The Diophantine problem in finitely generated commutative rings

Albert Garreta  Alexei Miasnikov  Denis Ovchinnikov*

Abstract

We study systems of polynomial equations in infinite finitely generated commutative associative rings with an identity element. For each such ring \( R \) we obtain an interpretation by systems of equations of a ring of integers \( O \) of a finite field extension of either \( \mathbb{Q} \) or \( \mathbb{F}_p(t) \), for some prime \( p \) and variable \( t \). This implies that the Diophantine problem (decidability of systems of polynomial equations) in \( O \) is reducible to the same problem in \( R \). If, in particular, \( R \) has positive characteristic or, more generally, if \( R \) has infinite rank, then, using some results due to Eisentraeger and Shlapentokh, we further obtain an interpretation by systems of equations of the ring \( \mathbb{F}_p[t] \) in \( R \). This implies that the Diophantine problem in \( R \) is undecidable in this case. In the remaining case where \( R \) has finite rank and zero characteristic, we see that \( O \) is a ring of algebraic integers, and then the long-standing conjecture that \( \mathbb{Z} \) is always interpretable by systems of equations in a ring of algebraic integers carries over to \( R \). If true, it implies that the Diophantine problem in \( R \) is also undecidable. Thus, in this case the Diophantine problem in every infinite finitely generated commutative unitary ring is undecidable.

The present is the first in a series of papers where we study the Diophantine problem in different types of rings and algebras.

1 Introduction

In this paper, we study the Diophantine problem, denoted \( \mathcal{D}(R) \), in infinite finitely generated commutative associative unitary rings \( R \). Recall that the Diophantine problem \( \mathcal{D}(R) \) asks whether there exists an algorithm that, given a finite system of equations \( S \) with coefficients in \( R \), determines if \( S \) has a solution in \( R \) or not. We show that in any such ring \( R \) one can interpret by systems of polynomial equations (in short, \( e \)-interpret, see Section 2.1 below) a ring of integers \( O \) of a number or of a global function field. This gives a reduction of \( \mathcal{D}(O) \) to \( \mathcal{D}(R) \), i.e. a polynomial time algorithm that for a given finite system \( \Sigma \) of polynomial equations with coefficients in \( O \) constructs a finite system \( \Sigma^* \) of polynomial equations with coefficients in \( R \) such that \( \Sigma \) has a solution in \( O \) if and only if \( \Sigma^* \) has a solution in \( R \). In particular, if \( \mathcal{D}(O) \) is undecidable then \( \mathcal{D}(R) \) is also undecidable. This relates the study of the Diophantine problem in rings \( R \) to the particular case of rings of integers \( O \), but it does not solve the original problem, since in general decidability of \( \mathcal{D}(O) \) is still unknown. Nevertheless, this technique allows us to further clarify the situation and prove undecidability of \( \mathcal{D}(R) \) for a wide variety of rings \( R \). Namely, relying on some results due to Eisentraeger and Shlapentokh, we prove that if \( R \) has

\*albert.garreta@eus.edu, corresponding author (University of the Basque Country, Bilbao, Spain); amiasnikov@gmail.com (Stevens Institute of Technology, Hoboken, NJ, USA); dovchinn@stevens.edu (Stevens Institute of Technology, Hoboken, NJ, USA)

MSC: 11D99, 11D72, 11U05
infinite rank (this is always the case if \( R \) has positive characteristic), then the ring of polynomials in one variable is e-interpretable in \( R \), hence, by Denef’s results \([5, 6]\) \( \mathcal{D}(R) \) is undecidable. In the remaining case when \( R \) has characteristic zero and the rank of \( R \) is finite, the ring \( O \) that is e-interpretable in \( R \) is the ring of integers of an algebraic number field. Decidability of \( \mathcal{D}(O) \) for such arbitrary \( O \) is still unknown, but is conjectured to be undecidable \([7, 29]\) - a major conjecture in number theory. If true, this would imply that \( \mathcal{D}(R) \) is undecidable for any infinite finitely generated commutative unitary ring \( R \).

The original modern version of the Diophantine problem (also called Hilbert’s Tenth Problem or generalized Hilbert’s Tenth Problem) was posed by Hilbert for the ring of integers \( \mathbb{Z} \). This was solved in the negative in 1970 by Matiyasevich \([26]\) building on the work of Davis, Putnam, and Robinson \([3]\). Subsequently the same problem has been studied in a wide variety of rings, most notably in \( \mathbb{Q} \) and in rings of algebraic integers \( O \) (integral closures of \( \mathbb{Z} \) in finite field extensions of \( \mathbb{Q} \)), where it remains widely open. As mentioned above, a long-standing conjecture \([7, 29]\) states that \( \mathbb{Z} \) is Diophantine in any such \( O \) (and thus \( \mathcal{D}(O) \) is undecidable). This conjecture has been verified in some particular cases \([15, 33, 37]\), and it has been shown to be true assuming the Safarevich-Tate conjecture \([27]\).

The situation is much clearer for rings of integers of global function fields, i.e. for finite field extensions of rational function fields of the form \( \mathbb{F}_p(t) \) for some variable \( t \) and some prime integer \( p \). Indeed, Shlapentokh \([34]\) showed that \( \mathbb{F}_p[t] \) is Diophantine in any such ring \( O \), and consequently that \( \mathcal{D}(O) \) is undecidable. Other results in this direction include undecidability of \( \mathcal{D}(K) \) for any function field \( K \) not containing the algebraic closure of a finite field \([10, 11, 34]\), and of \( \mathcal{D}(R[[t]]) \), where \( R \) is any integral domain \([5, 6]\).

Some commutative rings where the Diophantine problem remains open are most remarkably \( \mathbb{Q} \) (it is known however that this problem is undecidable in \( \mathbb{Z}[S^{-1}] \), for \( S \) an infinite set of primes of Dirichlet density 1 \([30]\); the rational functions \( \mathbb{C}(t) \) (even though \( \mathcal{D}(\mathbb{C}(t_1, t_2)) \) is undecidable \([22]\); and the field of Laurent series \( \mathbb{F}_p((t)) \). We refer to \([24, 29, 31, 37]\) for further information and surveys of results in this direction.

Regarding non-commutative rings, Romankov \([32]\) showed that \( \mathcal{D}(F) \) is undecidable in several types of free rings \( F \), which include free Lie rings, free associative or non-associative rings, and free nilpotent rings. One can view these rings as free \( \mathbb{Z} \)-algebras, it is essentail, since the proofs use undecidability of the Diophantine problem in the coefficients \( \mathbb{Z} \). Using different methods Kharlampovich and Miasnikov recently proved undecidability of \( \mathcal{D}(A) \), for any of the following rings \( A \): a free associative \( k \)-algebra, a free Lie \( k \)-algebra (of rank at least 3), and group \( k \)-algebras \( k(G) \) for various groups \( G \) (including free, torsion-free hyperbolic, right-angled Artin, and other groups) \([20, 21]\). In all these results the field \( k \) is arbitrary, possibly with decidable \( \mathcal{D}(k) \). We address the Diophantine problem in arbitrary finitely generated rings (i.e. possibly non-associative, non-commutative, and non-unitary) in a subsequent paper which makes use of significantly different techniques than the ones used in the present paper. In particular, in the subsequent paper we deal with infinite finitely generated commutative associative non-unitary rings.

To move forward we need to recall some definitions. Recall that a field \( K \) is a number field if it is a finite extension of \( \mathbb{Q} \), and \( K \) is a global function field if it is a finite extension of \( \mathbb{F}_p(t) \), for some prime \( p \). A ring of integers in such \( K \) is the integral closure in \( K \) of \( \mathbb{Z} \) or \( \mathbb{F}_p[t] \), respectively. The ring of integers in a number field \( K \) is called a ring of algebraic integers. Our main technical tool is that of interpretations by equations or e-interpretations, of which we remind the formal definitions in Section \([24]\). Roughly, an e-interpretation is a generalization of the usual notion of Diophantine definability (in the sense of Davis, Putnam, and Robinson) which also accommodates ring quotients.

The characteristic of a ring with multiplicative identity (i.e. a unitary ring) is the minimum
positive integer \( n \) such that \( 1 + \ldots + 1 = 0 \). By rank of a ring \( R \) we refer to the rank of \( R \) seen as an abelian group (i.e. forgetting its multiplication operation) in the sense of [14]; that is, the maximum number \( m \) of nonzero elements \( r_1, \ldots, r_m \in R \) such that whenever \( a_1 r_1 + \cdots + a_m r_m = 0 \) for some integers \( r_1, \ldots, r_m \), we have \( r_i a_i = 0 \) for all \( i = 1, \ldots, m \). If \( R \) is an integral domain, then its rank coincides with its dimension as a \( \mathbb{F}_p \)-vector space if \( R \) has positive characteristic \( p \), and otherwise it coincides with the dimension of \( R \) seen as a \( \mathbb{Z} \)-module.

The main result of the paper is the following.

