Studying the Diophantine problem in finitely generated rings and algebras via bilinear maps

Albert Garreta* Alexei Miasnikov† Denis Ovchinnikov‡

October 26, 2022

Abstract

We study systems of polynomial equations in several classes of finitely generated rings and algebras. For each ring R (or algebra) in one of these classes 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 Karp-reducible to the same problem in R. In several cases we further obtain an interpretation by systems of equations of the ring $\mathbb{F}_p[t]$ in R, which implies that the Diophantine problem in R is undecidable in this case. Otherwise, the ring 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.

Some of the classes of finitely generated rings studied in this paper are the following: all associative, commutative, non-unitary rings (a similar statement for the unitary case was obtained by Eisentraeger); all possibly non-associative, non-commutative non-unitary rings that are finitely generated as an abelian group; and several classes of finitely generated non-commutative rings. Analogous statements are obtained for algebras over finitely generated associative commutative unitary rings.

Another contribution of the paper is the technique by which the aforementioned results are obtained. More precisely, we show that given a bilinear map $f : A \times B \to C$ between finitely generated abelian groups (or modules), under some mild assumptions, there exists a certain ring (or algebra) R with nice properties which is interpretable by systems of equations in the multi-sorted structure $(A, B, C; f)$. This result fits nicely the study of rings (or algebras) since the multiplication operation of such structures can be seen as a bilinear map between abelian groups (or modules). This result is potentially applicable in many other settings, such as in the area of group theory, see for example [11].

Contents

*Basque Center of Applied Mathematics, Bilbao, Spain

†Stevens Institute of Technology, NJ, USA

‡Stevens Institute of Technology, NJ, USA

1 Introduction

In this paper, we study systems of polynomial equations in different classes of rings and algebras. For each R in one of these classes we interpret by systems of equations a ring of integers O of a number field or a global function field (i.e. O is the integral closure of $\mathbb{Z}$ or $\mathbb{F}_p[t]$ in a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$, respectively). In particular, this reduces the Diophantine problem (decidability of systems of polynomial equations) in O to the same problem in R. Hence if $\mathcal{D}(O)$ is undecidable, then also $\mathcal{D}(R)$ is undecidable. It is known that $\mathcal{D}(O)$ is undecidable if O has positive characteristic [36], and it is conjectured to be also undecidable if otherwise O is a ring of algebraic integers [5, 30].

A *number field* is a finite field extension of $\mathbb{Q}$. A *global function field* is a finite extension of $\mathbb{F}_p(t)$, for some prime p. A ring of integers of a number field is called a *ring of algebraic integers*.

The Diophantine problem in a structure R, denoted $\mathcal{D}(R)$, asks whether there exists an algorithm that, given a *system* of equations S with coefficients in R, determines if S has a solution in R or not. 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 [23] building on the work of Davis, Putnam, and Robinson [4]. 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, where it remains widely open. As mentioned above, a long-standing conjecture [5, 30] 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 [10, 34, 37], and it has been shown to be true assuming the Safarevich-Tate conjecture [24].

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 [35] showed that $\mathbb{F}_p[t]$ is Diophantine in any such ring O, and consequently that $\mathcal{D}(O)$ is undecidable.

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 [31]); the rational functions $\mathbb{C}(t)$ (even though $\mathcal{D}(\mathbb{C}(t_1, t_2))$ is undecidable [20]); and the field of Laurent series $\mathbb{F}_p((t))$. We refer to [21, 30, 32, 37] for further information and surveys of results in this direction.

Eisentraeger [7, Theorem 7.1] proved the general result that for any finitely generated associative commutative unitary ring R, the Diophantine problem $\mathcal{D}(R)$ is undecidable conditionally on the conjecture that $\mathcal{D}(O)$ is undecidable for any ring of algebraic integers. Moreover, she showed that $\mathcal{D}(R)$ is undecidable in many cases, see [7, Theorem 7.1] or Theorem 2.14 in this paper.

Regarding non-commutative rings, Romankov [33] 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) [15, 17]. In all these results the field k is arbitrary, possibly with decidable $\mathcal{D}(k)$.

We proceed to describe the results obtained in the present work. In this paper we convene that *all rings and algebras are possibly non-associative, non-commutative, and non-unitary* unless stated otherwise. A ring or algebra R is called *unitary* if and only if it has a multiplicative identity. Algebras will over be considered over associtative commutative unitary ring, and we fix Λ to denote such ring. Given a Λ-algebra L, we let L^2 be the Λ-module generated by all products of two elements of L. In this paper the notion of ring is equivalent to the notion of $\mathbb{Z}$-algebra.

he main tool used in this paper is the so-called *interpretability by systems of equations* (or *e-interpretability*), which is a variation of the classical notion of the first-order interpretability, where instead of arbitrary first-order formulas, finite systems of equations are used as the interpreting formulas (see Definition 2.5 for details). The main relevant property of such interpretations is that if A_1 is e-interpretable in A_2 then $\mathcal{D}(A_1)$ is Karp-reducible to $\mathcal{D}(A_2)$ by a polynomial time many-one reduction (Karp reductions). All reductions mentioned in this paper are of this type.

In number theoretic terms, an *interpretation by systems of equations* is roughly a Diophantine definition up to a Diophantine equivalence relation. Here Diophantine definitions are considered using systems of equations, as opposed to single equations. We convene that all systems of equations and all e-interpretations allow the use of any constant elements of the structures at hand, not necessarily in the signature. See Subsections 2.1.3, 2.1.2 and 2.3 for further comments on these matters.

One of the main results of the paper is the following. By $\mathcal{L}_{ring}$ we refer to the language of rings with constants. We write $(R;\mathcal{L})$ to indicate that a structure R is considered with a language $\mathcal{L}$.

Theorem 1.1. *Let A be a ring (possibly non-associative, non-commutative, and non-unitary). Assume that A is finitely generated as an abelian group, and that A^2 is infinite. Then there exists a ring of algebraic integers O such that $(O;\mathcal{L}_{ring})$ is e-interpretable (see below) in $(A;\mathcal{L}_{ring})$, and $\mathcal{D}(O;\mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(A,\mathcal{L}_{ring})$. If otherwise A^2 is finite, then $\mathcal{D}(R;\mathcal{L}_{ring})$ is decidable.*

Theorem 1.1 is further generalized to algebras. The language of Λ-modules $\mathcal{L}_{mod}$, or of Λ-algebras $\mathcal{L}_{alg}$, consists in the usual language of groups $\mathcal{L}_{group}$ or of rings $\mathcal{L}_{ring}$, respectively, together with unary functions $\{\cdot_\lambda \mid \lambda \in \Lambda\}$ representing multiplication by elements of Λ (see Subsection 2.3).

Theorem 1.2. *Let R be a (possibly non-associative, non-commutative, and non-unitary) algebra over a finitely generated associative commutative unitary ring Λ. Suppose that R is finitely generated as a Λ-module. Then if, $R^2 = \langle\{xy \mid x \in R, y \in R\}\rangle_\Lambda$ is infinite, there exists a ring of integers O of a number field or a global function field such that $(O;\mathcal{L}_{ring})$ is e-interpretable in $(R;\mathcal{L}_{alg})$, and the Diophantine problem $\mathcal{D}(O;\mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(R;\mathcal{L}_{alg})$. Moreover:*

1. *If R^2 is infinite and Λ has positive characteristic, then $(\mathbb{F}_p[t];\mathcal{L}_{ring})$ is e-interpretable in $(R;\mathcal{L}_{alg})$ for some prime integer p, and $\mathcal{D}(R;\mathcal{L}_{alg})$ is undecidable.*
2. *If R^2 is finite and $\mathcal{D}(R;\mathcal{L}_{mod})$ is decidable, then $\mathcal{D}(R;\mathcal{L}_{alg})$ is decidable.*

If Λ is a finite field, then all the above holds after replacing $(R;\mathcal{L}_{alg})$ by $(R;\mathcal{L}_{ring})$.

Theorems 1.1 and 1.2 are further extended to other classes of finitely generated rings and algebras, including associative commutative non-unitary rings. We say that a non-unitary ring R has characteristic $n \in \mathbb{N}$ if n is the smallest nonnegative integer such that $nr = 0$ for all $r \in R$.

Theorem 1.3. *Let A be a finitely generated associative commutative non-unitary ring, with A^2 infinite. Then there exists a ring of integers O of a number or a global function field such that $(O;\mathcal{L}_{ring})$ is e-interpretable in $(A;\mathcal{L}_{ring})$, and $\mathcal{D}(O;\mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(A;\mathcal{L}_{ring})$.*

Moreover, if A has positive characteristic, then the following holds: O is the ring of integers of a global function field; the ring of polynomials $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in A for prime integer p; and $\mathcal{D}(A; \mathcal{L}_{ring})$ is undecidable.

In [7, Theorem 7.1], Eisentraeger studied the Diophantine problem in finitely generated associative commutative unitary rings. The main result of that work is stated in this paper in Theorem 2.14. The above Theorem 1.3, together with the aforementioned result, provide insight on the Diophantine problem in finitely generated associative commutative rings, unitary or not. Indeed, for any such ring R, one can reduce $\mathcal{D}(O; \mathcal{L}_{ring})$ to $\mathcal{D}(R; \mathcal{L}_{ring})$ for some ring of integers O of a number or global function field, and in a wide variety of cases O turns out to be a ring of integers of a global function field, making $\mathcal{D}(R; \mathcal{L}_{ring})$ undecidable due to Shlapentokh's work [35].

We also prove a statement analogous to Theorem 1.3 for algebras:

Theorem 1.4. *Let L be a finitely generated associative commutative non-unitary algebra over a finitely generated associative commutative unitary ring Θ, with L^2 infinite. Then there exists a ring of integers O of a number field or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(L; \mathcal{L}_{alg})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(L; \mathcal{L}_{alg})$.*

Moreover, if Θ has positive characteristic, then O is the ring of integers of a global function field, $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in $(L; \mathcal{L}_{alg})$ for some prime integer p, and $\mathcal{D}(L; \mathcal{L}_{alg})$ is undecidable.

Our results also involve some classes of possibly non-associative and non-commutative algebras and rings. We only give the statement for algebras, keeping in mind that the statement for rings is obtained by taking $\Lambda = \mathbb{Z}$. We need the following definition: Let L be a Λ-algebra, and let T be a generating set of R. If R is non-unitary then we let $I_n(T)$ or I_n denote the Λ-ideal generated by all products of n elements of T. If L is unitary then we let $I_n(T)$, or I_n in short, denote the Λ-ideal generated by all products of n elements of $T \backslash \{\lambda \cdot 1 \mid \lambda \in \Lambda\}$, where 1 denotes the multiplicative identity of R. We say that L is *left-normed-generated* with respect to T if for all $n \geqslant 1$, $I_n(T)$ is generated as a Λ-module by a (possibly infinite) set of elements of the form $(t_1(t_2(\dots(t_{k-1}t_k)\dots)))$, with $k \geqslant n$ and $t_i \in T$ for all i.

Theorem 1.5. *Let L be a finitely generated algebra (possibly non-associative, non-commutative and non-unitary) over a finitely generated associative commutative unitary ring Λ. Suppose that L is left-normed-generated with respect to some finite generating set T, and that $(L/I_n(T))^2$ is infinite for some $n \geqslant 1$. Then there exists a ring of integers O of a number field or of a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(R; \mathcal{L}_{alg})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(L; \mathcal{L}_{alg})$. Moreover:*

1. *If Λ has positive characteristic p, then $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in $(L; \mathcal{L}_{alg})$, and $\mathcal{D}(L; \mathcal{L}_{alg})$ is undecidable.*
2. *If L is a ring (i.e. $\Lambda = \mathbb{Z}$) then O is a ring of algebraic integers.*

If Λ is $\mathbb{Z}$ or a finite field then all the above holds after replacing $(L; \mathcal{L}_{alg})$ by $(L; \mathcal{L}_{ring})$.

We obtain the following applications of the result above. By $[R/I_n, R/I_n]$ we denote the Λ-submodule of R/I_n generated by $\{[x, y] \mid x, y \in R/I_n\}$.

Corollary 1.6. *Let L be a finitely generated Lie Λ-algebra. Assume that $[R/I_n, R/I_n]$ is infinite for some $n \geqslant 1$, and that Λ is finitely generated. Then the conclusions of Theorem 4.10 hold for L.*

Corollary 1.7. *Let F be a finitely generated free associative Λ-algebra (possibly non-commutative and non-unitary) or a free Lie algebra of rank at least 2, with Λ finitely generated. Then the conclusions of Theorem 4.10 hold for F.*

This complements the previously mentioned results of Romankov [33] and of Kharlampovich and Miasnikov [15, 17] regarding free algebras. We remark that in [33] it is proved (among others) that the algebras of Corollary 4.13 actually have undecidable Diophantine problem if $\Lambda = \mathbb{Z}$.

It is known that the first order theory of any ring of integers of a number field or of a global function field is undecidable. Therefore we obtain the following consequence:

Theorem 1.8. *Suppose that A satisfies the hypotheses of any of the theorems and corollaries above. Then the first-order theory of A in the corresponding language with constants is undecidable.*

The above result extends Noskov's work [29] where it is proved that all finitely generated infinite associative commutative unitary rings have undecidable first-order theory.

From bilinear maps to associative commutative unitary algebras. The main techniques developed in this paper allow to move from studying arbitrary rings and algebras (possibly non-associative, non-commutative, and non-unitary) to studying finitely generated associative commutative unitary rings. The Diophantine problem in the latter scenario is more or less understood, modulo the Diophantine problem of rings of integers of number fields, as was shown in [7, Theorem 7.1].

The reduction from arbitrary rings (algebras) to associative commutative unitary rings (algebras) is achieved through the study of rings of scalars of bilinear maps between Λ-modules, where Λ is a finitely generated associative commutative unitary ring (when dealing with rings we have $\Lambda = \mathbb{Z}$). These are relevant for us because much of the structure of a Λ-algebra (or a ring) can be "seen" in its ring multiplication operation, which is indeed a Λ-bilinear map between Λ-modules. In fact, bilinear maps also arise naturally in other structures, and in some cases, it is possible to apply the methods presented in this paper to these, for example, in some classes of groups. In [11] we explore further this line of work for several classes of solvable groups.

Next we describe further our approach with bilinear maps. Some of the ideas we present now were introduced by the second named author in [25], and they have been used successfully to study different first-order theoretic aspects of different types of structures, including rings whose additive group is finitely generated [26], free algebras [16, 18, 19], and nilpotent groups [27, 28]. Our contribution is a treatment of these ideas by means of systems of equations.

Observe that ring multiplication $\cdot$ of a Λ-algebra R is, by definition, a Λ-bilinear map between Λ-modules. One can try to replace Λ by a "larger" associative commutative unitary ring Δ. To do so, one needs to find a ring Δ that acts on R by Λ-module endomorphisms (thus making the additive group of R into a Δ-module), in a way that $\cdot$ becomes a Δ-bilinear map between Δ-modules. In this case, we say that Δ is a *ring of scalars* of the multiplication map $\cdot$.

