A Structural Approach to Diophantine Definability

Dissertation

zur Erlangung des akademischen Grades
des Doktors der Naturwissenschaften
an der Universität Konstanz,
Fakultät für Mathematik und Informatik,

vorgelegt von

Mihai Prunescu

Datum der mündlichen Prüfung: 21.12.1998

1. Referent: Professor Dr. A. Prestel
2. Referent: Privatdozent Dr. J. Koenigsmann

Abstract

General and diophantine definability in number rings and their polynomial rings are studied from a model-theoretic point of view. The main tool used is a modern form of the Theorem of Beth.

For a ring R we consider the monoid $\mathfrak{End}_R(R^*)$ of all embeddings of a nonstandard enlargement R^* in itself which fix the standard elements. If R is a number ring or any field, the application of natural restriction $\mathfrak{Res}_{R^*}$ from $\mathfrak{End}_{R[T]}(R[T]^*)$ to $\mathfrak{End}_R(R^*)$ is a well defined homomorphism of monoids.

We give connections between the diophantine definability of the integers $\mathbb{Z}$ in a number ring R, a phenomenon of transfer of definability from the polynomial ring $R[T]$ to the ring R, and properties of the homomorphism $\mathfrak{Res}_{R^*}$.

In the case of the ring $\mathbb{Z}$ itself we get as a byproduct that the restriction

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

is an isomorphism of monoids, fact which is equivalent with the combination of two well known theorems of Y. Matiyasevich and J. Denef. We prove similar isomorphisms for some rings of algebraic integers. We believe that this is a property of all rings of algebraic integers.

Abstract

In dieser Arbeit werden Fragen der allgemeinen und der diophanischen Definierbarkeit in Zahlringen und in den entsprechenden Polynomringen untersucht. Als wesentliches Werkzeug verwenden wir hierzu eine moderne Version des Bethschen Definierbarkeitssatzes.

Für einen Ring R, betrachten wir den Monoid $\mathfrak{End}_R(R^*)$ aller Einbettungen der Nonstandard-Erweiterung R^* in sich selbst, die die Standard-Elemente festhalten. Ist R ein Zahlring oder ein Körper, so ist die natürliche Restriktionsabbildung $\mathfrak{Res}_{R^*}$ von $\mathfrak{End}_{R[T]}(R[T]^*)$ auf $\mathfrak{End}_R(R^*)$ ein wohldefinierter Homomorphismus von Monoiden.

Unsere Aussagen betreffen Verbindungen zwischen der diophantischen Definierbarkeit des Ringes der ganzen Zahlen $\mathbb{Z}$ in einem Zahlring R, der Übertragung der Definierbarkeit von $R[T]$ auf R, und Eigenschaften der Restriktionsabbildung $\mathfrak{Res}_{R^*}$. In dem Fall des Ringes $\mathbb{Z}$ selbst bekommen wir als Nebenergebnis daß die Restriktionsabbildung

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

ein Isomorphismus von Monoiden ist. Diese Tatsache ist inhaltlich mit der Zusammenfassung zweier bekannten Sätze von Y. Matiyasevich und J. Denef gleichbedeutend. Wir beweisen, daß ännliche Sätze für manchen Ringe ganzer algebraischer Zahlen gelten, und vermuten, daß jeder Ring ganzer algebraischer Zahlen diese Eigenschaft hat.

Motto

"According to a Beth's theorem it is not necessary to write out a definition to prove that some given relation is definable, but until now this promissing method has never begun to be applied."

Patrick Cegielski, Yuri Matiyasevich, Denis Richard
Journal of Symbolic Logic, vol. 61, nr.2, June 1996

Introduction

The initial motivation of this thesis was the Decision Problem for algebraic theories. This problem originates from two questions of David Hilbert. In his program Hilbert asked for a formalisation of Mathematics allowing a general decision method which should establish the truth value for every well-formed formal sentence. The Tenth Problem of the celebrated list presented by Hilbert to the Paris Congress of Mathematicians (1900) is a restricted variant of this question: he asked for such a decision method for just the class of sentences which state the solvability of diophantine equations in several variables over the set of naturals.

Since the answers to both problems are negative, it was the more general problem which was answered first. This was done in 1931 by Kurt Gödel (see [Gödel]). In contemporary notation his result can be read as follows:

Theorem 1 $\mathrm{Th}(\mathbb{N}, +, \Leftrightarrow, \cdot, 0, 1)$ *is undecidable.*

A possible proof (given today) would consist of: assuming the truth of Church Thesis, developing the Recursion Theory since we get the existence of a **recursively enumerable** but **not recursive** subset $M \subset \mathbb{N}$, and proving that M is **definable** in $\mathbb{N}$. The latter means to find a formula $\varphi(x)$ with x as the only free variable in the formal language of the Arithmetic such that:

$$\forall\, n \in \mathbb{N} \qquad \mathbb{N} \models \varphi(n) \Longleftrightarrow n \in M.$$

If we assume that the formal theory of $\mathbb{N}$ was decidable, we could list the set $\mathbb{N} \setminus M$ by verifying the truth values of the sequence of formal statements $(\varphi(n))$ with the decision method. This is in contradiction to the choice of M.

As we see, half of the job was done by the **definability** of M in $\mathbb{N}$. But for deducing the undecidability of algebraic theories corresponding to other structures, it is now enough to define $\mathbb{N}$ with its operations in the language of the respective structure. This idea was exemplary applied by Julia Robinson in 1959 when she proved (see [J. Robinson]):

Theorem 2 $\mathbb{N}$ *is definable in all number fields and in their rings of algebraic integers. All the corresponding theories are undecidable.*

In 1961 Martin Davis, Hilary Putnam and Julia Robinson succeded in a celebrated joint work (see [DPR]) in proving that all recursively enumerable sets are

definable over $\mathbb{N}$ in the language of Arithmetic expanded by a predicate for the exponential relation (a, b, a^b) so that the definition always consists of an existential prefix followed by an equation. In particular, a nonrecursive set admits such a definition, thus they got:

Theorem 3 *The existence of solutions for exponentially diophantine equations is undecidable.*

It was a general surprise when Yuri Matiyasevich in 1970 proved:

Theorem 4 *The exponential relation over* $\mathbb{N}$ *is definable using a formula consisting of an existential prefix followed by a diophantine equation (is* **diophantine***).*

We will call this result Theorem of Matiyasevich in **restricted sense**. Together with the Davis-Putnam-Robinson result we also get the Theorem of Matiyasevich in **extended sense**:

Theorem 5 *Any relation over* $\mathbb{N}$ *is recursively enumerable iff it is diophantine.*

In particular such relations which are not recursive are diophantine, so the class of diophantine equations is also undecidable. This gives a negative answer to the Tenth Problem of Hilbert.

After the result of Matiyasevich many researchers, among them Jan Denef, Leonhard Lipshitz, Thanases Pheidas, and Alexandra Shlapentokh improved the result of Julia Robinson in the new context, giving a diophantine definition of the naturals in different number rings. Their method was inspired by the work of Matiyasevich. They envisaged the possibility to define exponential relations in rings of algebraic integers using the Pell equations like Matiyasevich did. The general belief in the present (1998) is that this idea has been already exhausted without being applicable to all the rings of algebraic integers. The situation of the number fields is even worse: no case has been solved. It has been conjectured that the diophantine theory of the rationals $\mathbb{Q}$ is undecidable but the naturals $\mathbb{N}$ are not diophantine in $\mathbb{Q}$.

In this thesis we are looking for conditions which are equivalent to the diophantine definability of $\mathbb{N}$ in number rings and fields. Our approach is model-theoretic and our main tool is an improvement of the classical Theorem of Beth on definability. This tool has been used a few times, but in general it has been mistrusted for good reason, namely because of the lack of necessary knowledge about the structure of nonstandard extensions, which does not allow its successful application (see the motto). The possibility to work with embeddings of a nonstandard model in itself in connection with diophantine problems was already mentioned by L. Lipshitz (see [Lipshitz]) in a different context.

Our first observation was the fact that diophantine definitions for the natural numbers $\mathbb{N}$ are easier and work more generally in the polynomial rings over the number rings (or fields) than in the number rings themselves. The same happens

for example in the case of a relation with exponential increment defined in $\mathbb{Z}[T]$ compared to the same relation defined in $\mathbb{Z}$ (see Chapter 5 and the Appendix)

In Chapter 3 we prove the existence of a phenomenon of transfer of definability from the polynomial ring over a number ring (or field) to the ring (or field) itself. In Chapter 4 we prove that our transfer preserves the diophantine character of a definition iff $\mathbb{Z}$ (or $\mathbb{N}$) is diophantine in the number ring (or field). This fact is put in connection with the surjectivity of the application of restriction defined in the abstract.

The conclusion of Chapters 5 and 6 is our Isomorphism Theorem for the ring of rational integers $\mathbb{Z}$. Connections between this result and the classical theorems of Y. Matiyasevich and J. Denef are proven.

Chapter 7 deals with the injectivity of the application of natural restriction. It does not have an immediate significance for the Decision Problem anymore but for various definability problems.

The chapters should be read in their order.

Einführung

Ausgangspunkt dieser Arbeit sind Ergebnisse zu Entscheidungsproblemen algebraischer Theorien. Diese Problemstellung geht auf David Hilbert zurück. In seinem berühmten Programm stellte Hilbert die Frage, ob es eine Formalisierung der gesammten Mathematik gibt, die ein Verfahren zuläßt, das für jede formale Aussage entscheidet, ob sie richtig oder falsch ist. Das zehnte der 23 Probleme, die Hilbert 1900 in Paris dem Internationalen Kongreß der Mathematiker vorlegte, bestand ebenfalls aus der Frage nach einem solchen Entscheidungsverfahren, allerdings in diesem Fall nur für die Sätze, die die Lösbarkeit diophantischer Gleichungen über die natürlichen Zahlen behaupten.

