An Isomorphism between Monoids of External Embeddings: - About Definability in Arithmetic -

Mihai Prunescu [*†‡]

Abstract

We use a new version of the Definability Theorem of Beth in order to unify classical Theorems of Yuri Matiyasevich and Jan Denef in one structural statement. We give similar forms for other important definability results from Arithmetic and Number Theory.
A.M.S. Classification: Primary 03B99; Secondary 11D99.

1 Introduction

It would be nice if there were some analogon of Galois Theory concerning the general definability, or even more the definability with syntactical restrictions (existential, diophantine). Efforts put by people into searching for concrete equations defining the subring of rational integers or other important predicates would be then replaced by structural thinking. We would not care anymore about the Pell equation, which does not seem to work on essentially other rings of algebraic integers as the rings solved in [Denef 2], [Denef-Lipshitz], by Thanases Pheidas in [Pheidas] and independently by Alexandra Shlapentokh in [Shlapentokh2].

We will present now a tentative to start such a program. Our results have more a philosophical than a practical nature. We will use our method in order to analyze already proved statements and to produce new information.

We make the following convention: to speak about a T-definable or a T-diophantine relation over some polynomial ring $R[T]$ means to stress the fact that a constant $\underline{T}$ representing the element T occurs in the definition explicitly. We will use this notation only in some contexts where it is necessary.

The known statements, we want to analyze are the classical Theorems of Yuri Matiyasevich and Jan Denef:

Theorem 1.1 (Matiyasevich) *An arbitrary relation over the ring $\mathbb{Z}$ of all rational integers is diophantine in $\mathbb{Z}$ if and only if it is recursively enumerable according to a recursive presentation of $\mathbb{Z}$.*

Theorem 1.2 (Denef) *An arbitrary relation over the polynomial ring $\mathbb{Z}[T]$ is T-diophantine in $\mathbb{Z}[T]$ if and only if it is recursively enumerable according to a recursive presentation of $\mathbb{Z}[T]$.*

The recursive presentation of $\mathbb{Z}$ is trivial and does not appear explicitly in the different statements of the Theorem of Matiyasevich: it occurred here only for the sake of symmetry. Both proofs are

[*] These results occurred in author's Ph. D. dissertation at the University of Konstanz, Germany, ended in 1998. During this dissertation the author was partially supported by D.A.A.D. and by the University of Konstanz. The author kindly thanks his adviser, Prof. Alexander Prestel, for all support. The author also kindly thanks the anonymous referee, who did a great work for increasing the readability of this paper.

[†] Institut für Mathematik und Informatik, Universität Greifswald, Germany.

[‡] Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

difficult and make intensive use of Pell equations or properties of the Fibonacci numbers. The proofs refined in different directions the following Theorem of Martin Davis and Hilary Putnam:

Theorem 1.3 (Davis - Putnam) *There is a relation with exponential increment $\rho(u,v) \subset \mathbb{N}\times\mathbb{N}$ which is T-diophantine in $\mathbb{Z}[T]$. Consequently, all recursively enumerable relations over $\mathbb{N}$ are T-diophantine in $\mathbb{Z}[T]$.*

We will take this result as original reference or ground-knowledge. We will give a proof of theorem 1.3 in order to show the way how Pell 's equations are used for these problems in an easy context. All other applications of Pell's equations are infinitely more delicate. A possible motivation for the reader to look at the present paper can be that we are looking for structural facts which will possibly substitute Pell's equations (and other concrete proof methods with equations) after future improvements. For the moment we definitely cannot use this facts in order to give easier or more general decidability results, but we found some facts which are equivalent with known results. The paper has the following structure:

Section 1 contains a proof of Theorem 1.3.

Section 2 presents without proof an older Theorem of Beth on decidability together with a modern version of itself about the existential (respectively diophantine) decidability. These instruments will be repeatedly used across the paper.

Section 3 introduces a technique of extending automorphisms of the nonstandard extension $\mathbb{Z}^*$ of $\mathbb{Z}$ to automorphisms of the nonstandard extension $\mathbb{Z}[T]^*$ of the polynomial ring $\mathbb{Z}[T]$. The goal of this Section is to prove a Transfer Theorem for the property to be definable: relations over $\mathbb{Z}$ are definable over $\mathbb{Z}$ if and only if they are definable over $\mathbb{Z}[T]$. Both results are not used in the sequel, but the methods introduced here will be refined in Section 4.

Section 4 contains a method to extend embeddings of $\mathbb{Z}^*$ into itself to embeddings of $\mathbb{Z}[T]^*$ into itself. It is proved that the existence of this extension method is a fact equivalent on one hand with the Theorem of Matyiasevich 1.1 and on the other hand with a transfer property for the existential definability from $\mathbb{Z}[T]$ to $\mathbb{Z}$.

In Section 5 is proved that the extended embedding constructed in Section 4 is unique and that this fact is equivalent with the Theorem of Denef 1.2.

Section 6 contains the joint conclusion of the Sections 3 and 4:

Theorem 1.4 *The application of natural restriction:*

$$\mathfrak{Res}_{\mathbb{Z}^*} \;:\; \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \;\xrightarrow{\sim}\; \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$$

is an isomorphism of monoids. Moreover, assuming the Theorem of Davis and Putnam 1.3, this fact is equivalent with the joint statements of Yuri Matiyasevich 1.1 and Jan Denef 1.2.

In the Section 7 we discuss the importance of similar results and conjectures over other rings. We are mainly interested in the rings of algebraic integers of the number fields, but we speak also about the fields themselves when it is reasonable to consider them.

Now let us take a look to the proof of Theorem 1.3. Its proof consists in a clear application of **only one** Pell equation, and is really easy to sketch.

Proof: Firstly we recall that a relation with exponential increment (called also a Julia Robinson Predicate) is a relation $\rho(u,v) \subset \mathbb{N}\times\mathbb{N}$ such that for all $u,v \in \mathbb{N}$ with $u > 1$, if $\rho(u,v)$ then $v \leq u^u$ but for all $k \in \mathbb{N}$ there are $u,v \in \mathbb{N}$ such that $\rho(u,v)$, $u > 1$ and $v > u^k$.

Given $a \in \mathbb{N}$ with $a \geq 2$, the Pell equation

$$P_a: \quad x^2 - (a^2-1)y^2 = 1$$

has in $\mathbb{N}$ exactly the solutions of the form $(x, y) = (a_n, a'_n)$ defined by:

$$a_n + a'_n \sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n.$$

Comparing them with the solutions of the polynomial Pell equation:

$$P_T : \quad X^2 - (T^2 - 1)Y^2 = 1$$

in $\mathbb{Z}[T]$, which are the pairs of polynomials $(\pm X_n, \pm Y_n)$ given by:

$$X_n + Y_n \sqrt{T^2 - 1} = (T + \sqrt{T^2 - 1})^n,$$

and specialising $T \rightsquigarrow a$, we get

$$a_n = X_n(a) \quad ; \quad a'_n = Y_n(a).$$

Write now the classical Pell equation for $a = 2$:

$$x^2 - 3y^2 = 1.$$

In the notation of Davis and Putnam it has the solutions $(2_u, 2'_u)_{u \in \mathbb{N}}$ in $\mathbb{N}$, defined by:

$$2_u + 2'_u \sqrt{3} = (2 + \sqrt{3})^u.$$

One shows immediately that:

$$2^u < 2_u < 4^u.$$

This is the moment to define:

$$\rho(u, v) \;:\Leftrightarrow\; v = 2_u \;\wedge\; u > 3.$$

Claim: ρ has exponential increment.

$$2_u < 4^u < u^u.$$

If there were a $k \in \mathbb{N}$ such that $2_u \leq u^k$ for all $u > 3$, then $2^u < u^k$ for all $u > 3$, which is certainly false.

Claim: ρ is diophantine over $\mathbb{Z}[T]$.

We show that:

$$\begin{aligned} v = 2_u \quad &\Leftrightarrow \quad \exists X, Y \;\; X^2 - (\underline{T}^2 - 1)Y^2 = 1 \;\wedge \\ &\qquad \wedge\; \underline{T} - 2 \,|\, X - v \;\wedge\; \underline{T} - 1 \,|\, Y - u \;\wedge \\ &\qquad \wedge\; u \in \mathbb{N} \;\wedge\; v \in \mathbb{N}. \\ u > 3 \quad &\Leftrightarrow \quad \exists d \;\; d \in \mathbb{N} \;\wedge\; u = 4 + d. \end{aligned}$$

Indeed, $T - 1 \,|\, Y - u \longrightarrow u = Y(1) \longrightarrow Y = Y_u \longrightarrow X = X_u \longrightarrow$

$$v = X_u(2) = 2_u.$$

For a diophantine definition of $\mathbb{N}$ in $\mathbb{Z}[T]$, see the original paper of Davis and Putnam. An alternative diophantine definition was constructed in [Prunescu2].

Recalling the results of the joint work of Davis, Putnam and J. Robinson, we see that all the recursively enumerable relations over $\mathbb{N}$ are T-diophantine in $\mathbb{Z}[T]$. □

2 The Theorem of Beth

The classical statement of Beth's Definability Theorem says that the relations which are **implicitly** definable inside a formal theory are exactly those which are **explicitly** definable.

Definition: A relation P which is denoted by a symbol which does not belong to a formal language L is called **explicitly** L-definable in a theory T written in the language $L \cup \{P\}$ iff there is an L-formula ϕ with a number of free variables which equals the arity of P such that

$$\mathsf{T} \vdash \ \forall x_1, \dots, x_n \ (P(x_1, \dots, x_n) \longleftrightarrow \phi(x_1, \dots, x_n)).$$

The notion of implicit definability originally used by Beth was introduced as follows, see [Beth 1]:

Definition: The relation P is called **implicitly** definable iff the following condition holds: Take a new predicate symbol P' which does not occur in T and whose arity equals that of P. By substituting P with P' in every element of T we get a theory T'. Then P is called implicitly L-definable in T if

$$\mathsf{T} \cup \mathsf{T}' \vdash \ \forall x_1, \dots, x_n \ (P(x_1, \dots, x_n) \longleftrightarrow P'(x_1, \dots, x_n)).$$

Already in [Shoenfield] implicit definability was understood as the property to be preserved by the automorphisms of all the models of the given theory. Since in our context all theories considered are complete theories of the form Th_L (A) for a concrete L-structure A, it suffices to look at the automorphisms of a sufficiently saturated extension of the given structure A. In the case of the existential definability the automorphisms will be replaced by the embeddings of such a saturated structure into itself.