**Theorem 1.1.** Let \( R \) be an infinite finitely generated associative commutative unitary ring. Then there exists a ring of integers \( O_K \) of a number or a global function field \( K \) such that \( O_K \) is \( e \)-interpretable in \( R \), and \( D(O_K) \) is polynomial-time reducible to \( D(R) \). Moreover, one of the following holds:

1. If \( R \) has positive characteristic \( n > 0 \), then the following holds: \( O_K \) is the ring of integers of a global function field; the ring of polynomials \( \mathbb{F}_p[t] \) is \( e \)-interpretable in \( R \) for some transcendental element \( t \) and some prime integer \( p \); and \( D(R) \) is undecidable.

2. If \( R \) has zero characteristic and it has infinite rank then the same conclusions as above hold: \( O_K \) is the ring of integers of a global function field; the ring of polynomials \( \mathbb{F}_p[t] \) is \( e \)-interpretable in \( R \) for some \( t \) and \( p \); and \( D(R) \) is undecidable.

3. If \( R \) has zero characteristic and it has finite rank \( n \), then \( O_K \) is a ring of algebraic integers, and \( D(R) \) is undecidable provided that \( D(O_K) \) is undecidable. Additionally, \( K \) is a field extension of \( \mathbb{Q} \) of degree at most \( n \).

We note that if \( R \) is finite then its Diophantine problem is decidable. Hence, if the conjecture that \( D(O) \) is undecidable for any ring of algebraic integers \( O \) is true, then the Diophantine problem is undecidable in any infinite finitely generated commutative unitary ring. We stress that this is now confirmed by the results of this paper when \( R \) has infinite rank (for instance, for positive characteristic). We also obtain a partial result for rings \( R \) with finite rank:

**Theorem 1.2.** Let \( R \) be an infinite finitely generated associative commutative unitary ring of rank at most 2. Then the Diophantine problem \( D(R) \) of \( R \) is undecidable.

The paper is organized as follows. In Section 2 we provide all the necessary definitions and basic results regarding the Diophantine problem and the tools we use to study it. Section 3 includes definitions and known results about rings of integers of number or global function fields. Section 4 contains the main results of the paper: first in Subsection 4.1 we study subrings of number and global function fields, and then in Subsection 4.2 we go on to treat the general case.

If not said otherwise, throughout this paper \( R \) always denotes an infinite, associative, commutative, and unitary ring. We will often omit any further reference to these properties and refer to \( R \) as “a ring”.

## 2 Diophantine problems and reductions.

Let \( R \) be a ring. A polynomial equation in \( R \) is an expression of the form \( p(x_1, \ldots, x_k) = 0 \), where \( p \) is a polynomial with coefficients on \( R \) and on variables \( x_1, \ldots, x_k \). We will often refer to polynomial equations simply as equations.

The Diophantine problem in \( R \), denoted \( D(R) \), refers to the algorithmic problem of determining if each given system of polynomial equations in \( R \) has a solution. Sometimes this is also
called Hilbert’s Tenth Problem in \( R \). An algorithm \( L \) is a solution to \( \mathcal{D}(R) \) if, given a system of equations \( S \) in \( R \), it determines whether \( S \) has a solution or not. If such an algorithm exists, then \( \mathcal{D}(R) \) is called decidable, and, if it does not, undecidable.

The Diophantine problem is sometimes defined for single equations, instead of systems of equations. Both notions are equivalent in the case that \( R \) is an integral domain whose field of fractions is not algebraically closed, because then any system of equations is equivalent to a single equation. Note that since our rings are finitely generated, the field of fractions of \( R \) is never algebraically closed—we will use this fact repeatedly without referring to it. However, this is no longer the case in general, as shown in the upcoming Example 2.11.

Hence, in this paper, if \( R \) is a finitely generated integral domain, then the Diophantine problem can be thought to refer to single equations only, but if it is not, then our results apply only to systems of equations.

### 2.1 Interpretations by systems of equations

Interpretability by systems of equations (e-interpretable) is an analog of the classic model-theoretic notion of interpretability by first-order formulas (see 17, 23). More precisely, an e-interpretation is an interpretation in the classical sense where all formulas used are systems of polynomial equations with coefficients in the structure at hand (in our case, a ring).

From a number theoretic viewpoint, e-interpretability is roughly Diophantine definability (by systems of polynomial equations) up to a Diophantine definable equivalence relation.

**Definition 2.1.** In a ring \( R \), a subset \( A \subseteq R^n \) for some \( n \geq 1 \) is called definable by equations (or e-definable) in \( R \) if there exists a system of polynomial equations in \( R \), say \( \Sigma_A(x_1, \ldots, x_n, y_1, \ldots, y_m) \) on variables \( (x_1, \ldots, x_n, y_1, \ldots, y_m) \), such that for any tuple \( (a_1, \ldots, a_n) \in R^n \), one has that \( (a_1, \ldots, a_n) \in A \) if and only if the system \( \Sigma_A(a_1, \ldots, a_n, y_1, \ldots, y_m) \) on variables \( (y_1, \ldots, y_m) \) has a solution in \( R \). In this case \( \Sigma_A \) is said to e-define \( A \) in \( R \). The integer \( n \) is called the dimension of the e-definition.

From a number theoretic viewpoint, an e-definable set is a Diophantine definable set using systems of equations. From an algebraic geometric viewpoint, it is a projection onto some coordinates of an affine algebraic set.

**Definition 2.2.** Let \( R_1 \) and \( R_2 \) be two rings. One says that \( R_1 \) is interpretable by equations (or e-interpretable) in \( R_2 \) if there exists \( n \geq 1 \), a subset \( A \subseteq R_2^n \), and a surjective map \( \phi: A \to R_1 \) such that:

1. \( A \) is e-definable in \( R_2 \).

2. The preimage by \( \phi \) of the graph of the addition operation of \( R_1 \), i.e.

\[
\{(x, y, z) \in A^3 \mid \phi(x) + \phi(y) = \phi(z)\},
\]

is e-definable in \( R_2 \). Similarly, the preimage of the graph of multiplication in \( R_1 \), as well as the preimage \( \{(x, y) \in A^2 \mid \phi(x) = \phi(y)\} \) of the identity relation of \( R_1 \), are e-definable in \( R_2 \). In all these cases we say that \( \phi \) is an e-interpretation in \( R_2 \) of the addition and multiplication operations of \( R_1 \), and the equality relation of \( R_1 \), respectively.

The map \( \phi \) is called an e-interpretation of \( R_1 \) in \( R_2 \). We will say that \( A \) is e-interpretable in \( M \) if there exists an e-interpretation \( \phi \) of \( A \) in \( M \). It is usually clear, but not important, what the specific e-interpretation is.
Remark 2.3. The previous definitions, as well as most results in this section, can be easily formulated and generalized to abstract structures. See, for example, [16].

The next lemma illustrates a key example of an e-interpretation.

Lemma 2.4. Let \( R \) be a ring, not necessarily commutative or associative. Suppose \( I \subseteq R \) is an ideal that admits a 1-dimensional e-definition in \( R \). Then \( R/I \) is e-interpretable in \( R \).

Proof. Let \( \Sigma_I(x, y_1, \ldots, y_m) \) be a system of equations giving a 1-dimensional e-definition of \( I \) in \( R \), so that \( a \in R \) belongs to \( I \) if and only if \( \Sigma_I(a, y_1, \ldots, y_m) \) has a solution on \( y_1, \ldots, y_m \). It suffices to check that the natural epimorphism \( \pi : R \rightarrow R/I \) is an e-interpretation of \( R/I \) in \( R \). First observe that the preimage of \( \pi \) is the whole \( R \), which is clearly e-definable in \( R \). Regarding the preimage of the equality relation of \( R/I \), we have that \( \pi(a_1) = \pi(a_2) \) in \( R/I \) if and only if \( a_1 - a_2 \in I \), i.e. if and only if \( \Sigma_I(a_1 - a_2, y_1, \ldots, y_m) \) has a solution. From this it follows that the preimage of equality in \( R/I \), i.e. \( \{a_1, a_2 \in R \mid \pi(a_1) = \pi(a_2)\} \), is e-definable in \( R \) by the system of equations \( \Sigma_I(x_1, x_2, y_1, \ldots, y_m) \) obtained from \( \Sigma_I(x, y_1, \ldots, y_m) \) after substituting each occurrence of \( x \) by \( x_1 - x_2 \), where \( x_1 \) and \( x_2 \) are fresh new variables.

By similar arguments, the preimages of the addition and multiplication operations of \( R/I \) are e-definable in \( R \): indeed, for any three elements \( a_1, a_2, a_3 \in R \) we have that \( \pi(a_1) + \pi(a_2) = \pi(a_3) \) if and only if \( a_1 + a_2 - a_3 \in I \), and \( \pi(a_1)\pi(a_2) = \pi(a_3) \) if and only if \( a_1a_2 - a_3 \in I \).

Interestingly, all finitely generated ideals of a ring are e-interpretable in it:

Lemma 2.5. Let \( I \) be a finitely generated ideal of a ring \( R \). Then \( I \) is e-definable in \( R \). As a consequence, \( R/I \) is e-interpretable in \( R \).