Da die Antworten auf beide Fragen negativ sind, ist es nicht überraschend, daß die allgemeinere Frage als erstes beantwortet wurde. Dies ist 1931 Kurt Gödel gelungen (siehe [Gödel]). Sein unter *Gödelscher Unvollständigkeitssatz* bekanntes Ergebnis kann in heutiger Terminologie wie folgt formuliert und verstanden werden:

Satz 1 $\mathrm{Th}(\mathbb{N}, +, \Leftrightarrow, \cdot, 0, 1)$ *ist unentscheidbar.*

Um dies einzusehen genügt es - unter Voraussetzung der Churchschen These -, die Theorie der rekursiven Funktionen nur so weit zu entwickeln, daß die Existenz einer **definierbaren** Teilmenge M von $\mathbb{N}$ bewiesen werden kann, die **rekursiv-aufzählbar** aber **nicht rekursiv** ist. Sei etwa $\varphi(x)$ (x einzige freie Variable von φ), eine Formel die M definiert, das heißt:

$$\forall\, n \in \mathbb{N} \quad \mathbb{N} \models \varphi(n) \Longleftrightarrow n \in M.$$

Würde ein Entscheidungsverfahren für die Theorie von $\mathbb{N}$ vorliegen, so könnte man dadurch, indem man selbiges auf den Satz $\varphi(n)$ anwendet, entscheiden, ob n zu $\mathbb{N} \setminus M$ gehört. Aufgrund der Churchschen These heißt dies aber wiederum, daß $\mathbb{N} \setminus M$ auch rekursiv-aufzählbar und somit, im Widerspruch zur Voraussetzung, M rekursiv ist.

Neben der Bedeutung der Definierbarkeit für dieses grundlegende Ergebnis, findet sie Verwendung bei der Ableitung anderer Unentscheidbarkeitsresultate: gelingt es, $(\mathbb{N}, +, \cdot, \Leftrightarrow 0, 1)$ in einer Struktur zu definieren, so überträgt sich die Unentscheidbarkeit von $\mathrm{Th}(\mathbb{N})$ auf die Theorie selbiger Struktur. Beispielhaft wurde dies von Julia Robinson 1959 durchgeführt, um folgendes zu zeigen (siehe [J. Robinson]):

Satz 2 $\mathbb{N}$ *ist in allen Zahlkörpern und ihren Ringen ganzer Zahlen definierbar. Alle entsprechenden formalen Theorien sind unentscheidbar.*

Martin Davis, Hilary Putnam und Julia Robinson haben 1961 bewiesen (siehe [DPR]), daß alle rekursiv-aufzählbaren Mengen in der um das **exponentielle Prädikat** (a, b, a^b) erweiterten Sprache der Arithmetik, durch Gleichungen definierbar sind. Da eine beliebige nicht-rekursive rekursiv-aufzählbare Menge auch eine solche Definition hat, folgt daraus:

Satz 3 *Die Frage, ob eine exponentiell-diophantische Gleichung über* $\mathbb{N}$ *in natürlichen Zahlen lösbar ist, ist unentscheidbar.*

Zur allgemeinen Überraschung gelang es Yuri Matiyasevich 1970 die letzte Lücke zu einer negativen Antwort auf das 10. Hilbertsche Problem zu schließen, indem er bewies:

Satz 4 *Das exponentielle Prädikat ist über* $\mathbb{N}$ *durch eine Formel definierbar, die aus einem rein existentiellem Prefix, gefolgt von einer diophantischen Gleichung, besteht. (Das exponentielle Prädikat ist* **diophantisch***.)*

Dieses Ergebnis werden wir *Satz von Matiyasevich im engeren Sinne* nennen. Zusammen mit dem Satz von Davis, Putnam und Robinson folgt der *Satz von Matiyasevich im erweiterten Sinne*:

Satz 5 *Eine Relation über* $\mathbb{N}$ *ist genau dann rekursiv-aufzählbar, wenn sie diophantisch ist.*

Da eine beliebige nicht-rekursive solche Menge diophantisch ist, ist die Klasse der diophantischen Gleichungen über $\mathbb{N}$ auch unentscheidbar, und somit die Antwort auf das 10. Hilbertsche Problem negativ.

Nach der Arbeit von Matiyasevich haben Forscher wie Jan Denef, Leonhard Lipshitz, Thanases Pheidas und Alexandra Shlapentokh versucht die zwei erwähnten Forschungsrichtungen zu vereinigen. Sie haben $\mathbb{N}$ in verschiedenen Zahlringen diophantisch definiert, indem sie die Methode von Yuri Matiyasevich an die allgemeinere Situation angepaßt haben, das heißt insbesondere, daß in den betrachteten Zahlringen exponentielle Prädikate definiert wurden.

Gemäß allgemeiner Meinung scheinen damit im Fall von Zahlringen die Möglichkeiten dieser Methode weitgehend ausgeschöpft zu sein. Im Fall von Zahlkörpern liegen bis heute keinerlei Ergebnisse vor. Es wird vermutet daß die diophantische Theorie der rationalen Zahlen $\mathbb{Q}$ unentscheidbar ist und daß, anders als in den erwähnten Fällen, $\mathbb{N}$ nicht diophantisch in $\mathbb{Q}$ ist.

In dieser Doktorarbeit werden nun neue Bedingungen gesucht, die mit der diophantischen Definierbarkeit von $\mathbb{Z}$ (oder $\mathbb{N}$...) in Zahlringen und Zahlkörpern äquivalent sind. Der verwendete Zugang kommt aus der Modell-Theorie - Hauptwerkzeug ist eine Version des Bethschen Definierbarkeitssatzes. Auf diesem Satz

ist bisher sehr selten zurückgegriffen worden, da dazu zu wenig über Nonstandard-Erweiterungen bekannt ist. Allerdings hat schon L. Lipschitz die Möglichkeit bemerkt, Problemstellungen hinsichtlich der Struktur diophantisch-korrekter Nonstandard-Modellen der Arithmetik mittels Einbettungen der selben zu behandeln.

Grundlegend für die Arbeit ist die Beobachtung, daß sich $\mathbb{N}$ viel einfacher und uniformer in beliebigen Polynomringen definieren läßt, als in Zahlringen. Dies ist auch für Relationen mit exponentieller Wachstumsrate über $\mathbb{Z}$ der Fall (vergleiche den Kapitel 5 mit dem Appendix).

Nach Vorarbeiten in Kapitel 1 und 2, beweisen wir in dritten Kapitel die Existenz eines Übertragungsprinzips der Definierbarkeit von einem Polynomring über einem Zahlring auf den Zahlring selber. In Kapitel 4 wird bewiesen daß diese Übertragung genau dann diophantisch-treu ist, wenn $\mathbb{Z}$ im betrachteten Zahlring diophantisch ist. Die Verbindung mit der Surjektivität der im Abstract definierter Restriktionsabbildung wird auch bewiesen und erklärt.

Die Schlußfolgerung der Kapitel 5 und 6 ist unserer Isomorphiesatz für den Ring $\mathbb{Z}$ der ganzen Zahlen. Der Rückschluß von diesem Satz auf die klassischen Ergebnisse von Y. Matiyasevich und J. Denef wird ebenfalls bewiesen und erklärt.

In Kapitel 7 beschäftigen wir uns mit der Injektivität der Restriktionsabbildung über Zahlringe. Dies hat keine direkte Bedeutung mehr für das Entscheidungsproblem, aber für verschiedene Definierbarkeitsprobleme.

Die Kapitel sollten der Reihe nach gelesen werden.

Acknowledgements

I wish to thank all the people who supported this work directly or indirectly.

First of all, I would like to thank my Doktorvater Prof. Dr. A. Prestel. His assistance and criticism were always helpful and his demand for clarity and precision still challenges me. Without his continuous support and his permanent confidence this thesis would never exist.

The most important of my listeners were Prof. Dr. S. Basarab from the Mathematical Institute of the Romanian Academy, Dr. J. Koenigsmann, and Dr. U. Friedrichsdorf. In addition, T. Jacobi, M. Nüsken and W. Glas were involved in various conversations.

Furthermore, I am indebted to J. Koenigsmann and T. Jacobi for linguistic advice and proof-reading. T. Jacobi improved stilistically the German introduction, U. Gandbhir the English one.

I have to apologize to and thank all the people who were drawn into discussions by me, sometimes without understanding much of the story. All of them were a real support.

The University of Konstanz (Land Baden-Württemberg) and the Deutscher Akademischer Austauschdienst (D.A.A.D) supported my work successively. My first contact to the University of Konstanz was also possible due to D.A.A.D.

Contents

Chapter 1

A New Version of a Theorem of Beth

The aim of this chapter is to state and prove structural facts on definability and existential definability. We are interested in two modern forms of the Theorem of Beth, corresponding with the two notions of definability. Its classical statement 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

$$T \vdash \ \forall x_1, \ldots, x_n \ (P(x_1, \ldots, x_n) \longleftrightarrow \phi(x_1, \ldots, x_n)).$$

The notion of implicitly definable 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 those 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

$$T \cup T' \vdash \ \forall x_1, \ldots, x_n \ (P(x_1, \ldots, x_n) \longleftrightarrow P'(x_1, \ldots, x_n)).$$

Already in [Shoenfield] implicitly definable was understood as preserved by the authomorphisms of all the models of the given theory. Since in our context all the considered theories are complete theories of the form $\mathrm{Th}_L\ (\mathcal{A})$ for a concrete L-structure $\mathcal{A}$, it suffices to look just at the authomorphisms of a sufficient saturation of the given structure $\mathcal{A}$. In the case of the existential definability the authomorphisms will be replaced by the embeddings of such a saturated structure in itself. The results of this chapter will be used throughout this thesis as underlying model-theoretical basis.

The language L will be supposed finite.

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

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

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

We will call a structure $\mathcal{A}$ **saturated** iff it is card($\mathcal{A}$)-saturated. For a set of propositions , in the formal language L we will write: $\mathcal{A} \rightsquigarrow^{\Gamma} \mathcal{B}$ in the case that for all $\gamma \in$, , if $\mathcal{A} \models \gamma$ then $\mathcal{B} \models \gamma$. The following basic facts can be found in [Prestel], see pg. 127, 132, 159. We call them Separation, Embedding and Isomorphism.