The language L will be supposed finite.

Definition: An L-homomorphism f between two L-structures A and B will be called an L-**embedding** iff f is an injective function and for all relations $\mathsf{R} \in L$:

$$\mathsf{R}(\vec{x}) \ \Leftrightarrow \ \mathsf{R}(f(\vec{x})).$$

We have analogous conditions for the constants and operation symbols in L.

We will call a structure A **saturated** iff it is card(A)-saturated. For a set of formal statements Γ in the formal language L we will write: $\mathsf{A} \leadsto^{\Gamma} \mathsf{B}$ in the case that for all $\gamma \in \Gamma$, if $\mathsf{A} \models \gamma$ then $\mathsf{B} \models \gamma$. Now we can state our variant for the Theorem of Beth. This improvement was communicated to us by Alexander Prestel:

Theorem 2.1 *Let A be an L-structure and $P \subseteq \mathsf{A}^n$ a new relation defined over the underlying set of the structure A. Let (C, P) be a saturated $L \cup \{P\}$-structure with card(C) $\geq$ card(L) such that*

$$(\mathsf{C}, \mathsf{P}) \equiv (\mathsf{A}, P).$$

- *P is definable in terms of L iff all L-automorphisms of C are also P-automorphisms.*
- *P is existentially definable in terms of L iff for all L-embeddings η of C in itself $\eta(\mathsf{P}) \subset \mathsf{P}$.*

In both cases, the left condition will be true in any other structure which is elementarily equivalent with (A, P).

For a proof, see [Prunescu1]. A proof of the first case (general definability) can be found in [Shoenfield]. The other case is not really more difficult.

Remark 2.2 *If card $(\mathsf{A}) \leq 2^\omega$ we can use for C the classical ultrapower $\mathsf{A}^* = (\prod_{n \in \mathbb{N}} \mathsf{A})/ \equiv_{\mathsf{U}}$ because card $(\mathsf{A}^*)= 2^\omega$ and A^* is 2^ω - saturated.* □

We can already give an application of our new version of the Theorem of Beth. Following the Theorem of Matiyasevich 1.1 and its extended sense, a subset of $\mathbb{N}$ is recusivly enumerable iff it is existentially definable in $\mathbb{N}$ and is recursive iff both the set and its complement are existentially definable in $\mathbb{N}$. If we apply the Theorem of Beth 2.1 in the situation of Remark 2.2, we get directly:

Remark 2.3 Consider the set of the natural numbers $\mathbb{N}$ as an $L = \{+, -, \cdot, 0, 1\}$ -structure, a subset $M \subset \mathbb{N}$ and a new predicate M which will be interpreted over $\mathbb{N}$ as M. Let $\mathbb{N}^*$ be an ultrapower of $\mathbb{N}$ and $M^* \subset \mathbb{N}^*$ the corresponding nonstandard extension of M, i.e. the interpretation of M over $\mathbb{N}^*$. Then the following are true:

a) M is a recursively enumerable subset of $\mathbb{N}$ iff all L-embeddings of $\mathbb{N}^*$ into itself are $L \cup \{\mathsf{M}\}$-endomorphisms of $\mathbb{N}^*$.

b) M is a recursive subset of $\mathbb{N}$ iff all L-embeddings of $\mathbb{N}^*$ into itself are $L \cup \{\mathsf{M}\}$-embeddings of $\mathbb{N}^*$ into itself.

Remark 2.4 Let R be a ring that allows in some language L, which is an extension by constants of the formal language of rings, positive existential definitions containing only one equation for the relations $t \neq 0$, $x = 0 \vee y = 0$, $x = 0 \wedge y = 0$. Let $P \subseteq R^d$ be a new relation over R and $(\mathcal{R}, \mathcal{P})$ be a saturated $L \cup \{\mathsf{P}\}$-structure that is elementarily equivalent to (R, P). Then P is L-diophantine in R iff for all L-embeddings η of $\mathcal{R}$ into itself, $\eta(\mathcal{P}) \subset \mathcal{P}$. If $\mathrm{card}(R)$ is at most $\aleph_1$ we may apply Remark 2.2 and study just the L-embeddings of the classical ultrapower R^*.

The following definition is for future applications of this facts quite useful:

Definition: Let $A \subset B$ be two rings. We denote by $\mathfrak{Aut}_A(B)$ and by $\mathfrak{End}_A(B)$ the monoids of all automorphisms (embeddings) of B into itself, that fix the elements of A pointwise.

3 Automorphisms

Let us compare Matiyasevich's statement 1.1 with the older result of Davis and Putnam 1.3. We observe that the existence of a transfer of definability of relations over $\mathbb{Z}$, from the polynomial ring $\mathbb{Z}[T]$ to the ring $\mathbb{Z}$ itself, would imply the Theorem of Matiyasevich 1.1, provided that the transfer preserves also the existential and positive character of definitions. The transfer we wish is not a transfer in the classical sense of model-theory: we do not transfer the truth of formal statements, expressed by some closed well formed formulas. We transfer only the property of some relation to be definable in two different structures, without putting the condition that the same formula defines the relation simultaneously in both structures.

In this section we will prove the existence of a transfer of definability for relations over $\mathbb{Z}$, a transfer which works between $\mathbb{Z}[T]$ and $\mathbb{Z}$. This will succeed by extending automorphisms of the classical ultrapower $\mathbb{Z}^*$ to some special automorphisms of the corresponding ultrapower $\mathbb{Z}[T]^*$. This construction is only an invitation for the next section, where a more special transfer for the existential definability will be proved.

Definition: Let R be a ring. A function $F(\vec{\lambda}, x) : R^{l+1} \to R$ will be called a **Gödel function** iff the function encodes any finite sequence of elements of R in its parameters:

$$\forall n \in \mathbb{N} \;\; \forall (c_0, \dots, c_n) \subset R \;\; \exists \vec{\lambda} \in R^l \;\; \forall i \in \{0, \dots, n\} \quad F(\vec{\lambda}, i) = c_i.$$

Remark 3.1 *The ring of integers $\mathbb{Z}$ admits a definable Gödel function. Moreover, the definition is diophantine.*

To see this, let us recall the Gödel function over the structure $\mathbb{N}$ of the naturals $\beta : \mathbb{N}^2 \to \mathbb{N}$:

$$\beta(x, i) = z \Leftrightarrow \quad \exists u, v \leq x \quad \Big((u+v)(u+v+1) + 2u = 2x \; \wedge$$

$$z < iv + 1 \; \wedge \quad \exists w \leq u \quad (u = w(iv+1) + z)\Big).$$

The first equality defines the pairing function of Cantor. The coding works due to the Chinese Remainder Theorem. For a complete proof see for example [Kaye] (pg. 64). For getting the Gödel function over $\mathbb{Z}$, we recall that $\mathbb{N}$ and its complement $\mathbb{Z} \setminus \mathbb{N}$ are definable in $\mathbb{Z}$ by the Four Squares Theorem. If we take the length n of the sequence as an additional parameter, we obtain the following definition of $F : \mathbb{Z}^3 \longrightarrow \mathbb{Z}$:

$$\begin{aligned} & F(n,u,i) = v \Leftrightarrow \\ & \quad \Big((n,u,i) \in \mathbb{N}^3 \ \wedge\ i \leq n \ \wedge\ v = \beta(u, 2i) - \beta(u, 2i+1) \ \Big) \\ & \quad \vee \Big((n,u,i) \in \mathbb{N}^3 \ \wedge\ i > n \ \wedge\ v = 0 \Big) \ \vee \\ & \quad \vee \Big(n \notin \mathbb{N} \wedge v = 0 \Big) \ \vee \ \Big(u \notin \mathbb{N} \wedge v = 0 \Big) \ \vee \ \Big(i \notin \mathbb{N} \wedge v = 0 \Big). \end{aligned}$$

If we relativize all the variables used for defining β according to the definition of $\mathbb{N}$ in $\mathbb{Z}$, using new variables at each new relativization, we will find a formal definition of F in $\mathbb{Z}$. It is easy to verify that F is a Gödel function over $\mathbb{Z}$.

Now we can state our first transfer result:

Theorem 3.2 *Let $k \in \mathbb{N}$ be a natural number and let $M \subseteq R^k$ be any relation. Then:*

$$M \ is \ definable \ in \ \mathbb{Z} \ \Leftrightarrow \ M \ is \ T - definable \ in \ \mathbb{Z}[T].$$

Proof: For the easy direction $\Rightarrow$: $\mathbb{Z}$ is definable in $\mathbb{Z}[T]$. Let ψ be one formula which defines M in $\mathbb{Z}$. We relativize all variables (bounded and free) to $\mathbb{Z}$ using the definition of $\mathbb{Z}$. What we have got is a formula which defines M in $\mathbb{Z}[T]$ even without the constant $\underline{T}$.

For the difficult direction: Let $(\mathbb{Z}^*, M^*)$ be any saturated model that is elementarily equivalent to the structure $(\mathbb{Z}, \underline{M})$, where $\underline{M}$ is a new relation-symbol (predicate) for the set M. It is enough to prove that every automorphism $\varphi \in \mathfrak{Aut}_{\mathbb{Z}}(\mathbb{Z}^*)$ preserves the set M^* and to apply the Theorem of Beth for definability (2.1).

In fact we will prove that every automorphism $\varphi \in \mathfrak{Aut}_{\mathbb{Z}}(\mathbb{Z}^*)$ can be extended to an automorphmism $\bar{\varphi} \in \mathfrak{Aut}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$. Let us suppose that this were the case. Applying the Theorem of Beth in the other direction under the hypothesis that M is T-definable in $\mathbb{Z}[T]$ we get that $\bar{\varphi}(M^*) = (M^*)$. But $\bar{\varphi}(M^*) = \varphi(M^*)$ because $M^* \subseteq (\mathbb{Z}^*)^k$ and $\bar{\varphi}|_{\mathbb{Z}^*} = \varphi$, so $\varphi(M^*) = M^*$.

