$  is the function which sends a natural number  $n$  to  $2^n$ , is decidable.

Towards proving this, one has to study the behavior of 'exponential polynomials', e.g. of the form  $2^{2^{3x-1}} - 2^{5x+5} + 1$ . We will not go into the details.

**Exercise 1.4** Show that there is an algorithm which, given any diophantine equation  $f(x) = 0$  ( $x$  is a tuple of  $m$  variables and  $f$  a polynomial in  $x$  over  $\mathbb{Z}$ ), decides whether that has or does not have solutions in the set  $\{2^n : n \in \mathbb{N}\}^m$ .

**Remark** By results of [33] the statement of the Exercise is true for any finitely generated multiplicative (i.e. closed under multiplication) set, e.g. the set  $\{2^n 3^m : n, m \in \mathbb{N}\}$ .

### 1.4 The analogue of Hilbert's tenth problem for algebraic groups

The following (among several) result can be found in [30].

**Theorem 1.5** *There is an algorithm which, given any algebraic group  $G$  defined over  $\mathbb{Z}$  and any positive integer  $k$ , decides whether  $G(\mathbb{Z})$  contains a subgroup of index  $k$ .*

Two examples of such groups are:

1.  $\mathbb{Z}, \mathbb{Z} \times \mathbb{Z}$  etc. with the group structure of component-wise addition.

2. The solution set of the equation  $X^2 - dY^2 = 1$  where  $d$  is a square-free integer; the group law  $\oplus$  is defined by

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1).$$

This justifies the claim that ‘the more structure one has, the more likely decidability is’.

### 1.5 The results of Ax for ‘almost all primes’

In [1] Ax gave an algorithm which, for any given diophantine equation, tests whether the equation has a solution modulo every prime number. In [2] he extended this to an algorithm that decides the truth of a sentence of  $L_r$  in all finite fields. The proofs make use of Weil’s result on the congruence zeta function and of Čebotarev’s density theorem.

For further results in this direction see [27] and [65].

### 1.6 Model-completeness

A set (subset of a power of  $\mathbb{Z}$  or any effectively constructible countable set) is *recursive* if membership in it can be tested by an algorithm; it is *recursively enumerable* if its elements can be listed (eventually all) by an algorithm.

A theory of a language (finite or countable-and-recursive)  $L$  is a subset of the set of sentences of  $L$ . The theory of a structure (model)  $\mathcal{A}$  in a language  $L$  is *model-complete* if every formula of  $L$  is equivalent to an existential formula of  $L$  over  $\mathcal{A}$ .

The following is a classical decidability argument in Model Theory:

**Assume:**

- (a)  $\mathcal{A}$  is a countable and recursive structure in the countable language  $L$ .
- (b) The theory of  $\mathcal{A}$  in  $L$  is *effectively model-complete*, that is, there is an algorithm which to any sentence of  $L$  associates an equivalent (over  $\mathcal{A}$ ) existential sentence.

**Conclude:** The theory of  $\mathcal{A}$  in  $L$  is decidable.

*Proof* Let  $\sigma$  be a sentence of  $L$ . Find an existential sentence, say  $\exists x \phi(x)$ , equivalent to  $\sigma$ , and an existential sentence, say  $\exists y \psi(y)$ , equivalent to  $\neg\sigma$  where  $x$  is a tuple of  $m$  variables,  $y$  is a tuple of  $n$  variables and the formulas  $\phi$  and  $\psi$  are quantifier-free.

Enumerate the tuples of  $m$  elements of  $\mathcal{A}$  and the tuples of  $n$  elements

of  $\mathcal{A}$ . By day plug in  $\phi(x)$  tuples of  $m$  elements and check whether they make it true. By night do similarly with  $\psi$ .

One of  $\sigma$  or  $\neg\sigma$  is true, hence either we will satisfy  $\phi$  on a day (in which case  $\sigma$  is true) or we will satisfy  $\psi$  on a night (in which case  $\neg\sigma$  is true).  $\square$

**Exercise 1.6** (a) Prove that if in a theory  $T$  every universal formula is equivalent to an existential one then  $T$  is model-complete.

Consider the language  $L$  which extends the language of rings by a symbol  $\geq$  for the ordinary ordering relation. A polynomial (or rational function)  $f(x)$  in the  $m$  variables  $x$ , with coefficients in  $\mathbb{R}$ , is *positive-definite* if for all  $a \in \mathbb{R}^m$  we have  $f(a) \geq 0$ .

(b) Show that every positive-definite polynomial in one variable  $x$  is the sum of two squares of polynomials of  $x$  with coefficients in  $\mathbb{R}$ . (This admits a generalization to  $m$  variables: A positive-definite rational function in  $m$  variables is equal to the sum of  $2^m$ -many squares of rational functions; this is a positive answer to Hilbert's 17-th problem.)

(c) Use the positive answer to Hilbert's 17-th problem mentioned under (b) to prove that if  $f(x_1, \dots, x_m) \in \mathbb{Z}[x_1, \dots, x_m]$  is a polynomial, then the universal formula

$$\forall x_1 \dots \forall x_m f(x_1, \dots, x_m) \geq 0$$

(where the quantifiers range over  $\mathbb{R}$ ) is equivalent to an existential formula.

### 1.7 Complete theories

Suppose that  $T$  is a theory of the recursive language  $L$ . We say that  $T$  is *complete* if for any sentence  $\sigma$  of  $L$  either  $\sigma$  or  $\neg\sigma$  is a consequence of  $T$ . Then one sees easily that

**Theorem 1.7** *Assume that  $T$  is a recursively enumerable and complete theory of the recursive language  $L$ . Then there is an algorithm which tests any given sentence  $\sigma$  of  $L$  for being or not being a consequence of  $T$ .*

**Exercise 1.8** Give an outline of a proof of the Theorem.

For example, the theory of algebraically closed fields of a fixed characteristic (the axioms for a field, together with axioms which fix the characteristic, together with axioms which state, for each  $n$ , "every polynomial

of degree  $n$  has a zero”), which is known to be complete, has a recursive set of consequences.