These considerations apply in the same way if one starts with an arbitrary Λ-bilinear map $f : N \times N \to M$ between Λ-modules N and M. If f is full and non-degenerate (see Subsection 3.1) then one can define the *largest* ring of scalars of f, denoted $R(f)$. This ring constitutes an important feature of f, and in some sense, it provides an "approximation" to interpreting (in $(N, M; f; \mathcal{L}_{mod})$) multiplication of constant elements from N and M by integer variables, or by variables taking values in Λ. Another important property of $R(f)$ is that it is interpretable in $(N, M; f; \mathcal{L}_{mod})$ by first-order formulas without constants [25]. In this paper, we prove that this is still true if one uses systems of equations instead (with constants).

Theorem 1.9. *If f is full and non-degenerate, and if N and M are finitely generated, then both $Z(Sym(f))$ and the largest ring of scalars $R(f)$ of f are e-interpretable in the two sorted structure $(N, M; f, \mathcal{L}_{mod})$.*

By $End_\Lambda(N)$ we denote the algebra of Λ-endomorphisms of N. The ring $Sym(f)$ is defined as

$$Sym(f) = \{\alpha \in End_\Lambda(A) \mid f(\alpha x, y) = f(x, \alpha y) \ \forall \ x, y \in A\},$$

and $Z(Sym(f))$ denotes the center of $Sym(f)$ (i.e. the set of elements from $Sym(f)$ that commute with all elements from $Sym(f)$). The interest we have for $Z(Sym(f))$ is mostly technical. This is explained in Remark 3.12.

We next provide an idea of the proof of Theorem 1.9. There are two main observations. The first goes as follows: Both $Z(Sym(f))$ and $R(f)$ can be seen as subalgebras $End_\Lambda(N)$. Let $a_1, \ldots, a_k$ be a module generating set of N. Then each $\alpha \in End_\Lambda(N)$ can be identified with the tuple $(\alpha a_1, \ldots, \alpha a_k) \in$

N^k, and so we can think of $Z(Sym(f))$ and $R(f)$ as Λ-submodules of N^k with an extra ring multiplication operation. In particular we manage to first e-interpret the whole algebra $End_\Lambda(N)$ in $(N; \mathcal{L}_{alg})$, together with the action of any element of $End_\Lambda(N)$ on the elements $\{a_1, \ldots, a_k\}$.

The second idea is to use the properties of f in order to "express" statements about endomorphisms from $Z(Sym(f))$ and of $R(f)$ in terms of their actions on $a_1, \ldots, a_k$. For example, given $\alpha, \beta, \gamma \in Z(Sym(f))$, one has that $\gamma = \alpha\beta$ if and only if $f(\gamma a_i, a_j) = f(\beta a_i, \alpha a_j)$ for all $1 \leqslant i, j \leqslant k$ (this is proved using bilinearity of f and the fact that $f(\alpha\beta x, y) = f(\beta x, \alpha y)$ for all x and y). This and the considerations in the previous paragraph can be combined to show (after some work) that multiplication in $Z(Sym(f))$ is e-interpretable in $(N, M; f, \mathcal{L}_{mod})$. The rest of the proof follows in a similar fashion, with the e-interpretation of $R(f)$ being more involved but of a likewise spirit.

In Subsection 3.3 we generalize Theorem 1.9 to the following result.

Theorem 1.10. *Let $f : A \times B \to C$ be a Λ-bilinear map between finitely generated Λ-modules. Then there exists an associative commutative unitary ring Θ that is a Λ-algebra and is finitely generated as a Λ-module, with the property that $(\Theta; \mathcal{L}_{alg})$ is e-interpretable in $F = (A, B, C; f, \mathcal{L}_{mod})$. If Λ is the ring $\mathbb{Z}$ or a field, then $\mathcal{L}_{alg}$ and $\mathcal{L}_{mod}$ can be replaced by $\mathcal{L}_{ring}$ and $\mathcal{L}_{group}$, respectively.*

As mentioned above, the ring multiplication of any Λ-algebra R, finitely generated as a Λ-module, is a Λ-bilinear map $\cdot : R \times R \to R$ between finitely generated Λ-modules, and $(R, R, R; \cdot, \mathcal{L}_{mod})$ is e-interpretable in $(R; \mathcal{L}_{alg})$. Applying Theorem 1.10 and transitivity of e-interpretations we manage to move from the possibly non-associative, non-commutative, and non-unitary R to an associative, commutative, unitary algebra.

As we discussed in the abstract of the present paper, we believe that the above Theorem 1.10 constitutes one of the main contributions of the paper, with potential applicability to other structures other than rings or algebras.

2 Preliminaries

2.1 Interpretability by systems of equations

2.1.1 Multi-sorted structures

A *multi-sorted structure* $\mathcal{A}$ is a tuple $\mathcal{A} = (A_i; f_j, r_k, c_\ell \mid i \in I, j \in J, k \in K, \ell \in L)$, where the A_i are pairwise disjoint sets called *sorts*; the f_j are functions of the form $f_j : A_{i_1} \times \cdots \times A_{i_m} \to A_{i_{m+1}}$ for some $i_1, \ldots, i_{m+1} \in I$; the r_k are relations of the form $r_k : A_{i'_1} \times \cdots \times A_{i'_p} \to \{0, 1\}$, for some $i'_1, \ldots, i'_p \in I$; and the c_ℓ are constants, each one belonging to some sort. The tuple $(f_j, r_k, c_\ell \mid j \in J, k \in K, \ell \in L)$ is called the *signature* or the *language* of $\mathcal{A}$. We always assume that $\mathcal{A}$ contains the relations "equality in A_i", for all sorts A_i, but we do not write them in the signature.

All our terms will allow the use of any constant element in any sort, regardless of whether the constant is in the signature of the structure at hand. For this reason, and without losing generality, we will always work with (multi-sorted) structures without constants in the signature.

If $\mathcal{A}$ has only one sort then $\mathcal{A}$ is a structure in the usual sense. One can construct terms in a multi-sorted structure in an analogous way as in uniquely-sorted structures. In this case, when introducing a variable x, one must specify a sort where it takes values, which we denote A_x.

A set S of *generators* of $\mathcal{A}$ is a collection of elements from different sorts such that any element from any sort can be written as a term using only constants from S and from the signature of $\mathcal{A}$ (and using function symbols).

Example 2.1. A ring is a structure $(R, +, \cdot, =)$ with one sort R, the operations of addition $+$ and multiplication $\cdot$, and the equality relation $=$. When there is no risk of ambiguity we will always denote a classical one-sorted structure, such as a ring or a group, simply by its sort, that is we denote a ring $(R, +, \cdot, =)$ simply by R.

In this paper we understand left modules over a ring as one-sorted structures in the way explained in Section 2.3. An alternative formulation arises by considering two sorts A (the underlying abelian group) and R (the ring acting on A), a group addition $+_A$, ring addition and multiplication $+_R, \cdot_R$, equality relations $=_R$, $=_A$, and an action operation $\cdot : R \times A \to A$. We stress again that this is not the approach taken in this paper.

Let $\mathcal{A}_1, \ldots, \mathcal{A}_n$ be a collection of multi-sorted structures. We let $(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ be the multi-sorted structure that is formed by all the sorts, functions, relations, and constants of each $\mathcal{A}_i$. Given a function f or a relation r we use the notation $(\mathcal{A}, f)$ or $(\mathcal{A}, r)$ to denote the multi-sorted structure $\mathcal{A}$ with the additional function f or relation r.

Example 2.2. The following example will be used later in the paper. Let A, B, C be abelian groups, and let $f : A \times B \to C$ be a bilinear map, i.e. a map such that for all $a \in A$ the map $f(a, \cdot) : B \to C$ is a group homomorphism, and similarly, for all $b \in B$ the map $f(\cdot, b) : B \to C$ is a group homomorphism.

Then one can consider the multi-sorted structure (A, B, C, f). This is formed by the sorts A, B, C; the group operations and relations of A, B, and C, and the operation given by the map f.

An example of a terms in (A, B, C, f) is $f(x, b) + y$ where b is an element from B, and x, y are variables taking values in A and C, respectively.

2.1.2 Diophantine problems and reductions.

Let $\mathcal{A}$ be a multi-sorted structure. An *equation in* $\mathcal{A}$ is an expression of the form $r(\tau_1, \ldots, \tau_k)$, where r is a signature relation of $\mathcal{A}$ (typically, the equality relation), and each τ_i is a term in $\mathcal{A}$ (taking values in an appropriate sort) where some of its variables may have been substituted by elements of $\mathcal{A}$. Such elements are called the *coefficients* (or the *constants*) of the equation. These may not be signature constants. A system of equations is a finite conjunction of equations. A *solution* to a system of equations $\wedge_i \Sigma_i(x_1, \ldots, x_n)$ on variables $x_1, \ldots, x_n$ is a tuple $(a_1, \ldots, a_n) \in A_{x_1} \times \cdots \times A_{x_n}$ such that all equations $\Sigma_i(a_1, \ldots, a_n)$ are true in $\mathcal{A}$.

The *Diophantine problem* in $\mathcal{A}$, denoted $\mathcal{D}(\mathcal{A})$, refers to the algorithmic problem of determining if each given system of equations in $\mathcal{A}$ (with coefficients in a fixed computable set) has a solution. Sometimes this is also called *Hilbert's tenth problem* in $\mathcal{A}$. An algorithm L is a *solution* to $\mathcal{D}(\mathcal{A})$ if, given a system of equations S in $\mathcal{A}$, determines whether S has a solution or not. If such an algorithm exists, then $\mathcal{D}(\mathcal{A})$ is called *decidable*, and, if it does not, *undecidable*.

An algorithmic problem P_1 is said to be *Karp-reducible* (or *polynomial-time many-one reducible*) to another problem P_2 if there is a polynomial-time algorithm that transforms inputs to problem P_1 into inputs to problem P_2, such that both problems have the same output given an input and the transformed input, respectively.

A crucial observation is that if P_1 is undecidable, and P_1 is Karp-reducible to P_2, then P_2 is undecidable as well.

In some cases, one restricts the set of coefficients C that can be used in the input equations of the Diophantine problem of a structure. For instance, one typically takes $C = \mathbb{Z}$ when studying $\mathcal{D}(\mathbb{Q})$ (equivalently one can take $C = \{0, 1\}$). In this paper, we will always need that C contains certain coefficients, namely those used in a certain e-interpretation, and maybe also the preimage of some constants of the structure that is being e-interpreted. For this reason, and to simplify the exposition, we agree that C is always the whole structure, or a suitable computable subset if the structure is not countable.

2.1.3 Interpretations by systems of equations

In this section we review the notion of interpretability by systems of equations between multi-sorted structures. Here we use a much more general setting since our arguments will require handling a variety of multi-sorted structures.

Interpretability by systems of equations (e-interpretability) is the analog of the classic model-theoretic notion of interpretability by first-order formulas (see [13, 22]). In e-interpretability one requires that only systems of equations *with coefficients* are used, instead of first-order formulas. From a number theoretic viewpoint, e-interpretability is roughly Diophantine definability by systems of equations up to a Diophantine definable equivalence relation.

In this paper —in e-interpretations and Diophantine problems— we consider *systems* of equations and not just single equations. This may contrast with some number-theoretic settings, where systems of equations are equivalent to single equations, and both notions are treated interchangeably, i.e. when studying integral domains whose field of fractions is not algebraically closed.

Definition 2.3. Let $\mathcal{A}$ be a structure with sorts $\{A_i \mid i \in I\}$. A *basic set* of $\mathcal{A}$ is a set of the form $A_{i_1} \times \cdots \times A_{i_m}$ for some m and i_j's.

Definition 2.4. Let M be a basic set of a multi-sorted structure $\mathcal{M}$. A subset $A \subset M$ is called *definable by equations* (or *e-definable*) in $\mathcal{M}$ if there exists a system of equations $\Sigma_A(x_1, \ldots, x_m, y_1, \ldots, y_k)$ on variables $(x_1, \ldots, x_m, y_1, \ldots, y_k) = (\mathbf{x}, \mathbf{y})$ such that $\mathbf{x}$ takes values in M, and such that for any tuple $\mathbf{a} \in M$, one has that $\mathbf{a} \in A$ if and only if the system $\Sigma_A(\mathbf{a}, \mathbf{y})$ on variables $\mathbf{y}$ has a solution in $\mathcal{M}$. In this case Σ_A is said to *define* A in $\mathcal{M}$. The integer n is called the *dimension* of the e-definition.

From an algebraic geometric viewpoint, an e-definable set is a projection onto some coordinates of an affine algebraic set. From a number theoretic point, it is a Diophantine definable set, allowing to use systems of equations rather than a single equation.

Definition 2.5. Let $\mathcal{A} = (A_1, \ldots; f, \ldots, r \ldots)$ and $\mathcal{M}$ be two multi-sorted structures. One says that $\mathcal{A}$ is *interpretable by equations* (or *e-interpretable*) in $\mathcal{M}$ if for each sort A_i there exists a basic set $M(A_i)$ of $\mathcal{M}$, a subset $X_i \subseteq M_i$, and a surjective map $\phi_i : X_i \to A_i$ such that:

1. X_i is e-definable in $\mathcal{M}$, for all i.
2. For each function f and each relation r in the signature of $\mathcal{A}$ (including the equality relation of each sort), the preimage by $\boldsymbol{\phi} = (\phi_1, \ldots)$ of the graph of f (and of r) is e-definable in $\mathcal{M}$, in which case we say that f (or r) is e-interpretable in $\mathcal{M}$. The same terminology applies to functions and relations that are not necessarily in the signature of $\mathcal{A}$.

The tuple of maps $\boldsymbol{\phi} = (\phi_1, \ldots)$ is called an *e-interpretation* of $\mathcal{A}$ in $\mathcal{M}$. The map ϕ is called an *e-interpretation* of R_1 in R_2. We will say that $\mathcal{A}$ is *e-interpretable* in $\mathcal{M}$ if there exists an e-interpretation ϕ of $\mathcal{A}$ in $\mathcal{M}$. It is usually clear, but not important, what the specific e-interpretation is.

The next lemma illustrates a key application of e-interpretability.

Lemma 2.6. *Let R be a ring, not necessarily commutative or associative. Suppose $I \leqslant R$ 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 $\pi : R \to R/I$ is an e-interpretation of R/I in R. First observe that the preimage of π 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 $a_1 a_2 - a_3 \in I$. □

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

Lemma 2.7. *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 $a_1, \dots, a_n$ be a generating set of I. Then the equation $x = \sum x_i a_i$ on variables $(x, x_1, \dots, x_n)$ e-defines I in R. Lemma 2.6 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.