Proof. Let \( a_1, \ldots, a_n \) be a generating set of \( I \). Then the equation \( x = \sum x_i a_i \) on variables \( (x, x_1, \ldots, x_n) \) e-defines \( I \) in \( R \). Lemma 2.4 now implies that \( R/I \) is e-interpretable in \( R \).

Note that any finitely generated ring \( R \) (as all rings considered in this work) is Noetherian, i.e. all their ideals are finitely generated (this follows from Hilbert’s basis theorem). Thus any ideal \( I \) of \( R \) is e-definable in \( R \) and \( R/I \) is e-interpretable in \( R \).

We will also need the following observation.

Remark 2.6. Let \( R_1, \ldots, R_n \) be subrings of a ring \( R \) such that each \( R_i \) admits a 1-dimensional e-definition in \( R \). Then the intersection \( R_1 \cap \cdots \cap R_n \) also admits a 1-dimensional definition in \( R \).

Proof. For each \( i = 1, \ldots, n \), let \( \Sigma_i(x_i, y_{i1}, \ldots, y_{im_i}) \) be a system giving a 1-dimensional e-definition of \( R_i \) in \( R \). Let \( x \) be a new variable. Then the following system of equations provides a 1-dimensional e-definition of \( R_1 \cap \cdots \cap R_n \) in \( R \): \( \Sigma_1(x, y_{i1}, \ldots, y_{im_1}) \wedge \cdots \wedge \Sigma_n(x, y_{i1}, \ldots, y_{im_n}) \).

The next two results are fundamental. They follow from Lemma 2.9 which we present at the end of this subsection.

Proposition 2.7 (E-interpretability is transitive). Let \( R_1, R_2, R_3 \) be rings. If \( R_1 \) is e-interpretable in \( R_2 \) and \( R_2 \) is e-interpretable in \( R_3 \), then \( R_1 \) is e-interpretable in \( R_3 \).

Proposition 2.8 (Reduction of Diophantine problems). Let \( R_1 \) and \( R_2 \) be finitely generated rings such that \( R_1 \) is e-interpretable in \( R_2 \). Then \( \mathcal{D}(R_1) \) is polynomial-time reducible to \( \mathcal{D}(R_2) \). As a consequence, if \( \mathcal{D}(R_1) \) is undecidable, then so is \( \mathcal{D}(R_2) \).
Both Propositions 2.7 and 2.8 are a consequence of the following lemma, which states in technical terms that if one ring is e-interpretable in the other, then one may “express” any system of equations in the first as a system of equations in the second. This is a well-known fundamental result in model theory if one replaces system of equations by first-order sentences, see Theorem 5.3.2 from [17].

Lemma 2.9. Let $\phi$ be an e-interpretation of a ring $R_1$ in another ring $R_2$, where $\phi : A \subset R_2^m \rightarrow R_1$ using the notation of Definition 2.4. Let $\sigma(x_1, \ldots, x_m)$ be an arbitrary system of equations in $R_1$ on variables $x_1, \ldots, x_m$. Then there exists a system of equations $\Sigma_\sigma(y_1, \ldots, y_{1n}, \ldots, y_{mn})$ in $R_2$, such that a tuple $(b_1, \ldots, b_m, \ldots, b_{mn}) \in R_2^{mn}$ is a solution to

$$\Sigma_\sigma(y_1, \ldots, y_{1n}, \ldots, y_{mn})$$

if and only if $(b_1, \ldots, b_m) \in A$ for all $i = 1, \ldots, m$ and $\phi(b_1, \ldots, b_m) \in \Sigma_\sigma$ a solution to $\sigma$.

Moreover, if both $R_1$ and $R_2$ are finitely generated[1], then $\Sigma_\sigma$ can be obtained in polynomial time on the syntactic length of $\sigma$ (with constants given as products of generators).

Proof. First we claim that, by introducing new variables and new equations, we can rewrite $\sigma$ so that $\sigma$ consists in a conjunction of equations of the form $x + y = z$, $xy = z$, $x = y$, or $x = a$, where $x, y, z$ are some variables and $a \in R$. Moreover, if $R_1$ and $R_2$ are countably generated, we further claim that this rewriting can be done in polynomial time on the syntactic length of $\sigma$, which we denote $|\sigma|$. Indeed, we proceed by induction on $|\sigma|$, the base cases being clear. Let $f(x_1, \ldots, x_m)$ be a polynomial with coefficients in $R_1$ such that $\sigma$ is $f(x_1, \ldots, x_m) = 0$. Let $z$ be the last symbol of $f$ (either a variable or a generator of $R_1$). Then either $f(x_1, \ldots, x_m) = g(x_1, \ldots, x_m)z$ or $f(x_1, \ldots, x_m) = g(x_1, \ldots, x_m) + z$ for some polynomial $g(x_1, \ldots, x_m)$. Assume the first holds (the second case follows analogously). Now introduce a fresh new variable $w$ and replace $\sigma$ by the system of equations $w = g(x_1, \ldots, x_m)$ and $wz = 0$ (if the second case held then we would write $w + z = 0$ instead of $wz = 0$). Now we replace $wz = 0$ by $wz' = u \land u = 0 \land z' = z$ where $u$ and $z'$ are new variables (this is done to ensure that constants only appear in equations of the form $x = a$—observe that the equation $z' = z$ can be omitted if $z$ is a variable). Notice that this step takes linear time to realize. Now we can apply the induction hypothesis on $w = g(x_1, \ldots, x_m)$ in order to obtain a system of equations $\Delta$ in the desired form and in polynomial time. The final system of equations consists in $\Delta$ together with $w + z' = u$, $u = 0$, and $z' = z$. The claim is proved.

We now prove the lemma. By the above claim, $\sigma$ is equivalent to $\sigma_1 \land \cdots \land \sigma_n$, where for each $i = 1, \ldots, n$, $\sigma_i$ has one of the forms $x + y = z$, $xy = z$, $x = y$, or $x = a$, where $x, y, z$ are some variables and $a \in R$. By the definition of e-interpretable, $\sigma_i$ satisfies the statement of the lemma for all $i = 1, \ldots, n$. Thus, it suffices to take $\Sigma_\sigma$ to be $\Sigma_{\sigma_1} \land \cdots \land \Sigma_{\sigma_n}$. □

We will be using the following observation without referring to it.

Remark 2.10. Let $R_1, R_2$ be two rings with $R_1 \subseteq R_2$. Then $R_1$ is e-definable in $R_2$ if and only if the identity map $\text{id} : R_1 \subseteq R_2 \rightarrow R_1$ is an e-interpretation of $R_1$ in $R_2$.

Example 2.11. Here we provide an example of an associative, commutative, non-unitary finitely generated ring $R$ where single equations are decidable, but systems of equations are

---

[1] This result also holds for many classes of non-finitely generated rings, but one must make assumptions on the computability of $\phi$ and the rings.
not. Let \( \mathbb{Z}_h[a, b, c] \) be the ring of homogeneous polynomials on the variables \( a, b, c \), and take \( R \) to be the quotient \( \mathbb{Z}_h[a, b, c]/I \), where \( I \) is the ideal generated by the elements \( a^2, b^2, c^2, ac, bc \) and \( ab - c \). Note that \( R \) can be identified with the set \( \{\alpha a + \beta b + \gamma c ~|~ \alpha, \beta, \gamma \in \mathbb{Z} \} \). In what follows we make this identification implicitly.

To prove that single equations are decidable in \( R \), observe that one has that \( x^3 = 0 \) for any element \( x \in R \). From this it follows that any equation in \( R \) is equivalent to a system of linear integer equations together with a single quadratic polynomial equation in \( \mathbb{Z} \). Since this class of equations is decidable (see for example Lemma 1 of [8]), single equations in \( R \) are decidable as well.

On the other hand, we claim that the ring \( \mathbb{Z} \) is e-interpretable in \( R \), hence systems of equation in \( R \) are undecidable. The proof of the claim is analogous to the proof from [8] that the Diophantine problem is undecidable in the Heisenberg group. Here, the ring multiplication operation has the role of the commutator operation in the Heisenberg group. Let \( S = \{\gamma c ~|~ \gamma \in \mathbb{Z} \} \) and define \( \phi: S \to \mathbb{Z} \) as \( \phi(\gamma c) = \gamma \). We will prove that \( \phi \) is an e-interpretation of the ring \( \mathbb{Z} \) in \( R \). Indeed, the set \( S \) is e-definable in \( R \) by the polynomial equation \( x = yz \), i.e. an element from \( R \) belongs to \( S \) if and only if it is the product of two elements from \( R \). Moreover, the preimage by \( \phi \) of the addition operation of \( \mathbb{Z} \) is \( \{x, y, z \in S ~|~ x + y = z \} \), which is e-definable in \( R \). Similarly, the preimage of the equality relation is also e-definable in \( R \). We now prove that the preimage by \( \phi \) of the graph of the integer multiplication operation, denote it \( \phi^{-1}(\cdot) \), is e-definable in \( R \). Indeed, \( \phi^{-1}(\cdot) \) is precisely the set formed by the triples \( (x, y, z) \in R^3 \) for which there exists integers \( \lambda_1, \lambda_2 \) such that \( x = \lambda_1 c \), \( y = \lambda_2 c \), and \( z = \lambda_1 \lambda_2 \). Let \( \Sigma(w_1, w'_1, w_2, w'_2) \) be the following system of polynomial equations in \( R \) on variables \( w_1, w'_1, w_2, w'_2 \): \( w_1 b = w'_1 a = 0 \), \( w_1 a = w'_1 b \), \( w_2 b = w'_2 a = 0 \), and \( w_2 a = w'_2 b \). Let \( T \) be the set of tuples of the form \( (x, y, z) \in R^3 \) such that there exists a solution \( (r_1, r'_1, r_2, r'_2) \in R^4 \) to \( \Sigma(w_1, w'_1, w_2, w'_2) \) such that \( x = r_1 a \), \( y = r_2 a \) and \( z = r_1 r'_2 \). Writing each \( r_i \) in the form \( r_i = \alpha_i a + \beta_i b + \gamma_i c \) for some integers \( \alpha_i, \beta_i, \gamma_i \) (and similarly for the \( r'_i \)) and examining the equalities from \( \Sigma(\lambda r_1, r'_1, \lambda r_2, r'_2) \) we obtain that \( T \) is precisely the set \( \phi^{-1}(\cdot) \). Since \( T \) is e-definable in \( R \), this completes the proof of the claim.