**Exercise 1.9** Describe in detail the sentences (up to equivalence) of the latter theory.

The latter Theorem transforms the question of whether the set of consequences of a given theory is decidable (i.e. recursive) to the question of whether the theory is complete (whenever that is true). This is a very common approach in Model Theory to decidability questions.

It is obvious that the latter Theorem may be not true if  $T$  is not complete. Examples of this kind exist in the bibliography.

For relevant bibliography see [9].

### 1.8 Power-series and germs of analytic functions: existential decidability and Artin approximation

The ring-theories of  $\mathbb{Q}_p$  ( $p$  is a prime number) are decidable (results of Nerode, Ax and Kochen [3], Ershov [26], also cf. [42], [11], and [19]).

If  $F$  is a decidable field of characteristic 0 then the ring-theory of the field of formal fractional power series  $F((T))$  in one variable  $T$  (and that of  $F[[T]]$ ) is decidable ([36] and [70]).

But if  $T$  is two or more variables then we have undecidability ([16]).

For more relevant results see [5] and [22].

We wish to address the question of the decidability of the existential theory of a ring  $\mathcal{H}_z(D)$  of functions of a tuple of variables  $z$ , analytic on a set  $D$  (i.e. analytic on some open super-set of  $D$ ). We will address first the question for  $D$ =(a singleton), say  $D = \{0\}$ . Already in [36] it was shown that the ring-theory of  $\mathcal{H}_z(\{0\})$  is decidable. But the techniques of that paper do not transfer to bigger  $D$ , so we will look into other approaches. One approach is via ‘Approximation Properties’.

**Definition 1.10** (i) Let  $R$  be a local ring and  $\hat{R}$  be its completion. We say that  $R$  has the *Approximation Property* if every system of polynomial equations over  $R$ , which has a solution in  $\hat{R}$ , has a solution in  $R$ .

(ii)  $\mathbb{C}\langle z_1, \dots, z_q \rangle$  is the ring of formal power series, in the variables  $z_1, \dots, z_q$  over  $\mathbb{C}$ , which converge in some neighborhood of the origin.

(iii) Let  $k$  be a field. Then  $k\langle z_1, \dots, z_q \rangle$  denotes the ring of formal power series in  $z_1, \dots, z_q$  over  $k$  which are algebraic over  $k[z_1, \dots, z_q]$ .

Artin proved:

**Theorem 1.11** *Let  $k$  be any field. The following two rings have the Approximation Property:*

- (i)  $k\langle z_1, \dots, z_q \rangle$  and
- (ii)  $\mathbb{C}\{z_1, \dots, z_q\}$ .

**Theorem 1.12** *Let  $k$  be an arbitrary field. Then, a system of polynomial equations, with coefficients in  $k[[z_1, \dots, z_q]]$ , has solutions in  $k[[z_1, \dots, z_q]]$  if and only if, for any  $n \in \mathbb{N}^+$ , it has solutions modulo  $(z_1, \dots, z_q)^n$ .*

By Theorem 1.11, a system of equations, with coefficients in  $\mathbb{C}[z]$ , has solutions in  $\mathcal{H}_z(\{0\})$  if and only if it has solutions in  $\mathbb{C}\langle z \rangle$ .

A much stronger version of Theorem 1.12, suitable for algorithmic computation of solutions of equations, is true: for each system of equations, there is a constant  $N$ , depending on the system (actually: algorithmically computable and depending only on the number of variables and the degrees of the involved polynomials), such that the system has solutions in  $k[[z]]$  if and only if it has solutions modulo  $(z)^N$ . Results of this type occur in the literature under the name ‘Strong Approximation theorems’.

Strong Approximation implies decidability of the positive existential theory of  $k[[z]]$  (in order to see whether a system of equations has solutions, compute the constant  $N$  of the previous paragraph and check whether the system has solutions modulo  $(z)^N$ ). But, since our main interest is to investigate the possibility of adapting our arguments to  $\mathcal{H}_z(D)$  for  $D$  not a singleton, and because there is no known analogue of Strong Approximation for these rings, we will now present a decidability result, based only on Theorems 1.11 and 1.12. We will show how one can use these Theorems in order to detect whether a given system of polynomial equations, with coefficients in  $\tilde{\mathbb{Q}}[z]$  ( $z = (z_1, \dots, z_n)$  and  $\tilde{\mathbb{Q}}$  denotes the algebraic closure of  $\mathbb{Q}$ ), has solutions over  $\mathcal{H}_z(\{0\}^n)$ . Let such a system be given; by Theorem 1.11 it suffices to check whether the system has solutions over  $\mathbb{C}\langle z \rangle$ . First, observe that if the system has solutions over  $\mathbb{C}\langle z \rangle$  then it has solutions whose constant coefficients are algebraic numbers, that is, the system has solutions over  $\tilde{\mathbb{Q}}\langle z \rangle$ . So, here is an algorithm that decides whether the system has solutions over  $\mathcal{H}_z(\{0\}^n)$ : We run in parallel the following two processes. The first process lists the tuples of  $\tilde{\mathbb{Q}}\langle z \rangle$  and determines whether each one of them is a solution. The second process determines whether the system has solutions modulo  $z^m$  for  $m = 1, 2, \dots$  (observe that the reduction of the system modulo any

$z^m$  reduces to solving a new system over  $\tilde{\mathbb{Q}}$ , which can be done by an algorithm, since the existential theory of any algebraically closed field, such as  $\tilde{\mathbb{Q}}$ , is decidable). If the system has solutions over  $\tilde{\mathbb{Q}}\langle z \rangle$  then the first process will find them, eventually. If the system has no solutions, then the second process will eventually find an  $m$  for which the system has no solution modulo  $z^m$ . We note that a similar algorithm works for systems of algebraic differential equations (cf. [23]).