We can suppose $\mathbb{Z}^*$ and $\mathbb{Z}[T]^*$ to be classical nonstandard extensions obtained for example as ultrapowers. Together with both nonstandard rings we may consider the nonstandard extension of some other objects which have relevant set-theoretic connections with them and build a part of a nonstandard model of the Set Theory, for further details see [A. Robinson]. The main power of Nonstandard Analysis resides in the possibility to discuss in terms of **standard**, **internal** and **external** objects.

For example, the following set-theoretic description of the polynomials over a ring is a classical standard information: a polynomial is a sequence of elements of the ring which is ultimately zero. The elements of the sequence are called **coefficients**, their position in the sequence is denoted with a natural number and is called **index** and the index of the last not zero coefficient is called **degree**. Every polynomial has a degree. The degree of the polynomial 0 will be here declared to be 0. By transfering this to the nonstandard situation, we get that every $x \in \mathbb{Z}[T]^*$ has the shape

$$x = \sum_{i=0}^{\nu} a_i T^i,$$

where $\nu \in \mathbb{N}^*$ is a nonstandard natural number and $(a_i)_{i=0}^{\nu}$ is a $*$-finite internal sequence. Similarly every $*$-finite internal sequence over $\mathbb{Z}^*$ defines a nonstandard polynomial. Two $*$-finite internal sequences over $\mathbb{Z}^*$ define the same element of $\mathbb{Z}[T]^*$ **iff** the shorter sequence coincides elementwise with an initial segment of the longer sequence (is a truncation of the longer sequence) **and** the rest of the longer sequence consists only of zeros. The length of the $*$-finite internal sequences must be understood as a nonstandard natural number. Comparing lengths means to check the natural order over $\mathbb{N}^*$, which is a standard relation. We will write $a \approx b$ iff the $*$-finite internal sequences a and b define the same element of $\mathbb{Z}[T]$. We see that $\approx$ is a standard relation over the standard set of all $*$-finite internal sequences. All these facts are general and do not depend on the definability of $\mathbb{N}$ or of a Gödel function over $\mathbb{Z}$.

Let $\varphi \in \mathfrak{Aut}_L(\mathbb{Z}^*)$. For the element $x \in \mathbb{Z}[T]^*$ which has already been described, we define

$$\bar{\varphi}(x) := \sum_{j=0}^{\varphi(\nu)} \varphi(a_{\varphi^{-1}(j)})T^j.$$

Claim: $\bar{\varphi}$ is well defined.

This definition entails from the beginning at least two problems. First of all is its intuitive meaning: φ did not occur only applied to the coefficients, but also to the indices and to the degree. In fact, if x was defined as the $*$-finite internal sequence $(a_i)_{i=0}^{\nu}$ which could have been interpreted as the internal function $a : [0, \nu] \to \mathbb{Z}^*$, then $\bar{\varphi}(x)$ is nothing else as $\varphi \circ a \circ \varphi^{-1} : [0, \varphi(\nu)] \to \mathbb{Z}^*$. $\mathbb{N}$ being definable in $\mathbb{Z}$, is $\varphi(\mathbb{N}^*) = \mathbb{N}^*$ so $\varphi(\nu)$ is a nonstandard natural number. The order of $\mathbb{N}$ being also definable in $\mathbb{N}$ (remember the Four Squares Theorem) is true that $\varphi([0, \nu]) = [0, \varphi(\nu)]$ and that φ is monotone on the interval $[0, \nu]$. We are now convinced that our definition makes a formal sense.

The second problem is if $(\varphi \circ a \circ \varphi^{-1}(j))_{j=0}^{\varphi(\nu)}$ is not only a $*$-finite but also an internal sequence.

For this goal, let us first recall the properties of the Gödel function F. If we denote its nonstandard extension by F^*, the definability of F over $\mathbb{Z}$ means that for all $\vec{\lambda}, x, y \in \mathbb{Z}^*$ and all $\varphi \in \mathfrak{Aut}_{\mathbb{Z}}(\mathbb{Z}^*)$:

$$F^*(\vec{\lambda}, x) = y \;\Leftrightarrow\; F^*(\varphi(\vec{\lambda}), \varphi(x)) = \varphi(y).$$

The fact that F encodes every finite sequence of $\mathbb{Z}$ in a parameter of fixed length l over $\mathbb{Z}$ implies that F^* encodes every internal $*$-finite sequence of $\mathbb{Z}^*$ in a parameter in $\mathbb{Z}^*$ of the same length l. In our case for the internal sequence a there is a parameter $\vec{g} \in \mathbb{Z}^{*l}$ such that functionally:

$$a(\cdot)\,|_{[0,\nu]} = F^*(\vec{g}, \cdot)\,|_{[0,\nu]}.$$

Putting this together we get:

$$\varphi \circ a \circ \varphi^{-1}(\cdot)\,|_{[0,\varphi(\nu)]} = \varphi \circ F^*(\vec{g}, \cdot) \circ \varphi^{-1}(\cdot)\,|_{[0,\varphi(\nu)]} =$$

$$= F^*(\varphi(\vec{g}), \varphi(\cdot)) \circ \varphi^{-1}(\cdot)\,|_{[0,\varphi(\nu)]} = F^*(\varphi(\vec{g}), \cdot)\,|_{[0,\varphi(\nu)]},$$

so as restriction of the standard function F^* to the internal set $\{\varphi(\vec{g})\} \times [0, \varphi(\nu)]$ is our $*$-finite sequence internal.

The definition of $\bar{\varphi}$ does not depend on the choice of a special Gödel function or parameter. Anyway, if we preferred an apparently F, g-dependent definition as above, the independence would have been easy to prove.

On the other side, in order that $\bar{\varphi}$ be an application of $\mathbb{Z}[T]^*$ into itself, our definition must be independent of the choice of the representative sequence. Let σ_1, σ_2 be $*$-finite internal $\approx$-equivalent sequences such that $\sigma_1 \subseteq \sigma_2$ as initial segment. We denote by λ_i the length of σ_i,

$\lambda_1 \leq \lambda_2$. If $\sigma'_i = (\varphi \circ \sigma_i \circ \varphi^{-1})_{j=0}^{\varphi(\lambda_i)}$ then:

$$\begin{aligned}
\forall j \leq \lambda_1 \;\; \sigma_1(j) = \sigma_2(j) \;\; &\Rightarrow \;\; \forall k = \varphi(j) \leq \varphi(\lambda_1) \\
\varphi \circ \sigma_1 \circ \varphi^{-1}(k) \;\; &= \;\; \varphi \circ \sigma_2 \circ \varphi^{-1}(k) \; ;
\end{aligned}$$

$$\begin{aligned}
\forall \lambda_1 < j \leq \lambda_2 \;\; \sigma_2(j) = 0 \;\; &\Rightarrow \;\; \forall \varphi(\lambda_1) < k = \varphi(j) \leq \varphi(\lambda_2) \\
\varphi \circ \sigma_2 \circ \varphi^{-1}(k) \;\; &= \;\; 0.
\end{aligned}$$

This means $\sigma'_1 \approx \sigma'_2$ and the definition makes sense.
We remark immediately that $\bar{\varphi}(T) = T$ and $\forall r \in \mathbb{Z}^* \; \bar{\varphi}(r) = \varphi(r)$ hence $\bar{\varphi}$ extends φ. The **additivity** and the **injectivity** of $\bar{\varphi}$ are trivial and we will not include them. We will sketch shortly the proof that:

Claim: $\bar{\varphi}$ is surjective.

For an element $y \in \mathbb{Z}[T]^*$ we choose a representative sequence $(b_j)_{j=0}^{\nu}$ such that:

$$\begin{aligned}
y \;\; &= \;\; \sum_{j=0}^{\nu} b_j T^j. \text{ Let now:} \\
x \;\; &= \;\; \sum_{i=0}^{\varphi^{-1}(\nu)} \varphi^{-1}(b_{\varphi(i)}) T^i.
\end{aligned}$$

Then x is well defined as a polynomial representing the $\approx$-class of the $*$-finite internal sequence $F^*(\varphi^{-1}(\vec{h}), [0, \varphi^{-1}(\nu)])$, where $\vec{h}$ is the coding parameter for $(b_j)_{j=0}^{\nu}$. Of course $\bar{\varphi}(x) = y$. More difficult is to prove the:

Claim: $\bar{\varphi}$ is multiplicative.

First we recall the multiplication between two (standard) polynomials.

$$(\sum_{i=0}^{\mu} a_i T^i) \cdot (\sum_{j=0}^{\nu} b_j T^j) = \sum_{k=0}^{\mu+\nu} (\sum_{i+j=k} a_i b_j) T^k.$$

It is evident that the last summation symbol has a very different nature as the other three sums: it means a concrete addition and not the formal sum used to denote polynomials. One may see this $\sum$ as an operator defined on the set of all finite sequences of elements of $\mathbb{Z}$. Its nonstandard extension, which will be denoted also by $\sum$, operates consequently on all $*$-finite internal sequences in $\mathbb{Z}^*$. As we have defined the behavior of $\bar{\varphi}$ towards the formal sum, we would like φ to have a similar behavior towards the concrete internal sum. This says the following:

Lemma 3.3 (Changing the variable inside the sum) *Let L be an extension by constants of the formal language of rings and let R be a ring which is an L-structure such that the set of natural numbers $\mathbb{N}$ and a Gödel function F are L-definable in R. If $(a_i)_{i=0}^{\nu}$ is a $*$-finite internal sequence of elements of R^* and $\varphi \in \mathfrak{Aut}_L(R^*)$ then:*

$$\varphi(\sum_{i=0}^{\nu} a_i) = \sum_{j=0}^{\varphi(\nu)} \varphi(a_{\varphi^{-1}(j)}).$$

Proof: We know already that the sequence on the right side is internal, so it was legal to apply the sum operator. The difficulty is the following: the fact that φ commutes with every finite sum cannot be used for infinite sums. On the other side we may not use the saturation because φ is in general external. Fortunately, the way in which φ should act on the sequence resembles that proposed in the case of formal polynomial summations. This will help us to find a new definition for the internal summation.

We will denote the evaluation of polynomials in $T = 1$ by the German letter $\mathfrak{A}$ (coming from "Auswertung"). The value of $\mathfrak{A}$ is the sum of coefficients:

$$\mathfrak{A} : R[T] \longrightarrow R \quad ; \quad \mathfrak{A}(x) = x(1) = \sum_{i=0}^{n} a_i.$$

Its value is of course independent of the representative sequence.