Sep Let $\Sigma \cup$, $\cup \{\phi\}$ be a set of closed L-formulas (L-propositions) such that Σ is consistent and there are $\gamma_0, \gamma_1 \in$, with $\Sigma \vdash \gamma_0$ and $\Sigma \vdash \neg\gamma_1$. Suppose that for all models $\mathcal{A}$ and $\mathcal{B}$ of Σ

$$\mathcal{A} \rightsquigarrow^{\Gamma} \mathcal{B} \Longrightarrow \mathcal{A} \rightsquigarrow^{\phi} \mathcal{B}.$$

Then there is a finite subset $\{\gamma_{ij}\} \subseteq$, such that:

$$\Sigma \vdash (\phi \longleftrightarrow \bigvee_i \bigwedge_j \gamma_{ij}).$$

□

Emb Let $\mathcal{A}$ and $\mathcal{A}'$ be L-structures, such that $\mathcal{A}'$ is κ-saturated for an infinite cardinal number $\kappa \geq$ card ($\mathcal{A}$). If any existential proposition which is valid in $\mathcal{A}$ is also valid in $\mathcal{A}'$ (write $\mathcal{A} \rightsquigarrow^{\exists} \mathcal{A}'$) then there is an L-embedding $\mathcal{A} \hookrightarrow \mathcal{A}'$. □

Iso Two L-structures which are elementarily equivalent, saturated and of the same cardinality are L-isomorphic. □

Now we can state our variant for the Theorem of Beth. This improvement was communicated to us by A. Prestel:

Theorem 1.1 *Let $\mathcal{A}$ be an L-structure and $P \subseteq \mathcal{A}^n$ a new relation defined over the underlying set of the structure $\mathcal{A}$. Let $(\mathcal{C}, \mathcal{P})$ be a saturated $L \cup \{P\}$-structure with card($\mathcal{C}$) $\geq$ card(L) such that*

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

Old Beth: *P is definable in terms of L iff all L-automorphisms of $\mathcal{C}$ are also P-automorphisms.*

New Beth: *P is existentially definable in terms of L iff for all L-embeddings η of $\mathcal{C}$ in itself $\eta(\mathcal{P}) \subset \mathcal{P}$.*

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

Proof: The proof is almost the same for the both statements, except for an important point which will be emphasized. The directions $\Rightarrow$ of the two equivalences are trivial. In order to prove $\Leftarrow$ we do some short preparations.

For $n =$ arity (P) let $C = \{c_1, \ldots, c_n\}$ be a set of new constants. We define three new languages $LP = L \cup \{P\}$, $LC = L \cup C$ and $LPC = L \cup \{P\} \cup C$. $\Sigma = \mathrm{Th}_{LP}(\mathcal{A})$ is a complete theory, so of course consistent. The set of formal propositions $,_D := \{$ all closed formulas in LC $\}$ will be used for proving the Old Beth's Theorem, the set $,_E := \{$ all closed existential formulas in LC in prenex normal form $\}$ will be used for the New one. We put $\phi := P(c_1, \ldots, c_n)$, $\gamma_0 := \exists x(x = x)$ and $\gamma_1 := \exists x(x \neq x)$. Finally, let $\kappa := \mathrm{card}(\mathcal{C})$.

Now we verify the hypothesis of **Sep** for the language LPC. Choose $, \in \{, _D, , _E\}$. Suppose $(\mathcal{E}, P_\mathcal{E})$ and $(\mathcal{F}, P_\mathcal{F})$ to be models of Σ and $\vec{a} \in \mathcal{E}^n$, $\vec{b} \in \mathcal{F}^n$ to be interpretations of the constants C such that

$$(\mathcal{E}, P_\mathcal{E}, \vec{a}) \rightsquigarrow^\Gamma (\mathcal{F}, P_\mathcal{F}, \vec{b}).$$

We may substitute both structures with new saturated structures of cardinality κ, $\mathcal{E}'$ and $\mathcal{F}'$, which are LPC-elementarily equivalent to $\mathcal{E}$ and $\mathcal{F}$ respectively for well chosen interpretations $\vec{a'}$ and $\vec{b'}$ of the new constants. It is still true that:

$$(\mathcal{E}', P_{\mathcal{E}'}, \vec{a'}) \ \rightsquigarrow^\Gamma \ (\mathcal{F}', P_{\mathcal{F}'}, \vec{b'}).$$

If we forget the constants, we have two LP-elementarily equivalent saturated structures of the same cardinality κ. Using **Iso** we may identify both of them with $(\mathcal{C}, \mathcal{P})$ through isomorphisms which will transport $\vec{a'} \rightsquigarrow \vec{\alpha}$ say, and $\vec{b'} \rightsquigarrow \vec{\beta}$. We have got:

$$(\mathcal{C}, \mathcal{P}, \vec{\alpha}) \ \rightsquigarrow^\Gamma \ (\mathcal{C}, \mathcal{P}, \vec{\beta}).$$

Forgetting now P for a moment, we analyse the cases separately:

$\underline{, = , _D}$ The set $\{\gamma \in , _D \mid (\mathcal{C}, \vec{\alpha}) \models \gamma\}$ is the complete theory of $(\mathcal{C}, \vec{\alpha})$ in the language LC, which is then entirely valid on $(\mathcal{C}, \vec{\beta})$. Recalling again **Iso** we see that $(\mathcal{C}, \vec{\alpha})$ and $(\mathcal{C}, \vec{\beta})$, as LC-elementarily equivalent saturated structures of the same cardinality are LC-isomorphic. So there is an L-isomorphism $\iota : \mathcal{C} \tilde{\leftrightarrow} \mathcal{C}$ such that $\iota(\vec{\alpha}) = \vec{\beta}$. After our hypothesis ι must be also a P-isomorphism:

$$\iota(\mathcal{P}) = \mathcal{P}.$$

$\underline{,\ =\ ,\ _E}$ In this case $(\mathcal{C},\vec{\alpha}) \rightsquigarrow^{\exists} (\mathcal{C},\vec{\beta})$ and $(\mathcal{C},\vec{\beta})$ is card $(\mathcal{C})$ - saturated, so using **Emb** there is an LC-embedding $\eta : \mathcal{C} \hookrightarrow \mathcal{C}$ such that $\eta(\vec{\alpha}) = \vec{\beta}$. After the hypothesis it is true that:

$$\eta(\mathcal{P}) \subseteq \mathcal{P}.$$

Now suppose that $(\mathcal{E}, P_{\mathcal{E}}, \vec{a}) \models \phi$. This means:

$$P_{\mathcal{E}}(\vec{a}) \Leftrightarrow P_{\mathcal{E}'}(\vec{a'}) \Leftrightarrow \mathcal{P}(\vec{\alpha}).$$

Through ι or through η we get back:

$$\mathcal{P}(\vec{\beta}) \Leftrightarrow P_{\mathcal{F}'}(\vec{b'}) \Leftrightarrow P_{\mathcal{F}}(\vec{b}).$$

The last means that $(\mathcal{F}, P_{\mathcal{F}}, \vec{b}) \models \phi$. This is exactly:

$$(\mathcal{E}, P_{\mathcal{E}}, \vec{a}) \rightsquigarrow^{\phi} (\mathcal{F}, P_{\mathcal{F}}, \vec{b}).$$

The hypothesis of **Sep** has been verified. In consequence there is a finite set $\{\gamma_{ij}\} \subseteq ,$ such that:

$$\Sigma \vdash [\phi \longleftrightarrow \bigvee_i \bigwedge_j \gamma_{ij}],$$

in the language LPC. By substituting explicitly the constants from C, one gets:

$$\Sigma \vdash [P(c_1,\ldots,c_n) \longleftrightarrow \bigvee_i \bigwedge_j \gamma_{ij}(c_1,\ldots,c_n)].$$

But C were new constants which didn't belong to the language LP of the theory Σ. This fact permits us to apply the rule of generalization to get:

$$\Sigma \vdash \forall x_1,\ldots,x_n\ [P(x_1,\ldots,x_n) \longleftrightarrow \bigvee_i \bigwedge_j \gamma_{ij}(x_1,\ldots,x_n)].$$

Now remember just that $\Sigma = \mathrm{Th}_{LP}(\mathcal{A})$. It follows:

$$(\mathcal{A},\mathcal{P}) \models \forall x_1,\ldots,x_n\ [P(x_1,\ldots,x_n) \longleftrightarrow \bigvee_i \bigwedge_j \gamma_{ij}(x_1,\ldots,x_n)],$$

which is the desired L-definition of P in $\mathcal{A}$.

□□

Remark 1.2 *If card $(\mathcal{A}) \in \{\aleph_0, \aleph_1\}$ we can use for $\mathcal{C}$ the classical ultrapower $\mathcal{A}^* = (\prod_{n\in\mathbb{N}} \mathcal{A})/\equiv_{\mathcal{U}}$ because card $(\mathcal{A}^*) = \aleph_1$ and $\mathcal{A}^*$ is $\aleph_1$-saturated.* □

We can already give an application of our new version of the Theorem of Beth. Following the Theorem of Matiyasevich in extended sense, a subset of $\mathbb{N}$ is recusively 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 Beth's Theorem 1.1 in the situation of Remark 1.2, we get directly:

Remark 1.3 *Consider the set of the natural numbers $\mathbb{N}$ as an $L = \{+, \Leftrightarrow, \cdot, 0, 1\}$ -structure, a subset $M \subset \mathbb{N}$ and a new relation $\mathcal{M}$ 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 $\mathcal{M}$ over $\mathbb{N}^*$. Then the following are true:*

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

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

Chapter 2

From $\exists$-Definable to Diophantine

We will present the situation in which, over a ring, the families of existentially definable sets and respectively diophantine sets (in the classical sense, sets which are definable using an equation preceeded from some existential quantfiers) coincides. Our second aim is to introduce the main concrete rings which make the object of this thesis: the number fields, their rings of algebraic integers and the polynomial rings over all of them. Almost all the chapter will be used further.