It is evident that, in the domains where one has analogues of Theorems 1.11 and 1.12, one may expect decidability results similar to the above. Unfortunately, analogues of Theorem 1.12 in rings  $\mathcal{H}_z(D)$ , for  $D$  not a singleton, are not known. Theorem 1.11 has been extended to the very general case of an *excellent regular local Henselian* ring (by Spivakovski, see [61]). Surprisingly perhaps, there is a similar result for compact domains  $D$  by van den Dries:

**Theorem 1.13** ([63]) *Assume that  $D$  is a compact subset of  $\mathbb{C}$  and denote by  $\mathbb{C}_D\langle z \rangle$  the ring of functions on  $D$ , in the variable  $z$ , which are algebraic over  $\mathbb{C}(z)$  and analytic on an open superset of  $D$ . Let  $x = (x_1, \dots, x_m)$ ,  $f_i \in \mathbb{C}_D\langle z \rangle[x]$ . Let  $\epsilon > 0$ .*

*Assume that the system of equations  $\bigwedge_i f_i[x_1, \dots, x_m]$  has a solution  $\alpha = (\alpha_1, \dots, \alpha_m)$  in  $\mathcal{H}_z(D)$ . Then it also has a solution  $\beta = (\beta_1, \dots, \beta_m)$  with  $\beta_i \in \mathbb{C}_D\langle z \rangle$  and such that  $|\beta - \alpha|_\infty < \epsilon$  where  $|\cdot|_\infty$  denotes the supremum norm on  $D$ .*

It is easy to see that Theorem 1.11 reduces the question of decidability of the existential theory of  $\mathcal{H}_z(D)$ , for  $D$  compact, to the similar question for the existential theory of the ring of algebraic functions which are analytic on  $D$ . But the problem remains open:

**Question 1.14** Is the existential theory of  $\mathcal{H}_z(D)$  decidable for  $D = \mathbb{C}$ ? for  $D =$ (the open unit disc)? for  $D =$ (the closed unit disc)?

In a later section we give more information on this problem.

### 1.9 Positive-existential versus existential

In some cases we do have a decision method for the positive-existential theory of a ring but we do not know the similar result for the existential theory. Such is the case, for example, for the power series ring  $\mathbb{F}_p[[t]]$  where  $t$  is one variable.

In [24] it is shown that if there is Resolution of Singularities in positive characteristic  $p$  then the positive-existential theory of  $\mathbb{F}_p[[t]]$  is decidable.

**Exercise 1.15** Prove that for any prime  $p \geq 3$  the set  $\mathbb{F}_p[[t]]$  is positive-existentially definable in the field  $\mathbb{F}_p((t))$  in the following way:

For any  $x \in \mathbb{F}_p((t))$ ,  
 $x \in \mathbb{F}_p[[t]]$  if and only if  $\exists y[1 + tx^2 = y^2]$ .

Conclude that the existential theory of  $\mathbb{F}_p[[t]]$  is decidable if and only if the positive-existential theory of  $\mathbb{F}_p((t))$  is decidable.

A rough presentation of some ideas in the proof is the following:

Assume that  $V$  is a variety over  $\mathbb{F}_p((t))$ , given by a finite set of polynomial equations. We want to decide whether  $V$  has points rational over  $\mathbb{F}_p((t))$ .

*Step 1:* Resolve the singularities of  $V$ .

A Resolution of Singularities (RoS) of the variety  $V$  over the field  $\mathbb{F}_p((t))$  is a non-singular variety  $W$ , together with a surjective, birational and proper morphism  $f : W \rightarrow V$ . A basic observation is:

**Observation:** If every variety over a countable recursive field  $K$  has RoS then that is effective (that is, one can find a RoS).

This is done roughly as follows: List all possible pairs  $(W, f)$  and for each one of them, in the order of enumeration, check whether  $f$  maps onto  $V$  (this can be done effectively but we will not go into the details here). Since we have assumed that some RoS exists, at some point we will find one.

Existence of RoS is known (for any variety) over any field of zero characteristic (due to Hironaka), but unknown in positive characteristic. In what follows we will assume existence of RoS in characteristic  $p$ .

So we are reduced to the case in which the variety  $V$  is nonsingular, which we assume from now on.

*Step 2:* The variety  $V$  is described by a finite set of polynomial equations. By embedding  $V$  into the union of a finite set of affine spaces the existence of a point of  $V$ , rational over  $\mathbb{F}_p((t))$ , is translated into a finite set of questions each of which asks whether a system of equations, defining a nonsingular affine variety  $V'$ , together with a set of inequations which claims that the considered point is not on a variety  $Y$ , has solutions over  $\mathbb{F}_p[[t]]$ . For example, if  $V$  were a plane curve, given by the equation  $f(x_1, x_2) = 0$  (we work in affine space, the projective case is similar), then the existence of points of  $V$ , rational over  $\mathbb{F}_p((t))$ , is equivalent to the existence of points of the varieties

$[f(x_1^\delta, x_2^\epsilon) = 0 \wedge x_1 \diamond 0 \wedge x_2 \diamond 0]$ , for  $\delta, \epsilon \in \{-1, 1\}$  and where  $\diamond$  is either  $\neq$  or no relation (after clearing denominators in each system).

The next step depends, first on the non-singularity of  $V'$ , and second on the Hensel-Rychlik Lemma, which is a sort of formal analogue of the Implicit Function Theorem for real functions.