Remark 2.8. It is clear from the proof that an analog of Lemma 2.6 holds for other structures, such as groups with e-definable normal subgroups, modules with e-definable submodules, etc.

The following remark will be used several times without referring to it.

Remark 2.9. Let $\mathcal{A} = (A; f, \dots; r, \dots)$ and $\mathcal{B} = (B; f', \dots; r', \dots)$ be uniquely-sorted structures such that $A \subseteq B$ and all functions and relations of $\mathcal{A}$ are also functions and relations of $\mathcal{B}$. Assume A is e-definable in $\mathcal{B}$. Then, clearly, $\mathcal{A}$ is e-interpretable in $\mathcal{B}$.

The next two results are fundamental. They follow from Lemma 2.12, which we present at the end of this subsection.

Proposition 2.10 (E-interpretability is transitive)**.** *If $\mathcal{A}$ is e-interpretable in $\mathcal{B}$ and $\mathcal{B}$ is e-interpretable in $\mathcal{M}$, then $\mathcal{A}$ is e-interpretable in $\mathcal{M}$.*

Proposition 2.11 (Reduction of Diophantine problems)**.** *Let $\mathcal{A}$ and $\mathcal{M}$ be (possibly multi-sorted) finitely generated structures such that $\mathcal{A}$ is e-interpretable in $\mathcal{M}$. Then $\mathcal{D}(\mathcal{A})$ is Karp-reducible to $\mathcal{D}(\mathcal{M})$. As a consequence, if $\mathcal{D}(\mathcal{A})$ is undecidable, then so is $\mathcal{D}(\mathcal{M})$.*

Similarly, the first-order theory of $\mathcal{A}$ is Karp-reducible to the first-order theory (with constants[1]) of $\mathcal{M}$, and the second is undecidable if the first is.

Both Propositions 2.10 and 2.11 are consequences of the following lemma, which states in technical terms that if one structure is e-interpretable in the other, then one may "express" equations in the first as systems of equations in the second. Similar results to this with analogous proof are well-known. We include a proof for completeness.

Lemma 2.12. *Let $\boldsymbol{\phi} = (\phi_1, \dots)$ be an e-interpretation of a multi-sorted structure $\mathcal{A} = (A_1, \dots; f, \dots, r, \dots)$ in another multi-sorted structure $\mathcal{M}$, with $\phi_i : X_i \subset M(A_i) \to A_i$ (see Definition 2.5). Let $\sigma(\mathbf{x}) = \sigma(x_1, \dots, x_n)$ be an arbitrary system of equations in $\mathcal{A}$ with each variable x_i taking values in A_{j_i}. Then there exists a system of equations $\Sigma_\sigma(\mathbf{y}_1, \dots, \mathbf{y}_n)$ in $\mathcal{M}$, such that each tuple of variables $\mathbf{y}_i$ takes values in $M(A_{j_i})$, and such that a tuple $(\mathbf{b}_1, \dots, \mathbf{b}_n) \in \prod_{i=1}^n M(A_{j_i})$ is a solution to $\Sigma_\sigma(\mathbf{y}_1, \dots, \mathbf{y}_n)$ if and only if $(\mathbf{b}_1, \dots, \mathbf{b}_n) \in \prod_{i=1}^n X_{j_i}$ and $(\phi_{j_1}(\mathbf{b}_1), \dots, \phi_{j_n}(\mathbf{b}_n))$ is a solution to σ.*

Proof. We claim that, by introducing new variables and new equations, we can rewrite σ so that σ consists in a conjunction of equations $\sigma_1 \wedge \cdots \wedge \sigma_m$ such that the following holds: For all $i = 1, \dots, m$, σ_i is either of the form $z = f(x_1, \cdots x_n)$, $r(x_1, \dots, x_n)$, or $z = a$, where f is some function from $\mathcal{A}$, the symbol r is some relation from $\mathcal{A}$, the symbols $x_1, \dots, x_n, z$ are variables, and a is any element from the sorts of $\mathcal{A}$. The lemma follows from the claim, since by the definition of e-interpretability, the present lemma is true for each of σ_i, $i = 1, \dots, m$. Hence, it suffices to take Σ_σ to be $\Sigma_{\sigma_1} \wedge \cdots \wedge \Sigma_{\sigma_n}$.

We now prove the claim. We proceed by induction on the syntactic length $|\sigma|$ of σ, the base cases being clear. We can assume that σ consists on a single equation. Suppose first that σ does not have the desired form and that it is of the form $z = f(t_1, \dots, t_m)$ for some variable z, some function f, and some

[1]The considerations made regarding the use of constants in systems of equations and Diophantine problems apply as well for first-order formulas and their decidability problems (see Paragraph 3 of Subsection 2.3 or Subsection 2.1.2).

terms $t_1, \ldots, t_m$ depending on some variables $x_1, \ldots, x_k$. We can rewrite σ into the equivalent system of equations $z = f(y_1, \ldots, y_m) \wedge y_1 = t_1(x_1, \ldots, x_k) \wedge \cdots \wedge y_m = t_m(x_1, \ldots, x_k)$, where $y_1, \ldots, y_m$ are new variables. The syntactic length of each one of these equations is strictly less than $|\sigma|$, and then we can proceed by induction. If σ has the form $r(t_1, \ldots, t_m)$ for some relation r and some terms $t_1, \ldots, t_m$, we can proceed similarly by rewriting it as $r(y_1, \ldots, y_m) \wedge \wedge y_1 = t_1(x_1, \ldots, x_k) \wedge \cdots \wedge y_m = t_m(x_1, \ldots, x_k)$. Finally if σ has the form $f(t_1, \ldots, t_m) = g(t'_1, \ldots, t'_k)$ for some functions f, g and terms $t_1, \ldots, t_m, t'_1, \ldots, t'_k$, we can rewrite sigma in the form $z = f(t_1, \ldots, t_m) \wedge z = g(t'_1, \ldots, t'_k)$. Each one of the equations in the conjunction has syntactic length smaller than $|\sigma|$, and again we can proceed by induction. This proves the claim. □

We will use the following observations in different occasions:

Remark 2.13. Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{M}$ be (possibly multi-sorted) structures. Suppose that all sorts among the sorts of $\mathcal{A}$ and $\mathcal{B}$ are pairwise disjoint. Let $\mathcal{N}$ be a (possibly multi-sorted) structure which is the result of adding functions, relations, constants, or more sorts to $\mathcal{M}$. Suppose $\mathcal{A}$ is e-interpretable in $\mathcal{M}$. Then $\mathcal{A}$ is also e-interpretable in $\mathcal{N}$.

Moreover, if both $\mathcal{A}$ and $\mathcal{B}$ are e-interpretable in $\mathcal{M}$, then the multi-sorted structure $(\mathcal{A}, \mathcal{B})$ is also e-interpretable in $\mathcal{M}$.

2.2 The Diophantine problem in finitely generated associative commutative unitary rings

Recall that, given two associative commutative unitary rings R, S with $S \subseteq R$, and an element $r \in R$, we say that r is *integral* over S if there exists a monic polynomial $p(x) \in S[x]$ such that $p(r) = 0$. The *integral closure* of S in R is defined as the subset of integral elements of R, and it forms a subring of R. We will often denote it O_R when the ring S is understood from the context, and we will refer to O_R as the *ring of integers of* R.

A *number field* is a finite field extension of $\mathbb{Q}$. Given a field k, by $k(t)$ we denote the set of rational functions with coefficients in k and variable t. The integral closure of $\mathbb{Z}$ in a number field K is called a *ring of algebraic integers*. A *global function field* is a finite field extension of $\mathbb{F}_p(t)$ for some finite field $\mathbb{F}_p$ with a prime number p of elements.

Shlapentokh proved that the Diophantine problem is undecidable in any ring of integers of a global function field (see 10.6.2 from [37]). On the other hand, it is conjectured that the same is true for any ring of algebraic integers.

In the PhD thesis [7, Theorem 7.1] Eisentraeger proved the following relation between the Diophantine problem of any infinite finitely generated commutative associative unitary ring, and the Diophantine problem of rings of integers of number or global function fields. Recall that the *characteristic* of a ring with unity is the minimum positive integer n such that $1 + \overset{n}{\ldots} + 1 = 0$.

Theorem 2.14 (Theorem 7.1 in [7])**.** *Let A be an infinite finitely generated associative commutative unitary ring.*

1. *Assume that the characteristic of A is $n > 0$. If A has infinitely many elements, then Hilbert's Tenth Problem for A is undecidable.*
2. *Assume A has characteristic zero. If the Krull dimension of A is at least 2, then $\mathcal{D}(A; \mathcal{L}_{ring})$ is undecidable. If we assume that $\mathcal{D}(O_K; \mathcal{L}_{ring})$ is undecidable for any ring of algebraic integers O_K of integers of number fields is undecidable, then $\mathcal{D}(A; \mathcal{L}_{ring})$ is undecidable.*

We are interested in a variation, slightly stronger, formulation of this result, which we state below. The proof of this alternative formulation can be obtained from the proof of Theorem 2.14 [7] by making straightforward modifications. For completeness, we include an alternative yet similar proof in the appendix at the end of this paper.

We 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 [9].

Definition 2.15 ([9])**.** The *rank* of an abelian group A is the maximal number of nonzero elements $a_1, \ldots, a_n \in A$ such that whenever $\alpha_1 a_1 + \cdots + \alpha_n a_i = 0$ 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 2.16. 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 α_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 $R = \mathbb{Z}[x]/(px)$ 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.

Theorem 2.17. *Let R be an infinite finitely generated commutative ring with identity. Then there exists a ring of integers O of a number or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(R; \mathcal{L}_{ring})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(R; \mathcal{L}_{ring})$. Moreover, one of the following holds:*

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

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

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

Proof. See Appendix 5. □

2.3 Notation and conventions

Here we note and emphasize some relevant aspects of the notation used in the paper.

1. Unless stated otherwise, all rings and algebras are not necessarily associative, commutative, or unitary.

Given an algebra R over a ring Λ, and a subset $S \subseteq R$, we let $\langle S \rangle_\Lambda$ be the left Λ-submodule of R generated by a set S. We also let $R^2 = \langle xy \mid x, y \in R \rangle_\Lambda$.

All modules are assumed to be *left* modules over commutative associative unitary rings. Similarly, the underlying module of an algebra is assumed to be a left module over commutative associative unitary rings. All arguments work in the same way if we replace all left modules by right modules or all left module by bimodules.

3. The language of additive groups is $\mathcal{L}_{group} = (+)$. The language of Λ-modules is $\mathcal{L}_{mod} = (\mathcal{L}_{group}, \cdot\Lambda)$, where the $\cdot\Lambda = \{\cdot\lambda \mid \lambda \in \Lambda\}$ are unary functions representing multiplication by scalars: $\cdot_\lambda(x) = \lambda x$. The language of rings $\mathcal{L}_{ring}$ is $(+, \cdot)$. The language of Λ-algebras is $\mathcal{L}_{alg} = (+, \cdot, \cdot\Lambda)$. If Λ admits a finite generating set S, then one can replace $\cdot\Lambda$ by $\cdot S = \{\cdot_\lambda \mid \lambda \in S\}$ without loss of generality.

Hence, in an equation (or in a formula) over a Λ-module or Λ-algebra R, one is allowed to multiply any element of R by any constant element of Λ. But this is as far as one can involve Λ: no variable can take values in Λ, no quantification over Λ can be made, etc.

4. The notion of $\mathbb{Z}$-module or $\mathbb{Z}$-algebra with the languages above is equivalent, for the purposes of studying decidability of the Diophantine problem, to the notion of abelian group or ring, respectively.

5. Sometimes we will want to look at an algebra L over a ring Λ *as a* Λ*-module*, or *as a ring*, or *as a group*, forgetting about the corresponding additional operations of L. We will use the notation $(L;\mathcal{L}_{mod})$, $(L;\mathcal{L}_{ring})$, $(L;\mathcal{L}_{group})$ when this is done, respectively. We will also write $(L;\mathcal{L}_{alg})$ to emphasize that L is considered with all its Λ-algebra operations. A similar terminology will be used for other structures such as rings and modules.

This notation will be used extensively in expressions of the type $(L;\mathcal{L}_1)$ *is e-interpretable in* $(K;\mathcal{L}_2)$. This means that the structure L with the operations of the language $\mathcal{L}_1$ is e-interpretable in K considered with the operations of $\mathcal{L}_2$. In the particular case that $\mathcal{L}_1 = \mathcal{L}_2$ we will also say that L *is e-interpretable in* K *in the language* $\mathcal{L}_1$.

3 From bilinear maps to commutative rings and algebras

A brief description of the arguments used in this section can be found in the last part of the introduction.

3.1 Ring of scalars of a full non-degenerate bilinear map

Throughout this subsection, Λ denotes an associative, commutative, unitary ring, possibly infinitely generated.

A map $f : N \times N \to M$ between Λ-modules N and M is Λ-*bilinear* if, for all $a \in N$, the maps $\ell_a : N \to M$ and $r_a : N \to M$ defined as $\ell_a(b) = f(a,b)$ and $r_a(b) = f(b,a)$ are homomorphisms of Λ-modules. We call f *non-degenerate* if whenever $f(a,x) = 0$ for all $x \in N$, we have $a = 0$, and also whenever $f(x,a) = 0$ for all $x \in N$ we have $a = 0$. The map f is called *full* if the Λ-submodule generated by the image of f is the whole M.

The set of module endomorphisms of a Λ-module N, denoted $End_\Lambda(N)$, forms an associative unitary Λ-algebra once we equip it with the operations of addition and composition (henceforth called *multiplication*). Given $\alpha \in End_\Lambda(N)$ and $x \in N$, we write αx instead of $\alpha(x)$. An action of a ring Δ on N is a ring homomorphism $\phi : \Delta \to End_\Lambda(N)$. Any such action ϕ endows N with a structure of Δ-module. The action is called *faithful* if ϕ is an embedding.

Definition 3.1. Let Λ be a commutative associative unitary ring, let N and M be Λ-modules, and let $f : N \times N \to M$ be a Λ-bilinear map between N and M. A ring Δ is called a *ring of scalars* of f if it is associative, commutative, and unitary, and there exist faithful actions of Δ on M and N such that $f(\alpha x, y) = f(x, \alpha y) = \alpha f(x,y)$ for all $\alpha \in \Delta$ and all $x, y \in N$.

Since the actions of a ring of scalars Δ of f on M and N are faithful, there exist ring embeddings $\Delta \hookrightarrow End_\Lambda(M)$ and $\Delta \hookrightarrow End_\Lambda(N)$. For this reason and for convenience, we always assume that a ring of scalars of f is a subring of $End_\Lambda(N)$.

Definition 3.2. We say that Δ is the *largest* ring of scalars of f if for any other ring of scalars Δ' of f, one has $\Delta' \leqslant \Delta$ as subrings of $End_\Lambda(N)$. We denote such ring by $R(f)$.