The next remark belongs to the elementary algebra:

$$\mathfrak{A}(x) = b \Leftrightarrow (T-1) \,|\, x - b.$$

If we understand the summation symbol as internal sum, both facts remain true for the nonstandard extension $\mathfrak{A}^*$ of $\mathfrak{A}$: the value of $\mathfrak{A}^*$ does not depend on the chosen internal representative sequence and continues to be equivalent with the divisibility relation.

Our next intention is to prove the following equivalence:

$$(T-1) \,|\, y \Leftrightarrow (T-1) \,|\, \bar{\varphi}(y).$$

Of course, we may not use the multiplicativity of $\bar{\varphi}$ because it still has not been proved. The decisive fact which will be used is that the polynomials are divisible by $T-1$ iff their sequence of coefficients has a special form. That form, which will appear explicitly, is transferable in the context of the $*$-finite internal sequences with the same meaning. Let $y \in R[T]^*$.

$$(T-1) \,|\, y \Leftrightarrow \exists z \;\; y = (T-1)z \Leftrightarrow$$

$$\Leftrightarrow \exists (z_i)_{i=0}^{\alpha} \;\; y = z_\alpha T^{\alpha+1} + \sum_{i=1}^{\alpha} (-z_i + z_{i+1}) T^i - z_0 \Leftrightarrow$$

$$\bar{\varphi}(y) = \varphi(z_{\varphi^{-1}(\varphi(\alpha))}) T^{\varphi(\alpha+1)} + \sum_{j=1}^{\varphi(\alpha)} \varphi(-z_i + z_{i+1})_{i=\varphi^{-1}(j)} T^j - \varphi(z_0)$$

$$\bar{\varphi}(y) = \varphi(z_{\varphi^{-1}(\varphi(\alpha))}) T^{\varphi(\alpha)+1} + \sum_{j=1}^{\varphi(\alpha)} (-\varphi(z_{\varphi^{-1}(j)}) + \varphi(z_{\varphi^{-1}(j)+1})) T^j - \varphi(z_{\varphi^{-1}(0)})$$

$$\Leftrightarrow \exists z \;\; \bar{\varphi}(y) = (T-1)\bar{\varphi}(z) \Leftrightarrow (T-1) \,|\, \bar{\varphi}(y).$$

At the end we tacitly used the bijectivity of $\bar{\varphi}$. Now we are ready to conclude the Lemma.

$$\mathfrak{A}^*(x) = b \Leftrightarrow (T-1) \,|\, x - b \Leftrightarrow (T-1) \,|\, \bar{\varphi}(x) - \bar{\varphi}(b) \Leftrightarrow$$

$$\Leftrightarrow (T-1) \,|\, \bar{\varphi}(x) - \varphi(b) \Leftrightarrow \mathfrak{A}^*(\bar{\varphi}(x)) = \varphi(\mathfrak{A}^*(x)).$$

Expanding the last equality we obtain exactly:

$$\varphi(\sum_{i=0}^{\nu} a_i) = \sum_{j=0}^{\varphi(\nu)} \varphi(a_{\varphi^{-1}(j)}).$$

□

Now to verify the **multiplicativity** becomes just a matter of patience. For the moment we consider the Theorem as proven. A similar result will be however proven in the next section in a stronger context and in more detail. □□

Corollary 3.4 (Elimination of T) *Any relation over $\mathbb{Z}[T]$ consisting of (tuples of) constant polynomials only which is T-definable in $\mathbb{Z}[T]$ is definable in $\mathbb{Z}[T]$ also without using a constant for T.*

Corollary 3.5 *The homomorphism*

$$\mathfrak{Res}_{\mathbb{Z}^*} : \mathfrak{Aut}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \longrightarrow \mathfrak{Aut}_{\mathbb{Z}}(\mathbb{Z}^*)$$

is surjective.

Let us fix two formulas which define $\mathbb{N}$ and respectively a Gödel function over $\mathbb{Z}$. Repeating the same considerations which we have done in order to prove the Transfer Theorem 3.2 one can realize an algorithm which translates definitions over $R[T]$ in definitions over R by substituting the atomic formulas and by using at each step the two fixed formal definitions. Apparently such a result would be stronger: it would be effective and would not make use of tools like the nonstandard extension and the Theorem of Beth.

We had two reasons for our procedure. First of all we are interested in the transfer of definability just in order to motivate the next part of the work, for which Theorem 3.2 establishes the background. On the other hand, the proof of 3.2 is a technical preparation of a more difficult mechanism: the extension of the embeddings of $\mathbb{Z}^*$ in itself to embeddings of $\mathbb{Z}[T]^*$ in itself. Why and to what extent it is more difficult to extend embeddings than to extend automorphisms will be seen in the next section.

4 Embeddings going upwards

In order to extend embeddings of $\mathbb{Z}^*$ into itself to embeddings of $\mathbb{Z}[T]^*$ into itself, we need some more technical preparation, coming from the Theorem of Matiyasevich 1.1. We recall the fact that putting a bounded universal quantifier in front of a recursively enumerable relation, one again gets a recursively enumerable relation. A structural effect of this fact is the following:

Lemma 4.1 (Beth-Matiyasevich) *If $D(i, \vec{\lambda})$ is any diophantine relation over $\mathbb{N}$ and $\eta : \mathbb{N}^* \hookrightarrow \mathbb{N}^*$ is an L-embedding then for all elements and tuples $\mu, \vec{\lambda} \in \mathbb{N}^*$:*

$$\forall i < \mu \; D^*(i, \vec{\lambda}) \Rightarrow \forall i < \eta(\mu) \; D^*(i, \eta(\vec{\lambda})).$$

In the next lemma variables like i, j, k are supposed to mean (nonstandard) natural numbers. This convention will be used also in some other situations. We do not find it necessary to develop a whole many-sorted formal language in this context.

Remark 4.2 Let $D(\iota, \vec{\lambda})$ be any diophantine relation over $\mathbb{Z}$, $\mu \in \mathbb{N}^*$, $\eta : \mathbb{Z}^* \hookrightarrow \mathbb{Z}^*$ be some embedding and $\vec{\lambda} \in (\mathbb{Z}^*)^d$ be some tuple. Then as above:

$$\forall i < \mu \; D^*(i, \vec{\lambda}) \Rightarrow \forall i < \eta(\mu) \; D^*(i, \eta(\vec{\lambda})).$$

Proof: The restriction $\eta |_{\mathbb{N}^*}$ determines η uniquely. We interpret D diophantinely over $\mathbb{N}$ and apply 4.1.

For fixed elements $\mu \in \mathbb{N}^*$ and $\vec{\lambda} \in (\mathbb{Z}^*)^d$ suppose that:

$$\mathbb{Z}^* \models \forall i < \mu \; D^*(i, \vec{\lambda}).$$

Suppose also that $D(\iota, \vec{\lambda})$ has the following diophantine definition over $\mathbb{Z}$:

$$\exists \vec{x} \; P(\iota, \vec{\lambda}, \vec{x}) = 0 \text{ with } P \in \mathbb{Z}[\iota, \vec{\lambda}, \vec{x}].$$

For a variable x (respectively λ) we introduce two new variables v_1^x v_2^x which have not occurred in D or in any other substitution. All of the new variables are interpreted as (nonstandard) natural numbers. Now $\exists x\,(\dots)$ becomes $\exists v_1^x,\, v_2^x\,(\dots)$, x becomes $(v_2^x - v_1^x)$, and λ becomes $(v_2^\lambda - v_1^\lambda)$. After applying 4.1 we repeat the same procedure backwards. □

The following statement is the main result of this section:

Theorem 4.3 *Assuming the Theorem of Davis and Putnam 1.3, the following three statements are equivalent:*

1. *The Theorem of Matiyasevich 1.1.*
2. *The natural application of restriction* $\mathfrak{Res}_{\mathbb{Z}^*} : \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \to \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$ *is a surjective homomorphism of monoids.*
3. *For all* $d \in \mathbb{N}$ *and every relation* $M \subseteq \mathbb{Z}^d$*:*

$$M \text{ is diophantine in } \mathbb{Z} \Leftrightarrow M \text{ is } T-\text{diophantine in } \mathbb{Z}[T].$$

Proof: The implications $2 \Rightarrow 3$ and $3 \Rightarrow 1$ are very easy. For $2 \Rightarrow 3$ we apply our version of Beth's Definability Theorem. For $3 \Rightarrow 1$ we recall the result of Davis and Putnam 1.3 and apply the transfer rule 3 directly.

Let us deal with the non-trivial implication $1 \Rightarrow 2$. First of all we observe that the application of natural restriction is well defined with the given codomain: remember that $\mathbb{Z}$ is diophantine in $\mathbb{Z}[T]$.

In order to better understand what happens, let us recall the extension of an automorphism. If $\varphi \in \mathfrak{Aut}_{\mathbb{Z}}(\mathbb{Z}^*)$, the action of its extension $\bar{\varphi}$ to $\mathbb{Z}[T]^*$ on a nonstandard polynomial x described by the $*$-finite internal sequence $(a_i)_{i=0}^{\nu} = F^*(\vec{\lambda}, \cdot)\,|_{[0,\nu]}$ was a polynomial represented by the sequence:

$$\varphi(a_{\varphi^{-1}(j)})_{j=0}^{\varphi(\nu)} = F^*(\varphi(\vec{\lambda}), \cdot)\,|_{\varphi([0,\nu])} = F^*(\varphi(\vec{\lambda}), \cdot)\,|_{[0,\varphi(\nu)]},$$

an internal sequence as image of a standard function restricted on an internal set.

But an arbitrary $\eta \in \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$ is a not necessarily surjective external embedding. As positive facts we remark that the naturals $\mathbb{N}$ and their ordering are diophantine in $\mathbb{Z}$, so $\eta(\mathbb{N}^*) \subseteq \mathbb{N}^*$ and $\eta|_{\mathbb{N}^*}$ is monotone. As negative facts, in general $\eta([0,\nu]) \neq [0, \eta(\nu)]$ and is not an internal set.

Suppose that the description of x has been done using our already defined Gödel function which is diophantine in $\mathbb{Z}$. Let us define the action of the extension $\bar{\eta}$ on the nonstandard polynomial x described above to be the polynomial given by the following sequence:

$$\bar{\eta}(x) = F^*(\eta(\vec{\lambda}), \cdot)\,|_{[0,\eta(\nu)]}.$$

We remark that the definition depends formally this time on the choice of a representative $*$-finite internal sequence, of a diophantine Gödel function and of the coding parameter λ. At least the sequence written above is also $*$-finite internal, being a restriction of a standard function to an internal set.