*Step 3:* We consider the varieties  $V'$  and  $Y$  defined in the previous step. Using the Hensel-Rychlik Lemma, one proves that if  $V'$  has points rational over  $\mathbb{F}_p[[t]]$ , then it has points which are not points of  $Y$ , except if that is formally impossible, that is, the variety  $V'$  (which is here assumed irreducible) is contained in  $Y$  over an algebraic closure of  $\mathbb{F}_p((t))$ . To see the point, consider the similar situation for varieties  $V'$  and  $Y$  over the real or complex numbers; say  $V'$  is given by  $f(x, y) = 0$  and  $Y$  is given by  $y \neq 0$ . If  $V'$  has a point  $(x_0, y_0)$ , then that point is a non-singular point (since  $V'$  is non-singular), hence either the partial derivative of  $f$ ,  $f_y$ , with respect to  $y$ , or  $f_x$ , is non-zero at  $(x_0, y_0)$ ; say it is  $f_y$ . Then, by the Implicit Function Theorem, one can vary  $y$  around  $y_0$  and still get an  $x$  so that  $f(x, y) = 0$ ; hence one obtains a solution for which  $y \neq 0$ . A similar argument holds if  $f_x$  is non-zero at  $(x_0, y_0)$ . The exceptional case of ‘formal impossibility’ is illustrated by the example in which the varieties  $V$  and  $Y$  coincide; this can be decided algorithmically by examining whether the variety  $V \setminus Y$  has any points over an algebraic closure of the field  $\mathbb{F}_p((t))$  (observe that this can be decided by an effective elimination of quantifiers for algebraically closed fields of characteristic  $p$ , then compare Exercise 1.1).

Hence the question of existence of points of  $V' \setminus Y$ , rational over  $\mathbb{F}_p[[t]]$ , is reduced to the existence of points of  $V'$  (which is defined by equations only) over  $\mathbb{F}_p[[t]]$ .

*Step 4:* A variance of Greenberg’s Theorem, due to Denef and Lipshitz in [23], gives an effective way to examine a system of equations for possessing a solution over  $\mathbb{F}_p[[t]]$ , that is to say, the positive-existential theory of  $\mathbb{F}_p[[t]]$  is decidable. Hence one can check whether  $V'$  has points over  $\mathbb{F}_p[[t]]$ .

## 2 Part B: A qualitative analogue of HTP and the Conjectures of S. Lang

We want to address the following

**Question 2.1** *Is there an algorithm which, given any variety  $V$  over*

$\mathbb{Q}$ , decides whether  $V$  has infinitely many points over some number field  $K$ ?

For example, due to the proof by Faltings of Mordell's Conjecture, the question has a positive answer for curves:

*Any curve of geometric genus  $\geq 2$  has only a finite number of points over any given number field  $K$ .*

And it is known that curves of genus 0 or 1 have infinitely many points over some number field  $K$ . Hence the algorithm is: Compute the genus of the curve  $V$  (the genus is a geometric invariant and known to be computable). If it is  $\leq 1$  reply YES, otherwise NO.

In [37] (and more extensively in [68] and from a different point of view in [8]) S. Lang announced a number of conjectures, which, if true, would imply that varieties that have infinitely many points over some number field are characterized by certain geometric properties. As an example,

**Conjecture 2.2** (Lang) *Any hyperbolic variety has only a finite number of points over any number field.*

A variety  $V$  is *hyperbolic* if every complex analytic map  $f : \mathbb{C} \rightarrow V$  is constant (this is one of several equivalent definitions). For example, the (irreducible) curves (varieties of dimension 1) that are hyperbolic are precisely those with geometric genus  $\geq 2$ .

What are the implications of this for Question 2.1? If true, Conjecture 2.2 reduces Question 2.1 to deciding whether a given variety has certain geometric properties. Some of those properties (e.g. genus) are known to be decidable; but some other properties are not known (to be decidable or undecidable). As an example of the second kind (to the best of the authors' knowledge), we ask

**Question 2.3** *Is there an algorithm which, given a variety  $V$  over  $\mathbb{Q}$ , decides whether that is hyperbolic?*

In the following sub-section we will address this question.

Even if the answer to it turns out to be positive, there still remain certain geometric properties which have to be decidable if the answer to Question 2.1 is positive.

As we will see in the next sub-section, there is an undecidability result for some type of 'geometric problem'; but it is probably too early to conjecture that Question 2.1 has a negative answer.

Now we give a more precise account of the conjectures of Lang and Vojta. The main notions involved are the following properties of an algebraic variety  $V$ , defined over  $\mathbb{Q}$  (or a number field):

1.  $V$  has only finitely many points over any number field.
2.  $V$  is hyperbolic
3.  $V$  is Kobayashi hyperbolic. This means that  $V$  is hyperbolic and is, in addition, equipped with a metric with some special properties ([37]).
4.  $V$  and all its subvarieties are *of general type* (a notion defined in terms of algebraic geometry).

The union of the conjectures connecting these properties is that all four properties are equivalent. The only part which has been proved is that property 2 (hyperbolic varieties) is equivalent to property 3 (Kobayashi hyperbolic varieties); this is due to Brody [7]. All the other equivalences are conjectures.

(We are indebted to Professor Campana for explaining to us some of the details for these notions).

### 2.1 A language for geometric problems

When we study the decidability question for a ring of functions of one (or more) variable  $z$ , we usually augment the language of rings by a name (constant symbol) for  $z$ . This has as a result that the varieties that we study have coefficients in  $\mathbb{Z}[z]$  (or a bigger ring) and are not invariant under even the most elementary geometric transformations, for example  $z \mapsto z + \beta$  with  $\beta$  in the base field (field of constant functions). Since we want a language that does not have this defect, we define the language

$$L_T = \{+, \cdot, =, T; 0, 1\}$$

which augments the language of rings by the one-place predicate  $T$ , which will be interpreted by

$$T(x) \leftrightarrow (\text{the function } x \text{ is not a constant}).$$

Notice that, given a variety  $V$  through a finite set of defining polynomials, the sentence ‘*The variety  $V$  is hyperbolic*’ can be expressed in  $L_T$  over  $\mathcal{H}_z(\mathbb{C})$ .