2.1 General Facts

Definition: Let R be a commutative ring with 1 and L be an extension with constants of the formal language of rings $\{+, \Leftrightarrow, \cdot, 0, 1\}$. For some $k \in \mathbb{N}$ we call a set $A \subseteq R^k$ **L-diophantine** iff it is positive-existentially L-definable, i.e. it has an L-definition in R of the following form:

$$\vec{x} \in A \Leftrightarrow \exists\, t_1, t_2, \ldots, t_m \bigvee_i \bigwedge_j P_{ij}(x_1, \ldots, x_k, t_1, \ldots, t_m) = 0,$$

where $P_{ij} \in R[x_1, \ldots, x_n, t_1, \ldots, t_m]$ are polynomials whose coefficients are constant terms built up from the constants of L.

Positive means that we are not allowed to use negations inside the disjunctive normal form. Apparently the class of diophantine sets (called also diophantine relations or predicates) should be strictly smaller than the class of all existentially definable sets. We are interested in the situations when the two classes coincide, in order to apply the New Beth's Theorem to diophantine sets.

Lemma 2.1 *Let R be a ring and L be an extension with constants of the formal language of rings, interpreted over R, such that the unary relation $t \in R \setminus \{0\}$, shortly denoted $t \neq 0$, is L-diophantine. Then every existentially L-definable relation is L-diophantine.*

Proof: Let $P(x_1, \ldots, x_n)$ be an existentially definable relation. As we have seen proving 1.1, P is in fact of the form $\bigvee_i \bigwedge_j \gamma_{ij}(x_1, \ldots, x_n)$, where the γ_{ij} consist of existential prefixes followed by boolean expresions of positive and negated equalities. All negated equalities can be removed using the diophantine definition of $t \neq 0$. We must only use new variables for every new substitution. As last syntactical operation we carry the quantifiers at the beginning. □

Definition: A ring R will be called **adequate** with respect to a language L iff all existentially L-definable relations over R are L-diophantine over R.

A ring R is adequate with respect to L iff the relation $t \neq 0$ is L-diophantine, because the empty prefix is also existential. We will work essentially only with adequate rings. The next counterexample motivates a future choice for a formal language.

Theorem 2.2 *Let Δ be a commutative ring not necessarily with 1.*

1. *Let L be an extension with constants of the formal language of rings interpreted over Δ. Let T be a transcendental over Δ. Then the ring $\Delta[T]$ is not adequate with respect to L.*

2. *Let $\Omega = \Delta[T_1, T_2, \ldots, T_n, \ldots]$ be the polynomial ring in $\aleph_0$ variables over Δ. Then there is no extension with constants L of the formal language of rings such that Ω is adequate with respect to L.*

Proof of 1: Let $\mathcal{L} = \{+, \Leftrightarrow, \cdot, (\underline{a})_{a \in \Delta}\}$ be a new language which contains a name (constant) for every element of Δ. Of course we can consider that $L \subseteq \mathcal{L}$, so the fact that $\Delta[T] \setminus \{0\}$ is not $\mathcal{L}$-diophantine over $\Delta[T]$ implies that it is also not L-diophantine over $\Delta[T]$. For $\Delta[T]$ we define the language $\mathcal{LT} = \mathcal{L} \cup \{\underline{T}\}$, with $\underline{T}$ interpreted as T. Suppose now that the subset $\Delta[T] \setminus \{0\}$ is $\mathcal{L}$-diophantine in $\Delta[T]$. Its positive existential definition can be put in the normal form:

$$\Delta[T] \models t \neq \underline{0} \Longleftrightarrow \exists X_1, \ldots, X_n \bigvee_i \bigwedge_j P_{ij}(t, X_1, \ldots, X_n) = \underline{0},$$

where $P_{ij} \in \Delta[t, X_1, \ldots, X_n]$ have coefficients which are constant terms over $\mathcal{L}$ and do not contain $\underline{T}$.

We remark that for an element $a \in \Delta \setminus \{0\}$ is $aT \in \Delta[T] \setminus \{0\}$. (This is a precaution for the case that the ring has no 1. Normally we work with the polynomial T.) We fix a choice of polynomials $Y_1(T), \ldots, Y_n(T)$ and an index i_0 such that

$$\Delta[T] \models \bigwedge_j P_{i_0,j}(\underline{aT}, Y_1(\underline{T}), \ldots, Y_n(\underline{T})) = \underline{0}.$$

For the ring Δ with respect to $\mathcal{L}$ this is a conjunction of true polynomial identities in a new constant $\underline{T}$. The new constant may be substituted with every constant

from $\mathcal{L}$, leading to true sentences. This is possible because T is transcendental over Δ. We substitute $\underline{T}$ with $\underline{0}$. From an algebraic point of view this is the evaluation in $T = 0$ of a polynomial function. We get:

$$\Delta \text{ and } \Delta[T] \models \bigwedge_j P_{i_0,j}(\underline{0}, Y_1(\underline{0}), \ldots, Y_n(\underline{0})) = \underline{0}.$$

We remark that $\forall k\ X_k := Y_k(0) \in \Delta \subset \Delta[T]$. X_k are again constant $\mathcal{L}$-terms. The crucial fact that $\underline{T}$ did not occur in the coefficients of P_{ij} allowed us to keep and get back these polynomials after the evaluation. Now:

$$\Delta[T] \models \quad \exists X_1, \ldots, X_n \quad \bigwedge_j P_{i_0,j}(\underline{0}, X_1, \ldots, X_n) = \underline{0},$$
$$\Delta[T] \models \quad \exists X_1, \ldots, X_n \quad \bigvee_i \bigwedge_j P_{ij}(\underline{0}, X_1, \ldots, X_n) = \underline{0}.$$

If we remember the way in which we have defined $t \neq 0$, we get finally:

$$\Delta[T] \models\ \underline{0} \neq \underline{0}.$$

This is a contradiction. □

Proof of 2: We are following the proof of 2.2.1 insisting on some differences. We introduce the language $\mathcal{LT}_\infty = \mathcal{L} \cup \{\underline{T_1}, \underline{T_2}, \ldots\}$. It is the strongest extension with constants of the formal language of rings for Ω, in the sense that all elements of Ω can be represented as constant $\mathcal{LT}_\infty$-terms. We prove that the subset $\Omega \setminus \{0\}$ is not $\mathcal{LT}_\infty$-diophantine in Ω, and it is sufficient for our conclusion.

As before suppose that $\Omega \setminus \{0\}$ was $\mathcal{LT}_\infty$-diophantine and had a positive existential definition in prenex normal form given by $P_{ij} \in \Omega[t, X_1, \ldots, X_n]$. Only a finite set of variable-names may occur in the P_{ij}'s, say without restricting the generality $\underline{T_1}, \underline{T_2}, \ldots, \underline{T_m}$. These are the constants which will not be subjected to any substitution. We write also $\Delta_m := \Delta[T_1, T_2, \ldots, T_m]$ and $\mathcal{LT}_m = \mathcal{L} \cup \{\underline{T_1}, \underline{T_2}, \ldots, \underline{T_m}\}$.

Now for $a \in \Delta \setminus \{0\}$ is again $aT_{m+1} \in \Omega \setminus \{0\}$. We choose and fix elements $Y_1, \ldots, Y_n \in \Omega$ and one index i_0 such that:

$$\Omega \models \bigwedge_j P_{i_0,j}(\underline{aT_{m+1}}, Y_1, \ldots, Y_n) = \underline{0}.$$

Only a finite number of variable-names can occur in the Y_k's, say $\underline{T_1}, \underline{T_2}, \ldots, \underline{T_m}$, $\underline{T_{m+1}}, \ldots, \underline{T_{m+p}}$. If it happens in fact that the Y_k's are already elements in Δ_m, it is anyway true for some $p \geq 1$.

$\underline{T_{m+1}}, \ldots, \underline{T_{m+p}}$ are new constants over $(\Delta_m, \mathcal{LT}_m)$ and may be substituted with any other constants. We substitute $\underline{T_{m+1}}$ with $\underline{0}$ and $\underline{T_{m+2}}, \ldots, \underline{T_{m+p}}$ with

arbitrary other constants from $\mathcal{L}$, say $\underline{a_{m+2}}, \ldots, \underline{a_{m+p}}$. If we denote now by $X_k := Y_k(T_1, \ldots, T_m, 0, a_{m+2}, \ldots, a_{m+p}) \in \Delta_m \subset \Omega$, we get:

$$\Delta_m \text{ and } \Omega \models \exists X_1, \ldots, X_n \bigwedge_j P_{i_0,j}(\underline{0}, X_1, \ldots, X_n) = \underline{0},$$

which means the contradiction $\Omega \models \underline{0} \neq \underline{0}$. The crucial facts were the following: First $\underline{T_1}, \underline{T_2}, \ldots, \underline{T_m}$ have not been substituted, permitting us to get back the P_{ij}'s and the diophantine definition. Second, no possible formal definition could use infinitely many constants (in our case, variable-names). □□

Using the same procedure we can prove the following:

Remark 2.3 *If Δ is a commutative ring with 1 and L an extension with constants of the formal language of rings interpreted over Δ, then the unary singleton relation $\{T\}$ is not L-diophantine over $\Delta[T]$.*

Definition: An L-diophantine set defined using **exactly one** equation whose coefficients are constant L-terms and which is existentilly quantified will be called **strongly L-diophantine**. From now on we will mention the language L just if it will be necessary.

Lemma 2.4 *If R is an integral domain, every union of two strongly diophantine sets is again strongly diophantine. Every disjunction of strongly diophantine relations is again strongly diophantine.*

Proof: Let P and Q be two n-ary strongly diophantine relations defined as $P(\vec{x}) \Leftrightarrow \exists \vec{\lambda}\ p(\vec{x}, \vec{\lambda}) = 0$ respectively $Q(\vec{x}) \Leftrightarrow \exists \vec{\theta}\ q(\vec{x}, \vec{\theta}) = 0$. The two parameter vectors must not have the same length. Then:

$$(P \vee Q)(\vec{x}) \Longleftrightarrow \exists \vec{\lambda}, \vec{\theta}\ p(\vec{x}, \vec{\lambda}) q(\vec{x}, \vec{\theta}) = 0.$$

□

Definition: A ring in which any union of two strongly diophantine sets is strongly diophantine will be called **disjunctive**. A ring is disjunctive iff the binary diophantine relation $x = 0 \vee y = 0$ is strongly diophantine. We have already seen that integral domains are disjunctive with respect of the formal language of rings.