3 Rings of integers of number and function fields

First we recall some terminology. A number field is a finite field extension of \( \mathbb{Q} \). A function field \( F \) over a field \( k \) is a finite field extension of a one-variable field of rationals \( k(t) \), for some field \( k \). If \( k \) is a finite field then \( F \) is called a global function field. A global field is either a number field or a global function field.\(^2\)

For terminology purposes, we fix a variable \( t \) and agree that a global function field is a finite field extension of \( \mathbb{F}_p[t] \) for some prime \( p \). As usual, \( \mathbb{F}_p \) denotes the finite field with \( p \) elements.

Let \( R_1 \) and \( R_2 \) be two rings such that \( R_1 \subseteq R_2 \). An element \( r \in R_2 \) is integral over \( R_1 \) if there exists a monic polynomial from \( R_1[t] \) that has \( r \) as a root. The integral closure of \( R_1 \) in \( R_2 \) is the set of all elements of \( R_2 \) that are integral over \( R_1 \). Such set is a subring of \( R_2 \). An integral domain \( D \) is called integrally closed if the integral closure of \( D \) in its field of fractions is \( D \) itself.

Let \( K \) be a number field or a field of functions over \( k \). The ring of integers of \( K \), denoted \( \mathcal{O}_K \), is the integral closure of \( \mathbb{Z} \) or \( k[t] \) in \( K \). In the first case, \( \mathcal{O}_K \) is called a ring of algebraic integers.

\(^2\)We will not be using this last term, but it is used in relevant literature, [37]

Rings of \( S \)-integers or holomorphy rings Our main references for this section are [12, 37, 38]. Throughout the end of this section we let \( K \) be either a number field or a function field
over a field $k$. A (non-archimedean) valuation of $K$ is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ that satisfies all of the following:

1. $v$ induces a homomorphism $v : K^* \to \mathbb{Z}^+$ from the multiplicative group of $K$ into the additive group of $\mathbb{Z}$.
2. $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.
3. $v(x) = \infty$ if and only if $x = 0$.
4. $v(x) \neq 0$ for some $x \in K \setminus \{0\}$.
5. If $K$ is a finite extension of $k(t)$ for some field $k$, then $v(c) = 0$ for all $c$ in the algebraic closure of $k$ in $K$.

We will refer to a non-archimedean valuation simply as a valuation (archimedean valuations are never considered in this paper). Two valuations $v_1$ and $v_2$ are equivalent if $\{x \in K \mid v_1(x) \geq 0\} = \{x \in K \mid v_2(x) \geq 0\}$. An equivalence class of a valuation $v$ is called a prime. We identify $v$ with its equivalence class, and we write $\text{ord}_v(x)$ instead of $v(x)$, for any $x \in K$.

Let $S$ be a (finite or infinite) set of primes of $K$. The ring of $S$-integers of $K$ is defined as

$$O_{K,S} = \{x \in K \mid \text{ord}_p(x) \geq 0 \quad \forall p \notin S\}.$$  

In some texts $O_{K,S}$ is called a holomorphy ring when $K$ is a function field.

**Remark 3.1.** The family of rings of $S$-integers contains all rings of integers of number and function fields. Indeed, if $K$ is a number field, then $O_{K,S}$ is precisely the ring of algebraic integers $O_K$ of $K$. This follows, for example, from the fact that $O_K$ is the intersection of all valuation rings of $K$ containing $O_K$ (Corollary 5.22 of [1]), but such intersection is precisely $\bigcap_{p \text{ prime}} O_{K,p} = O_{K,S}$, where $p$ denotes all primes but $p$.

Now suppose that $K$ is a function field over $k$, so that $K$ is a finite extension of $k[t]$. The ring of integers of $k(t)$ is $O_{k(t)} = O_{k(t), (v_\infty)}$, where $v_\infty$ is the prime of $k(t)$ defined by $v_\infty(f/g) = \deg(g) - \deg(f)$. Furthermore, the ring of integers of $K$ is $O_{K,S_\infty}$, where $S_\infty$ is the set of all primes of $K$ that lie above $v_\infty$ (see B.1.22 of [37] or 1.2.2 and 3.2.6 of [38]), i.e. those primes that, when restricted to $k(t)$, coincide with $v_\infty$. The set $S_\infty$ is finite (B.1.11 of [37]), and each $p \in S_\infty$ is called a pole of $t$. Notice that if $S$ is an arbitrary set of primes of $K$ and $O_{K,S}$ contains $k[t]$, then $S_\infty \subset S$, by definition of $O_{K,S}$ and $S_\infty$.

We will also need the following:

**Remark 3.2.** The field of fractions of $O_{K,S}$ is $K$, for any number or global function field $K$ and any set of primes of $K$ (if $K$ is a function field, we require $S_\infty \subset S$). Indeed, by the previous remark $O_K \subseteq O_{K,S}$, so the field of fractions $F$ of $O_{K,S}$ contains the field of fractions of $O_K$, which is $K$. But since $O_{K,S} \subseteq K$, we have $F \subseteq K$, hence $F = K$.

**Proposition 3.3** (Propositions B.1.21 and B.1.27 of [37]; alternatively see Corollary 3.2.8 of [38]). Let $R$ be a subring of a number or a global function field $K$ such that $K$ is the field of fractions of $R$. Then $R$ is integrally closed in $K$ if and only if $R = O_{K,S}$, where $S$ is some set of primes of $K$.

We will also need the following result which is known in the folklore, though we could not find a reference. We provide a proof for completeness.

**Lemma 3.4.** Let $K$ be a number or a global function field and let $S$ be a set of primes of $K$. Suppose that $O_{K,S}$ is finitely generated as a ring. Then there exists a finite subset $S_0$ of $S$ such that $O_{K,S} = O_{K,S_0}$.
Proof. Let \( r \) be either \( \mathbb{Z} \) or a finite field \( \mathbb{F}_p \), depending on the characteristic of \( K \). Let \( X = \{x_1, \ldots, x_n\} \) be a finite generating set of \( O_{K,S} \). Let \( S_0 \) be the subset of \( S \) consisting in all primes \( p \) of \( K \) such that \( \text{ord}_p(x) \neq 0 \) for some \( x \in X \). It is well known that for any \( z \in K \) there are only finitely many primes \( p \) of \( K \) such that \( \text{ord}_p(z) \neq 0 \) (see B.1.18 of [37]). Therefore \( S_0 \) is finite. By assumption, for all \( z \in O_{K,S} \) there exists a polynomial \( q \in \mathfrak{r}[x_1, \ldots, x_n] \) such that \( z = q \) in \( O_{K,S} \). Using the axioms of non-archimedean valuations and the fact that \( \text{ord}_p(x) = 0 \) for all \( p \not\in S_0 \) and all \( x \in X \), we claim that \( \text{ord}_p(z) \geq 0 \) for all \( z \in O_{K,S} \) and all \( p \not\in S_0 \).

Indeed, writing \( q = \sum_i r_i m_i \) for some \( r_i \in r \) and some products \( m_i = x_{i_1} \ldots x_{i_{q_i}} \), we have \( \text{ord}_p(z) \geq \min \{ \text{ord}_p(r_i m_i) \mid i \} = \min \{ \text{ord}_p(r_i) \mid i \} \). But now \( \text{ord}_p(r_i) \geq 0 \) for all \( i \) because \( r_i \in r \) and \( r \) is either \( \mathbb{Z} \) (in which case \( p \) is a \( p \)-adic valuation, see B.1.15 in [37]) or \( \mathbb{F}_p \) (in which case \( \text{ord}_p(r_i) = 0 \) by Axiom 5 in the definition of non-archimedean valuations). This proves the claim. We thus obtain that \( O_{K,S} \subseteq O_{K,S_0} \). The opposite inclusion is immediate, since \( S_0 \subset S \).

\[ \square \]

4 From infinite finitely generated rings to rings of integers of number or global function fields

In this section we prove the main result of the paper, namely Theorem 4.14. We begin with the following auxiliary lemma.