We ask:

**Question 2.4** Is the theory (resp. existential theory, positive-existential theory) of  $L_T$  over  $\mathcal{H}_z(\mathbb{C})$  decidable? over  $\mathbb{C}(z)$ ? over  $\mathbb{C}[z]$ ?

The only known relevant results are given by the following two theorems:

**Theorem 2.5** ([50]) *The positive-existential theory in  $L_T$  of a polynomial ring  $F[z]$  over a field  $F$  is undecidable.*

**Theorem 2.6** ([56]) *The existential theory in  $L_T$  of the ring  $\mathcal{H}_z(U)$  is decidable, where  $U$  is either the open or the closed unit disc.*

The analogous question for fields of rational functions and for  $\mathcal{H}_z(\mathbb{C})$  are open.

An outline of the proof of Rubel's Theorem 2.6 is:

Let  $V$  be an affine variety defined over  $\mathbb{Q}$  (or  $\tilde{\mathbb{Q}}$ ), defined by a finite set of equations  $f_i(X) = 0$  ( $X = (X_1, \dots, X_m)$  is a tuple of variables and  $f_i \in \mathbb{Q}[X]$ ).

We want to determine whether  $V$  has points over  $\mathcal{H}_z(U)$ . We consider the system of differential equations and inequations

$$S : \left( \bigwedge_i f_i(X) = 0 \right) \wedge \left( \bigwedge_j \frac{dX_j}{dz} \neq 0 \right).$$

One examines  $S$  for solutions in a differentially closed field which extends  $\mathcal{H}_z(U)$ . This is effective by results of Seidenberg. If the answer is negative then we are done: the answer over  $\mathcal{H}_z(U)$  is also negative. If the answer is positive, then, by a theorem of Ritt,  $S$  has a solution  $\bar{X}(z)$  such that each  $\bar{X}_i$  is analytic in a neighborhood of  $z = 0$ . Substitute  $z$  by  $cz$ , for a suitable constant  $c$ , to obtain the solution  $\bar{X}(cz)$  (here we need the fact that the  $f_i$  are polynomials over  $\mathbb{Q}$ , hence their coefficients do not involve  $z$ ) which is analytic on  $U$ .

## 2.2 A geometric problem

Let  $K$  be a number field. We consider the following problem:

**Question 2.7** *Is there an algorithm to decide whether an arbitrary variety over  $K$  contains a rational curve?*

Note that for varieties of dimension one, the answer to this question is positive. Indeed if  $V$  is a variety of dimension one, then  $V$  will contain a

rational curve if and only if one of its irreducible components is a curve of genus 0 and this curve contains a  $K$ -rational point. Since, given a variety over  $K$  we can explicitly determine all its irreducible components, and given the fact that the genus of a curve is computable, one easily gets the algorithm asked for in the question.

For higher dimensional varieties the problem is open. However the following conjecture gives some information for surfaces:

**Conjecture** (S. Lang) *Let  $V$  be a variety of general type defined over a number field  $K$ . Then there exists a proper closed subvariety  $W$ , defined over  $K$  such that for any number field  $L$  containing  $K$ ,  $V(L) \setminus W(L)$  is finite.*

Let  $V$  be a surface of general type, defined over  $K$ . If  $V$  contains a rational curve  $C$  which has a parametrization defined over  $K$ , then  $V(K)$  is infinite.

Conversely, suppose that  $V$  contains infinitely many points, then by Lang's conjecture there exists a subvariety, i.e. a one-dimensional variety, such that at least one of its irreducible components is a curve which contains infinitely many points (i.e. this curve is either rational or an elliptic curve of positive rank).

Summarizing we have: determining whether a surface contains a curve of genus at most 1 is as difficult as determining whether the surface has infinitely many points or not.

In view of the results in the previous section, one is lead to believe that determining whether a variety defined over  $K$  contains a  $K$ -rational curve is as difficult as  $\text{HTP}(K)$ .

**Remark 2.8** It is tempting to use induction on the dimension to use the similar argument for arbitrary varieties. Unfortunately this does not work: the subvariety  $W$  of  $V$  which Lang's conjecture asserts to exist if  $V$  is of general type, needs itself not be of general type.

### 2.3 Varieties with an infinite number of points over a ring

Here we address the decision problem of whether a given variety has an infinite number of points over a fixed ring.

Consider a commutative domain  $R$  whose fraction field is not algebraically closed. Let  $R_0$  be a infinite recursive subring of  $R$  with fraction

field  $k_0$ . Suppose further that the algebraic closure of  $k_0$  is not contained in  $R$ . Denote the cardinality of  $R$  by  $|R|$ , and for any polynomial  $f$  in several variables, with coefficients in  $k_0$ , write  $N_R(f)$  for the cardinality of the solution set of  $f$  over  $R$ .

Let  $\mathcal{S}$  be an arbitrary proper subset of  $\mathbb{N} \cup \{|R|\}$ .

**Theorem 2.9** *Consider the following two decision problems:*

(a) *Is there an algorithm to decide for an arbitrary polynomial with coefficients in  $k_0$  whether  $N_R(f) \in \mathcal{S}$ ?*

(b) *Is there an algorithm to decide for an arbitrary polynomial with coefficients in  $k_0$  whether  $N_R(f) = 0$ ?*

*A negative answer to (b) implies a negative answer to (a).*

This implies that deciding whether a polynomial has infinitely or finitely many solutions in  $R$  is as difficult as deciding whether it has a solution or not. This result was proved by M. Davis for  $R = \mathbb{Z}$  and was generalized by the second author.