The next result is intended to ilustrate the behaviour of disjunctivity over rings which are not domains. It will not be used along this thesis. Its proof will be displayed in an appendix.

Theorem 2.5 *The commutative ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is disjunctive iff $n = p^k$ is a prime power.*

Analogous considerations lead to the notion of conjunctive rings:

Lemma 2.6 *Let R be a ring such that the binary singleton relation $\{(0,0)\}$ is strongly L-diophantine in R. Then every intersection between two strongly diophantine sets is again strongly diophantine. Every conjunction of two strongly diophantine relations is again strongly diophantine.*

Proof: Let P and Q be two n-dimensional strongly diophantine sets as before and let $(a,b) = (0,0) \Leftrightarrow \exists \vec{\chi}\ \ \mathfrak{R}(a,b,\vec{\chi}) = 0$ the strongly diophantine definition of the singleton $\{(0,0)\}$. Then:

$$(P \wedge Q)(\vec{x}) \Longleftrightarrow \exists \vec{\lambda}, \vec{\theta}, \vec{\chi}\ \ \mathfrak{R}(p(\vec{x},\vec{\lambda}), q(\vec{x},\vec{\theta}), \vec{\chi}) = 0.$$

Definition: A ring in which every intersection between two strongly diophantine sets is again strongly diophantine will be called **conjunctive**.

A ring is conjunctive iff the binary singleton diophantine relation $(x,y) \in \{(0,0)\} \Leftrightarrow x = 0 \wedge y = 0$ is strongly diophantine. It is not difficult to see that the field $\mathbb{C}$ is not conjunctive. If a set $\{(x,y) \in \mathbb{C}^2 \mid \exists \vec{\lambda}\, P(x,y,\vec{\lambda}) = 0\}$ is not empty, it contains already a not empty set $\{(x,y) \in \mathbb{C}^2 \mid P(x,y,\vec{\lambda_0}) = 0\}$ which has complex dimension ≥ 1 so may not be a geometric point in the complex plane.

Lemma 2.7 *Let R be a domain of characteristic 0 such that the algebraic closure of $\mathbb{Q}$ (denoted $\tilde{\mathbb{Q}}$) is not contained in the field of fractions* Quot*(R). Then R is conjunctive with respect to the formal language of rings.*

Proof: The hypothesis assures the existence of a polynomial $r(X) \in \mathbb{Z}[X]$ which has not zeros in $\mathrm{Quot}(R)$. This means for the homogenized $\mathfrak{R}(X,Y)$ of $r(X)$ that:

$$R, \mathrm{Quot}(R) \models \mathfrak{R}(a,b) = 0 \Longleftrightarrow a = 0 \wedge b = 0.$$

□

In order to indicate the nontrivial behaviour of the conjunctivity in the case of rings which are not domains, we will prove in the appendix the following result:

Theorem 2.8 *The commutative ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is conjunctive iff $n = p_1 \ldots p_s$ is square-free.*

To sum up, in a conjunctive and disjunctive adequate ring every existentially definable relation is strongly diophantine. All the concrete rings which will be studied here have these properties. That's why we will speak only about **L-diophantine relations** (sets) for understanding subsets of R^k defined using a formula with k free variables consisting of an existentially quantified equation.

Definition: We call a ring R **diophantine** with respect to a formal language L extending with constants the formal language of rings iff R is adequate, conjunctive and disjunctive with respect to L. Applying our new version of the Theorem of Beth 1.1 we get the following:

Remark 2.9 *Let R be a ring which is diophantine with respect to L. Let $P \subseteq R^d$ a new relation over R and $(\mathcal{R}, \mathcal{P})$ a saturated $L \cup \{P\}$-structure which 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 card(R) is at most $\aleph_1$ we may apply Remark 1.2 and study just the L-embeddings of the nonstandard extension R^*.*

Before starting to speak about the concrete rings which will be considered, we indicate two other classical properties of diophantine sets:

Remark 2.10 *Projections of existentially definable sets are still existentially definable. The same is true for diophantine sets.*

Proof: Of course, adding an existential quantifier in front of an existential prefix preserves it existential and does not introduce any new negation. □

Is the complement of a diophantine set again diophantine? In some cases yes. An important example will be given in Lemma 4.1. But in general not. Showing a counterexample will be a good occasion to introduce the concrete part of the chapter.

Remark 2.11 *Even for adequate rings, where relations like $t \neq 0$ are diophantine, the class of diophantine sets doesn't build in general a Boolean algebra.*

Proof: We will consider the ring of rational integers $(\mathbb{Z}, +, \Leftrightarrow, \cdot, 0, 1)$. This ring is diophantine: first of all it is disjunctive being a domain and conjunctive because $\tilde{\mathbb{Q}} \not\subset \mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$. Before proving the adequacy, let us observe that the set $\mathbb{N}$ of naturals is diophantine in $\mathbb{Z}$ as immediate application of the celebrated Four Squares Theorem of Legendre:

$$\mathbb{Z} \models \ x \in \mathbb{N} \Longleftrightarrow \exists x_1, \ldots, x_4 \ x = x_1^2 + \cdots + x_4^2.$$

Now it is evident that $\mathbb{Z}$ is adequate:

$$\mathbb{Z} \models t \neq 0 \Longleftrightarrow \exists x \in \mathbb{N} \ (t = x + 1 \vee t = \Leftrightarrow x \Leftrightarrow 1).$$

Every diophantine subset of the naturals is diophantine in $\mathbb{Z}$. For translating a definiton one has to relativize all its free and bounded variables to the predicate $x \in \mathbb{N}$ which is diophantine over $\mathbb{Z}$ using for every new relativization new supplementary variables. Also every subset of the naturals which is diophantine over $\mathbb{Z}$ is diophantine over $\mathbb{N}$. For the new translation one has to replace any occurrence of a **bounded** variable x of the definition with a difference $u \Leftrightarrow v$ of two new variables which depend only on x (not on the occurrence) and the corresponding quantifier $\exists x \ldots$ with the pair $\exists u \exists v \ldots$. This procedure works because every rational integer is the difference of two naturals.

Now we recall the Theorem of Matiyasevich in its extended form (sometimes called "The Davis-Putnam-Robinson-Matiyasevich Theorem" in the literature),

see [Matiyasevich]. It says that exactly the recursively enumerable sets are diophantine in $\mathbb{N}$. Let us choose such a set $M \subset \mathbb{N}$ whose complement is not recursively enumerable. M is diophantine in $\mathbb{N}$, thus in $\mathbb{Z}$ too. If its complement in $\mathbb{Z}$ was also diophantine in $\mathbb{Z}$, we would make the conjunction between its definition in $\mathbb{Z}$ and those of $\mathbb{N}$ to remark that $\mathbb{N} \setminus M$ was diophantine in $\mathbb{Z}$. Now we apply the second translation algorithm to conclude that $\mathbb{N} \setminus M$ is diophantine in $\mathbb{N}$, which is a contradiction. □

Cumulating the proof of the Remark 2.11 with the Theorem of Beth 1.1 we get the following remark, which is an important background fact. For stating it, we recall that $\mathbb{Z}^*$ denotes an ultrapower of $\mathbb{Z}$ and is a saturated ring elementarily equivalent to $\mathbb{Z}$.

Corollary 2.12 *There are embeddings of $\mathbb{Z}^*$ into itself which are not surjective (i.e. they are not automorphisms).*

Proof: If all embeddings were automorphisms, every definable set would have been diophantine. As we have seen, the complement of a nonrecursive recursively enumerable subset of $\mathbb{N}$ is L-definable but not L-diophantine. □

2.2 Number Rings

Our main objects are the number fields and their rings of algebraic integers. The number fields are extensions of $\mathbb{Q}$ of finite degree. An element of a number field which annulates some monic polynomial over $\mathbb{Z}$ is called an algebraic integer. They build a subring of the number field which is a free $\mathbb{Z}$ module of finite rank. We will also be interested in the polynomial rings over number fields and their rings of algebraic integers.

Now we will define **appropriate formal languages** for all the concrete rings in question.

Definition: For $\mathbb{Z}$ and $\mathbb{Q}$ we understand as appropriate language just the formal language of rings $L = \{+, \cdot, \Leftrightarrow, 0, 1\}$.

For any number field K with $[K : \mathbb{Q}] = n$ the appropriate language will be $L = \{+, \cdot, \Leftrightarrow, 0, 1, \underline{\alpha}\}$, where the new constant $\underline{\alpha}$ will be interpreted as a fixed primitive element of K over $\mathbb{Q}$ in the sense of Lagrange: $K = \mathbb{Q}[\alpha]$.

For any ring of algebraic integers $\mathcal{O} = \mathcal{O}_K$ of a number field K of degree $[K : \mathbb{Q}] = n$ the appropriate language will be $L = \{+, \cdot, \Leftrightarrow, 0, 1, \underline{\gamma}_2, \ldots, \underline{\gamma}_n\}$, where $\{1, \gamma_2, \ldots, \gamma_n\}$ is a fixed integral basis of the $\mathbb{Z}$-module $\mathcal{O}$. For the fact that one can always choose an integral basis which contains 1 see for example [D. Marcus], Theorem 13 of Chapter 2.

Finally, for any ring R as above, the appropriate language of the polynomial ring $R[T]$ will be called $LT := L \cup \{\underline{T}\}$, where L is the appropriate language for R and the new constant has the evident interpretation T.

We notice that all languages were chosen to allow definability for all elements as constant terms. The meaning of L, respectively LT will be clear from the context.