Lemma 4.1. Let \( R \) be a Noetherian ring, and let \( A \subseteq R \) be a subring of \( R \) such that \( R \) is finitely generated as an \( A \)-module. Then \( R \) is \( e \)-interpretable in \( A \).

Proof. Let \( r_1, \ldots, r_n \) be a finite set of generators of \( R \) as an \( A \)-module, with \( n \) minimal, and let \( A^n \) be the direct product of \( n \) copies of \( A \), i.e. the free \( A \)-module of rank \( n \). Let \( \bar{r}_1, \ldots, \bar{r}_n \) be a base of \( A^n \) as an \( A \)-module. Consider the natural projection \( \phi : A^n \to R \) induced by sending \( \bar{r}_i \) to \( r_i \) for all \( i = 1, \ldots, n \). We will prove that \( \phi \) is an \( e \)-interpretation of \( R \) in \( A \). First note that \( \phi \) is surjective and that \( \phi^{-1}(R) = A^n \) is \( e \)-definable in \( A \).

We now check that the preimage of the equality relation of \( R \) is \( e \)-definable in \( A \). Since \( A \) is Noetherian, \( R \) is finitely presented as an \( A \)-module. In other words, \( R \) is isomorphic to \( A^n/N \) where \( N \) is a finitely generated \( A \)-submodule, say \( N = \langle w_1, \ldots, w_m \rangle \), where \( w_j = \sum_{i=1}^n a_{j,i} \bar{r}_i \) for some \( a_{j,i} \in A \) (\( j = 1, \ldots, m \)). The isomorphism \( R \cong A^n/N \) is obtained by sending each \( r_i \) to \( \bar{r}_i + N \). Any equality between two elements of \( R \) can be expressed as \( \sum_{i=1}^n x_i \bar{r}_i = \sum_{i=1}^n y_i \bar{r}_i \), where \( x_i, y_i \in A \) for all \( i \). This equality holds in \( R \) if and only if \( \sum_{i=1}^n x_i \bar{r}_i + N = \sum_{i=1}^n y_i \bar{r}_i + N \) is true in \( A^n/N \), which holds if and only if

\[
\sum_{i=1}^n x_i \bar{r}_i = \sum_{i=1}^n y_i \bar{r}_i + \sum_{j=1}^m z_j w_j
\]

holds in \( A^n \) for some variables \( z_1, \ldots, z_m \) taking values in \( A \). Replacing each \( w_j \) by \( \sum_{i=1}^n a_{j,i} \bar{r}_i \), and collecting terms with the same \( \bar{r}_i \), we conclude that

\[
\sum_{i=1}^n x_i \bar{r}_i = \sum_{i=1}^n y_i \bar{r}_i \quad \text{in } R \quad \text{if and only if} \quad \sum_{j=1}^m \left( x_i - y_i \right) = \sum_{j=1}^m z_j a_{j,i} \quad \text{in } A. \tag{1}
\]

The right-hand side of (1) is a finite system of equations on variables \( \{x_i, y_i \mid i = 1, \ldots, n\} \cup \{z_i \mid i = 1, \ldots, m\} \). This defines in \( A \) the preimage of equality in \( R \).

Next we prove that the preimage of the graph of the ring multiplication in \( R \) is \( e \)-definable in \( A \). For each \( 1 \leq i,j,k \leq n \) let \( b_{j,k,i} \in A \) be such that \( r_j r_k = \sum_{i=1}^m b_{j,k,i} \bar{r}_i \) in \( R \). Take any three
elements $x, y, z$ of $R$, and let $x_j, y_k, z_i$ be elements of $A$ such that $x = \sum_{j=1}^{n} x_j r_j$, $y = \sum_{k=1}^{n} y_k r_k$, and $z = \sum_{i=1}^{n} z_i r_i$. Then the equality in $R$

$$xy = \left( \sum_{j=1}^{n} x_j r_j \right) \left( \sum_{k=1}^{n} y_k r_k \right) = \sum_{i=1}^{n} z_i r_i = z$$

is equivalent to

$$\sum_{i=1}^{n} \left( \sum_{j,k=1}^{n} x_j y_k b_{j,k,i} \right) r_i = \sum_{i=1}^{n} z_i r_i. \quad (2)$$

By (1) we see that (2) holds if and only if a certain conjunction of equalities involving $x_i, y_i, z_i$, and some extra variables, holds in $A$. This yields an e-interpretation in $A$ of the multiplication operation of $R$.

Finally, e-interpretability of the addition operation of $R$ follows in a similar way using (1) and a generic expression for addition in $R$, $\sum_{i=1}^{n} x_i r_i + \sum_{i=1}^{n} y_i r_i = \sum_{i=1}^{n} (x_i + y_i) r_i$, where $x_i, y_i \in R$, $i = 1, \ldots, n$.

### 4.1 Subrings of number and global function fields

The goal of this section is to prove the next result. The necessary background can be found in Section 3. Upon completion of the present paper, we were informed that the positive characteristic part of this result can be derived in another, perhaps simpler, way using some of the techniques in [37], together with the results in [10]. In particular, this alternative method consists in e-interpreting in $R$ the field of fractions of the integral closure of $R$. We maintain our original writing here to maintain a similar style arguments for zero and positive characteristic cases.

**Theorem 4.2.** Let $R$ be a finitely generated integral domain whose field of fractions $K$ is a number or a global function field. In the case that $K$ is a global function field of characteristic $p$, assume that $R$ contains $\mathbb{F}_p[t]$. Then the ring of integers of $K$ is e-interpretable in $R$. Furthermore, if $K$ has positive characteristic $p$, then $\mathbb{F}_p[t]$ is e-interpretable in $R$, and the Diophantine problem $D(R)$ is undecidable.

To obtain the proof we combine the techniques developed in the previous sections with some known results. Most of the known results we use can be found in Shlapentokh’s book [37]. We will follow the notation and terminology there closely. The proof consists of two steps. First we prove that $O_K$ is e-interpretable in $O_{K,S}$ for any suitable finite set of primes (see Corollary 4.4), and then we prove that there exists such $S$ so that $O_{K,S}$ is e-interpretable in $R$. We begin with the following definition. As we will see, it provides an alternative notion of e-definability.

**Definition 4.3** (Definition 2.1.5 [37]). Let $R_1$ and $R_2$ be two integral domains with fields of fractions $F_1$ and $F_2$, respectively. Assume that neither $F_1$ nor $F_2$ is algebraically closed. Let $F$ be a finite extension of $F_2$ such that $F_1 \subseteq F$. Further, assume that for some integers $k$ and $m$ there exists a base $\{\omega_1, \ldots, \omega_k\}$ of $F$ over $F_2$ and a polynomial $f(a_1, \ldots, a_k, b, x_1, \ldots, x_m)$ with coefficients in $R_2$ such that $f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0$ implies that $b \neq 0$, and

$$R_1 = \{ \sum_{i=1}^{k} t_i \omega_i \mid \exists a_1, \ldots, a_k, b, x_1, \ldots, x_m \in R_2, bt_1 = a_1, \ldots, bt_k = a_k, f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \}.$$ 

Then we say that $R_1$ is Dioph-generated over $R_2$. 

10
The next definition will be used only in an auxiliary manner in Lemma 4.5

**Definition 4.4** (Definition 2.1.1 [[37]].) Let $R$ be an integral domain with field of fractions $F$. Let $k, m$ be positive integers and let $A \subseteq F^k$ be some subset of $F^k$. Assume further that there exists a polynomial $f(a_1, \ldots, a_k, b, x_1, \ldots, x_m)$ with coefficients in $R$ such that, for all $a_1, \ldots, a_k, b, x_1, \ldots, x_m \in R$, we have $f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0 \Rightarrow b \neq 0$, and

$$A = \{(t_1, \ldots, t_k) \in F^k \mid \exists a_1, \ldots, a_k, b, x_1, \ldots, x_m \in R, bt_1 = a_1, \ldots, bt_k = a_k, f(a_1, \ldots, a_k, b, x_1, \ldots, x_m) = 0\}.$$ 

Then $A$ is said to be field-Diophantine over $R$.

Next we provide a condition for Dioph-generation to imply e-definability.

**Lemma 4.5.** Let $R_1, R_2$ be integral domains with $R_1 \subseteq R_2$. Then $R_1$ is Dioph-generated over $R_2$ if and only if $R_1$ admits a 1-dimensional definition in $R_2$.

**Proof.** Suppose $R_1$ is Dioph-generated over $R_2$. By Corollary 2.1.10 in [[37]], $R_1$ is field-Diophantine over $R_2$. Now by Lemma 2.1.2 in [[37]] (taking $A$ to be $R_1$, $R$ to be $R_2$, and $k = 1$) we have that $R_1$ is e-definable in $R_2$ (note that in [[37]], an e-definition is called Diophantine definition, see 1.2.1 [[37]]). Moreover, from the proof of Lemma 2.1.2 in [[37]] we see immediately that the e-definition is 1-dimensional.