We will also need the following notation:

Definition 3.3. Let Λ be an associative commutative unitary ring, and let N be a Λ-module. We define the following subsets of $End_\Lambda(N)$:

$$Sym(f) = \{\alpha \in End_\Lambda(N) \mid f(\alpha x, y) = f(x, \alpha y) \text{ for all } x, y \in N\}, \tag{1}$$

$$Z(Sym(f)) = \{\alpha \in Sym(f) \mid \alpha\beta = \beta\alpha \text{ for all } \beta \in Sym(f)\}. \tag{2}$$

It is straightforward to check that both $Sym(f)$ and $Z(Sym(f))$ are Λ-modules.

The next result was proved by the second author in [25]. We recover its proof since we will need to elaborate on it in the next subsection.

Theorem 3.4 (cf. [25])**.** *Let Λ be an associative commutative unitary ring, and let $f : N \times N \to M$ be a full non-degenerate bilinear map between Λ-modules. Then the largest ring of scalars $R(f)$ of f exists and is unique.*

Proof. First observe that for all $\alpha_1, \alpha_2 \in Z(Sym(f))$ and all $x, y \in N$,

$$f(\alpha_1\alpha_2 x, y) = f(\alpha_2 x, \alpha_1 y) = f(x, \alpha_2\alpha_1 y) = f(x, \alpha_1\alpha_2 y),$$

and thus $\alpha_1\alpha_2 \in Sym(f)$. Since both α_1 and α_2 commute with any element from $Sym(f)$, so does $\alpha_1\alpha_2$. Hence, $\alpha_1\alpha_2 \in Z(Sym(f))$, and so $Z(Sym(f))$ is a Λ-subalgebra of $End_\Lambda(N)$.

Next, let Δ be an arbitrary ring of scalars of f. We will show Δ is a subring of $Z(Sym(f))$. Indeed, by definition, $\Delta \subseteq Sym(f)$. To see that $\Delta \subset Z(Sym(f))$, let $\alpha \in \Delta$ and $\beta \in Sym(f)$. Then, for all $x, y \in N$,

$$f(\alpha\beta x, y) = \alpha f(\beta x, y) = \alpha f(x, \beta y) = f(\alpha x, \beta y) = f(\beta\alpha x, y).$$

Hence $f((\alpha\beta - \beta\alpha)x, y) = 0$ for all $x, y \in N$. Since f is non-degenerate and y is arbitrary, $(\alpha\beta - \beta\alpha)x = 0$ for all $x \in N$. It follows that $\alpha\beta = \beta\alpha$, and thus $\Delta \subseteq Z(Sym(f))$.

By what we have seen so far, $Z(Sym(f))$ is an associative commutative unitary Λ-algebra that acts faithfully on N. We now wish to find a subring of $Z(Sym(f))$, call it Θ, that acts on M. Since f is full, for all $z \in M$ we have $z = \sum_i f(x_i, y_i)$ for some $x_i, y_i \in N$. Hence, one may try to define the following action:

$$\alpha z = \sum f(\alpha x_i, y_i) \quad \text{for} \quad \alpha \in \Delta. \tag{3}$$

However, this is not necessarily well-defined, because the same $z \in M$ may have different expressions as sums of elements $f(x_i, y_i)$. With this in mind, we let Θ be the set of all $\alpha \in Z(Sym(f))$ such that

$$\sum f(\alpha x_i, y_i) = \sum f(\alpha x_i', y_i') \quad \text{whenever} \quad \sum f(x_i, y_i) = \sum f(x_i', y_i'). \tag{4}$$

Clearly, Θ is closed under addition and multiplication, and therefore it is a subring of $Z(Sym(f))$ with a well-defined action on M given by (3). Since the action of Θ on N is faithful, and f is a non-degenerate map, the action of Θ on M is faithful as well. It follows that Θ is a ring of scalars of f. Moreover, any other ring of scalars Δ of f satisfies (4), and thus, since $\Delta \subset Z(Sym(f))$ by our previous argument, we have $\Delta \leqslant \Theta$. We conclude that Θ is the unique largest ring of scalars of f. □

Remark 3.5. It is clear from the proof above that $R(f)$ is closed under multiplication by Λ. Hence, $R(f)$ admits the structure of a Λ-algebra.

3.2 E-interpreting $Z(Sym(f))$ and the largest ring of scalars

Throughout this subsection Λ denotes a *Noetherian* associative commutative unitary ring (possibly infinitely generated). Recall that a ring is *Noetherian* if for every infinite ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$ there exists n such that $I_n = I_m$ for all $m \geqslant n$. In this case, any finitely generated Λ-module is Noetherian and finitely presented (see [6] or [12]). We refer to Subsection 2.3 for important notation and terminology conventions.

The goal of this subsection is to prove the following result.

Theorem 3.6. *Let $f : N \times N \to M$ be a full non-degenerate bilinear map between finitely generated Λ-modules. Then both $Z(Sym(f))$ (see Definition 3.3) and the largest ring of scalars $R(f)$ of f are finitely generated as Λ-modules, and they are e-interpretable as Λ-algebras in $F = (N, M; f, \mathcal{L}_{mod})$. Moreover,*

1. *$Z(Sym(f))$, $R(f)$, N, and M are all simultaneously finite, or they are all simultaneously infinite.*
2. *If Λ is a field, then $(Z(Sym(f)); \mathcal{L}_{ring})$ is e-interpretable in $(N, M; f, \mathcal{L}_{group})$ (i.e. multiplication by scalars is not required).*
3. *If $\Lambda = \mathbb{Z}$, then both $(Z(Sym(f)); \mathcal{L}_{ring})$ and $(R(f); \mathcal{L}_{ring})$ are e-interpretable in $(N, M; f, \mathcal{L}_{group})$.*

We state some lemmas and observations before proving Theorem 3.6, starting with a useful description of $End_\Lambda(N)$.

Remark 3.7. Let N be a Λ-module with finite module presentation $\langle a_1, \ldots, a_m \mid \sum_i x_{j,i} a_i,\ j = 1, \ldots, T \rangle_\Lambda$, where $x_{j,i} \in \Lambda$ for all i, j. Each element α of $End_\Lambda(N)$ uniquely determines an m-tuple $(\alpha a_1, \ldots, \alpha a_m) \in N^m$, and one has $\sum_i x_{j,i}(\alpha a_i) = 0$ for all j. Conversely, any m-tuple from N^m with this last property determines an element from $End_\Lambda(N)$. Thus $End_\Lambda(N)$ can be identified with the set of m-tuples $(\alpha_1, \ldots, \alpha_m) \in N^m$ that satisfy $\sum_i x_{j,i}\alpha_i = 0$ for all j.

In the particular case that Λ is a field we have that N is a vector space. In particular, N is a free Λ-module, and so it admits a finite presentation with an empty set of relations. In this case, $End_\Lambda(N) = N^{m'}$ for some $m' \leqslant m$. Let us mention a particular case when N is a free Λ-module. In this case N admits a finite presentation with an empty set of relations. In this case, $End_\Lambda(N) = N^{m'}$ for some $m' \leqslant m$. This happens, for example, if Λ is a field or if $\Lambda = \mathbb{Z}$ and N is torsion-free.

The above identification of $End_\Lambda(N)$ with a subset of N^m is used to prove the following result.

Lemma 3.8. *Let N be a finitely generated Λ-module. Then the following hold:*

1. *$(End_\Lambda(N); \mathcal{L}_{mod})$ is e-interpretable in $(N; \mathcal{L}_{mod})$.*
2. *Let $S_N = \{a_1, \ldots, a_m\}$ be a generating set of N, and define maps $\cdot a_i : End_\Lambda(N) \to N$ so that $\cdot a_i$ sends each $\alpha \in End_\Lambda(N)$ to $\alpha a_i \in N$. Denote $\cdot S_N = \{\cdot a_1, \ldots, \cdot a_m\}$. Then the two-sorted structure $END_\Lambda(N) = (End_\Lambda(N), N; \cdot S_N, \mathcal{L}_{mod})$ is e-interpretable in $(N; \mathcal{L}_{mod})$.*
3. *In the particular case that Λ is a field or the ring of integers $\mathbb{Z}$, the previous statements are still valid after replacing $\mathcal{L}_{mod}$ by $\mathcal{L}_{group}$ in all structures.*

Proof. As mentioned above, since Λ is a Noetherian associative commutative unitary ring, any finitely generated Λ-module is finitely presented with respect to any finite generating set. Let $\sum x_{j,i} a_i,\ j = 1, \ldots, T$ be a finite set of relations of N, with $x_{j,i} \in \Lambda$ for all i, j.

Following Remark 3.7, identify each element α of $End_\Lambda(N)$ with the m-tuple $(\alpha_1, \ldots, \alpha_m) = (\alpha a_1, \ldots, \alpha a_m) \in N^m$. By this same remark, any m-tuple $\alpha = (\alpha_1, \ldots, \alpha_m) \in N^m$ belongs to $End_\Lambda(N)$ if and only if $\sum x_{j,i}\alpha_i = 0$ for all j. This is a finite system of equations in $(N; \mathcal{L}_{mod})$ with variables α_i, and so $End_\Lambda(N)$ as a set is e-definable in $(N; \mathcal{L}_{mod})$. As observed in Remark 3.7, if Λ is a field then $End_\Lambda(N) = N^{m'}$ for some $m' \leqslant m$, and so the e-definition consists in an empty equation. In particular, it does not use multiplication by scalars. Hence $End_\Lambda(N)$ is e-definable as a set in $(N; \mathcal{L}_{group})$.

The group addition of two tuples from the Λ-module $End_\Lambda(N)$ is obtained by component-wise addition. Hence the graph of the addition operation of $End_\Lambda(N)$ (which is a subset of N^{3m}) is e-definable in $(N, \mathcal{L}_{mod})$. By similar reasons, so are the graphs of the equality relation of $End_\Lambda(N)$ and of multiplication by fixed elements of Λ (i.e. multiplication by scalars). This proves that $(End_\Lambda(N); \mathcal{L}_{mod})$ is e-interpretable in $(N; \mathcal{L}_{mod})$. In the case that Λ is a field, $(End_\Lambda(N); \mathcal{L}_{group})$ is e-interpretable in $(N; \mathcal{L}_{group})$.

It follows that the two-sorted structure $(End_\Lambda(N), N; \mathcal{L}_{mod})$ is e-interpretable in $(N; \mathcal{L}_{mod})$. Finally, notice that, for $\alpha = (\alpha_1, \ldots, \alpha_m) \in End_\Lambda(N)$ and $x \in N$, the tuple $(\alpha, x) = N^m \times N$ belongs to

the graph of $\cdot a_i$ if and only if $x = \alpha a_i = \alpha_i$. In other words, for any tuple $(y_1, \ldots, y_{m+1}) \in N^{m+1}$ we have

$$(y_1, \ldots, y_{m+1}) \in \mathit{Graph}(\cdot a_i) \subseteq N^{m+1} \quad \text{if and only if} \quad y_i = y_{m+1},$$

hence the graph of $\cdot a_i$ is e-definable in $(N; \mathcal{L}_{group})$. This completes the proof that $\mathit{END}_\Lambda(N)$ is e-interpretable in $(N; \mathcal{L}_{mod})$.

If Λ is a field then multiplication by scalars was not used in any equation other than when e-interpreting the scalar multiplication of $\mathit{End}_\Lambda(N)$. If $\Lambda = \mathbb{Z}$ then a Λ-module is just a group, because $nx = x + \overset{n}{\ldots} + x$ for all $n \in \mathbb{Z}$. Hence, Item 3 holds. □

Remark 3.9. It follows from Lemma 3.8 and Remark 2.13 that there exists an e-interpretation $\boldsymbol{\phi}$ of the three-sorted structure

$$F_1 = (\mathit{End}_\Lambda(N), N, M; f, \cdot S_N, \mathcal{L}_{mod})$$

in $F = (N, M; f, \mathcal{L}_{mod})$. If Λ is a field or $\mathbb{Z}$, then one can replace $\mathcal{L}_{mod}$ by $\mathcal{L}_{group}$.

Thus by transitivity of e-interpretations (Proposition 2.10), in order to prove that $(R(f); \mathcal{L}_{alg})$ or $(Z(\mathit{Sym}(f)); \mathcal{L}_{alg})$ is e-interpretable in F it suffices to show that it e-interpretable in F_1. For this one must keep in mind that an equation in F_1 can involve constants and variables from N, M, and $\mathit{End}_\Lambda(N)$; the map f; actions of endomorphisms on the a_i's given by $\cdot S_N$; and the operations of $(N; \mathcal{L}_{mod})$, $(M; \mathcal{L}_{mod})$, and $(\mathit{End}_\Lambda(N); \mathcal{L}_{mod})$ without its ring multiplication. For example, the equation $f(\alpha a_i, a_j) = f(a_i, \alpha a_j)$ on the variable α is valid in F_1, whereas $\alpha_1\alpha_2 a_i = \alpha_2\alpha_1 a_i$ or $\alpha x = a_i$ is not (for variables $\alpha_1, \alpha_2, \alpha \in \mathit{End}_\Lambda(N)$, $x \in N$).

We next prove the main result of this subsection.

Proof of Theorem 3.6. First observe that $\mathit{End}_\Lambda(N)$ is finitely generated as a Λ-module, because N^m is a Noetherian module and $\mathit{End}_\Lambda(N)$ embeds as a Λ-module into N^m, by Remark 3.7. By the same reason both $R(f)$ and $Z(\mathit{Sym}(f))$ are finitely generated as Λ-modules.

Denote $F = (N, M; f, \mathcal{L}_{mod})$. We proceed to prove that $(Z(\mathit{Sym}(f)); \mathcal{L}_{alg})$ is e-interpretable in F. By the previous Remark 3.9, it suffices to show that $(Z(\mathit{Sym}(f)); \mathcal{L}_{alg})$ is e-interpretable in F_1 for some generating set $S_N = \{a_1, \ldots, a_n\}$ of N.

We start by proving that $\mathit{Sym}(f)$ can be e-defined as a subset of $\mathit{End}_\Lambda(N)$ in F_1. Indeed, take any $x, y \in N$ and write $x = \sum x_i a_i$ and $y = \sum y_i a_i$ for some $x_i, y_i \in \Lambda$. Since $\alpha x = \sum x_i \alpha a_i$ for all $\alpha \in \mathit{End}_\Lambda(N)$, we have $f(\alpha x, y) = \sum x_i y_j f(\alpha a_i, a_j)$, and similarly for $f(x, \alpha y)$. It follows that

$$\mathit{Sym}(f) = \{\alpha \in \mathit{End}_\Lambda(N) \mid f(\alpha a_i, a_j) = f(a_i, \alpha a_j) \text{ for all } 1 \leqslant i, j \leqslant n\}. \tag{5}$$

Observe that $\alpha a_i = \cdot a_i(\alpha)$ for all $i = 1, \ldots, n$. Hence (5) can be written as a first-order sentence in F_1. We conclude that $\mathit{Sym}(f)$ is e-definable as a set in F_1 by the system of equations

$$\bigwedge_{1 \leqslant i, j \leqslant n} \left[f(\cdot a_i(\alpha), a_j) = f(a_i, \cdot a_j(\alpha)) \right] \tag{6}$$

on the single variable α taking values in $\mathit{End}_\Lambda(N)$. Note that (6) does not use multiplication by scalars Λ.