Proposition 2.13 *The number fields and their rings of algebraic integers are diophantine rings with respect to the formal language of rings. In consequence, they are diophantine rings also with respect to their appropriate languages L.*

Proof: All those rings are disjunctive since they are domains. There is no number field $K = \mathrm{Quot}(\mathcal{O})$ which contains $\tilde{\mathbb{Q}}$, so all are also conjunctive. The number fields (like all other fields) are trivially adequate: $K \models x \neq 0 \Leftrightarrow \exists y\ xy = 1$.

The adequacy proof which was done for $\mathbb{Z}$ can not be generalized to any other number ring. Fortunately a very simple idea works, see for example [Sauerland]:

$$\mathcal{O} \models (t \neq 0) \Longleftrightarrow \exists s \in \mathcal{O}\ t \,|\, (2s \Leftrightarrow 1)(3s \Leftrightarrow 1).$$

Indeed, if the divisibility takes place, t may not be 0 because $\frac{1}{2}$ and $\frac{1}{3}$ do not belong to $\mathcal{O}$. If t is any nonzero element of $\mathcal{O}$, it is enough to find a natural number s such that the norm $N_{K/\mathbb{Q}}(t) \,|\, (2s \Leftrightarrow 1)(3s \Leftrightarrow 1)$ in $\mathbb{Z}$, because $t \,|\, N_{K/\mathbb{Q}}(t)$ already in $\mathcal{O}$ and $t = 0 \Leftrightarrow N_{K/\mathbb{Q}}(t) = 0$. Let $\pm N_{K/\mathbb{Q}}(t)$ be a natural number whose decomposition in primes looks like $2^n 3^m q$ where 2 and 3 do not divide q. Using the Chinese Remainder Theorem for 2^n and $3^m q$ and the fact that 2 and 3 are units in the rings $\mathbb{Z}/3^m q\mathbb{Z}$ and $\mathbb{Z}/2^n\mathbb{Z}$, we get a natural number s such that

$$\begin{aligned} 2s &\equiv 1 \mod(3^m q), \\ 3s &\equiv 1 \mod(2^n). \end{aligned}$$

This means that $\pm N_{K/\mathbb{Q}}(t) = 2^n 3^m q \,|\, (2s \Leftrightarrow 1)(3s \Leftrightarrow 1)$, and we are done. □

Now about the polynomial rings. The following fact will be of even greater importance than the diophantine character of these rings:

Theorem 2.14 *If $\mathcal{O}$ is the ring of algebraic integers in a number field K, then the relation $x \in \mathcal{O}$ is L-diophantine in the polynomial ring $\mathcal{O}[T]$. This means, the coefficients in the defining diophantine formula are constant as polynomials in T. On the other side K is trivially L-diophantine in $K[T]$.*

Proof: Before starting with the proof of this theorem, I will shortly comment on its history. For $\mathcal{O} = \mathbb{Z}$ this was known by Putnam and Davis, see [Davis-Putnam]. Their defining equation has really constant coefficients and was one of the first applications of the Pell equation for defining $\mathbb{Z}$. On the other hand Alexandra Shlapentokh diophantinely defined $\mathbb{Z}$ in $R[T]$ in a uniform manner for all domains R of characteristic 0. Using her result and the appropriate language for $\mathcal{O}$ it is quite trivial to define $\mathcal{O}$. But the resulting definition would have not constant coefficients because her definition displays T explicitly. A. Shlapentokh's idea is

also based on Pell's equation, like almost all the results in this area. Our method is quite different.

Let K =Quot($\mathcal{O}$) be the corresponding number field and $\mathfrak{p}$ any prime of K. After [Rumely] the valuation ring $\mathcal{O}_\mathfrak{p}$ is L-diophantine in K:

$$K \models (x \in \mathcal{O}_\mathfrak{p} \Longleftrightarrow \exists x_1, \ldots, x_n \; P(x, x_1, \ldots, x_n) = 0).$$

We introduce new variables $y_1, \ldots, y_n$ and z which are interpreted as elements in $\mathcal{O}$ such that for all i one has $x_i = \frac{y_i}{z}$. Multiplying $P(x, \frac{x_1}{z}, \ldots, \frac{x_n}{z})$ with a suitable power of z we obtain the partially homogenized polynomial $Q(x, x_1, \ldots, x_n, z)$. Now we claim:

$$\mathcal{O}[T] \models (x \in \mathcal{O} \Longleftrightarrow \exists x_1, \ldots, x_n, z \; Q(x, x_1, \ldots, x_n, z) = 0 \wedge z \neq 0).$$

Denote the subset of $\mathcal{O}[T]$ defined on the right above by S; $S \subseteq \mathcal{O}[T]$. We prove $S = \mathcal{O}$:

$\underline{\mathcal{O} \subseteq S}$**:** If $x \in \mathcal{O}$ then as element of K is $x \in \mathcal{O}_\mathfrak{p}$ and thus x trivially satisfies the definition of S.

$\underline{S \subseteq \mathcal{O}}$**:** Suppose $x \in S \setminus \mathcal{O}$ and look at x as nonconstant polynomial function on K. Choose polynomials $y_1, \ldots, y_n, z$ with $Q(x, y_1, \ldots, y_n, z) = 0$ and $z \neq 0$. As polynomial z is not identical 0, so the set of elements of K which are zeros for z is at most finite.

Let $v_\mathfrak{p}$ be the valuation on K corresponding to $\mathfrak{p}$. For all nonconstant polynomials x the set

$$\{u \in K \mid v_\mathfrak{p}(x(u)) < 0\}$$

is infinite, so we choose an $u \in K$ such that $v_\mathfrak{p}(x(u)) < 0$ and $z(u) \neq 0$.

But $P(x(u), \frac{y_1(u)}{z(u)}, \ldots, \frac{y_n(u)}{z(u)}) = 0$ implies $v_\mathfrak{p}(x(u)) \geq 0$. Contradiction.

In order to prove the diophantine character of this definition we must now eliminate the negation. Without being able to define diophantinely $z \neq 0$ in $\mathcal{O}[T]$ using only constant coefficients (see 2.2), we find a tricky way for this particular situation. We claim that in $\mathcal{O}[T] \models$:

$$(x \in \mathcal{O}) \Longleftrightarrow \exists x_1, \ldots, x_n, z, s \; Q(x, x_1, \ldots, x_n, z) = 0 \;\wedge\; z \mid (2s \Leftrightarrow 1)(3s \Leftrightarrow 1).$$

Suppose $x \in \mathcal{O}$ and $x_1, \ldots, x_n \in K$ such that $P(x, x_1, \ldots, x_n) = 0$. K being in fact $\frac{\mathcal{O}}{\mathbb{N}\setminus\{0\}}$ one can find a common denominator $z \in \mathbb{N} \setminus \{0\}$ such that all $x_i = \frac{y_i}{z}$ and depending on z find $s \in \mathbb{N}$ as in 2.13. On the other side if $(x, \vec{y}, z, s) \subset \mathcal{O}[T]$ is any solution of the system, we must have $z \neq 0$ because $\frac{1}{2}$ and $\frac{1}{3}$ do not belong to $\mathcal{O}[T]$, and we may repeat the proof to conclude that $x \in \mathcal{O}$.

For the other case,

$$K[T] \models x \in K \Longleftrightarrow (\exists y\ xy = 1) \vee (x = 0).$$

□□

Now we can prove the diophantine character for the polynomial rings:

Proposition 2.15 *The polynomial rings over number fields and rings of algebraic integers are diophantine rings with respect to the formal language of rings. In particular, they are diophantine rings with respect to their appropriate languages LT.*

Proof: The conjunctivity and the disjunctivity follow exactly as in 2.13. In order to prove the adequacy we will unify the cases considering again a ring $R \in \{K, \mathcal{O}\}$. Then

$$R[T] \models t \neq 0 \Longleftrightarrow \exists a, b\ (a \in R \wedge b \in R \setminus \{0\} \wedge \underline{T} \Leftrightarrow a\,|\,t \Leftrightarrow b).$$

Indeed R is a diophantine subset in $R[T]$ as already proven in 2.14 and $R \setminus \{0\}$ is a diophantine subset in R because R is adequate (2.13). The definition is hence diophantine and says that a polynomial is not the null polynomial iff its associate polynomial function takes at least one nonzero value. In order to write down the evaluation of a polynomial in the given language we used a classical elementary result on vanishing polynomials which is sometimes called Theorem of Bezout. We can choose a diophantine definition of $\mathcal{O}$ in $\mathcal{O}[T]$ which contains only coefficients in $\mathbb{Z}$. It leads to a definition of $\mathcal{O}[T] \setminus \{0\}$ using just the formal language of rings and no supplementary constants. □

We used the new constant $\underline{T}$ for only one occurrence in the proof of the adequacy. Because of Theorem 2.2, we could not avoid to use it.

The Theorem 2.14 will permit us to define an application of natural restriction which is the central object of this thesis.

Definition: The set of all injective L-endomorphisms of a ring A in itself will be denoted $\mathfrak{End}_L(A)$. It forms a monoid with the operation of composition $\circ$. The identity plays the role of 1. The invertible endomorphisms form the group $\mathfrak{Aut}_L(A)$ of all automorphisms. If $B \subset A$ is a subring it is usual to denote with $\mathfrak{End}_B(A)$ (respectively $\mathfrak{Aut}_B(A)$) the monoid (group) of injective endomorphisms (automorphisms) which fix B elementwise. Our appropriate languages L and LT were chosen such that all elements of a number field or of its ring of algebraic integers R (or even of the polynomial rings $R[T]$) are definable as constant terms, so in this case:

$$\mathfrak{End}_R(R^*) = \mathfrak{End}_L(R^*)\ \ ;\ \ \mathfrak{End}_{R[T]}(R[T]^*) = \mathfrak{End}_{LT}(R[T]^*),$$

where for a ring A we denote A^* a nonstandard extension of A. The same meaning will have $\mathfrak{Aut}_R(R^*)$, respectively $\mathfrak{Aut}_{R[T]}(R[T]^*)$.