Now assume $R_1$ admits a 1-dimensional e-definition in $R_2$. Then again by Lemma 2.1.2 in [[37]] we have that $R_1$ is field-Diophantine over $R_2$. Moreover, the proof of this lemma shows that $R_1$ is field-Diophantine over $R_2$ taking $k = 1$ in the notation of Definition 4.4 (and taking $A$ to be $R_1$, and $R$ to be $R_2$). We now claim that $R_1$ is Dioph-generated over $R_2$. Indeed, it suffices to take, following the notation in Definition 4.5, $F = F_2$, the basis $\{1\}$ of $F$ over $F_2$, and the polynomial $f$ from the field-Diophantine definition of $R_1$ in $R_2$. 

The next statement was originally proved by Shlapentokh in [[35]].

**Theorem 4.6** (10.6.2 [[37]], alternatively see [[35]].) Suppose that $K$ is a finite extension of $\F_p(t)$ for some prime $p$ and some transcendental element $t$, and let $O_K$ be its ring of integers. Then $\F_p[t]$ is Dioph-generated over $O_K$.

We quickly obtain the same statement for e-definability:

**Corollary 4.7.** Under the assumptions of Theorem 4.6, $\F_p[t]$ is e-interpretable in $O_K$, and $\mathcal{D}(O_K)$ is undecidable.

**Proof.** By Lemma 4.5 $\F_p[t]$ and Theorem 4.6 is e-definable in $O_K$. This in particular implies that $\F_p[t]$ is e-interpretable in $O_K$ since $\F_p[t] \subseteq O_K$ (see Remark 2.10). Now $\mathcal{D}(O_K)$ is undecidable because $\mathcal{D}(\F_p[t])$ is reducible to $\mathcal{D}(O_K)$ by Proposition 2.8 and $\mathcal{D}(\F_p[t])$ is undecidable by 6.

We will also use the fact, stated below, that “integrality at a prime” (following the terminology in [[37]]) is e-definable in a number or global function field. For global function fields this was proved by Shlapentokh in [[36]]. For number fields this can be found in [[22]]. See also [[12]] or Theorems 4.2.4 and 4.3.4 of [[37]] for a unified account of these results.

**Theorem 4.8** (E-definability of integrality at a prime for number or global function fields). Let $K$ be a number or a global function field, let $p$ be a prime of $K$, and let $S$ be the set of all primes of $K$ but $p$. Then the ring of $S$-integers $O_{K,S} = \{x \in K \mid \text{ord}_p(x) \geq 0\}$ is e-definable in $K$ by a 1-dimensional definition.
As a consequence we have:

**Corollary 4.9** ([37]). Let $O_K$ be the ring of integers of a number or global function field $K$. Let $S$ be a finite set of primes of $K$. In the case that $K$ is a global function field, say a finite extension of $\mathbb{F}_p(t)$, assume further that $S$ contains all the poles of $t$, i.e. that $S_\infty \subseteq S$ (see Remark 2.6). Then $O_K$ is $e$-definable in $O_{K,S}$.

This result is stated in Subsections 2.3.2 and 2.3.3 of [37] for number fields and global function fields, respectively, though we could not find full direct proofs. In any case, it follows quickly from several results of the cited reference, as we see now.

**Proof of Corollary 4.9.** We connect some results from Shlapentokh’s book [37] while following its terminology and numeration.

Denote the complement of a set of primes $W$ by $W^c$ (we take the complement in the set of all non-archimedean primes). Suppose that $K$ is a number field and that we know that $O_{K,S^c}$ is Dioph-generated over $O_{K,S}$. In 2.19 in [37] it is seen that the intersection of finitely many subrings of an integral domain $R$, each Dioph-generated over $R$, is still Dioph-generated over $R$. Hence $O_K = O_{K,\emptyset} = O_{K,S^c} \cap O_{K,S}$ is Dioph-generated over $O_{K,S}$. Since $O_K \subseteq O_{K,S}$, we have then that $O_K$ is $e$-definable in $O_{K,S}$ by Lemma 4.5. Therefore, $O_K$ is $e$-interpretable in $O_{K,S}$ (see Remark 2.10).

Suppose that $K$ is a global function. Recall that in this case $O_K = O_{K,S_\infty}$ (see Remark 3.1). Assume that we know that $O_{K,(S,S_\infty)}^\circ$ is Dioph-generated over $O_{K,S}$. Then by similar arguments as before, $O_K = O_{K,S_\infty} = O_{K,(S,S_\infty)}^\circ \cap O_{K,S}$, hence $O_K$ is Dioph-generated over $O_{K,S}$. Since $O_K = O_{K,S_\infty} \subseteq O_{K,S}$ because $S_\infty \subseteq S$, we obtain again that $O_K$ is $e$-interpretable in $O_{K,S}$.

It remains to prove that $O_{K,W^c}$ is Dioph-generated over $O_{K,S}$ for any finite set of primes $W$ of $K$. Observe that

$$O_{K,W^c} = \{ x \in K \mid \text{ord}_p(x) \geq 0 \forall p \in W \} = \bigcap_{p \in W} \{ x \in K \mid \text{ord}_p(x) \geq 0 \} = \bigcap_{p \in W} O_{K,(p)}^\circ.$$  

Since $W$ is finite, this intersection is finite, and since each ring in this intersection admits a 1-dimensional $e$-definition in $K$ by the previous Theorem 4.8, we obtain that also $O_{K,W^c}$ admits a 1-dimensional $e$-definition in $K$ (see Remark 2.6). By Lemma 4.5, $O_{K,W^c}$ is Dioph-generated over $K$. Now Lemma 2.2.2 in [37] states that the field of fractions of an integral domain $D$ is Dioph-generated over $D$, provided that the set of non-zero elements of $D$ is $e$-definable in $D$. In Proposition 2.2.4 in [37] it is proved that $O_{K,U}$ satisfies this last condition for any set of primes $U$ (recall that 1-dimensional $e$-definability, used in this paper, and Diophantine definability, used in [37], are equivalent terms when used on integral domains whose field of fractions is not algebraically closed). As discussed in Section 3 the field of fractions of $O_{K,S}$ is $K$, and therefore $K$ is Dioph-generated over $O_{K,S}$, and by transitivity of Dioph-geneneration (Theorem 2.1.15 in [37]), $O_{K,S^c}$ is Dioph-generated over $O_{K,S}$.

We will also need the following auxiliary result.

**Lemma 4.10** (See, for example, Corollary 4.6.5 of [18]). Let $R$ be a finitely generated integral domain, and let $K$ be a finite extension of the field of fractions of $R$. Then the integral closure $\overline{R}$ of $R$ in $F$ is finitely generated as a $R$-module.

We can now prove the main theorem of this section.
Proof of Theorem 4.2: Let $\bar{R}$ be the integral closure of $R$ in $K$. The field of fractions of $\bar{R}$ is $K$ itself, and hence by Proposition 3.3 $\bar{R} = O_{K,S}$ for some set $S$ of primes of $K$. Moreover by Lemma 4.10 $\bar{R}$ is finitely generated as an $R$-module, hence $\bar{R}$ is finitely generated as a ring, because $\bar{R}$ is. Therefore Lemma 3.1 yields that we can assume $S$ to be finite. Moreover, Lemma 4.11 implies that $\bar{R}$ is $e$-interpretable in $R$. In the case that $K$ is a finite extension of $\mathbb{F}_p(t)$, we have by hypothesis that $\mathbb{F}_p[t] \subseteq R$, and so $\mathbb{F}_p[t] \subseteq O_K \subseteq \bar{R} = O_{K,S}$. By Remark 3.4 if $K$ is a global function field, then $\bar{R}$ contains all the poles of $t$ in $K$. Hence, independently of whether $K$ is a number or global function field, Corollary 4.7 yields that the ring of integers $O_K$ of $K$ is $e$-interpretable in $O_{K,S} = \bar{R}$. By transitivity $O_K$ is $e$-interpretable in $R$. The last part of the theorem is a consequence of Corollary 4.7.

\[\square\]

4.2 Finitely generated commutative rings

In this subsection we prove the main result of the paper, namely Theorem 4.14. We first discuss some necessary definitions.

Recall that the characteristic of a ring with unity is the minimum positive integer $n$ such that $1 + \ldots + 1 = 0$. We also need the notion of rank of an abelian group, and by extension of a ring. This is defined in a variety of manners throughout the literature. Here we follow [14].

Definition 4.11 ([14]). The rank of an abelian group $A$ is the maximal number of nonzero elements $a_1, \ldots, a_n \in A$ such that whenever $\alpha_1 a_1 + \ldots + \alpha_n a_n = 0$ for some integers $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$, then $\alpha_i a_i = 0$ for all $i = 1, \ldots, n$.

The rank of a ring is defined as the rank of $R$ seen as an abelian group (i.e. forgetting its multiplication operation).

Remark 4.12. Let $R$ be an integral domain. If $R$ has zero characteristic then the rank of $R$ coincides with the dimension of $R$ seen as a $\mathbb{Z}$-module, which is the maximum number of $\mathbb{Z}$-linearly independent elements in $R$, i.e. elements $a_1, \ldots, a_r$ such that whenever $\sum_{i=1}^r \alpha_i a_i = 0$ for some integers $\alpha_i$, we have $\alpha_i = 0$ for all $i = 1, \ldots, r$. If $R$ has positive characteristic $p > 0$, then the rank of $R$ is the dimension of $R$ as a $\mathbb{F}_p$-vector space.