### 3 Part C: Hilbert's tenth problem for analytic and meromorphic functions

We will look more closely into Question 1.14. Let  $L_{z,C}$  denote the language which extends the language of rings by a constant symbol for the variable  $z$  and by the predicate  $C$  which is interpreted by ' $C(x)$  if and only if the function  $x$  is constant. The main existing results are:

**Theorem 3.1** (R. Robinson [55]) *Assume that  $D$  contains a real open interval. Then the first order theory of  $\mathcal{H}_D(z)$  in  $L_{z,C}$  is undecidable.*

*Proof* First we state:

**Lemma 3.2** (Huuskonen [32]) *Assume that  $D \subset \mathbb{C}$  has nonempty interior. Then the set of constants (i.e. of constant functions) in  $\mathcal{H}_z(D)$  is first order definable in the language  $\{+, \cdot; 0, 1, z\}$ .*

For simplicity work in the case  $q = 1$  so that  $z = z_1$  and assume that the line segment  $[0, 1]$  is contained in  $D$ ; the general case is left to the

reader. The following formula is equivalent to  $\alpha \in \mathbb{N} \setminus \{0\}$ :

$$C(\alpha) \wedge \exists x [x(0) = 1 \wedge x(1) = 0] \\ \wedge \forall y [(y \in \mathbb{C} \wedge y \neq 0 \wedge y + 1 \neq 0) \\ \rightarrow (x\left(\frac{1}{y}\right) = 0 \rightarrow (x\left(\frac{1}{y+1}\right) = 0) \vee y = \alpha)].$$

Of course the expressions of the form  $\frac{1}{z}$  do not belong to  $L_z$  but they can be replaced by new variables  $w$  preceded by  $\exists w : z \cdot w = 1$ .

The  $\leftarrow$  direction holds because if  $\alpha \notin \mathbb{N}$ , then the formula implies that each point  $\frac{1}{n}$ , with  $n \in \mathbb{N} \setminus \{0\}$ , is a zero of the analytic function  $x$ , while  $x(0) = 1$ , which is impossible by the continuity of  $x$ ; for the  $\rightarrow$  direction, observe that, for  $n \in \mathbb{N} \setminus \{0\}$ , the formula is realized by taking

$$x = (-1)^{n-1}(n-1)!(z-1)\left(z-\frac{1}{2}\right) \cdots \left(z-\frac{1}{n-1}\right).$$

□

It is obvious that the proof of this Theorem shows the similar result for any ring of functions which are continuous on  $[0, 1]$ , containing the identity function.

**Theorem 3.3** ([41]) *The positive-existential theory of the ring  $\mathcal{H}_{p,z}(\mathbb{C}_p)$  of functions of the variable  $z$  which are analytic on the  $p$ -adic complex plane  $\mathbb{C}_p$ , in the language which extends the language of rings by a constant symbol for  $z$ , is undecidable.*

**Theorem 3.4** (Vidaux, [67]) *The positive-existential theory of the field  $\mathcal{M}_{p,z}(\mathbb{C}_p)$  of functions of the variable  $z$  which are meromorphic on the  $p$ -adic complex plane  $\mathbb{C}_p$ , in the language which extends the language of rings by a constant symbol for  $z$  and by a predicate symbol for the property ‘the function  $x$  has  $z = 0$  as a zero’, is undecidable.*

The analogous questions over the field of complex numbers  $\mathbb{C}$  are open.

#### 4 Part D: Comments on the analogue of Hilbert’s tenth problem for $\mathbb{Q}$

As mentioned earlier, a major open problem in the area of decidability of existential theories of rings is the analogue of Hilbert’s tenth problem for the field  $\mathbb{Q}$  of rational numbers.

**Question 4.1** *Does the analogue of Hilbert's tenth problem for  $\mathbb{Q}$  have a negative answer?*

A naive approach might seek a possible positive answer to the following:

**Question 4.2** *Is the set  $\mathbb{Z}$  existentially definable in the field  $\mathbb{Q}$ ?*

which, if true, would imply obviously a YES answer to Question 4.1. But the following observation seems to make such an expectation unlikely: All known examples of algebraic varieties over  $\mathbb{Q}$  have the property that the real topological closure of the Zariski closure of their rational (over  $\mathbb{Q}$ ) points has finitely many connected components.

In consequence Mazur asked whether this is true for all algebraic varieties ([44]). He also stated a more general similar statement (an analogue where the real topology is substituted by the  $p$ -adic topologies). These questions remain open. An implication of a possible positive answer to Mazur's Question would be that Question 4.2 has a negative answer: Finitely many components project onto finitely many components, hence existential sets of  $\mathbb{Q}$  (being projections of varieties) would have only finitely many components, hence  $\mathbb{Z}$  cannot be one of them. Actually the implications are much deeper (cf. [12]). Some of us doubt the truth of Mazur's Question (mainly because the analogue of the  $p$ -adic version fails in global fields of positive characteristic). But still, most (if not all) of us, expect the answer to Question 4.2 to be negative.

In [49] a programme is presented for proving Question 4.1. It is based on interpreting the rational integers as the points (over  $\mathbb{Q}$ ) of an elliptic curve of rank 1 over  $\mathbb{Q}$ . Addition among points is given by the addition law on the curve. It therefore suffices to express existentially (in terms of the coordinates of the points) 'multiplication' among points. Since this seems inaccessible for the moment, one may, as a first step, try to define divisibility among points. Modulo conjectures (by Cornelissen and Everest) this may be existential. But even this does not suffice due to the fact that, as we saw, the existential theory of addition and divisibility over  $\mathbb{Z}$  is decidable. Hence more (existentially definable) structure is needed. A proposal of [49] to this effect seems unlikely (by arguments of Cornelissen). But Cornelissen proposed a possible remedy: Look, not at the points of an elliptic curve, but to the points (over  $\mathbb{Q}$ ) of an abelian variety with a group of points which, given a natural additional structure of multiplication, is isomorphic to a real quadratic extension of  $\mathbb{Z}$  (say  $\mathbb{Z}[\sqrt{5}]$ ). Such varieties do exist! If one can define existentially divisibility among points of such a variety, then a YES answer to Question 4.1 will

result from the undecidability of the existential theory of addition and divisibility over  $\mathbb{Z}[\sqrt{5}]$ ! See [13] for additional information on this type of approach.