Since the signature of F_1 contains all operations of $(\mathit{End}_\Lambda(N); \mathcal{L}_{mod})$, we have that $\mathit{Sym}(f) \leqslant \mathit{End}_\Lambda(N)$ as a Λ-module is e-interpretable in F_1.

Next, we show that $Z(\mathit{Sym}(f))$ is e-definable as a set in F_1. As before, this immediately implies that the Λ-module $(Z(\mathit{Sym}(f)); \mathcal{L}_{mod})$ is e-interpretable in F_1. Let $\beta_1, \ldots, \beta_k$ be a finite generating set of $(\mathit{Sym}(f); \mathcal{L}_{mod})$. Then, $\alpha \in Z(\mathit{Sym}(f))$ if and only if $\alpha \in \mathit{Sym}(f)$ and $\alpha\beta_t = \beta_t\alpha$ for all $t = 1, \ldots, k$. This implies that

$$f(\alpha a_i, \beta_t a_j) = f(a_i, \alpha\beta_t a_j) = f(a_i, \beta_t \alpha a_j) = f(\beta_t a_i, \alpha a_j) \quad \text{for all } i, j, t. \tag{7}$$

We claim that (7) is a sufficient condition for an endomorphism $\alpha \in Sym(f)$ to belong to $Z(Sym(f))$. As a consequence one has that $Z(Sym(f))$ is definable as a set in F_1 by means of the following system of equations on the variable α:

$$\bigwedge_{\substack{t=1,\dots,k,\\ 1\leqslant i,j\leqslant n}} \big[f(\cdot a_i(\alpha), \cdot a_j(\beta_t)) = f(\cdot a_i(\beta_t), \cdot a_j(\alpha))\big], \tag{8}$$

together with the system (6), which ensures that $\alpha \in Sym(f)$. Again, recall that αa_i and $\beta_t a_j$ are written in F_1 in the form $\cdot a_i(\alpha)$ and $\cdot a_j(\beta_t)$. As before, (8) does not use multiplication by the scalars Λ.

To prove the claim, i.e. that (7) is a sufficient condition for $\alpha \in Sym(f)$ to belong to $Z(Sym(f))$, suppose (8) holds. Then $f(\beta_t\alpha a_i, a_j) = f(\alpha\beta_t a_i, a_j)$ for all i, j, t, and thus, for fixed i and t, $f([\beta_t, \alpha]a_i, a_j) = 0$ for all j, where $[\beta_t, \alpha] = \beta_t\alpha - \alpha\beta_t$. By bilinearity of f and the fact that $a_1, \dots, a_n$ generate N, we have that $f([\beta_t, \alpha]a_i, x) = 0$ for all $x \in N$ and for all i, t. Since f is non-degenerate, $[\beta_t, \alpha]a_i = 0$ for all i, t. This implies that $[\beta_t, \alpha]x = 0$ for all $x \in N$, and thus $[\beta_t, \alpha] = 0$ for all t. This completes the proof of the claim.

We have seen that the Λ-module $(Z(Sym(f)); \mathcal{L}_{mod})$ is e-interpretable in F_1. Moreover, multiplication by scalars Λ is only used for defining the the scalar multiplication of $(Z(Sym(f)); \mathcal{L}_{mod})$. Hence in fact $Z(Sym(f))$ as a group is e-interpretable in $(End_\Lambda(N), N, M; f, \cdot S_N, \mathcal{L}_{group})$ (i.e. F_1 after replacing $\mathcal{L}_{mod}$ by $\mathcal{L}_{group}$).

By analogous reasons as above, for any triple $\gamma_1, \gamma_2, \gamma_3 \in Z(Sym(f))$ the equality $\gamma_3 = \gamma_1\gamma_2$ holds if and only if

$$f(\gamma_3 a_i, a_j) = f(\gamma_2 a_i, \gamma_1 a_j) \quad \text{for all } 1 \leqslant i, j \leqslant n. \tag{9}$$

Hence the ring multiplication of $Z(Sym(f))$ is e-interpretable in F_1 by means of (9) and appropriate systems of the form (6) and (8) (which ensure that $\gamma_i \in Z(Sym(f))$). We conclude that $Z(Sym(f))$ as a Λ-algebra is e-interpretable in F_1, and hence in $F = (N, M; f, \mathcal{L}_{mod})$.

We now prove Items 2 and 3 of the statement of the Theorem 3.6. As observed in the arguments above, multiplication by scalars of F_1 was only used in order to e-interpret multiplication by scalars of $Z(Sym(f))$. Hence $(Z(Sym(f)); \mathcal{L}_{ring})$ is e-interpretable in $(End_\Lambda(N), N, M; f, \cdot S_N, \mathcal{L}_{group})$. By Lemma 3.8 and Remark 3.9, if Λ is either $\mathbb{Z}$ or a field, then the latter structure is e-interpretable in $(M, M; f, \mathcal{L}_{group})$. Hence $(Z(Sym(f)); \mathcal{L}_{ring})$ is e-interpretable as a ring in $(M, M; f, \mathcal{L}_{group})$. This concludes the proof of Items 2 and 3.

Next we show that $(R(f); \mathcal{L}_{alg})$ is e-interpretable in $(N, M; f, \mathcal{L}_{mod})$. By the previous arguments and by transitivity of e-interpretations, it suffices to prove that $(R(f); \mathcal{L}_{alg})$ is e-interpretable in F_1. First recall from the proof of Theorem 3.4 that $R(f)$ is the set of all $\alpha \in Z(Sym(f))$ such that

$$\text{if } \sum_{i=1}^{t} f(x_i, y_i) = \sum_i f(x'_i, y'_i), \quad \text{then } \sum_{i=1}^{t} f(\alpha x_i, y_i) = \sum_i f(\alpha x'_i, y'_i),$$

for any $t \geqslant 1$ and elements $x_1, \dots, x_t, y_1, \dots, y_t, x'_1, \dots, x'_t, y_1, \dots, y'_t$ in N^t. This condition is equivalent to

$$\text{if } \sum_{i=1}^{t} f(x_i, y_i) = 0, \quad \text{then } \sum_{i=1}^{t} f(\alpha x_i, y_i) = 0. \tag{10}$$

We claim that $\alpha \in Z(Sym(f))$ satisfies (10) if and only if it satisfies the following condition:

$$\text{if } \sum_{1\leqslant j,k\leqslant n} z_{j,k} f(a_j, a_k) = 0 \text{ for some } z_{j,k} \in \Lambda\ (1 \leqslant j, k \leqslant n), \text{ then } \sum_{1\leqslant j,k\leqslant n} z_{j,k} f(\alpha a_j, a_k) = 0. \tag{11}$$

Indeed, the direct implication is immediate. Conversely, suppose that α satisfies (11), and let $t \geqslant 1$ and $x_1, \dots, x_t, y_1, \dots, y_t \in N$ be such that $\sum_{i=1}^{t} f(x_i, y_i) = 0$. Write each x_i and y_i in terms of the

generators $a_1, \ldots, a_n$,

$$x_i = \sum_{j=1}^{n} x_{i,j} a_j, \quad \text{and} \quad y_{i=1}^{n} = \sum_{k} y_{i,k} a_k, \quad x_{i,j}, y_{i,k} \in \Lambda.$$

Since f is bilinear,

$$\sum_{i=1}^{t} f(x_i, y_i) = \sum_{1 \leqslant j,k \leqslant n} \left(\sum_{i=1}^{t} x_{i,j} y_{i,k} \right) f(a_j, a_k) = 0.$$

Thus by (11),

$$0 = \sum_{1 \leqslant j,k \leqslant n} \sum_{i=1}^{t} x_{i,j} y_{i,k} f(\alpha a_j, a_k) = \sum_{i=1}^{t} f(\alpha x_i, y_j).$$

This completes the proof of the claim.

The set S of all tuples $(z_{i,j}) \in \Lambda^{n^2}$ such that $\sum_{1 \leqslant i,j \leqslant n} z_{i,j} f(a_i, a_j) = 0$ forms a submodule of Λ^{n^2}, and so it admits a finite generating set, say $X = \{\mathbf{s}_i \mid i = 1, \ldots, T\}$. Write $\mathbf{s}_i = (s_{i,j,k} \mid 1 \leqslant j, k \leqslant n)$. Then $\alpha \in Z(Sym(f))$ belongs to $R(f)$ if and only if

$$\sum_{1 \leqslant j,k \leqslant n} \left(\sum_{i=1}^{t} q_i s_{i,j,k} \right) f(\alpha a_j, a_k) = 0, \quad \text{for all} \quad q_1, \ldots, q_t \in \Lambda. \tag{12}$$

Equivalently,

$$\sum_{i=1}^{t} q_i \left(\sum_{1 \leqslant j,k \leqslant n} s_{i,j,k} f(\alpha a_j, a_k) \right) = 0, \quad \text{for all} \quad q_1, \ldots, q_t \in \Lambda. \tag{13}$$

By making appropriate choices for the q_i's, one sees that (13) holds if and only if each one of the expressions inside the parenthesis is 0. It follows that $R(f)$ is e-definable as a set in F_1. Consequently, $R(f)$ is e-interpretable as a Λ-algebra in F_1, since all the operations of $(R(f); \mathcal{L}_{alg})$ are already present in the signature of the latter. It follows that $R(f)$ is e-interpretable as a Λ-algebra in $(N, M; f, \mathcal{L}_{mod})$.

Finally we prove Item 1, i.e. that $Z(Sym(f))$, $R(f)$, N, and M are all simultaneously either finite, or all simultaneously infinite. We first claim that, in general, if Θ is an associative commutative unitary ring, then any finitely generated faithful Θ-module K is infinite if and only if Θ is infinite. Indeed, if K is finite, then $End_\Theta(K)$ is finite as well, because $End_\Theta(K)$ embeds as a Θ-module into K^n, for some n (see Remark 3.7). Since K is a faithful Θ-module, there exists an embedding $\Theta \hookrightarrow End_\Theta(K)$, and hence Θ is finite as well. On the other hand, if K is infinite, then, since K is finitely generated, there must exist $k \in K$ such that the set $\{\theta k \mid \theta \in \Theta\}$ is infinite, hence Θ is infinite. The claim follows.

Observe that both N and M are faithful $R(f)$-modules, and that N is also a faithful $Z(Sym(f))$-module. We claim that both these modules are finitely generated. Indeed, let $\Lambda_N = \{\lambda \in \Lambda \mid \lambda n = 0 \text{ for all } n \in N\}$, and define Λ_M analogously. Then N (resp. M) is a finitely generated faithful Λ/Λ_N-module (resp. Λ/Λ_M-module). Using that f is full and non-degenerate, one can see that N is also a faithful Λ/Λ_M-module under the action $(\lambda + \Lambda_M)x = \lambda x$. With this action, Λ/Λ_M becomes a ring of scalars of f, and so by maximality of $R(f)$ we have $\Lambda/\Lambda_M \leqslant R(f) \leqslant Z(Sym(f))$ as subrings of $End_\Lambda(N)$. Similar arguments yield $\Lambda/\Lambda_N \leqslant R(f) \leqslant Z(Sym(f))$. Since N is finitely generated as a Λ/Λ_N-module, it is also finitely generated as a $R(f)$-module. Similarly, N is finitely generated as a $Z(Sym(f))$-module, and M is finitely generated as a $R(f)$-module. Observe also that all these modules are faithful since $Z(Sym(f))$ and $R(f)$ embed in $End_\Lambda(N)$ by construction. This completes the proof of the claim. Item 1 of the statement of the theorem follows now from this and the previous claim. □

3.3 Arbitrary bilinear maps

In this subsection we keep the assumption that Λ is a Noetherian associative commutative ring with identity (possibly infinitely generated). Our next goal is to generalize Theorem 3.6 to arbitrary bilinear maps. Given a map Λ-bilinear map between finitely generated Λ-modules $f : A \times B \to C$, we let the left and right *annihilators* of f be, respectively,

$$Ann_l(f) = \{a \in A \mid f(a, y) = 0 \text{ for all } y \in B\},$$
$$Ann_r(f) = \{b \in B \mid f(x, b) = 0 \text{ for all } x \in A\}.$$

Theorem 3.10. *Let $f : A \times B \to C$ be a Λ-bilinear map between finitely generated Λ-modules. Then there exists an associative, commutative, unitary Λ-algebra Θ such that $(\Theta; \mathcal{L}_{alg})$ is finitely generated as a Λ-module and it is e-interpretable in $F = (A, B, C; f, \mathcal{L}_{mod})$. Moreover,*

1. *In case that Λ is a field or the ring $\mathbb{Z}$, then $(\Theta; \mathcal{L}_{ring})$ is e-interpretable in $(A, B, C; f, \mathcal{L}_{group})$.*
2. *Θ is infinite if and only if both Λ-modules $\langle f(A, B)\rangle_\Lambda$ and $A/Ann_l(f) \times B/Ann_r(f)$ are infinite, respectively. Here $\langle f(A, B)\rangle_\Lambda$ denotes the Λ-submodule of C generated by the set $\{f(a, b) \mid a \in A, b \in B\}$.*

The proof of this result relies on constructing from f a suitable full non-degenerate bilinear map of the form $g : X \times X \to Y$, so that we can apply Theorem 3.6 to it. Observe that f induces a full non-degenerate Λ-bilinear map

$$f_1 : A/Ann_l(f) \times B/Ann_r(f) \to \langle f(A, B)\rangle_\Lambda. \tag{14}$$

Let us denote $F = (A, B, C; f, \mathcal{L}_{mod})$, $A_1 = A/Ann_l(f)$, $B_1 = B/Ann_r(f)$, $C_1 = \langle f(A, B)\rangle_\Lambda$, and $F_1 = (A_1, B_1, C_1; f_1, \mathcal{L}_{mod})$. Note that A_1, B_1 and C_1 are finitely generated since A, B and C are Noetherian modules. If $A_1 = B_1$, then f_1 satisfies the hypothesis of Theorem 3.6. Otherwise consider the map

$$\begin{aligned} f_2 :&\big(A_1 \times B_1\big) \times \big(A_1 \times B_1\big) \to C_1 \times C_1 \\ &\big((a, b), (a', b')\big) \mapsto \big(f_1(a, b'), f_1(a', b)\big). \end{aligned} \tag{15}$$

One can easily check that f_2 is a full non-degenerate Λ-bilinear map between finitely generated Λ-modules. Denote $F_2 = (A_1 \times B_1, C_1 \times C_1; f_2, \mathcal{L}_{mod})$. Either f_1 or f_2 are of the desired form, hence Theorem 3.6 can be applied to at least one of them. Moreover:

Lemma 3.11. *Both F_1 and F_2 are e-interpretable in F. The same is true if one replaces $\mathcal{L}_{mod}$ with $\mathcal{L}_{group}$ in F_1, F_2, and F.*

Proof. Let $S_A = \{a_1, \dots, a_n\}$ and $S_B = \{b_1, \dots, b_m\}$ be generating sets of A and B, respectively. The submodules $Ann_l(f)$ and $Ann_r(f)$ are e-definable as sets in F by the systems of equations $f(x, b_i) = 0$, $i = 1, \dots, m$, and $\wedge_i f(a_i, y) = 0$, $i = 1, \dots, n$, respectively. Here x and y are variables taking values in A and in B, respectively. An element $c \in C$ belongs to $C_1 = \langle f(A, B)\rangle_\Lambda$ if and only if there exist elements λ_{ij}, $i = 1, \dots, n$, $j = 1, \dots, m$, such that

$$c = \sum_{1 \leqslant i,j \leqslant n,m} \lambda_{i,j} f(a_i, b_j) = \sum_{j=1}^{m} f\left(\sum_{i=1}^{n} \lambda_{i,j} a_i, b_j\right).$$

It follows that C_1 is e-definable as a set in F by the equation $z = \sum_j f(x_j, b_j)$ on variables z and $X = \{x_j \mid j = 1, \dots, n\}$. The variable z takes values in C and the variables from X take values in A.