What we have done is a kind of internal closure of the external partially defined sequence

$$[\text{``}\eta\text{''}(x)]_j = \begin{cases} \eta(a_i) = F^*(\eta(\vec{\lambda}), \eta(i)) & \text{if } j = \eta(i) \in \eta([0,\nu]), \\ \text{not defined}, & \text{else}; \end{cases}$$

introducing "new born elements" like $F^*(\eta(\vec{\lambda}), j)$, where $j \in [0, \eta(\nu)] \setminus \eta([0,\nu])$.

Claim: $\bar{\eta}$ is well defined.

First we prove that given a representing sequence for x, the above defined representing sequence for $\bar{\eta}(x)$ does not depend on the choice of the diophantine Gödel function and of the parameter. We recall the convention that letters like i, j, k, l denote only (nonstandard) natural numbers. Suppose that we have encoded the sequence $(a_i)_{i=0}^{\nu}$ twice, using not necessarily different diophantine Gödel functions F_1, F_2 and two coding parameters $\vec{\lambda}_1, \vec{\lambda}_2$. This means:

$$\forall i \leq \nu \;\; F_1^*(\vec{\lambda}_1, i) = F_2^*(\vec{\lambda}_2, i).$$

$F_{1,2}$ are both diophantine over $\mathbb{Z}$. If we substitute the functions with their definitions we obtain a diophantine relation and as prefix a restricted universal quantifier on (nonstandard) naturals. We apply 4.1 and get:

$$\forall i \leq \eta(\nu) \;\; F_1^*(\eta(\vec{\lambda}_1), i) = F_2^*(\eta(\vec{\lambda}_2), i).$$

(As before the universally quantified variables remain η-free.)

Let us consider two $*$-finite internal sequences which represent the same nonstandard polynomial, i.e. are $\approx$-equivalent. This means that, say $\forall i \leq \nu_1 \; a_{1i} = a_{2i}$ **and** $\forall i \; \nu_1 \leq i \leq \nu_2 \Rightarrow a_{2i} = 0$. We encode the two sequences using a diophantine Gödel function F and two nonstandard parameters $\vec{\lambda}_1, \vec{\lambda}_2$. As before the two image sequences will coincide on the interval $[0, \eta(\nu_1)]$. The situation on the added interval can be described by a diophantine formula like:

$$\begin{aligned} \forall i \leq \nu_2 - \nu_1 - 1 \qquad & F^*(\vec{\lambda}_2, \nu_1 + 1 + i) = 0, \\ \forall i \leq \eta(\nu_2) - \eta(\nu_1) - 1 \qquad & F^*(\eta(\vec{\lambda}_2), \eta(\nu_1) + 1 + i) = 0. \end{aligned}$$

The images of the two sequences are $\approx$-equivalent, so $\bar{\eta}$ is an application of $\mathbb{Z}[T]^*$ in itself.

Claim: $\bar{\eta}$ is injective.

Let $x, y \in \mathbb{Z}[T]^*$ such that $\bar{\eta}(x) = \bar{\eta}(y)$. We choose two representing sequences for x and y. If one of them is shorter, we may extend it with zeros and make it of the same length as the other without representing another polynomial. Say, the common length was ν. After the definition of $\bar{\eta}$, the common image must have a representing sequence of length $\eta(\nu)$. This sequence has two types of elements: old and new born. Let us consider an old one. Its index is a $j = \eta(i)$, for an $i \in [0, \nu]$. If a_i and b_i are the corresponding elements of the two sequences, we see that $\eta(a_i) = \eta(b_i) =$ the old element. But η is injective, thus $a_i = b_i$. The old elements has been chosen arbitrarily, hence the two representing sequences are equal and $x = y$.

Claim: $\bar{\eta}$ extends η.

Suppose that we use for coding exactly the Gödel function which was constructed in 3.1. For $a_0 \in \mathbb{Z}^*$, considered as polynomial, the shortest representing sequence has length 1 and the only element is a_0 itself written as $F^*(0, \lambda, 0) = a_0$ for a parameter $\lambda \in \mathbb{N}^*$. The image consists of only one old element. It is:

$$\bar{\eta}(a_0) = F^*(0, \eta(\lambda), 0) = \eta(F^*(0, \lambda, 0)) = \eta(a_0).$$

Claim: $\bar{\eta}(T) = T$.

The sequence $(0, 1) \subset \mathbb{Z}$ is the shortest representing sequence for T and is encoded modulo F^* with the standard parameter $(1, \lambda) \in \mathbb{N}^2$:

$$F^*(1, \lambda, 0) = 0 \;\; ; \;\; F^*(1, \lambda, 1) = 1.$$

But $\eta(\lambda) = \lambda$, so $\bar{\eta}(T) = T$.

Claim: $\bar{\eta}$ is additive.

Consider $x, y, z \in \mathbb{Z}[T]^*$ such that $x + y = z$. We choose a nonstandard natural number ν which is at least max (degree(x), degree(y)). Then we can represent x, y, z as internal sequences of length ν:

$$x = F^*(\vec{\lambda}, \cdot)\,|_{[0,\nu]}, \quad y = F^*(\vec{\gamma}, \cdot)\,|_{[0,\nu]}, \quad z = F^*(\vec{\epsilon}, \cdot)\,|_{[0,\nu]}$$

We define now a relation which models polynomial addition.

$$\mathcal{R}_+(\nu, \vec{\lambda}, \vec{\gamma}, \vec{\epsilon}) :\Leftrightarrow \forall i \leq \nu \;\; F^*(\vec{\lambda}, i) + F^*(\vec{\gamma}, i) = F^*(\vec{\epsilon}, i).$$

Using again 4.1 we find that $\mathcal{R}_+(\nu, \vec{\lambda}, \vec{\gamma}, \vec{\epsilon}) \Rightarrow \mathcal{R}_+(\eta(\nu), \eta(\vec{\lambda}), \eta(\vec{\gamma}), \eta(\vec{\epsilon}))$ which means $\bar{\eta}(x) + \bar{\eta}(y) = \bar{\eta}(z)$.

Claim: $\bar{\eta}$ is multiplicative.

We start again with $xy = w$ in $\mathbb{Z}[T]^*$. We use the same elements x and y which have been described for proving the additivity. As before, it is a standard fact over $\mathbb{Z}[T]^*$ that the product of two polynomials accepting both of which are represented by sequences of length ν is represented by a sequence of length 2ν.

We choose now the diophantine Gödel function defined in 3.1 above. We put:

$$\begin{aligned} x = \;& F^*(\vec{\lambda}, \cdot)\,|_{[0,\nu]} &= (a_i)_{i=0}^{\nu}, \\ y = \;& F^*(\vec{\gamma}, \cdot)\,|_{[0,\nu]} &= (b_i)_{i=0}^{\nu}\,, \\ w = \;& F^*(\vec{\theta}, \cdot)\,|_{[0,2\nu]} &= (t_i)_{i=0}^{2\nu}\;. \end{aligned}$$

We must model diophantinely over $\mathbb{Z}$ that w is a product. The facts used in proving 3.3 concerning the internal sum will be again of crucial importance. We remember that an internal sum of a $*$-finite internal sequence is equal with the evaluation of the nonstandard polynomial represented by the respective sequence in $T \rightsquigarrow 1$. In the following lines we will denote some polynomials occurring in expresions of an algebraic nature by displaying directly a representing sequence. Because $w = xy$ we get:

$$\forall k \leq 2\nu \qquad t_k = F^*(\vec{\theta}, k) = \sum_{i=0}^{k} a_i b_{k-i},$$

$$\forall k \leq 2\nu \qquad T - 1 \mid (\sum_{i=0}^{k} a_i b_{k-i} T^i) - F^*(\vec{\theta}, k).$$

We remark that $F^*(\vec{\theta}, k) \in \mathbb{Z}^* \subset \mathbb{Z}[T]^*$ and the relation of divisibility is meant in the latter ring. For a complete description of the polynomial product we have to diophantinely model now this relation of polynomial divisibility inside $\mathbb{Z}^*$. First of all, for every $k \leq 2\nu$ the sequence $(a_i b_{k-i})_{i=0}^{k}$ is $*$-finite internal as result of the standard function

$$\{\vec{a}, \vec{b}; k\} := (a_0 b_k, a_1 b_{k-1}, \ldots, a_k b_0) = \overrightarrow{a} \cdot_k \overleftarrow{b}\,,$$

which is in fact an elementwise product of the finite sequence $\overrightarrow{a'}$ with the reversed finite sequence $\overleftarrow{b'}$, where $a' = a\,|_{[0,k]}$, and the same holds for b'. Being $*$-finite internal, it admits a Gödel coding of the shape $F^*(\vec{\zeta}, \cdot)\,|_{[0,k]}$ for a parameter $\vec{\zeta} \in R^*$. Now we may translate the divisibility in expressions like:

$$\exists \vec{\beta} \quad \sum_{j=0}^{k} F^*(\vec{\zeta}, j) T^j = (T - 1)(\sum_{j=0}^{k-1} F^*(\vec{\beta}, j) T^j)$$

where $\vec{\beta}$ is a new coding parameter.