Let us mention here that most, if not all, of the above approaches to resolve Question 4.1 would also disprove Mazur's Question.

Relevant material may be found also in [45] and the surveys [51] and [52].

## References

- [1] J. Ax, Solving diophantine equations modulo every prime, *Annals of Mathematics* 85-2 (1967), 161-183.
- [2] J. Ax, The elementary theory of finite fields, *Annals of Mathematics* 88 (1968), 239-271.
- [3] J. Ax and S. Kochen, Diophantine problems over local fields: III Decidable fields, *Annals of Mathematics* 83 (1966), 437-456.
- [4] J. Becker, J. Denef and L. Lipshitz, Further remarks on the elementary theory of power series rings, in *Model theory of algebra and arithmetic (Proc. Conf., Karpacz, 1979)*, pp. 1-9, Lecture Notes in Math., 834, Springer, Berlin-New York, 1980.
- [5] J. Becker, J. Denef, L. Lipshitz and L. van den Dries, Ultraproducts and approximation in local rings I, *Inventiones Mathematicae* 51 (1979), 189-203.
- [6] A. Bel'tyukov, Decidability of the universal theory of the natural numbers with addition and divisibility, *Seminars of the Steklov Math. Inst. (Leningrad)*, 60 (1976), 15-28.
- [7] R. Brody, Compact manifolds in hyperbolicity, *Trans. Amer. Math. Soc.* 235 (1978), 213-219.
- [8] F. Campana, Special varieties and classification theory: an overview. Monodromy and differential equations, (Moscow, 2001). *Acta Appl. Math.* 75 (2003), no. 1-3, 29-49.
- [9] G. Cherlin, *Model theoretic Algebra*, Lecture Notes Math. 521 (1976), Springer.
- [10] G. Cherlin and F. Point, On extensions of Presburger arithmetic, in *Proc. Fourth Easter conf. on model theory, Humboldt Univ. (1986)*, 17-34.
- [11] P. Cohen, Decision procedures for real and p-adic fields, *Comm. Pure Appl. Math.* 22 (1969), 131-151.
- [12] G. Cornelissen and K. Zahidi, Topology of Diophantine Sets: Remark's on Mazur's Conjectures, in *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, Contemporary Mathematics 270 (2000), 253-260.
- [13] G. Cornelissen and K. Zahidi, Complexity of undecidable formulae in the rationals and inertial Zsigmondy theorems for elliptic curves, ArXiv, [math.NT/0412473](https://arxiv.org/abs/math.NT/0412473), to appear in *Journal für die Reine und Angewandte Mathematik*
- [14] M. Davis, Hilbert's tenth problem is unsolvable, *American Mathematical Monthly* 80, 233-269 (1973).
- [15] M. Davis, Y. Matijasevic and J. Robinson, Hilbert's tenth problem. Dio-

- phantine equations: positive aspects of a negative solution, *Proc. Sympos. Pure Math.* 28 (1976), Amer. Math. Soc. 323-378.
- [16] F. Delon, Indécidabilité de la théorie des anneaux de séries formelles à plusieurs variables, *Fund. Math.* CXII (1981), 215-229.
  - [17] J. Denef, The diophantine problem for polynomial rings and fields of rational functions, *Transactions of the American Mathematical Society*, 242(1978),391-399.
  - [18] J. Denef, The diophantine problem for polynomial rings of positive characteristic, in *Logic Colloquium 78*, North Holland (1984), 131-145.
  - [19] J. Denef,  $p$ -adic semi-algebraic sets and cell decomposition, *J. Reine Angew. Math.* 369 (1986), 154-166.
  - [20] J. Denef and M. Gromov (communication by G. Cherlin), The ring of analytic functions in the disk has undecidable theory, 1985 (letter)
  - [21] J. Denef and L. van den Dries,  $p$ -adic and real subanalytic sets, *Ann. Math.*, 128 (1988), 79-138.
  - [22] J. Denef and L. Lipshitz, Ultraproducts and Approximation in local rings II, *Math. Ann.* 253 (1984)
  - [23] J. Denef and L. Lipshitz, Power series solutions of algebraic differential equations, *Math. Ann.* 267 (1980), 1-28.
  - [24] J. Denef and H. Schoutens, On the decidability of the existential theory of  $\mathbb{F}_p[[t]]$ , *Fields Inst. Comm.*, 33 (2003), 43-59
  - [25] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, 1966.
  - [26] Yu. Ershov, On elementary theories of local fields, *Algebra i Logika* 4 (1965), 5-30.
  - [27] M. Fried and G. Sacerdote, Solving Diophantine problems over all residue class fields of a number field and all finite fields *Ann. of Math.* 104 (1976), 203-233.
  - [28] M. Greenberg, Strictly local solutions of diophantine equations, *Pacific J. Math.*, 51 (1974), 143-153.
  - [29] F. Grunewald and D. Segal, The solubility of certain decision problems in arithmetic and algebra, *Bull. Amer. Math. Soc.* 1-6 (1979), 915-918.
  - [30] F. Grunewald and D. Segal, Some general algorithms I and II, *Ann. Math.*, 112 (1980), 531-617.
  - [31] C. Ward Henson and L. Rubel, Some applications of Nevanlinna Theory to mathematical logic: identities of exponential functions, *Trans. Amer. Math. Soc.* 282 (1984), 1-32 (also: corrections).
  - [32] T. Huuskonen, Constants are definable in fields of analytic functions, *Proc. Amer. Math. Soc.* 122 (1994), 697-702.
  - [33] N. Katz and S. Lang, Finiteness theorems in geometric classfield theory. (With an appendix by Kenneth A. Ribet), *Enseign. Math. (2)* 27-3,4 (1981), 285-319.
  - [34] K. Kim and F. Roush, An approach to rational diophantine undecidability, *Proc. Asian Math. Conf.*, World Scient. Press, Singapore (1992), 242-257.
  - [35] K. Kim and F. Roush, Diophantine undecidability of  $\mathbb{C}(t_1, t_2)$ , *J. Algebra* 150 (1992), 35-44.
  - [36] S. Kochen, The model theory of local fields, in *Proc. Internat. Summer Inst. and Logic Colloq., Kiel, 1974*, 384-425, Springer Lecture Notes in Math. 499 (1975).
  - [37] S. Lang, Hyperbolic diophantine analysis, *Bulletin of the American Math-*