The operations of $Ann_l(f), Ann_r(f)$ and C_1 are e-interpretable in F because they are already present in the signature of F. Hence by Lemma 2.6 and Remark 2.8, $(A_1; \mathcal{L}_{mod})$ and $(B_1; \mathcal{L}_{mod})$ are e-interpretable as Λ-modules in $(A; \mathcal{L}_{mod})$ and $(B; \mathcal{L}_{mod})$, respectively. Moreover, from the proof of

Lemma 2.6 and the fact that the e-definitions in F of $Ann_l(f)$ and $Ann_r(f)$ do not use multiplication by scalars, we have that $(A_1; \mathcal{L}_{group})$ and $(B_1; \mathcal{L}_{group})$ are e-interpretable in $(A; \mathcal{L}_{group})$ and $(B; \mathcal{L}_{group})$, respectively.

The preimage in F of the graph of f_1 is e-definable in F by the system consisting on the two equations $z = f(x, y)$ and $z = \sum_j f(x_j, b_j)$ on variables $z, x, y, X = \{x_1, \ldots, x_m\}$ taking values in C, A, B, and A, respectively (note that the second equation is added to ensure that z takes values in C_1). Again this equation does not use multiplication by scalars. We conclude that $F_1 = (A_1, B_1, C_1; f_1, \mathcal{L}_{mod})$ is e-interpretable in $(A, B, C; f, \mathcal{L}_{mod})$, and that the same holds if one drops multiplication by scalars in both structures.

Finally, we claim that $(A_1 \times B_1; \mathcal{L}_{mod})$ is e-interpretable in $(A_1, B_1; \mathcal{L}_{mod})$, and $(C_1 \times C_1; \mathcal{L}_{mod})$ is e-interpretable in $(C_1; \mathcal{L}_{mod})$. Indeed, both $A_1 \times B_1$ and $C_1 \times C_1$ are basic sets of (A_1, B_1) and C_1, and so they are defined as sets by empty systems of equations. Similarly as before, the equations $z = f_1(x, y')$ and $z' = f_1(x', y)$ on variables x, y, x', y', z, z' taking values in $A_1, B_1, A_1, B_1, C_1, C_1$, respectively, e-define the graph of f_2 in F_1. It follows that the whole two-sorted structure F_2 is e-interpretable in F_1, and also in F by transitivity of e-interpretations. Moreover, in all e-interpretations we constructed, multiplication by scalars Λ in one structure is only used to e-interpret multiplication by scalars Λ in the other structure. Hence F_2 is still e-interpretable in F if one replaces $\mathcal{L}_{mod}$ by $\mathcal{L}_{group}$ in the F_2 and F. □

Proof of Theorem 3.10. The result follows immediately after using Theorem 3.6 in order to e-interpret $(Z(Sym(f_2)); \mathcal{L}_{alg})$ or $(Z(Sym(f_1)); \mathcal{L}_{alg})$ in F_2 or F_1, depending on whether or not $A_1 = B_1$, respectively. Items 1 and 2 are a direct consequence of Items 1 and 3 of Theorem 3.6. □

Remark 3.12. In Theorem 3.10 we e-interpreted $Z(Sym(f_2))$ in F_2 (or $Z(Sym(f_1))$ in F_1 if $A_1 = B_1$). Alternatively one can also e-interpret the largest ring of scalars $R(f_2)$ of f_2 in F_2 (similarly for f_1). This may have some advantages if one seeks to study the structure of A, B, C and f, because $R(f_2)$ is determined by "more properties" of these than $Z(Sym(f_2))$. However, when it comes to the Diophantine problem, $Z(Sym(f_2))$ is a more practical choice than $R(f_2)$, because it uses a simpler e-interpretation. For instance, as we have seen, if Λ is a field then one can drop multiplication by scalars in the e-interpretation of $(Z(Sym(f_2)); \mathcal{L}_{ring})$, whereas there is no apparent way to do the same with $(R(f_2); \mathcal{L}_{ring})$.

4 Rings and algebras over finitely generated associative commutative unitary rings

The following lemma is a combination of the results obtained so far. It constitutes the main "general tool" presented in this paper. We will explore its consequences throughout the rest of the section. In [11] it is applied further to the area of group theory. We refer again to Subsection 2.3 for important notation and terminology conventions.

Lemma 4.1. *Let Λ be a associative commutative unitary ring, let $f : A \times B \to C$ be a Λ-bilinear map between finitely generated Λ-modules, and write $C_1 = \langle Im(f) \rangle_\Lambda$. Suppose that $(A, B, C; f, \mathcal{L}_{mod})$ is e-interpretable in some structure $\mathcal{M}$. Then there exists an associative, commutative, unitary Λ-algebra R such that R is finitely generated as a Λ-module and $(R; \mathcal{L}_{alg})$ is e-interpretable in $\mathcal{M}$. Moreover, R is infinite if and only if C_1 is infinite.*

Furthermore, if C_1 is infinite and Λ is finitely generated, then there exists a ring of integers O of a number field or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(R; \mathcal{L}_{ring})$, and in $\mathcal{M}$. Additionally in this case:

1. *If Λ has positive characteristic p, then the ring of polynomials $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in $\mathcal{M}$, and $\mathcal{D}(\mathcal{M})$ is undecidable.*

2. *If $\Lambda = \mathbb{Z}$ then O is a ring of algebraic integers.*

If Λ is $\mathbb{Z}$ or a field, then the whole lemma holds after replacing $(A, B, C; f, \mathcal{L}_{mod})$ by $(A, B, C; f, \mathcal{L}_{group})$ and $(R; \mathcal{L}_{alg})$ by $(R; \mathcal{L}_{ring})$, i.e. multiplication by scalars is not required.

Proof. By Theorem 3.10, there exists an associative commutative unitary Λ-algebra R such that R is finitely generated as a Λ-module and $(R; \mathcal{L}_{alg})$ is e-interpretable in $(A, B, C; f, \mathcal{L}_{mod})$. Hence $(R; \mathcal{L}_{alg})$ is e-interpretable in $(R; \mathcal{L}_{alg})$ by transitivity of e-interpretations. The statement regarding the cardinality of R follows from Item 2 of Theorem 3.10.

Suppose that C_1 is infinite and that Λ is finitely generated. Then R is infinite and finitely generated as a ring. Hence, by Theorem 2.17 there exists a ring of integers O of a number field or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(R; \mathcal{L}_{ring})$, and hence in $\mathcal{M}$.

If Λ has positive characteristic $p > 0$, then so does R, because it is a unitary algebra over Λ. Hence $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in $\mathcal{M}$, by Item 1 of Theorem 2.17 and by transitivity. If $\Lambda = \mathbb{Z}$, then R is finitely generated as an abelian group, hence O is a ring of algebraic integers by Item 3 of Theorem 2.17.

If Λ is $\mathbb{Z}$ or a field, then $(R; \mathcal{L}_{ring})$ is e-interpretable in $(A, B, C; f, \mathcal{L}_{group})$, by Item 1 of Theorem 3.10. Therefore if the latter is e-interpretable in $\mathcal{M}$, then the lemma holds after replacing $\mathcal{L}_{alg}$ by $\mathcal{L}_{ring}$ and $\mathcal{L}_{mod}$ by $\mathcal{L}_{group}$. □

4.1 Rings and algebras which are finitely generated as modules

Throughout this subsection, Λ denotes a finitely generated associative commutative unitary ring, possibly infinitely generated.

The following is one of the main results of the paper. The case $\Lambda = \mathbb{Z}$ will be considered separately afterwards. We recall that the language $\mathcal{L}_{alg}$ of a Λ-algebra refers to the language of rings together with multiplication by any constant element from Λ (however variables cannot take values in Λ), see Subsection 2.3 for more details.

Theorem 4.2. *Let R be a (possibly non-associative, non-commutative, and non-unitary) algebra over a finitely generated associative commutative unitary ring Λ. Suppose that R is finitely generated as a Λ-module. Then if, $R^2 = \langle \{xy \mid x \in R, y \in R\} \rangle_\Lambda$ is infinite, there exists a ring of integers O of a number field or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(R; \mathcal{L}_{alg})$, and the Diophantine problem $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(R; \mathcal{L}_{alg})$. Moreover:*

1. *If R^2 is infinite and Λ has positive characteristic, then $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in $(R; \mathcal{L}_{alg})$ for some prime integer p, and $\mathcal{D}(R; \mathcal{L}_{alg})$ is undecidable.*

2. *If R^2 is finite and $\mathcal{D}(R; \mathcal{L}_{mod})$ is decidable, then $\mathcal{D}(R; \mathcal{L}_{alg})$ is decidable.*

If Λ is a finite field, then all the above holds after replacing $(R; \mathcal{L}_{alg})$ by $(R; \mathcal{L}_{ring})$.

Proof. The ring multiplication operation $\cdot$ of R induces a Λ-bilinear map between finitely generated Λ-modules $\cdot : R \times R \to R$, with $\langle Im(\cdot) \rangle_\Lambda = R^2$. Since the three-sorted structure $(R, R, R; \cdot, \mathcal{L}_{mod})$ is e-interpretable in $(R; \mathcal{L}_{alg})$, the result, except Item 2, follows from Lemma 4.1.

We now prove Item 2. Let Σ be a system of equations in the Λ-algebra R. By adding new variables and equations in an analogous way as done in the proof of Lemma 2.12, we may rewrite that Σ into an equivalent system of equations, still denoted Σ, of the following form: the new Σ consists in a system of equations in the Λ-module $(R; \mathcal{L}_{mod})$ (i.e. a system of Λ-linear equations), in conjunction with a system of equations of the form $x_1 = y_1 z_1, x_2 = y_2 z_2, \ldots, x_k = y_k z_k$ where the $x_1, \ldots, x_k, y_1, \ldots, y_k, z_1, \ldots, z_k$ are variables taking values in R. Note that no variable appears more than once in this last part of the system.

Note that $Ann_l(\cdot)$ and $Ann_r(\cdot)$ are finite index submodules of R, by Item 2 of Theorem 3.10. Let $S_l = \{a_1, \ldots, a_s\}$ and $S_r = \{b_1, \ldots, b_t\}$ be full systems of coset representatives of $R/Ann_l(\cdot)$ and $A/Ann_r(\cdot)$, respectively. Let also S_R be a finite generating set of R.

For each variable $y \in \{y_1, \ldots, y_k\}$, do the following: choose a coset representative $a \in \{a_1, \ldots, a_s\}$, and introduce a new variable y'. Then replace each occurrence of y in Σ by $a + y'$. We now wish to make y' to take values in $Ann_l(\cdot)$. The system of equations $\wedge_{r \in S_R} ur = 0$ on the variable u e-defines $Ann_l(\cdot)$ in R. Hence, we add the system $\wedge_{r \in S_L} y'r = 0$ to Σ in order to ensure that y' takes values in $Ann_l(\cdot)$. Notice that $\wedge_{r \in S_L} y'r = 0$ is a system of equations in the Λ-module $(R; \mathcal{L}_{mod})$.

We now proceed in an analogous way with each variable $z \in \{z_1, \ldots, z_k\}$, this time replacing z by $b + z'$ for some $b \in \{b_1, \ldots, b_t\}$, and adding the system of equations $\wedge_{r \in S_R} rz' = 0$ to Σ, in order to ensure that z' takes values in $Ann_r(\cdot)$.

Let Σ' be the resulting system of equations after making all the above transformations. Since there are finitely many coset representatives, the number of all possible resulting systems Σ' is finite. Let $\Sigma_1, \ldots, \Sigma_m$ be all of them. It is clear that Σ has a solution if and only if Σ_i has a solution for some $i = 1, \ldots, m$.

We now prove that it is possible to decide algorithmically if each one of the Σ_i has a solution or not, in which case our proof is concluded. Indeed, each Σ_i consists in some equations in the Λ-module $(R; \mathcal{L}_{mod})$, together with some equations of the form $x = (a + y')(b + z')$, where y' and z' are variables taking values in $Ann_l(\cdot)$ and in $Ann_r(\cdot)$, respectively. Hence each equation $x = (a + y')(b + z')$ can be replaced by $x = ab$, which is an equation in $(R; \mathcal{L}_{mod})$. Thus Σ_i is equivalent to a system of Λ-linear equations. By assumption, we can algorithmically check if Σ_i has a solution. □

The following is a particular case of the previous Theorem 4.2. It is stated separately due to its independent interest.

Theorem 4.3. *Let A be a ring (possibly non-associative, non-commutative, and non-unitary). Assume that A is finitely generated as an abelian group, and that A^2 is infinite. Then there exists a ring of algebraic integers O such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(A; \mathcal{L}_{ring})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(A, \mathcal{L}_{ring})$. If otherwise A^2 is finite, then $\mathcal{D}(R; \mathcal{L}_{ring})$ is decidable.*

Proof. The first part of the theorem follows in the same way as Theorem 4.2, taking $\Lambda = \mathbb{Z}$ and observing that here O is a ring of algebraic integers by Item 2 of Lemma 4.1. The last part follows by Item 2 of Theorem 4.2, since here $(A; \mathcal{L}_{mod})$ is a finitely generated abelian group and $\mathcal{D}(A; \mathcal{L}_{group})$ is decidable [8], hence $\mathcal{D}(A; \mathcal{L}_{mod})$ is decidable. □

4.2 Finitely generated associative, commutative non-unitary rings and algebras

In this subsection we study associative commutative rings and algebras that do not have an identity element. We begin with a lemma that allows us to e-interpret a certain unitary algebra.