Hence the notion of rank generalizes dimension of $\mathbb{Z}$-modules and of vector spaces. As an example we have that the rank of the non-integral domain $\mathbb{Z}[x]/(px)$ is infinite. However, note that $R$ has only one linearly independent element over $\mathbb{Z}$, hence $R$ seen as a $\mathbb{Z}$-module has dimension 1. On the other hand, $R$ does not admit the structure of a vector space over a finite field. Another illustrative example is given by the integral domain $\mathbb{Z}[\frac{1}{2}]$, which has rank 1.

In the following we summarize some properties of rank that we will need:

Remark 4.13. Let $R$ be a countable commutative ring of finite rank and positive characteristic $k$. Then $R$ is finite: indeed, this follows from one of Prufer theorems, as in this case $R$ is a bounded abelian group since $kR = 0$ (see Theorem 5.2 in [14]).

Furthermore, if $1 \to R_1 \to R_2 \to R_3 \to 1$ is a short exact sequence of rings, then the rank of $R_2$ is at least the rank of $R_1$, and at most the rank of $R_1$ plus the rank of $R_3$ (see Exercise 3, Chapter 3.4 in [14]). Finally, if $A$ is a finitely generated $R$-module, and $R$ has finite rank, then $A$ as an abelian group also has finite rank (this follows from the fact that an abelian group $B$ has rank $k$ if and only if $k$ is the largest integer such that $B$ contains a subgroup $B_k$ which is the direct sum of $k$ cyclic groups, and for all $b \in B$ there exists an integer $n \neq 0$ such that $nb \in B_0$).

We are ready to state and prove the main result of the paper.

Theorem 4.14. Let $R$ be an infinite finitely generated associative commutative unitary ring. Then there exists a ring of integers $O_K$ of a number or a global function field $K$ such that $O_K$
is e-interpretable in $R$, and $\mathcal{D}(O_K)$ is polynomial-time reducible to $\mathcal{D}(R)$. Moreover, one of the following holds:

1. If $R$ has positive characteristic $\kappa > 0$, then the following holds: $O_K$ is the ring of integers of a global function field; the ring of polynomials $\mathbb{F}_p[t]$ is e-interpretable in $R$ for some transcendental element $t$ and some prime integer $p$; and $\mathcal{D}(R)$ is undecidable.

2. If $R$ has zero characteristic and it has infinite rank then the same conclusions as above hold: $O_K$ is the ring of integers of a global function field; the ring of polynomials $\mathbb{F}_p[t]$ is e-interpretable in $R$ for some $t$ and $p$; and $\mathcal{D}(R)$ is undecidable.

3. If $R$ has zero characteristic and it has finite rank $\kappa$, then $O_K$ is a ring of algebraic integers, and $\mathcal{D}(R)$ is undecidable provided that $\mathcal{D}(O_K)$ is undecidable. Additionally, $K$ is a field extension of $\mathbb{Q}$ of degree at most $\kappa$.

This theorem is proved by reducing it to the case when $R$ is a subring of a number or global function field and then applying the main theorem of the previous subsection. To make such a reduction we follow some ideas from Noskov’s paper [28], where the author proved that any infinite finitely generated ring has undecidable first-order theory.

**Remark 4.15.** Upon completion of the paper, it was brought to our attention that, if one restricts to integral domains, then Items 1 and 2 of the main Theorem 4.14 can be derived in a perhaps simpler way by combining techniques from [37] and [10].

**Proof of Theorem 4.14.** Throughout the proof we will use the facts that e-interpretability is transitive, by Proposition 2.7 and that the quotient by any ideal of a Noetherian ring $R$ is e-interpretable in $R$, by Lemma 2.5. More precisely, we successively replace $R$ by appropriate quotients of $R$ until obtaining an infinite finitely generated subring $R'$ of a number or a global function field $K$. We then use Theorem 4.2 from the previous section, and obtain first an e-interpretation of $O_K$ in $R'$ for some number or global function field $K$, and then an e-interpretation in $R$ by the aforementioned transitivity property and Lemma 2.5. Moreover, since $R'$ is a quotient of $R$, Items 1 and 3 of the statement follow rather quickly. Item 2, the case when $R$ has infinite rank and zero characteristic, requires an extra intermediate step where a suitable quotient of the form $R/pR$ is found, for some prime $p$.

**Step 1: Reduction to integral domains.** Let $R$ be a finitely generated infinite commutative ring. Suppose first that $R$ is not an integral domain. We will find a quotient of $R$ which is an infinite finitely generated integral domain and which is e-interpretable in $R$. Let $N = \{x \in R \mid x^m = 0 \text{ for some } m \in \mathbb{N}\}$ be the nilradical of $R$, i.e. the ideal formed by all nilpotent elements of $R$. Equivalently, $N$ is the intersection of all minimal prime nonzero ideals of $R$. There are finitely many such ideals $q_1, \ldots, q_n$ in a Noetherian ring (see Theorem 87 of [19]), hence $N = q_1 \cap \cdots \cap q_n$. We claim that $n \geq 1$. Indeed, $R$ contains at least one nonzero maximal ideal, since otherwise $R$ would be a finitely generated ring which is a field, and so $R$ would be finite (see Exercise 6 in Chapter 7 of [1]). Since maximal ideals are prime, we have $n \geq 1$.

We now claim that there exists $i$ such that $R/q_i$ is infinite. We also claim that if $R$ has infinite rank, then there exists $i$ such that $R/q_i$ has infinite rank (in particular, $R/q_i$ is infinite by Remark 4.13). Indeed, note first that $R/N$ admits an embedding into the direct sum $R/q_1 \oplus \cdots \oplus R/q_n$ via the well-defined map $r + N \mapsto (r + q_1) \oplus \cdots \oplus (r + q_n)$. Hence, if all $R/q_i$ are finite, then $R/N$ is finite. If all $R/q_i$ have finite rank, then also $R/N$ has finite rank by Remark 4.13.

Now, the $R/N$-module $N^i/N^{i+1}$ is finitely generated as a $R/N$-module (since it is finitely generated as a ring) for all $i = 1, \ldots, n - 1$. It follows that if $R/N$ is finite then $N^i/N^{i+1}$ is also finite. The same is true for the rank: if $R/N$ has finite rank, then $N^i/N^{i+1}$ also has finite rank,
Step 3: Reduction to Krull dimension 1. From now on we assume that either the hypothesis of Item 1 or of Item 3 of the statement of the theorem hold. Hence $R$ is an infinite finitely generated integral domain either of finite rank and zero characteristic, or of infinite rank and positive characteristic. The Krull dimension of $R$ is the largest integer $k$ for which there exists a proper ascending chain of prime ideals $p_0 < p_1 < \ldots < p_k < R$. Such $k$ is finite under our assumptions (see Section 8.2.1 of [4]). It is not possible that $k = 0$, since in this case $R$...
would be a finitely generated Artinian domain (see Proposition 9.1 in [9]), and thus a finitely generated field (see Proposition 8.30 of [2]), a contradiction because, as referred to earlier, a finitely generated ring which is a field is necessarily finite. Hence \( k \geq 1 \). We may assume that \( k = 1 \), since if \( k \geq 2 \) then \( R/p_{k-1} \) is a finitely generated integral domain, \( \epsilon \)-interpretable in \( R \), and of Krull dimension 1. The latter implies that \( R/p_{k-1} \) is infinite. This implies that \( R/p_{k-1} \) has finite rank and zero characteristic, or infinite rank and positive characteristic, depending on which of these two properties \( R \) satisfies, respectively.

**Step 4: Reduction to a subring of a number or a global function field.** Assume \( R \) is a finitely generated infinite integral domain of Krull dimension 1, either of infinite rank and positive characteristic, or of finite rank and zero characteristic. We claim that one of the following hold:

1. \( R \) is a subring of a number field (if \( R \) has zero characteristic). This is proved in 2.2 of [28].

2. There exists a prime integer \( p \) and a transcendental element \( t \in R \) over \( \mathbb{F}_p \) such that \( \mathbb{F}_p[t] \subseteq R \) and \( R \) is integral over \( \mathbb{F}_p[t] \). It follows that \( R \) is a subring of a finite field extension \( K \) of \( \mathbb{F}_p(t) \), with \( \mathbb{F}_p[t] \subseteq R \). In particular, \( R \) has positive characteristic.

This follows from the Noether normalization lemma (Theorem A1 of Chapter 8.2 in [9]), which states that any finitely generated \( k \)-algebra is a finitely generated module over \( k[y_1, \ldots, y_d] \), where \( k \) is any field and \( d \) is the Krull dimension of the algebra. Hence in our case \( R \) is a finitely generated \( \mathbb{F}_p[t] \)-module, and so it is integral over \( \mathbb{F}_p[t] \).