The next relation will be denoted by $\mathcal{R}.(\nu, \vec{\lambda}, \vec{\gamma}, \vec{\theta})$. It is diophantine and sums up all our considerations.

$$\begin{aligned} \forall k \leq 2\nu \ \exists \vec{\zeta} \ \exists \vec{\beta} \qquad \Big[\qquad & \Big(F^*(\vec{\zeta}, 0) - F^*(\vec{\theta}, k) = F^*(\vec{\beta}, 0) \Big) \wedge \\ \Big(\forall i \leq k \quad & F^*(\vec{\zeta}, i) = F^*(\vec{\lambda}, i) F^*(\vec{\gamma}, k-i) \Big) \wedge \\ \Big(\forall j \leq k \quad & F^*(\vec{\zeta}, j+1) = -F^*(\vec{\beta}, j+1) + F^*(\vec{\beta}, j) \Big) \Big]. \end{aligned}$$

The Gödel function was chosen such that the length of a sequence was displayed as parameter and for some index $i >$ as the length of the encoded sequence, F is equal zero. It will happen for terms like $F^*(\vec{\lambda}, i)$ with $i > \nu$ and like $F^*(\vec{\zeta}, k+1)$. This little trick makes the diophantine modeling formula possible:

$$\mathcal{R}.(\nu, \vec{\lambda}, \vec{\gamma}, \vec{\theta}) \Rightarrow \mathcal{R}.(\eta(\nu), \eta(\vec{\lambda}), \eta(\vec{\gamma}), \eta(\vec{\theta})).$$

If we denote now:

$$\begin{aligned} \eta(x) = & \quad F^*(\eta(\vec{\lambda}), \cdot) \,|_{[0, \eta(\nu)]} & = (a_i')_{i=0}^{\eta(\nu)}, \\ \eta(y) = & \quad F^*(\eta(\vec{\gamma}), \cdot) \,|_{[0, \eta(\nu)]} & = (b_i')_{i=0}^{\eta(\nu)}, \\ \eta(w) = & \quad F^*(\eta(\vec{\theta}), \cdot) \,|_{[0, 2\eta(\nu)]} & = (t_i')_{i=0}^{2\eta(\nu)}, \end{aligned}$$

and we read the relation $\mathcal{R}$ in the new parameters, we get:

$$\begin{aligned} \forall k \leq 2\eta(\nu) \qquad & T - 1 \mid (\sum_{i=0}^{k} a_i' b_{k-i}' T^i) - F^*(\eta(\vec{\theta}), k), \\ \forall k \leq 2\eta(\nu) \qquad & t_k' = F^*(\eta(\vec{\theta}), k) = \sum_{i=0}^{k} a_i' b_{k-i}'. \end{aligned}$$

We observe that the last equality is now true also for new born elements t_k'. That is why the Theorem of Matiyasevich 1.1 was essential. We obtained

$$\eta(x)\eta(y) = \eta(z).$$

As last we remark that we need not verify for every operation the independence of the choice of a representing sequence because this independence is a standard fact. □□

In order to keep the symmetry with 3.4, we state the following:

Corollary 4.4 (Diophantine elimination of T) *All relations M over $\mathbb{Z}$ which are T-diophantine in $\mathbb{Z}[T]$ are also diophantine in $\mathbb{Z}[T]$ without using a constant for T.*

Proof: The definition of M in $\mathbb{Z}$ exists and can be relativized to the definition of $\mathbb{Z}$ in $\mathbb{Z}[T]$. It leads to an diophantine definition of M in $\mathbb{Z}[T]$. □

5 Embeddings going downwards

In this section an analogous result to the Theorem of Denef 1.2 will be presented. The analogy with the preceding section is as follows: if there we transferred the notion of diophantine definability from the polynomial ring $\mathbb{Z}[T]$ to the ring $\mathbb{Z}$, now we transfer the notion of recursive enumerability from $\mathbb{Z}$ to $\mathbb{Z}[T]$. For this goal we define a recursive presentation of $\mathbb{Z}[T]$ that will play the same role as Gödel funtions before. This notion has been introduced by Michael Rabin in a very general setting, see [Rabin]. It was also called "structure of recursive ring".

Definition: A bijective map $\theta : \mathbb{N} \to \mathbb{Z}[T]$ for which the inverse images of polynomial addition and multiplication are recursive ternary relations over $\mathbb{N}$ is called a **recursive presentation of** $\mathbb{Z}[T]$.

Definition: An arbitrary relation $M \subset \mathbb{Z}[T]^d$ is called **recursively enumerable** with respect to the recursive presentation θ iff $\theta^{-1}(M)$ is a recursively enumerable subset of $\mathbb{N}$.

We will implicitely prove that this notion does not depend on the choice of any particular recursive presentation θ.

The main result of this section is the following:

Theorem 5.1 *Assuming the Theorem of Davis and Putnam 1.3, the following statements are equivalent:*

1. *The Theorem of Denef 1.2.*
2. *The natural application of restriction* $\mathfrak{Res}_{\mathbb{Z}^*} : \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \longrightarrow \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$ *is an injective homomorphism of monoids.*
3. *There is a surjective* $\lambda : \mathbb{N} \longrightarrow \mathbb{Z}[T]$ *which is* T*-diophantine in* $\mathbb{Z}[T]$.
4. *All recursive presentations* $\theta : \mathbb{N} \longrightarrow \mathbb{Z}[T]$ *are* T*-diophantine in* $\mathbb{Z}[T]$.

Proof: The proof works again circularly. Apparently the weakest statement is 3, so let's start with it.

3 ⇒ 2: We know that the corresponding relation

$$\mathcal{R}_\lambda(n, F) \Leftrightarrow n \in \mathbb{N} \ \wedge \ F = \lambda(n)$$

is T-diophantine in $\mathbb{Z}[T]$. Let $\alpha, \beta \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$ be such that $\mathfrak{Res}_{\mathbb{Z}^*}(\alpha) = \mathfrak{Res}_{\mathbb{Z}^*}(\beta)$. Take an $F \in \mathbb{Z}[T]^*$. λ is a surjective function, hence there is some $n \in \mathbb{N}^*$ such that $\mathcal{R}^*_\lambda(n, F)$. Since $\mathcal{R}_\lambda$ is also diophantine,

$$\mathbb{Z}[T]^* \models \mathcal{R}^*_\lambda(\alpha(n), \alpha(F)) \ \wedge \ \mathcal{R}^*_\lambda(\beta(n), \beta(F))$$

due again to Theorem 2.1.

But $\alpha(n) = \beta(n) = \nu \in \mathbb{N}^*$ because $\mathbb{N}$ is diophantine in $\mathbb{Z}[T]$, so $\alpha(F) = \beta(F) = \lambda^*(\nu)$. F was chosen arbitrarily, so $\alpha = \beta$.

2 ⇒ 4: Let θ be some recursive presentation of $\mathbb{Z}[T]$ and let $\alpha \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$ be some embedding. By Theorem 2.1 it is sufficient to prove that for all $n \in \mathbb{N}^*$ and corresponding $F \in \mathbb{Z}[T]^*$:

$$\mathcal{R}^*_\theta(n, F) \quad \Rightarrow \quad \mathcal{R}^*_\theta(\alpha(n), \alpha(F)).$$

Denote $\beta := \mathfrak{Res}_{\mathbb{Z}^*}(\alpha) \in \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$. The nonstandard extension of θ is itself a bijection. Moreover θ^* is a standard function, and thus $(\theta^*)^{-1} = (\theta^{-1})^*$. We define the following external function:

$$\begin{aligned} \bar{\beta} :\ & \mathbb{Z}[T]^* \ \longrightarrow \ \mathbb{Z}[T]^* \\ & \bar{\beta}(F) = \theta^* \circ \beta \circ (\theta^*)^{-1}(F). \end{aligned}$$

The definition makes sense because $\mathbb{N}$ is diophantine over $\mathbb{Z}$. We show that $\bar{\beta} \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$ and $\mathfrak{Res}_{\mathbb{Z}^*}(\bar{\beta}) = \beta = \mathfrak{Res}_{\mathbb{Z}^*}(\alpha)$, in order to apply the injectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$. We are now developing a machinery for extending embeddings which differs from this one used in the previous section. The role of the diophantine Gödel function is now taken by the recursive presentation of Rabin.

Claim: $\bar{\beta}$ is injective.

$\bar{\beta} = \theta^* \circ \beta \circ (\theta^*)^{-1}$, so is injective as a composition of three injective functions. Moreover, if $\alpha \in \mathfrak{Aut}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$ then $\beta \in \mathfrak{Aut}_{\mathbb{Z}}(\mathbb{Z}^*)$ and $\bar{\beta}$ is bijective as a composition of three bijective functions.

Claim: $\bar{\beta}$ is an endomorphism.

Let $\mathfrak{op} \in \{+, \cdot\}$ be one of the two ring-operations. The relation

$$\mathcal{R}_{\mathfrak{op}}(a,b,c) \; \Leftrightarrow \theta(a) \; \mathfrak{op} \; \theta(b) = \theta(c)$$

is a recursive relation over $\mathbb{N}$. By the Theorem of Davis and Putnam 1.3 $\mathcal{R}_{\mathfrak{op}}$ is diophantine over $\mathbb{Z}[T]$. We avoid the Theorem of Matiyasevich 1.1.

Take arbitrary $P, Q, R \in \mathbb{Z}[T]^*$ (say $P = \theta^*(a)$, $Q = \theta^*(b)$, $R = \theta^*(c)$) which satisfies $P \; \mathfrak{op} \; Q = R$ in $\mathbb{Z}[T]^*$. Surely is true that:

$$\mathcal{R}^*{}_{\mathfrak{op}}(a,b,c).$$

Hence $\mathcal{R}^*{}_{\mathfrak{op}}(\alpha(a), \alpha(b), \alpha(c))$. This relation takes place in $\mathbb{N}^*$, $\alpha(\mathbb{N}^*) \subset \mathbb{N}^*$ and $\alpha\,|_{\mathbb{N}^*} = \beta$. This means:

$$\mathcal{R}^*{}_{\mathfrak{op}}(\beta(a), \beta(b), \beta(c)),$$

hence $\theta^*(\beta(a)) \; \mathfrak{op} \; \theta^*(\beta(b)) = \theta^*(\beta(c))$, so finally

$$\bar{\beta}(P) \; \mathfrak{op} \; \bar{\beta}(Q) = \bar{\beta}(R).$$

Claim: $\bar{\beta}\,|_{\mathbb{Z}[T]} = \mathbf{1}_{\mathbb{Z}[T]}$.

For $x \in \mathbb{Z}[T]$, $x = \theta^*(t) = \theta(t)$, where $t \in \mathbb{N}$ is a standard natural number.
Hence $\bar{\beta}(x) = \theta^*(\beta(t)) = \theta^*(t) = x$.

Claim: $\bar{\beta}\,|_{\mathbb{Z}^*} = \beta$.

This is the only nontrivial step. We make use of the following:

Lemma 5.2 *The* **corestriction** *of* θ *on* $\mathbb{N}$*:*

$$\mathfrak{theta}\ (n,m) \; :\Leftrightarrow \; n \in \mathbb{N} \; \wedge \; m \in \mathbb{N} \; \wedge \; \theta(n) = m,$$

is a recursively enumerable relation over $\mathbb{N}$.