- ematical Society* 14, 159-205 (1986).
- [38] L. Lipshitz, The diophantine problem for addition and divisibility, *Transactions of the American Mathematical Society* 235, (1978), 271-283.
  - [39] L. Lipshitz, Undecidable existential problems for addition and divisibility in algebraic number rings, II, *Proceedings of the American Mathematical Society*, 64 (1977), 122-128.
  - [40] L. Lipshitz, Undecidable existential problems for addition and divisibility in algebraic number rings, *Transactions of the American Mathematical Society*, 241 (1978), 121-128.
  - [41] L. Lipshitz and T. Pheidas, An analogue of Hilbert's Tenth Problem for  $p$ -adic entire functions, *The Journal of Symbolic Logic*, 60-4 (1995), 1301-1309
  - [42] A. Macintyre, On definable subsets of  $p$ -adic fields, *J. Symb. Logic* 41 (1976), 605-610.
  - [43] Y. Matijasevich, Enumerable sets are diophantine, *Doklady Akademii Nauka SSSR*, 191(1970), 272-282.
  - [44] B. Mazur, The topology of rational points, *Journal of Experimental Mathematics*, 1-1 (1992), 35-45.
  - [45] B. Mazur, Questions of decidability and undecidability in number theory, *The Journal of Symbolic Logic*, 59-2 (1994), 353-371.
  - [46] C. Michaux and R. Villemaire, Presburger arithmetic and recognizability of sets of natural numbers by automata: new proofs of Cobham's and Semenov's theorems, *Ann. Pure Appl. Logic* 77 (1996), 251-277.
  - [47] T. Pheidas, Extensions of Hilbert's Tenth Problem, *The Journal of Symbolic Logic*, 59-2 (1994), 372-397.
  - [48] T. Pheidas, Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic, *Journal of Algebra* 273 (2004), no. 1, 395-411.
  - [49] T. Pheidas, An effort to prove that the existential theory of  $\mathbb{Q}$  is undecidable, *Contemporary Mathematics* 270 (2000), 237-252.
  - [50] T. Pheidas and K. Zahidi, Undecidable existential theories of polynomial rings and function fields, *Communications in Algebra*, 27-10 (1999), 4993-5010.
  - [51] T. Pheidas and K. Zahidi, Undecidability of existential theories of rings and fields: A survey, *Contemporary Mathematics*, 270 (2000), 49-106.
  - [52] B. Poonen, Hilbert's Tenth Problem over rings of number-theoretic interest, obtainable from <http://math.berkeley.edu/~poonen/>
  - [53] J. Robinson, Definability and decision problems in arithmetic, *Journ. Symb. Logic* 14 (1949), 98-114.
  - [54] J. Robinson, Existential definability in arithmetic, *Trans. Amer. Math. Soc.* 72 (1952), 437-449.
  - [55] R. Robinson, Undecidable rings, *Trans. Amer. Math. Soc.* 70 (1951), 137.
  - [56] L. Rubel, An essay on diophantine equations for analytic functions, *Expositiones Mathematicae*, 14(1995),81-92.
  - [57] R. Rumely, Arithmetic over the ring of all algebraic integers, *Journ. Reine und Angew. Math.* 368 (1986), 127-133.
  - [58] A. Semenov, Logical theories of one-place functions on the set of natural numbers, *Math. USSR Izvestija*, 22 (1984), 587-618.
  - [59] A. Shlapentokh, Hilbert's tenth problem over number fields, a survey, *Contemporary Mathematics*, 270 (2000), 107-137.
  - [60] A. Seidenberg, Constructions in Algebra, *Trans. Amer. Math. Soc.* 197

- (1974), 273–313.
- [61] M. Spivakovski, A new proof of D. Popescu's theorem on smoothing of ring homomorphisms, *J. Amer. Math. Soc.* 12, 381-444
  - [62] A. Tarski, *A decision method for elementary algebra and geometry*, RAND Corporation, Santa Monica, Calif. (1948).
  - [63] L. van den Dries, A specialization theorem for analytic functions on compact sets, *Proceedings Koninklijke Nederlandse Academie van Wetenschappen (A)*, 85-4 (1988),391-396.
  - [64] L. van den Dries, Elimination theory for the ring of algebraic integers, *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 388 (1988), 189-205.
  - [65] L. van den Dries, A remark on Ax's theorem on solvability modulo primes, *Math. Z.* 208 (1991), 65-70.
  - [66] L. van den Dries, Analytic Ax-Kochen-Ersov theorems, in *Proceedings of the International Conference on Algebra, Part 3 (Novosibirsk, 1989)*, 379–398, Contemp. Math. 131, Amer. Math. Soc., Providence, RI, 1992.
  - [67] X. Vidaux, An analogue of Hilbert's 10th problem for fields of meromorphic functions over non-Archimedean valued fields, *Journal of Number Theory*, 101 (2003), 48-73.
  - [68] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, Springer-Verlag, 1239 (1987)
  - [69] P. Vojta, Diagonal quadratic forms and Hilbert's Tenth Problem, *Contemporary Mathematics* 270, 261-274 (2000).
  - [70] V. Weispfenning, Quantifier elimination and decision procedures for valued fields in *Models and Sets*, Lect. Notes Math. 1103, Springer-Verlag (1984), 419-472.