**Step 5: Reduction to rings of integers.** Assume \( R \) satisfies Item 1 or Item 2 of the previous step. Then the field of fractions \( K \) of \( R \) is a number or a global function field. Since \( R \) is finitely generated, Theorem 4.2 implies that the ring of integers \( O_K \) of \( K \) is \( \epsilon \)-interpretable in \( R \) (note that Item 2 above grants us the requirement that \( R \) contains \( \mathbb{F}_p[t] \)). By transitivity (Proposition 2.2, \( O_K \) is \( \epsilon \)-interpretable in \( R \), and therefore \( D(O_K) \) is polynomial-time reducible to \( D(R) \) (Proposition 2.2).

If \( R \) has finite rank \( n \), then it has zero characteristic, because it is infinite. Hence, \( R \) is a subring of a number field, and \( O_K \) is a ring of algebraic integers. Moreover, since \( R \) as a \( \mathbb{Z} \)-module has dimension \( n \), we have that \( K \) is an \( n \)-dimensional \( \mathbb{Q} \)-vector space, i.e. \( K \) is field extension of \( \mathbb{Q} \) of degree \( n \).

If \( R \) has characteristic \( p > 0 \), then Theorem 4.2 and transitivity of \( \epsilon \)-interpretations and reduction of Diophantine problems (Propositions 2.3 and 2.5) yield that \( \mathbb{F}_p[t] \) is \( \epsilon \)-interpretable in \( R \), and that \( D(R) \) is undecidable.

**Step 6: Conclusion.** Let \( R \) be the ring given initially in the statement of the theorem, and let \( O_K \) be the ring of integers obtained in the previous Step 5. As discussed at the beginning of the proof, \( O_K \) is \( \epsilon \)-interpretable in \( R \) and \( D(O_K) \) is reducible to \( R \). Moreover, we have, following each one of the previous Steps 1 through 5, that each one of Items 1, 2, and 3 in the statement hold: indeed, Item 2 reduces to Item 1, and in the rest of cases the fact that \( R \) has zero or positive characteristic does not change throughout all steps. Hence the Items 1 and 3 hold due to Step 5.

We now derive some consequences of Theorem 4.14.

**Theorem 4.16.** Let \( R \) be an infinite associative commutative unitary ring of rank at most 2. Then the Diophantine problem \( D(R) \) of \( R \) is undecidable.

**Proof.** Note that \( R \) has zero characteristic, since otherwise it would be finite. Let \( O_K \) be the ring of integers given by Theorem 4.14 so that \( O_K \) is \( \epsilon \)-interpretable in \( R \). By this same theorem, \( K \) is a field extension of \( \mathbb{Q} \) of degree at most \( 2 \). By [9], we have that the Diophantine problem in
$O_K$ is undecidable, and hence the Diophantine problem of $R$ is also undecidable by Proposition 2.8.

The following is a direct consequence of Theorem 4.14.

**Theorem 4.17.** Assume that the Diophantine problem is undecidable in any ring of algebraic integers. Then the Diophantine problem is undecidable in any finitely generated infinite associative commutative unitary ring.

## 5 Acknowledgements

We are grateful to Alexandra Shlapentokh for insightful remarks.
This work was supported by the Mathematical Center in Akademgorodok.
The first named author was supported by the ERC grant PCG-336983, by the Basque Government grant IT974-16, and by the Ministry of Economy, Industry and Competitiveness of the Spanish Government Grant MTM2017-86802-P.

## References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] P. L. Clark. *Commutative algebra*, 2015. Available at [http://math.uga.edu/~pete/integral.pdf](http://math.uga.edu/~pete/integral.pdf).

[3] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Annals of Mathematics*, 74(3):425–436, 1961.

[4] J. Denef. Hilbert’s tenth problem for quadratic rings. *Proceedings of the American Mathematical Society*, 48(1):214–220, 1975.

[5] J. Denef. The Diophantine problem for polynomial rings and fields of rational functions. *Trans. Amer. Math. Soc.* 242, pages 391–399, 1978.

[6] J. Denef. The Diophantine problem for polynomial rings of positive characteristic. In Maurice Boffa, Dirkvan Dalen, and Kenneth Mcaloon, editors, *Logic Colloquium ’78*, volume 97 of *Studies in Logic and the Foundations of Mathematics*, pages 131 – 145. Elsevier, 1979.

[7] J. Denef and L. Lipshitz. Diophantine sets over some rings of algebraic integers. *Journal of the London Mathematical Society*, s2-18(3):385–391, 1978.

[8] M. Duchin, H. Liang, and M. Shapiro. Equations in nilpotent groups. *Proc. Amer. Math. Soc.*, 143(11):4723–4731, 2015.

[9] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995.

[10] K. Eisenträger and A. Shlapentokh. Hilbert’s tenth problem over function fields of positive characteristic not containing the algebraic closure of a finite field. *Journal of the European Mathematical Society*, 19(7):2103–2138, January 2017.

[11] K. Eisenträger. Hilbert’s Tenth Problem for algebraic function fields of characteristic 2. *Pacific Journal of Mathematics*, 210, 2002.
[12] K. Eisenträger. Integrality at a prime for global fields and the perfect closure of global fields of characteristic $p^2/2$. *Journal of Number Theory*, 114(1):170 – 181, 2005.

[13] M. D. Fried and M. Jarden. *Field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1986.

[14] L. Fuchs, J.P. Kahane, A.P. Robertson, and S. Ulam. *Abelian Groups*. ISSN. Elsevier Science, 2014.

[15] N. Garcia-Fritz and H. Pasten. Towards Hilbert’s Tenth Problem for rings of integers through Iwasawa theory and Heegner points. *Mathematische Annalen*, 377(3):989–1013, 2020.

[16] A. Garreta, A. Miasnikov, and D. Ovchinnikov. Diophantine problems in solvable groups. *Bulletin of Mathematical Sciences*, 10(01):2050005, 2020.

[17] W. Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993.

[18] C. Huneke and I. Swanson. *Integral Closure of Ideals, Rings, and Modules*. Number v. 13 in Integral closure of ideals, rings, and modules. Cambridge University Press, 2006.

[19] I. Kaplansky. *Commutative Rings*. Chicago lectures in mathematics. University of Chicago Press, 1974.

[20] O. Kharlampovich and A. Miasnikov. Undecidability of equations in free Lie algebras. *Transactions of the American Mathematical Society*, 08 2017.

[21] O. Kharlampovich and A. Myasnikov. Equations in algebras. *International Journal of Algebra and Computation*, 28(08):1517–1533, 2018.

[22] K. H. Kim and F. W. Roush. An approach to rational Diophantine undecidability. In *Proceedings of Asian Mathematical Conference*, page 242–248, River Edge, NJ, 1990. World Sci. Publ.

[23] K. H. Kim and F. W. Roush. Diophantine undecidability of $c(t1, t2)$. *Journal of Algebra*, 150(1):35 – 44, 1992.

[24] J. Koenigsmann. *Undecidability in Number Theory*, pages 159–195. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[25] D. Marker. *Model Theory : An Introduction*. Graduate Texts in Mathematics. Springer New York, 2002.

[26] Y. V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[27] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. *Inventiones mathematicae*, 181(3):541–575, 2010.

[28] G. A. Noskov. Elementary theory of a finitely generated commutative ring. *Mathematical notes of the Academy of Sciences of the USSR*, 33(1):12–15, 1983.

[29] T. Pheidas and K. Zahidi. Undecidability of existential theories of rings and fields: A survey. *Contemporary Mathematics*, 270, 49-106, 2000.
[30] B. Poonen. Hilbert’s tenth problem and mazur’s conjecture for large subrings of \( \mathbb{Q} \). Journal of the American Mathematical Society, 16(4):981–990, 2003.

[31] B. Poonen. Hilbert’s Tenth Problem over rings of number-theoretic interest. http://math.mit.edu/~poonen/papers/aws2003.pdf, 2003. Notes for Arizona Winter School on “Number theory and logic”.

[32] V. A. Roman’kov. Unsolvability of the endomorphic reducibility problem in free nilpotent groups and in free rings. Algebra and Logic, 16(4):310–320, 1977.

[33] H. N. Shapiro and A. Shlapentokh. Diophantine relationships between algebraic number fields. Communications on Pure and Applied Mathematics, 42(8):1113–1122, 1989.

[34] A. Shlapentokh. Hilbert’s Tenth Problem for rings of algebraic functions in one variable over fields of constants of positive characteristic. Transactions of the American Mathematical Society, 333(1):275–298, 1992.

[35] A. Shlapentokh. Diophantine relations between rings of \( S \)-integers of fields of algebraic functions in one variable over constant fields of positive characteristic. The Journal of Symbolic Logic, 58(1):158–192, 1993.

[36] A. Shlapentokh. Diophantine classes of holomorphy rings of global fields. Journal of Algebra, 169(1):139 – 175, 1994.

[37] A. Shlapentokh. Hilbert’s Tenth Problem: Diophantine Classes and Extensions to Global Fields. New Mathematical Monographs. Cambridge University Press, 2007.

[38] H. Stichtenoth. Algebraic Function Fields and Codes. Springer Publishing Company, Incorporated, 2nd edition, 2008.