Proof: Suppose the unique $a, b \in \mathbb{N}$ such that $\theta(a) = 0$ and $\theta(b) = 1$ to be known. We denote the reversed image of the polynomial addition by $\oplus$:

$$\theta(x) + \theta(y) = \theta(z) \Leftrightarrow \mathcal{R}_+(x,y,z) \Leftrightarrow x \oplus y = z.$$

Since $\mathcal{R}_+$ is recursive, $\oplus$ is algorithmically computable. We construct the following pairs: $(a, 0)$, $(b, 1)$, $(b \oplus b, 2)$, $\dots$ (n, m), $(n \oplus b, m+1)$, $\dots$. If the pair (n, m) appears in the list, then:

$$\theta(n) = \theta(b \oplus b \oplus \cdots \oplus b) = 1 + 1 + \cdots + 1 = m.$$

It is easy to see that our algorithmically generated list enumerates $\mathfrak{theta}$ exhaustively. At the end of the proof we remark that $\mathfrak{theta}$ is related with the 5-ary relation used by Denef for proving his Theorem 1.2, see [Denef 3]. □

Because of the Theorem of Davis and Putnam 1.3, $\mathfrak{theta}$ is diophantine in $\mathbb{Z}[T]$. So for $n, m \in \mathbb{N}^*$:

$$\mathfrak{theta}^*(n,m) \; \Rightarrow \; \mathfrak{theta}^*(\alpha(n), \alpha(m)),$$

which means in fact $\mathfrak{theta}^*(\beta(n), \beta(m))$. From the surjectivity of θ, for all $m \in \mathbb{N}^*$ there is an $n \in \mathbb{N}^*$ such that $\mathfrak{theta}^*(n, m)$. Choose an arbitrary $m \in \mathbb{N}^*$ and fix it.

$$\bar{\beta}(m) = \bar{\beta}(\theta^*(n)) = \theta^* \circ \beta \circ (\theta^*)^{-1}(\theta^*(n)) = \theta^* \circ \beta(n) = \beta(m),$$

thus really $\mathfrak{Res}_{\mathbb{Z}^*}(\bar{\beta}) = \beta = \mathfrak{Res}_{\mathbb{Z}^*}(\alpha)$.

Now, due to the supposed injectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$ we get $\alpha = \bar{\beta}$. Recall that we fixed at the beginning a pair (n, F) such that $\mathcal{R}^*_\theta(n, F)$. Using only the definition of $\mathcal{R}_\theta$, we get that $\mathcal{R}^*_\theta(\beta(n), \theta^*(\beta(F)))$; in our notation $\mathcal{R}^*_\theta(\beta(n), \bar{\beta}(F))$. But $\beta(n) = \alpha(n)$ and $\bar{\beta}(F) = \alpha(F)$, so we finally have got:

$$\mathcal{R}^*_\theta(\alpha(n), \alpha(F)).$$

$\alpha \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$ was arbitrary, so $\mathcal{R}_\theta$ is diophantine in $\mathbb{Z}[T]$.

$4 \Rightarrow 1$: Let us fix such a θ, recursive presentation of $\mathbb{Z}[T]$. We know that θ is diophantine over $\mathbb{Z}[T]$. If a relation is diophantine over $\mathbb{Z}[T]$, its preimage under θ is a recursively enumerable relation on $\mathbb{N}$. Conversely, if a relation has a θ^{-1}-image that is recursively enumerable over $\mathbb{N}$, this inverse image must be diophantine over $\mathbb{Z}[T]$ by the Theorem of Davis and Putnam 1.3. θ is diophantine over $\mathbb{Z}[T]$, so the relation is itself diophantine over $\mathbb{Z}[T]$, by repeated relativization with always new variables.

$1 \Rightarrow 3$: Let θ be an arbitrary recursive presentation of $\mathbb{Z}[T]$. The function θ considered as a relation is recursively enumerable with respect to itself, so it must be diophantine in $\mathbb{Z}[T]$. It is also surjective, so we define $\lambda := \theta$. □□

Remark 5.3 *There is no recursive presentation θ of the ring $\mathbb{Z}[T]$ which is diophantine without using a constant $\underline{T}$ expressing T.*

Proof: $\mathbb{N}$ is diophantine in $\mathbb{Z}[T]$ with constant coefficients following results from [Prunescu2] and a complement of a point in $\mathbb{N}$ is also trivially diophantine, writing

$$x \in \mathbb{N} \setminus \{m\} \Leftrightarrow x = 0 \vee x = 1 \vee \cdots \vee x = m - 1 \vee (\exists n\; n \in \mathbb{N} \wedge x = m + n + 1).$$

If θ was diophantine without using T, we could have defined $\mathbb{Z}[T] \setminus \{0\}$ diophantinely in $\mathbb{Z}[T]$ without using T. This contradicts the first theorem presented in [Prunescu2]. □

In the last section we developed another technique to extend embeddings as that used here. The injectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$ tells us that any such extension is uniquely determined.

Theorem 5.4 (Structure of embeddings) *Assuming the theorems of Davis - Putnam 1.3 and Jan Denef 1.2 but without using the Theorem of Matiyasevich 1.1 we get that all $\eta \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$ must have the form:*

$$\eta(\sum_{i=0}^{\nu} a_i T^i) = \sum_{j=0}^{\gamma(\nu)} F^*(\gamma(\vec{\lambda}), j) T^j,$$

where $\gamma = \mathfrak{Res}_{\mathbb{Z}^*}(\eta)$, F is any diophantine Gödel function over $\mathbb{Z}$ and $\vec{\lambda}$ parameters such that

$$\forall\; i \in [0, \nu] \quad F(\vec{\lambda}, i) = a_i.$$

Proof: After getting $\gamma = \mathfrak{Res}_{\mathbb{Z}^*}(\eta)$, we extend γ back to $\mathbb{Z}[T]^*$ as we did in the last section. Any recursive enumerable relation in $\mathbb{N}$ which might have been used for this extension is diophantine over $\mathbb{Z}[T]^*$ because of the Davis - Putnam Theorem 1.3. After extending γ to a $\bar{\gamma}$, we apply the injectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$ to decide that $\bar{\gamma} = \eta$ and we are done. □□

6 Main result

Theorem 6.1 *The application of natural restriction:*

$$\mathfrak{Res}_{\mathbb{Z}^*} \;:\; \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \;\xrightarrow{\sim}\; \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$$

is an isomorphism of monoids. Moreover, assuming the Theorem of Davis and Putnam 1.3, this fact is equivalent with the joint statements of Yuri Matiyasevich 1.1 and Jan Denef 1.2.

Proof: Immediate consequence of the last two sections. □□

The author hopes that this result contributes to the understanding of the deeper connections between Recursion Theory, Algebra and Set Theory. Observing the structural but completely non-arithmetic nature of this statement, he asks if it would be possible to give definition-free proofs for the Theorem of Matiyasevich 1.1 and for the Theorem of Denef 1.2 by doing a direct, set-theoretic proof of 6.1. We put this question remarking that in order to understand the content of 6.1 we need only two set-theoretic constructions (polynomial ring and ultrapower) and any set-theoretic definition of $\mathbb{Z}$, but we don't need any form of Number Theory.

We get also a small Corollary, based on the remark that the automorphisms are exactly the invertible embeddings.

Corollary 6.2 *The application of natural restriction*

$$\mathfrak{Res}_{\mathbb{Z}^*} \;:\; \mathfrak{Aut}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \;\xrightarrow{\sim}\; \mathfrak{Aut}_{\mathbb{Z}}(\mathbb{Z}^*)$$

is an isomorphism of groups.

7 Similar interpretations for other definability results

Most of the results presented in this last survey section are given without proof. All the proofs work as above and can be consulted in [Prunescu1]. In the following we will call any finite algebraic extension of $\mathbb{Q}$ a **number field**. We begin considering again results of general definability, for example:

Theorem 7.1 (Julia Robinson) *If R is a number field or its ring of algebraic integers, the ring $\mathbb{Z}$ is definable in R.*

It has been proven by Alexandra [Shlapentokh1], that for all domains Δ of characteristic 0, $\mathbb{Z}$ is T-diophantine in the polynomial ring $\Delta[T]$. If we want an easier definition of $\mathbb{Z}$, more similar to the Theorem of Davis and Putnam 1.3, we may apply the following remark of Jan Denef, see [Denef 1]:

$$x \in \mathbb{Z} \Leftrightarrow \exists X, Y \in \Delta[T]\ (X^2 - (\underline{T}^2 - 1)Y^2 = 1 \wedge \underline{T} - 1 \,|\, Y - x \wedge x \in \Delta).$$

If Δ is any field, it is diophantine in $\Delta[T]$ as set of elements which have multiplicative inverses or are equal 0. If Δ is a ring of algebraic integers, we may use the T-free definition given in [Prunescu1] and [Prunescu2]. Anyway, using this remark we can prove easily the following:

Theorem 7.2 *If R is a number field or its ring of algebraic integers, the following three statements are equivalent:*

1. *The Theorem of Julia Robinson 7.1 for R.*
2. *The natural application of restriction $\mathfrak{Res}_{R^*} : \mathfrak{Aut}_{R[T]}(R[T]^*) \to \mathfrak{Aut}_R(R^*)$ is a surjective homomorphism of groups.*

3. *For all $d \in \mathbb{N}$ and every relation $M \subseteq R^d$:*

$$M \ is \ definable \ in \ R \Leftrightarrow M \ is \ T - definable \ in \ R[T].$$

Consequently, for every T-definable relation over $R[T]$ consisting of constant polynomials only, one can find a T-free definition (i.e. we can eliminate the transcendental).

Let O be a ring of algebraic integers in some number field K. A natural remark like

$$\mathsf{O}[T] \models \quad P \in \mathbb{Z}[T] \Leftrightarrow P(\mathbb{Z}) \subseteq \mathbb{Z},$$

leads to an easy proof of the following:

Lemma 7.3 *For every ring of algebraic integers O, the complement $\mathsf{O}[T] \setminus \mathbb{Z}[T]$ is diophantine in $\mathsf{O}[T]$. Consequently, $\mathbb{Z}[T]$ is definable in $\mathsf{O}[T]$.*

This observation leads now to the following Isomorphism Theorem:

Theorem 7.4 *For all rings of algebraic integers O, the application of natural restriction*

$$\mathfrak{Res}_{\mathsf{O}^*} \ : \ \mathfrak{Aut}_{\mathsf{O}[T]}(\mathsf{O}[T]^*) \ \xrightarrow{\sim} \ \mathfrak{Aut}_{\mathsf{O}}(\mathsf{O}^*)$$

is an isomorphism of groups. Moreover, assuming the T-definability of $\mathbb{Z}$ in $\mathsf{O}[T]$, the surjection part of this statement implies the Theorem of Julia Robinson 7.1 for O.