Remark 2.16 *If L is an extension with constants of the formal language of rings, the injective L-endomorphisms of a ring are exactly its L-embeddings in itself.*

As R is L-diophantine in $R[T]$, following 2.9, we get that $\eta(R^*) \subseteq R^*$ is true for all embeddings $\eta \in \mathfrak{End}_L(R[T]^*)$. This is a very strong fact which will not be used. But because $L \subset LT$, R is trivially LT-diophantine so for all LT-embeddings $\eta \in \mathfrak{End}_{LT}(R[T]^*)$ one has $\eta(R^*) \subseteq R^*$. Thus we get the last proposition of the chapter:

Proposition 2.17 *Let R be a number field or its ring of algebraic integers. The application of natural restriction:*

$$\mathfrak{Res}_{R^*} : \mathfrak{End}_{R[T]}(R[T]^*) \Leftrightarrow\!\!\rightarrow \mathfrak{End}_R(R^*),$$

given by $\mathfrak{Res}_{R^*}(\eta) := \eta\,|_{R^*}$, is a well defined homomorphism of monoids. The same is true for the map $\mathfrak{Res}_{R^*}$ restricted as follows:

$$\mathfrak{Res}_{R^*} : \mathfrak{Aut}_{R[T]}(R[T]^*) \Leftrightarrow\!\!\rightarrow \mathfrak{Aut}_R(R^*).$$

In this case is $\mathfrak{Res}_{R^*}$ a well defined homomorphism of groups.

Chapter 3

The Transfer of Definability

This chapter presents a connection between the class of definable relations in some integral domains which are close to the classical domains of the Arithmetic and the definable relations in their polynomial rings. Our technique is somehow more important than the result. This technique will be further developed in the next chapter for the stronger notion of diophantine definability.

3.1 Gödel Functions

Let R be an integral domain of characteristic 0.

Definition: 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:

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

The next lemma is well-known; see [Rumely] for a stronger form. The proof given here will be refined in the next chapter for the diophantine case.

Lemma 3.1 *$\mathbb{Q}$, $\mathbb{Z}$, all the number fields K and all their rings of algebraic integers $\mathcal{O}$ admit Gödel functions which are definable in the respectively appropriate languages.*

Proof: We start recalling the classical Gödel function $\beta : \mathbb{N}^2 \to \mathbb{N}$ for the naturals:

$$\begin{aligned} \beta(x, i) = z \iff \;\; & \exists u, v \leq x \quad \Big((u+v)(u+v+1) + 2u = 2x \;\wedge \\ & z < iv + 1 \;\wedge \quad \exists w \leq u \quad (u = w(iv+1) + z) \Big). \end{aligned}$$

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).

We present directly the number field case. The other case is similar and less difficult. In our construction the length n of the sequence which should be encoded occurs also in the defining formula as a free variable to be understood as parameter. We denote $[K:\mathbb{Q}] = m$ and we remember that $K = \mathbb{Q}[\alpha]$. In the next formula j abbreviates the product $(2m+1)\cdot i$. The Gödel function $F : K^3 \Leftrightarrow\!\!\rightarrow K$ is defined as follows:

$$
\begin{aligned}
&F(n,u,i) = v \Longleftrightarrow \\
&\quad \Big((n,u,i) \in \mathbb{N}^3 \ \wedge\ i \le n \ \wedge \\
&\qquad \wedge\ v\cdot\beta(u,j) = \beta(u,j+1) \Leftrightarrow \beta(u,j+2) + \\
&\qquad\qquad + \ \underline{\alpha}\quad [\beta(u,j+3) \Leftrightarrow \beta(u,j+4)] + \ldots\ldots \\
&\qquad\qquad + \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\qquad\qquad + \ \underline{\alpha}^{m-1}\,[\beta(u,j+2m \Leftrightarrow 1) \Leftrightarrow \beta(u,j+2m)]\Big) \ \vee \\
&\vee \ \Big((n,u,i) \in \mathbb{N}^3 \ \wedge\ i > n \ \wedge\ v = 0 \Big) \ \vee \\
&\vee \ \Big(n \notin \mathbb{N} \wedge v = 0 \Big) \ \vee\ \Big(u \notin \mathbb{N} \wedge v = 0 \Big) \ \vee\ \Big(i \notin \mathbb{N} \wedge v = 0 \Big).
\end{aligned}
$$

The naturals $\mathbb{N}$ and also their complement $K \setminus \mathbb{N}$ are definable in K by the celebrated result of Julia Robinson. If we relativize all the variables used for defining β to one fixed definition of $\mathbb{N}$ in K, using new variables at each new relativization, we will find a formal definition of F in K. We must now verify that F is a Gödel function.

Suppose that the finite sequence $(k_0,\ldots,k_n) \subset K$ was given to encode. We choose and fix not uniquely determined natural numbers $k_i^{j\xi}$ and k_i^0 such that $\forall i \in \{0,\ldots,n\}$:

$$
k_i = \frac{(k_i^{1+} \Leftrightarrow k_i^{1-}) + \underline{\alpha}(k_i^{2+} \Leftrightarrow k_i^{2-}) + \cdots + \underline{\alpha}^{m-1}(k_i^{m+} \Leftrightarrow k_i^{m-})}{k_i^0}.
$$

In the case if $k_i = 0$ we may take $k_i^0 = 1$. Applying the fact that β is a Gödel function over $\mathbb{N}$, we find for the sequence of chosen natural numbers an $u \in \mathbb{N}$ such that for all $p \in \{1,\ldots,m\}$ and $i \in \{0,\ldots,n\}$:

$$
\begin{aligned}
k_i^0 &= \beta(u, i(2m+1)), \\
k_i^{p-} &= \beta(u, i(2m+1) + 2p), \\
k_i^{p+} &= \beta(u, i(2m+1) + 2p \Leftrightarrow 1).
\end{aligned}
$$

Then $F(n,u,i) = c_i$ for all $i \le n$.

For the rings of algebraic integers we can write a similar formula which does not contain denominators and uses an integral basis instead of the powers of the primitive element. $\mathbb{Z}$ and $\mathbb{Q}$ are included as particular cases. $\square$

3.2 The General Transfer

The next theorem describes the phenomenon which was already announced in the title of the chapter. In the future we will refer directly to the concrete case of number fields and number rings. We speak about general transfer as transfer of general definability versus the transfer of diophantine definability which will be presented in the next chapter. This will mean that the general transfer preserves in some cases the property of the defining formula to be existentially quantified and not to contain negations.

Theorem 3.2 (Transfer of Definability) *Let L be an extension of the formal language of rings by constants interpreted over a ring R. Suppose that:*

1. *$\mathbb{N}$ is L-definable in R, and*

2. *There is an L-definable Gödel function F on R.*

If $M \subseteq R^k$ is any relation which is LT-definable in the polynomial ring $R[T]$, where $LT = L \cup \{\underline{T}\}$, then M is L-definable in R.

Proof: Let (R^*, M^*) be any saturated model which is elementarily equivalent to the structure $(R, \underline{M})$, where $\underline{M}$ is a new relation-symbol (predicate) for the set M. It is enough to prove that every automorphism $\varphi \in \mathfrak{Aut}_L(R^*)$ preserves the set M^* and to apply the Theorem of Beth for definability (1.1).

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

Following Chapter 1, all the saturated extensions of R which have equal cardinality are isomorphic, and in order to apply the Theorem of Beth it is not important which of the saturated elementarily equivalent structures is considered. So we can suppose R^* and $R[T]^*$ to be classical nonstandard extensions obtained for example as ultrapowers. Together with the two 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. This technique, classically called Nonstandard Analysis, was introduced by Abraham Robinson. For a rigorous presentation of this theory see [A. Robinson]. Its power 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 $x \in R[T]^*$ 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 R^* defines a nonstandard polynomial. Two $*$-finite internal sequences over R^* define the same element of $R[T]^*$ **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 just 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 $R[T]$. 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 R.

Let $\varphi \in \mathfrak{Aut}_L(R^*)$. For the element $x \in R[T]^*$ which has just 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 puts 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 $a : [0, \nu] \to R^*$, then $\bar{\varphi}(x)$ is nothing else as $\varphi \circ a \circ \varphi^{-1} : [0, \varphi(\nu)] \to R^*$. $\mathbb{N}$ being definable over R, is $\varphi(\mathbb{N}^*) = \mathbb{N}^*$ so really $\varphi(\nu)$ 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 has 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 R means that for all $\vec{\lambda}, x, y \in R^*$ and all $\varphi \in \mathfrak{Aut}_L(R^*)$:

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

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

On the other side, in order that $\bar{\varphi}$ was an application of $R[T]^*$ in 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:

$$\forall j \leq \lambda_1 \;\; \sigma_1(j) = \sigma_2(j) \implies \forall k = \varphi(j) \leq \varphi(\lambda_1)$$

$$\varphi \circ \sigma_1 \circ \varphi^{-1}(k) = \varphi \circ \sigma_2 \circ \varphi^{-1}(k)\ ;$$

$$\forall \lambda_1 < j \leq \lambda_2 \;\; \sigma_2(j) = 0 \implies \forall \varphi(\lambda_1) < k = \varphi(j) \leq \varphi(\lambda_2)$$

$$\varphi \circ \sigma_2 \circ \varphi^{-1}(k) = 0.$$

This means $\sigma_1' \approx \sigma_2'$ and the definition makes sense.

We remark immediately that $\bar{\varphi}(T) = T$ and $\forall r \in R^* \bar{\varphi}(r) = \varphi(r)$ hence $\bar{\varphi}$ extends φ. The **additivity** and the **injectivity** of $\bar{\varphi}$ are trivial and we will not insist on them. We will sketch shortly the proof that:

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

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

$$y = \sum_{j=0}^{\nu} b_j T^j. \text{ Let now:}$$

$$x = \sum_{i=0}^{\varphi^{-1}(\nu)} \varphi^{-1}(b_{\varphi(i)}) T^i.$$

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 R. Its nonstandard extension, which will be denoted also by $\sum$, operates consequently on all $*$-finite internal sequences in R^*. 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) *Let L be an extension with 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 here 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 to 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 $T = 1$ with the german letter $\mathfrak{A}$ (coming from "Auswertung"). The value of $\mathfrak{A}$ is the sum of coefficients:

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

Its value is of course independent of the representative sequence.