Lemma 4.4. *Let A be a finitely generated associative commutative non-unitary algebra over a (possibly infinitely generated) associative commutative unitary ring Θ. Then there exists an associative commutative unitary ring Λ and an associative commutative unitary Λ-algebra B such that B is finitely generated as a Λ-module, and $(B; \mathcal{L}_{alg})$ is e-interpretable in $(A; \mathcal{L}_{alg})$. Additionally, A^2 is infinite if and only if B is infinite.*

Proof. Define $\Lambda = \Theta \oplus A$ to be the set of formal sums of elements from Θ and from A, equipped with the natural addition and multiplication operations. More precisely, $\Lambda = \Theta \oplus A = \{(\theta, a) \mid \theta \in \Theta, a \in A\}$ and Λ is endowed with the following ring operations: $(\theta_1, a_1) + (\theta_2, a_2) = (\theta_1 + \theta_2, a_1 + a_2)$ and $(\theta_1, a_1) \cdot (\theta_2, a_2) = (\theta_1\theta_2, \theta_1 a_2 + \theta_2 a_1 + a_1 a_2)$. We have that Λ is an associative commutative unitary ring.

Moreover, Λ acts naturally by endomorphisms on A, i.e. $(\theta, a) \cdot a' = \theta a' + aa'$ for all $(\theta, a) \in \Lambda$ and all $a' \in A$. With this action A is a Λ-algebra. During this proof we write A_Λ and A_Θ to refer to A seen as a Λ-algebra or as a Θ-algebra, respectively. The operation of multiplication by a given scalar $\theta \oplus a \in \Lambda$ is e-interpreted in $(A_\Theta; \mathcal{L}_{alg})$ by the equation $y = \theta x + ax$ on variables y, x taking values in

A. Hence $(A_\Lambda; \mathcal{L}_{alg})$ is e-interpretable in $(A_\Theta; \mathcal{L}_{alg})$. Suppose that A_Θ is generated as a Θ-algebra by n elements $S_A = \{a_1, \ldots, a_n\}$. Then, since each element of A can be written as a linear combination of monomials from $\Theta[a_1, \ldots, a_n]$, we have that A_Λ is generated as a Λ-module by S_A, since for all $x \in A$ there exists $y_1, \ldots, y_n \in \Lambda$ such that $x = \sum_i y_i a_i$. Hence A is finitely generated as a Λ-module.

The ring multiplication of A_Λ is a Λ-bilinear map between finitely generated Λ-modules $\cdot : A \times A \to A$. Moreover, $(A_\Lambda, A_\Lambda, A_\Lambda; \cdot, \mathcal{L}_{mod})$ is e-interpretable in $(A_\Lambda; \mathcal{L}_{alg})$, which in turn is e-interpretable in $(A_\Theta; \mathcal{L}_{alg})$. Hence, by the first part of Lemma 4.1, and by transitivity of e-interpretations, there exists an associative commutative unitary Λ-algebra D_Λ, which is finitely generated as a Λ-module, and $(D_\Lambda; \mathcal{L}_{alg})$ is e-interpretable in $(A_\Theta; \mathcal{L}_{alg})$.

Finally, we note that $(A_\Lambda)^2 = \langle Im(\cdot)\rangle_\Lambda$ is infinite if and only if D_Λ is also infinite, by Lemma 4.1. □

We are ready to study associative commutaty non-unitary algebras. We convene that the *characteristic* of a non-unitary ring A is defined as the maximum positive integer n such that $nx = 0$ for all $x \in R$.

Theorem 4.5. *Let L be a finitely generated associative commutative non-unitary algebra over a finitely generated associative commutative unitary ring Θ, with L^2 infinite. Then there exists a ring of integers O of a number field or of a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(L; \mathcal{L}_{alg})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(L; \mathcal{L}_{alg})$.*

Moreover, if Θ has positive characteristic, then O is the ring of integers of a global function field, $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in $(L; \mathcal{L}_{alg})$ for some prime integer p, and $\mathcal{D}(L; \mathcal{L}_{alg})$ is undecidable.

Proof. Let B be the associative commutative unitary Λ-algebra, finitely generated as a Λ-module, given by Item 1 of Lemma 4.4, where $\Lambda = \Theta \oplus B$. Suppose that L^2 is infinite. By this same lemma, B is infinite, and since B is unitary we have that $B^2 = B$ is infinite as well. Note further that if Θ has positive characteristic then so does Λ. The result now follows by transitivity of e-interpretations and by Theorem 4.2 applied to B. □

Finally, we formulate and slightly modify the previous Theorem 4.5 for the particular case when L is a ring, i.e. when $\Theta = \mathbb{Z}$.

Theorem 4.6. *Let A be a finitely generated associative commutative non-unitary ring, with A^2 infinite. Then there exists a ring of integers O of a number or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(A; \mathcal{L}_{ring})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(A; \mathcal{L}_{ring})$.*

Moreover, if A has positive characteristic, then the following holds: O is the ring of integers of a global function field; the ring of polynomials $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in A for prime integer p; and $\mathcal{D}(A; \mathcal{L}_{ring})$ is undecidable.

Proof. Let n be the characteristic of A. Then A is a finitely generated $\mathbb{Z}/n\mathbb{Z}$-algebra, where if $n = 0$ we understand that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$. Moreover, multiplication by scalars from $\mathbb{Z}/n\mathbb{Z}$ is e-interpretable in $(A, \mathcal{L}_{ring})$ since $(k + n\mathbb{Z}) \cdot x = x \overset{k}{+} \ldots + x$ for any $x \in A$ and any equivalence class $(k + n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$ with representative $0 \leqslant k \leqslant n - 1$. Hence $(A, \mathcal{L}_{alg})$ is e-interpretable in $(A, \mathcal{L}_{ring})$. The result now follows by applying the previous Theorem 4.5 on $(A, \mathcal{L}_{alg})$, and by transitivity of e-interpretations. □

4.3 Finitely generated rings and algebras satisfying an infiniteness condition

In this subsection Λ denotes an associative commutative unitary ring, possibly infinitely generated.

We next apply Theorems 4.2 and 4.3 to certain classes of non-commutative finitely generated rings and algebras L which are not necessarily finitely generated as modules. The approach consists in e-defining an ideal I_n in L that contains "enough" products of at least n elements of L (for example, the ideal generated by all such products), so that the quotient L/I_n is infinite and finitely generated as a module. Then it suffices to apply the results from Section 4.1, together with transitivity of e-interpretations. This approach presents two challenges:

1. I_n can be difficult to e-define if L is non-associative (hence Definition 4.8).

2. L/I_n may be finite. For instance, if L is unitary (i.e. it has an identity element) one cannot simply take I_n to be the ideal generated by all products of n elements of L, since then $I_n = L$, and $L/I_n = 0$ (hence the next definition).

Definition 4.7. Let L be a Λ-algebra, and let T be a generating set of L. If L is non-unitary then we let $I_n(T)$ or I_n denote the Λ-ideal generated by all products of n elements of T.

If L is unitary then we let $I_n(T)$ or I_n denote the Λ-ideal generated by all products of n elements of $T \backslash \{\lambda \cdot 1 \mid \lambda \in \Lambda\}$, where 1 denotes the multiplicative identity of L.

Throughout the rest of the section, L denotes a finitely generated Λ-algebra, possibly non-associative, non-commutative, non-unitary, and not finitely generated as a Λ-module. We fix a finite set $T = \{a_1, \dots, a_m\}$ as in Definition 4.7, and we define the ideals I_n accordingly.

Definition 4.8. Let L be a Λ-algebra and let $T = \{a_1, a_2, \dots\}$ be a generating set of L. Then L is called *left-normed-generated* with respect to T if, for all $n \geqslant 1$, $I_n(T)$ is generated as a Λ-module by all left-normed products $\{(a_{i_1}(a_{i_2}(\dots(a_{i_{k-1}}a_{i_k})\dots))) \mid k \geqslant n,\ 1 \leqslant i_1, \dots, i_k\}$.

Notice that any associative algebra is left-normed-generate with respect to any generating set.

Lemma 4.9. *Suppose that L is a left-normed-generated Λ-algebra with respect to some finite generating set, and let $n \geqslant 1$. Then $(L/I_n; \mathcal{L}_{ring})$ and $(L/I_n; \mathcal{L}_{alg})$ are e-interpretable in $(L; \mathcal{L}_{ring})$ and $(L; \mathcal{L}_{alg})$, respectively. Moreover, L/I_n is a Λ-algebra which is finitely generated as a Λ-module.*

Proof. Let $T = \{a_1, \dots, a_m\}$ be a finite generating set of L. Then each element of I_n is a finite sum of elements of the form

$$\lambda(a_{i_1}(a_{i_2}(\dots(a_{i_{k-1}}a_{i_k})\dots))), \quad \lambda \in \Lambda, \quad k \geqslant n. \tag{16}$$

Hence each element as in (16) can be written as $(a_{i_1}(\dots(a_{i_{n-1}}y)\dots))$ for some $y \in L$ in the non-unitary case. Consequently, if L is non-unitary, then I_n is e-definable as a set in $(L; \mathcal{L}_{ring})$ by the equation

$$x = \sum_{1 \leqslant i_1, \dots, i_{n-1} \leqslant m} (a_{i_1}(\dots(a_{i_{n-1}}y_{i_1,\dots,i_{n-1}})\dots)) \tag{17}$$

on variables x and $\{y_{i_1,\dots,i_{n-1}}\}$ (the e-definition is in $(L; \mathcal{L}_{ring})$ because it makes no use of multiplication by scalars Λ). Observe however that (17) would not work in the case that L is unitary, since a solution to (17) may yield $x \in I_{n-1}$, for example if each $y_{i_1,\dots,i_{n-1}}$ is a Λ-multiple of 1. This can be solved by, in this case, taking the equation

$$x = \sum_{1 \leqslant i_1, \dots, i_n \leqslant m} (a_{i_1}(\dots(a_{i_{n-1}}(a_{i_n}y_{i_1,\dots,i_n}))\dots)) \tag{18}$$

instead of (17). Hence, in both cases $(L/I_n; \mathcal{L}_{ring})$ and $(L/I_n; \mathcal{L}_{alg})$ are e-interpretable in $(L; \mathcal{L}_{ring})$ and $(L; \mathcal{L}_{alg})$ by Lemma 2.6.

Finally, note that L/I_n is generated as a Λ-module by the projection of all products of less than n elements of T, together with $1 + I_n$ if L is unitary. It follows that L/I_n is finitely generated as a Λ-module. □

We now state the main result of this subsection. The ideals I_n are defined with respect to any set T satisfying the conditions of Definition 4.7.

Theorem 4.10. *Let L be a finitely generated algebra (possibly non-associative, non-commutative and non-unitary) over a finitely generated associative commutative unitary ring Λ. Suppose that L is left-normed-generated with respect to some finite generating set, and that $(L/I_n)^2$ is infinite for some $n \geqslant 1$. Then there exists a ring of integers O of a number field or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(L; \mathcal{L}_{alg})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is Karp-reducible to $\mathcal{D}(L; \mathcal{L}_{alg})$. Moreover:*

1. *If Λ has positive characteristic p, then $(\mathbb{F}_p[t]; \mathcal{L}_{ring})$ is e-interpretable in $(L; \mathcal{L}_{alg})$, and $\mathcal{D}(L; \mathcal{L}_{alg})$ is undecidable.*

2. *If L is a ring (i.e. $\Lambda = \mathbb{Z}$) then O is a ring of algebraic integers.*

If Λ is $\mathbb{Z}$ or a finite field then all the above holds after replacing $(L; \mathcal{L}_{alg})$ by $(L; \mathcal{L}_{ring})$.

Proof. By Lemma 4.9, L/I_n is a Λ-algebra, it is finitely generated as a Λ-module, and it is e-interpretable as an algebra in $(L; \mathcal{L}_{alg})$. The same result states that $(L/I_n, \mathcal{L}_{ring})$ is e-interpretable as a ring in $(L; \mathcal{L}_{ring})$. By hypothesis, we can take n so that $(L/I_n)^2$ is infinite. Now the result follows by Theorems 4.2 and 4.3 applied to L/I_n, and by transitivity of e-interpretations. □

We next apply the previous theorem to the class of Lie algebras, which are popular examples of non-associative, non-commutative and non-unitary algebras. First, we prove that Lie algebras are left-normed-generated.

Lemma 4.11. *Any countably generated Lie algebra L is left-normed-generated with respect to any countable generating set.*

Proof. Let $A = \{a_1, a_2, \dots\}$ be a generating set of L. In [2] it is proved that any free Lie algebra $F = F(b_1, b_2, \dots)$ generated by $B = \{b_1, b_2, \dots\}$ is freely generated as a module by a subset of the set $B = \{(b_{i_1}(b_{i_2}(\dots(b_{i_{k-1}}b_{i_k})\dots))) \mid k \geqslant 1,\ 1 \leqslant i_1, \dots, i_k\}$. In particular, it is left-normed-generated with respect to B. Let $\pi : F \to L$ be the natural projection of F onto L sending b_i to a_i for all $i \geqslant 1$. We denote by I_n^F and I_n^L the ideals of F and L, respectively, generated by all products of at least n elements from B and from A, respectively. Observe that $\pi(I_n^F) = I_n^L$.

For each $n \geqslant 1$, let S_n be a subset of $\{[b_{i_1}, [b_{i_2}, [\dots, [b_{i_{k-1}}, b_{i_k}]\dots]]] \mid k \geqslant n,\ 1 \leqslant i_1, \dots, i_k\}$ such that the ideal I_n^F of F is generated by all Λ-multiples of S_n. Then $\pi(I_n^F) = I_n^L$ is generated by all Λ-multiples of $\pi(S_n)$. Now $\pi(S_n)$ is a subset of

$$\{[\pi(b_{i_1}), [\pi(b_{i_2}), [\dots, [\pi(b_{i_{k-1}}), \pi(b_{i_k})]\dots]]] \mid k \geqslant n,\ 1 \leqslant i_1, \dots, i_k\},$$

hence L is left-normed generated with respect to $\pi(B) = A$. □

The next two corollaries follow immediately from Theorem 4.10 and Lemma 4.11. By $[L/I_n, L/I_n]$ we denote the Λ-submodule of L/I_n generated by $\{[x, y] \mid x, y \in L/I_n\}$.