We emphasize again that $\mathbb{Z}$ is always T-definable (and even T-diophantine) in $\mathsf{O}[T]$ for all rings of algebraic integers O.

The question of whether a statement like Theorem 7.4 is true also for number fields remains **open**.

What about embeddings and diophantine definitions? By improving a little bit the technical preparations around diophantine Gödel functions and recursive presentations one gets easily:

Theorem 7.5 (Transfer of Diophantine Definability) *Let R be a number field or its ring of algebraic integers. If we assume the Theorem of Davis and Putnam 1.3 and the fact that $\mathbb{Z}$ is always T-diophantine in $R[T]$, the following statements are equivalent:*

1. *$\mathbb{Z}$ is diophantine in R.*
2. *The application of natural restriction $\mathfrak{Res}_{R^*} : \mathfrak{End}_{R[T]}(R[T]^*) \to \mathfrak{End}_R(R^*)$ is a surjective homomorphism of monoids.*
3. *For all $d \in \mathbb{N}$ and relation $M \subseteq R^d$:*

$$M \ is \ diophantine \ in \ R \Leftrightarrow M \ is \ T - diophantine \ in \ R[T].$$

Corollary 7.6 (Diophantine elimination of T) *If R is a number ring or field, $\mathbb{Z}$ is diophantine in R iff all relations M which are T-diophantine in $R[T]$ and consist of constant elements only are also diophantine in $R[T]$ without using a constant for T.*

Theorem 7.7 *Let O be a ring of algebraic integers. If we assume the Theorem of Davis and Putnam 1.3, following assertions are equivalent:*

1. *There is a surjective $\lambda : \mathbb{N} \longrightarrow \mathsf{O}[T]$ which is T-diophantine in $\mathsf{O}[T]$.*
2. *The application of natural restriction $\mathfrak{Res}_{\mathsf{O}^*} : \mathfrak{End}_{\mathsf{O}[T]}(\mathsf{O}[T]^*) \longrightarrow \mathfrak{End}_{\mathsf{O}}(\mathsf{O}^*)$ is an injective homomorphism of monoids.*

3. *All recursive presentations $\theta : \mathbb{N} \longrightarrow \mathsf{O}[T]$ are T-diophantine in $\mathsf{O}[T]$.*

4. *All relations M over $\mathsf{O}[T]$ are T-diophantine in $\mathsf{O}[T]$ iff they are recursively enumerable with respect to some recursive presentation θ of $\mathsf{O}[T]$.*

5. *$\mathbb{Z}[T]$ is T-diophantine in $\mathsf{O}[T]$.*

Jan Denef and Leonard Lipshitz proved that for all totally real number field K, $\mathbb{Z}$ is diophantine in its ring of algebraic integers $\mathsf{O} = \mathsf{O}_K$, see [Denef-Lipshitz]. Karim Zahidi proved very recently that for such rings of algebraic integers there is a T-diophantine recursive presentation of $\mathsf{O}[T]$, see [Zahidi]. The direct consequence is the following:

Theorem 7.8 *If O is the ring of all algebraic integers in some totally real number field, then the application of natural restriction*

$$\mathfrak{Res}_{\mathsf{O}^*} \;:\; \mathfrak{End}_{\mathsf{O}[T]}(\mathsf{O}[T]^*) \;\overset{\sim}{\longrightarrow}\; \mathfrak{End}_{\mathsf{O}}(\mathsf{O}^*)$$

is an isomorphism of monoids. Moreover, assuming the Theorem of Davis and Putnam 1.3, this fact is equivalent with the results of [Denef-Lipshitz] and [Zahidi], or with the joint information that $\mathbb{Z}$ is diophantine in O and $\mathbb{Z}[T]$ is diophantine in $\mathsf{O}[T]$.

Reading the statement above someone could think about the similarity between O as a $\mathbb{Z}$-algebra and $\mathsf{O}[T]$ as a $\mathbb{Z}[T]$-algebra and ask if it is possible to find a diophantine formula which defines simultaneously $\mathbb{Z}$ in O and $\mathbb{Z}[T]$ in $\mathsf{O}[T]$. In [Prunescu1] it is proven that there is no diophantine definition of $\mathbb{Z}[T]$ in any $\mathsf{O}[T]$ avoiding the use of T, so the question about the one and only equation has always a negative answer.

According to some conjectures of Barry Mazur and Serge Lang, the author does also not believe that $\mathbb{Z}$ is diophantine in any number field. It is very easy to see that if $\mathbb{Z}$ isn't diophantine in $\mathbb{Q}$, it is also not diophantine in any other number field K. So, it is not reasonable to hope that for any number field an Isomorphism Theorem for embeddings would hold.

The author was not able to find definability results equivalent to the injectivity of $\mathfrak{Res}_{K^*}$ as homomorphism between monoids of embeddings and stress this question as another **open** problem. Finally, the author **conjectures** that all rings of algebraic integers O have isomorphisms between their corresponding monoids of embeddings and also **asks** what happens over the wider class of all finitely generated domains of characteristic 0. We recall that if a ring of algebraic integers O satisfies the Isomorphism Theorem then in particular $\mathbb{Z}$ is diophantine in O and Hilbert's Tenth Problem over O is undecidable.

References

[Beth 1] **Evert W. Beth**: *On Padoa's method in the theory of definition.* Proceedings of the Royal Academy of Sciences, Amsterdam, ser. A 56, 1953.

[Beth 2] **Evert W. Beth**: *The Foundations of Mathematics.* North Holland, 1959.

[Davis-Putnam] **Martin Davis, Hilary Putnam**: *Diophantine Sets over Polynomial Rings.* Illinois Journal of Mathematics 7, 251 - 256, 1963.

[DPR] **Martin Davis, Hilary Putnam, Julia Robinson**: *The decison problem for exponential diophantine equations.* Annals of Mathematics, Second Series 74(3), 425 - 436, 1961.

[Denef 1] **Jan Denef**: *The Diophantine Problem for Polynomial Rings and Fields of Rational Functions.* Transactions of the A.M.S. 242, 391- 399, 1978.

[Denef 2] **Jan Denef**: *Hilbert's Tenth Problem for Quadratic Rings.* Proceedings of the A.M.S. 48.1, 214 - 220, 1975.

[Denef 3] **Jan Denef**: *Diophantine sets over* $\mathbb{Z}[T]$. Proceedings of the A.M.S. 69.1, 148 - 150, 1978.

[Denef-Lipshitz] **Jan Denef, Leonard Lipshitz**: *Diophantine sets over some Rings of Algebraic Integers.* The Journal of the London Mathematical Society 18 (2), 385 - 391, 1978.

[Gödel] **Kurt Gödel**: *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme.* Monatshefte für Mathematik und Physik 38 (1), 173 - 198, 1931.

[Kaye] **Richard Kaye**: *Models of Peano Arithmetic.* Oxford Logic Guides 15, 1991.

[Lipshitz] **Leonard Lipshitz**: *Diophantine correct models of Arithmetic.* Procedings of the A.M.S. 73(1), 107 - 108, 1979.

[D. Marcus] **Daniel A. Marcus**: *Number Fields.* Springer Verlag, 1977.

[Matiyasevich] **Yuri V. Matiyasevich**: *Hilbert's Tenth Problem.* MIT Press, 1993.

[B. Mazur] **Barry Mazur**: *On the Diophantine Sets over the Rationals.* Experimental Mathematics 1, 1 - 21, 1990.

[Prestel] **Alexander Prestel**: *Einführung in die mathematische Logik und Modelltheorie.* Vieweg Verlag, 1992.

[Pheidas] **Thanases Pheidas**: *Hilbert's Tenth Problem for a Class of Rings of Algebraic Integers.* Proceedings of the A.M.S. 104, 611 - 620, 1988.

[Prunescu1] **Mihai Prunescu**: *A structural approach to diophantine definability.* Dissertation Universität Konstanz, Hartungs-Gorre Verlag Konstanz, 1999.

[Prunescu2] **Mihai Prunescu**: *Defining constant polynomials.* Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, Contemporary Mathematics 270, 139 - 145, 2000.

[Pourchet] **Yves Pourchet**: *Sur la representation en somme de carres des polynomes sur un corps de nombres algebriques.* Acta Arithmeticae 19, 89-104, 1971.

[Rabin] **Michael O. Rabin**: *Computable Algebra, General Theory and Theory of Computable Fields.* Transactions of A.M.S. 95 , 341-360, 1960.

[A. Robinson] **Abraham Robinson**: *Non-Standard Analysis.* Studies in Logic and the Foundations of Mathematics, North-Holland, 1974.

[J. Robinson] **Julia Robinson**: *The Undecidability for Algebraic Rings and Fields.* Proceedings of the A.M.S. 10, 950 - 957, 1959.

[Rumely] **Robert S. Rumely**: *Undecidability and Definability for the Theory of Global Fields.* Transactions of the A.M.S. 262 (1), 195 - 217, 1980.

[Sauerland] **Ulrich Sauerland**: *Entscheidbarkeitsprobleme in Ringen algebraischer Zahlkörper.* Diplomarbeit Universität Konstanz, 1993.

[Shlapentokh1] **Alexandra Shlapentokh**: *Diophantine Definitions for Some Polynomial Rings.* Communications of Pure and Applied Mathematics, Vol. XLIII, 1055 - 1066, 1990.

[Shlapentokh2] **Alexandra Shlapentokh**: *Extension of Hilbert's tenth problem to some algebraic number fields.* Communications of Pure and Applied Mathematics, Vol. XLII, 1113 - 1122, 1989.

[Shoenfield] **Joseph R. Shoenfield**: *Mathematical Logic.* Reading Mass.: Addison-Wesley 1976.

[Smorynski] **Craig Smorynski**: *Logical Number Theory.* Springer Verlag, 1991.

[Zahidi] **Karim Zahidi**: *On diophantine sets over polynomial rings.* Proceedings of the A.M.S. 128, 877 - 884, 2000.