Corollary 4.12. *Let L be a finitely generated Lie Λ-algebra. Assume that $[L/I_n, L/I_n]$ is infinite for some $n \geqslant 1$, and that Λ is finitely generated. Then the conclusions of Theorem 4.10 hold for L.*

Corollary 4.13. *Let F be a finitely generated free associative Λ-algebra (possibly non-commutative and non-unitary) or a free Lie algebra of rank at least 2, with Λ finitely generated. Then the conclusions of Theorem 4.10 hold for F.*

Proof. If F is a free Lie algebra, let I_n be taken with respect to any free generating set of F, $n \geqslant 1$. If F is a free associative algebra freely generated by $\{1, a_1, \dots, a_m\}$, let I_n be taken with respect to $\{a_1, \dots, a_m\}$, $n \geqslant 1$. In both cases $(F/I_n)^2$ is infinite for all $n \geqslant 3$. Therefore the result follows from Theorem 4.10 and the previous Corollary 4.12. □

Corollary 4.13 complements Romankov's [33], and Kharlampovich and Miasnikov's [15, 17] papers on free algebras. In the first reference [33], it is proved that $\mathcal{D}(F; \mathcal{L}_{ring})$ is undecidable for many types of free rings F. In particular, it is proved that the algebras of Corollary 4.13 have undecidable Diophantine problem if $\Lambda = \mathbb{Z}$. In [15, 17] it is proved that $\mathcal{D}(F; \mathcal{L}_{ring})$ is undecidable if Λ is an arbitrary field, and F is a free associative non-commutative unitary algebra, or a free Lie algebra of rank at least 3. Note that an infinite field is necessarily infinitely generated, hence our Corollary 4.13 does not intersect with [15, 17].

4.4 Undecidability of first-order theories

The *first-order theory* T (or *elementary theory*) of a structure M in a language $\mathcal{L}$ is the set of all first-order sentences in $\mathcal{L}$ that are true in M. One says that T is decidable if there exists an algorithm that, given a sentence ϕ in $\mathcal{L}$, determines if ϕ is true in M or not, i.e. if ϕ belongs to T. If such an algorithm does not exist then T is said to be undecidable.

The first-order theory *with constants* of M in the language $\mathcal{L}$ is the set of first order sentences that are true in M, allowing the use of any constant element from M in the sentences.

Noskov proved in [29] that the first-order theory of an infinite finitely generated associative commutative unitary ring is undecidable in the language of rings with constants. In particular this is true for the ring of integers of any number field or global function field. Hence using transitivity of e-interpretations and Proposition 2.11 we immediately obtain the following:

Theorem 4.14. *Let L be a ring or an algebra satisfying the hypotheses of one of the Theorems 2.17, 4.2, 4.3, 4.5, 4.6, 4.10, or Corollaries 4.12 and 4.13. Assume L^2 is infinite. Let $\mathcal{L}$ denote $\mathcal{L}_{ring}$ if L is a ring (this includes the case when L is a $\mathbb{Z}$-algebra) or if L is an algebra over a field and it does not satisfy the hypothesis of Theorem 4.5. Otherwise let $\mathcal{L} = \mathcal{L}_{alg}$. Then the first-order theory of L in the language $\mathcal{L}$ with constants is undecidable.*

5 Appendix: finitely generated associative commutative unitary rings

In this section we prove Theorem 2.17, which we restate next. The definition of rank we use is given in Definition 2.15.

Theorem 5.1. *Let R be an infinite finitely generated commutative ring with identity. Then there exists a ring of integers O of a number or a global function field such that $(O; \mathcal{L}_{ring})$ is e-interpretable in $(R; \mathcal{L}_{ring})$, and $\mathcal{D}(O; \mathcal{L}_{ring})$ is polynomial-time Karp-reducible to $\mathcal{D}(R; \mathcal{L}_{ring})$. Moreover, one of the following holds:*

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

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

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

As we mentioned, this result is almost identical to Theorem 7.1 in Eisentraeger thesis [7] (see Theorem 2.14 in this paper for the statement in [7]). Since we are interested in having an e-interpretation of a ring of integers O in R, rather than just a reduction of the Diophantine problems, and for completeness, we provide a proof in this appendix.

We postpone the proof for later in this section. Next we introduce some intermediate notions and results that we will need.

Proposition 5.2. *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 O 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 $\mathcal{D}(R)$ is undecidable.*

We proceed to provide a proof. First, we review some necessary notions and results. Proposition 5.2 is essentially a restatement of some of the results from [37]. There, instead of e-interpretability, the notion of Dioph-generation is used:

Definition 5.3 (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.

The corresponding statement is the following:

Theorem 5.4 ([37])**.** *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 O of K is Dioph-generated over R. Furthermore, if R has positive characteristic p, then $\mathbb{F}_p[t]$ is Dioph-generated over R, and the Diophantine problem $\mathcal{D}(R)$ is undecidable.*

Next we use the above Theorem 5.4 in order to prove Proposition 5.4. It suffices to prove a suitable equivalence between the notions of e-interpretability and of Dioph-generation.

The next definition will be used only in an auxiliary manner in the next Lemma 5.6.

Definition 5.5 (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 5.6. *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 e-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 5.5 (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 5.3, $F = F_2$, the basis $\{1\}$ of F over F_2, and the polynomial f from the field-Diophantine definition of R_1 in R_2. □

Proof of Proposition 5.2. It follows immediately from Theorem 5.4, Lemma 5.6, and Remark 2.9. □

We will need the following observation:

Remark 5.7. Let R be a countable commutative ring of finite rank and positive characteristic k. Then R is finite: indeed, this follows from one of Prüfer theorems, as in this case R is a bounded abelian group since $kR = 0$ (see Theorem 5.2 in [9]).

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 [9]). 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_0 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 prove Theorem 5.1.

Proof of Theorem 5.1. Throughout the proof we will use the facts that e-interpretability is transitive, by Proposition 2.10; and that the quotient by any ideal of a Noetherian ring R is e-interpretable in R, by Lemma 2.7. 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 Proposition 5.2 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 2.7. 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 [14]), hence $N = q_1 \cap \cdots \cap q_n$. We claim that $n \geqslant 1$. 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 $n \geqslant 1$.

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 5.7). 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 5.7.

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 by Remark 5.7. Since $N^m = 0$ for some m, it follows that if R/N is finite then also R is finite, a contradiction. Similarly, it follows that if R/N has finite rank then so does R, by Remark 5.7. Hence the claim is proved.

Note that if R has zero characteristic and finite rank then R/q_i has also zero characteristic, since otherwise it would be finite.

In views of the previous arguments, we can assume from now on that R is an infinite finitely generated integral domain. Note that, by Remark 2.16, now the notion of rank is the same as vector space dimension (for positive characteristic) and of $\mathbb{Z}$-module dimension (for zero characteristic).

Step 2: The case of infinite rank and zero characteristic. We now assume that R is a finitely generated integral domain of zero characteristic and infinite rank. We will e-interpret in R an infinite finitely generated integral domain of positive characteristic. This will allow us to assume, in the next

steps of the proof, that R either has finite rank and zero characteristic, or infinite rank and positive characteristic. In particular, this reduces the hypothesis of Item 2 in the statement of the theorem to the hypothesis of Item 1.

Note that for every prime integer p, R/pR is e-interpretable in R by Lemma 2.7. Hence this step will be complete once we prove that there exists a prime p such that R/pR is infinite.

We first claim that R must contain a transcendental element over $\mathbb{Q}$ (we identify R with its embedding in its field of fractions, which is a field extension of $\mathbb{Q}$). Indeed, assume not, so that every element of R is a root of a polynomial with integer coefficients. In particular, each element in a finite generating set of R, say $r_1, \ldots, r_\ell$, is the root of some polynomial in $\mathbb{Z}[x]$. Since R is generated as a ring by $r_1, \ldots, r_\ell$, the field of fractions of R is generated as a field by $r_1, \ldots, r_\ell$. Since all r_i are algebraic over $\mathbb{Q}$ ($i = 1, \ldots, \ell$), the field of fractions of R is a finite field extension of $\mathbb{Q}$, i.e. it is a finite-dimensional $\mathbb{Q}$-vector space. It follows that R has finitely many $\mathbb{Z}$-linearly independent elements, and so R has finite rank, a contradiction. The claim is proved.

Now pick a transcendental element $x \in R$. Then the subring of R generated by 1 and x is isomorphic to $\mathbb{Z}[x]$. We identify this subring with $\mathbb{Z}[x]$. Given an integer prime q let $\phi_q : R \to R/qR$ be the natural quotient map. We will show that $\phi_q(\mathbb{Z}[x])$ is infinite for some q. This will imply immediately that R/qR is infinite as well, and hence this step will be complete.

Let $\phi_q|_{\mathbb{Z}[x]}$ be the restriction of ϕ_q on $\mathbb{Z}[x]$. We will find a prime q such that $\ker(\phi_q|_{\mathbb{Z}[x]}) = q\mathbb{Z}[x]$, from where it follows that $\phi_q(\mathbb{Z}[x]) \cong \mathbb{F}_q[x]$ is infinite.

Indeed, first note that $\ker(\phi_q|_{\mathbb{Z}[x]}) = qR \cap \mathbb{Z}[x]$. Define $A = \{r \in R \mid nr \in \mathbb{Z}[x] \text{ for some } n \in \mathbb{N}\backslash\{0\}\}$. We have $\ker(\phi_q|_{\mathbb{Z}[x]}) = qR \cap \mathbb{Z}[x] = qA \cap \mathbb{Z}[x]$. If $A = \mathbb{Z}[x]$ it follows that $\ker(\phi_q|_{\mathbb{Z}[x]}) = q\mathbb{Z}[x]$ as required. Hence assume $\mathbb{Z}[x] \subsetneq A$. Note that A is a finitely generated subring of R and that it can be identified with a subring of $\mathbb{Q}[x]$. Hence any element of $\mathbb{Q}[x]$ can be written as $p(x)/n$ for some $p(x) \in \mathbb{Z}[x]$ and some $n \in \mathbb{N}\backslash\{0\}$. Let $a_1, \ldots, a_k$ be a finite generating set of A as a ring, and let $p_1(x), \ldots, p_k(x)$ and $n_1, \ldots, n_k$ be polynomials from $\mathbb{Z}[x]$ and non-zero integers, respectively, such that $a_i = p_i(x)/n_i$ for all $i = 1, \ldots, k$. Since $\mathbb{Z}[x] \subsetneq A$, at least one of the n_i is larger than 1. Let q be a prime integer that is coprime with all n_i. It follows that every element of A can be written in the form $p(x)/n$ where $n \geqslant 1$ is coprime with q, and $p(x) \in \mathbb{Z}[x]$. Then any element from qA which belongs to $\mathbb{Z}[x]$ must belong to $q\mathbb{Z}[x]$. Hence $\ker(\phi_q|_{\mathbb{Z}[x]}) = qA \cap \mathbb{Z}[x] = q\mathbb{Z}[x]$, as required.

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 fintely 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 [6]). It is not possible that $k = 0$, since in this case R would be a finitely generated Artinian domain (see Proposition 9.1 in [6]), and thus a finitely generated field (see Proposition 8.30 of [3]), a contradiction because, as referred to earlier, a finitely generated ring which is a field is necessarily finite. Hence $k \geqslant 1$. We may assume that $k = 1$, since if $k \geqslant 2$ then R/p_{k-1} is a finitely generated integral domain, e-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 [29].
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 [6]), 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, Proposition 5.2 implies that the ring of integers O_K of K is e-interpretable in R (note that Item 2 above grants us the requirement that R contains $\mathbb{F}_p[t]$). By transitivity (Proposition 2.11), O_K is e-interpretable in R, and therefore $\mathcal{D}(O_K)$ is Karp-reducible to $\mathcal{D}(R)$ (Proposition 2.11).

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 Proposition 5.2, and transitivity of e-interpretations and reduction of Diophantine problems (Propositions 2.10 and 2.11) yield that $\mathbb{F}_p[t]$ is e-interpretable in R, and that $\mathcal{D}(R)$ 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 e-interpretable in R and $\mathcal{D}(O_K)$ is Karp-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. □

6 Bibliography

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

[2] E. S. Chibrikov. A right normed basis for free Lie algebras and Lyndon-Shirshov words. *J. Algebra*, 302(2):593–612, 2006.

[3] P. L. Clark. Commutative algebra, 2015. Available at `http://math.uga.edu/~pete/integral.pdf`.

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

[5] 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.

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

[7] K. Eisentraeger. *Hilbert's Tenth Problem and Arithmetic Geometry*. PhD thesis, 2003.

[8] Y. Ershov. Elementary group theories. *Dokl. Akad. Nauk SSSR*, 203:1240–1243, 1972.

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

[10] 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.

[11] A. Garreta, A. Miasnikov, and D. Ovchinnikov. Diophantine problems in solvable groups. *ArXiv e-prints*, May 2018.

[12] K. R. Goodearl and R. B. Warfield. *An Introduction to Noncommutative Noetherian Rings*. London Mathematical Society St. Cambridge University Press, 2004.

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

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

[15] O. Kharlampovich and A. G. Miasnikov. Equations in algebras. *ArXiv e-prints*, 2016.

[16] O. Kharlampovich and A. G. Miasnikov. What does a group algebra of a free group know about the group? *ArXiv e-prints*, 2016.

[17] O. Kharlampovich and A. G. Miasnikov. Undecidability of equations in free Lie algebras. *ArXiv e-prints*, 2017.

[18] O. Kharlampovich and A. G. Miasnikov. Undecidability of the first order theories of free non-commutative Lie algebras. *ArXiv e-prints*, 2017.

[19] O. Kharlampovich and A. G. Miasnikov. Tarski-type problems for free associative algebras. *Journal of Algebra*, 500:589 – 643, 2018. Special Issue dedicated to Efim Zelmanov.

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

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

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

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

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

[25] A. G. Miasnikov. Definable invariants of bilinear mappings. *Siberian Mathematical Journal*, 31(1):89–99, 1990.

[26] A. G. Miasnikov, F. Oger, and S. Sohrabi. Elementary equivalence of rings with finitely generated additive groups. *Annals of Pure and Applied Logic*, 2018.

[27] A. G. Miasnikov and M. Sohrabi. Groups elementarily equivalent to a free nilpotent group of finite rank. *Annals of Pure and Applied Logic*, 162(11):916 – 933, 2011.

[28] A. G. Miasnikov and M. Sohrabi. Elementary coordinatization of finitely generated nilpotent groups. *ArXiv e-prints*, 2013.

[29] 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.

[30] T. Pheidas and K. Zahidi. Undecidability of existential theories of rings and fields: A survey. *Contemporary Mathematics, 270, 49-106*, 2000.

[31] B. Poonen. Hilbert's tenth problem and mazur's conjecture for large subrings of Q. *Journal of the American Mathematical Society*, 16(4):981–990, 2003.

[32] 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"*.

[33] 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.

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

[35] 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.

[36] 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.

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