The next remark belongs to the elementay algebra:

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

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:

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

Of course, we may not use the multiplicativity of $\bar{\varphi}$ because it still has not been proven. The decisive fact which will be used is that the polynomials are divisible by $T \Leftrightarrow 1$ 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 $y \in R[T]^*$.

$$(T \Leftrightarrow 1) \,|\, y \Longleftrightarrow \exists z \quad y = (T \Leftrightarrow 1)z \Longleftrightarrow$$

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

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

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

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

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

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

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

Developping 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 chapter in a stronger context and in more detail. □□

We remark the following partial reciprocal: For an integral domain Δ of characteristic 0, the transfer of definability implies always the definability of $\mathbb{N}$ in Δ. This follows from the fact that $\mathbb{N}$ is always definable in $\Delta[T]$, as will be seen in Theorem 4.6. We believe that it will not be the case with Gödel functions.

For concluding the chapter we state the:

Theorem 3.4 *Let R be a number field or its ring of algebraic integers and L its appropriate formal language. Let $k \in \mathbb{N}$ be a natural number and $M \subseteq R^k$ be any relation. Then:*

$$M \text{ is } L\Leftrightarrow definable \text{ in } R \iff M \text{ is } LT\Leftrightarrow definable \text{ in } R[T].$$

Proof: The direction $\Leftarrow$ is already done in the Theorem 3.2 because $\mathbb{N}$ is definable in R after [J. Robinson] and a Gödel function was defined in 3.1.

For the other direction $\Rightarrow$: R is definable in $R[T]$ with lemma 2.14. Let ψ be one formula which defines M in R. We relativize all variables (bounded and free) to R using the definition of R. What we have got is a formula which defines M in $R[T]$ even without the constant $\underline{T}$. □□

Corollary 3.5 (Elimination of T) *Let a ring R be a number field or its ring of algebraic integers. Any relation over $R[T]$ consisting of (tuples of) constant polynomials only which is LT-definable in $R[T]$ is L-definable in $R[T]$.*

Corollary 3.6 *The homomorphism*

$$\mathfrak{Res}_{R^*} : \mathfrak{Aut}_{R[T]}(R[T]^*) \Leftrightarrow\!\!\rightarrow \mathfrak{Aut}_R(R^*)$$

is surjective.

Some comments before we continue. Let us fix two formulas which define $\mathbb{Z}$ and respectively a Gödel function over R. 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, in which 3.2 and 3.4 establish the background. Second, the proof of 3.2 is a technical preparation of a more difficult mechanism: the extension of the embeddings of R^* in itself to embeddings of $R[T]^*$ in itself. Why and to what extent it is more difficult to extend embeddings than to extend automorphisms will be seen in the next chapter.

Chapter 4

On the Diophantine Definability of $\mathbb{Z}$

The goal of this chapter is to find a structural property which is equivalent with the diophantine definability of $\mathbb{Z}$ in the rings of algebraic integers. At the same time the results of the second chapter will be refined. We start again with a sequence of lemmata. First we will explore some consequences of the hypothesis that $\mathbb{Z}$ would be diophantine in a number field or in its ring of algebraic integers.

4.1 Diophantine Gödel Functions

Lemma 4.1 *Let R be a number field or its ring of algebraic integers such that $\mathbb{Z}$ is L-diophantine in R. Then the naturals $\mathbb{N}$ and their complement $R \setminus \mathbb{N}$ are also L-diophantine in R.*

Proof: $\mathbb{N}$ is diophantine in R using the 4-Squares Theorem

$$x \in \mathbb{N} \Longleftrightarrow \exists a_1, a_2, a_3, a_4 \quad a_1 \in \mathbb{Z} \wedge \cdots \wedge a_4 \in \mathbb{Z} \wedge x = a_1^2 + \cdots + a_4^2,$$

and the fact that $\mathbb{Z}$ is diophantine in R. Every ocurence of a formula like $a \in \mathbb{Z}$ may be substituted by the diophantine definition of $\mathbb{Z}$ in the variable a. At every new substitution the defining equation should be transcribed using new variables. In this way we find a defining diophantine system for $\mathbb{N}$. For the following definitions, which will be built stepwise using all the time already defined sets, we will insist no more on this fact.

For the complement $R \setminus \mathbb{N}$ we will differentiate again two cases. The trivial one is that of algebraic integers. Let $R = \mathcal{O}$ a ring of algebraic integers with integral basis $\{\alpha_1, \ldots, \alpha_m \,|\, \alpha_1 = 1\}$. We recall that one can always choose an integral basis which contains 1, see [D. Marcus]. For the second case let $R = K = \mathbb{Q}[\alpha]$

a number field, $[K:\mathbb{Q}]=m$. Then:

$$\underline{x\in\mathcal{O}\setminus\mathbb{Z}} \iff \underline{\exists x_1,\ldots,x_m\in\mathbb{Z}}\ \ x_2^2+\cdots+x_m^2\neq 0\wedge x=x_1+x_2\underline{\alpha}_2+\cdots+x_m\underline{\alpha}_m.$$

$$\underline{x\in\mathcal{O}\setminus\mathbb{N}} \iff \underline{x\in\mathcal{O}\setminus\mathbb{Z}}\vee(\underline{\exists y\in\mathbb{N}}\ x+y+1=0).$$

$$\underline{x\in\mathbb{Q}} \iff \exists a,b\ \underline{a\in\mathbb{Z}}\wedge\underline{b\in\mathbb{Z}}\wedge a\neq 0\wedge ax=b.$$

$$\underline{x\in(0,1)\cap\mathbb{Q}} \iff \underline{x\in\mathbb{Q}}\wedge\underline{\exists y_1,\ldots,y_4\in\mathbb{Q}}\ x=y_1^2+\cdots+y_4^2\wedge \wedge\underline{\exists z_1,\ldots,z_4\in\mathbb{Q}}\ 1\Leftrightarrow x=z_1^2+\cdots+z_4^2\wedge \wedge x\neq 0\wedge 1\Leftrightarrow x\neq 0.$$

$$\underline{x\in\mathbb{Q}\setminus\mathbb{Z}} \iff \underline{x\in\mathbb{Q}}\wedge\exists u,v\ (\underline{u\in(0,1)\cap\mathbb{Q}}\wedge\underline{v\in\mathbb{Z}}\wedge x=u+v).$$

$$\underline{x\in K\setminus\mathbb{Z}} \iff \underline{\exists x_1,\ldots,x_m\in\mathbb{Q}}\ (x=x_1+x_2\underline{\alpha}+\cdots+x_m\underline{\alpha}^{m-1}\wedge \wedge(x_2^2+\cdots+x_m^2\neq 0\vee\underline{x_1\in\mathbb{Q}\setminus\mathbb{Z}})).$$

$$\underline{x\in K\setminus\mathbb{N}} \iff \underline{x\in K\setminus\mathbb{Z}}\vee(\underline{\exists y\in\mathbb{N}}\ x+y+1=0).$$

We remember that the relation $t\neq 0$ is diophantine in all number rings according to Lemma 2.14 and in the number fields with $t\neq 0\Leftrightarrow\exists w\ tw=1$. We used also the Four Squares Theorem for $\mathbb{Q}$. □

Lemma 4.2 *If R is a number field or its ring of algebraic integers such that $\mathbb{Z}$ is L-diophantine in R, then there is a Gödel function $F(n,u,i):R^3\to R$ which is L-diophantine over R.*

Proof: Let F be the Gödel function defined in lemma 3.1. Like before we relativize the defining formula to the sets $\mathbb{N}$ and $R\setminus\mathbb{N}$. They are diophantine (see 4.1) and the resulting definition is diophantine too. □

4.2 Bounded Universal Quantifiers

Our second goal is to expose a nonstandard consequence of the Theorem of Matiyasevich. It is the main technical instrument of the chapter.

Lemma 4.3 (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 $\mu, \vec{\lambda} \in \mathbb{N}^*$:*

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

Proof: We have chosen this name for the lemma because its proof consists in putting the two theorems together. The relation $E(\mu,\vec{\lambda}) \Leftrightarrow \forall i < \mu D(\mu,\vec{\lambda})$ is recursively enumerable in $\mathbb{N}$, so using the Theorem of Matiyasevich in its extended sense, E is diophantine over $\mathbb{N}$. We apply to E the existential form of the Theorem of Beth (1.1) to get:

$$E^*(\mu,\vec{\lambda}) \Longrightarrow E^*(\eta(\mu),\eta(\vec{\lambda})).$$

□

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.

Lemma 4.4 *Let R be a number field or its ring of algebraic intergers. We suppose that $\mathbb{Z}$ is diophantine in (R,L). Let also $D(\iota,\vec{\lambda})$ be any diophantine relation over R, $\mu \in \mathbb{N}^*$, $\eta : R^* \hookrightarrow R^*$ be some L-embedding and $\vec{\lambda} \in (R^*)^d$ be some tuple. Then like before:*

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

Proof: $\mathbb{N}$ is diophantine in R using 4.1. Hence (1.1) $\eta(\mathbb{N}^*) \subseteq \mathbb{N}^*$ and the restriction $\eta\,|_{\mathbb{N}^*}$ determines η uniquely. That's why the ideea is to interpret D diophantinely over $\mathbb{N}$ and to apply 4.3.

Let R be a number field with $[R:\mathbb{Q}] = m$, $R = \mathbb{Q}(\alpha)$. (A constant $\underline{\alpha} \in L$ denotes a primitive element $\alpha \in R$.) For fixed elements $\mu \in \mathbb{N}^*$ and $\vec{\lambda} \in (R^*)^d$ suppose that:

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

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

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

Now we modify the defining formula for D making some substitutions like in 3.1. For a variable x (respectively λ) we introduce new variables $v_0^x, v_1^x, \ldots, v_{2m}^x$ which have not occurred in D or in any other substitution. All of the new variables are interpreted as (nonstandard) natural numbers. Now

$$\begin{array}{rll} \exists x\,(\ldots) & \text{becomes} & \ldots\ldots\ldots\ldots\ldots\ldots \exists v_0^x, v_1^x, \ldots, v_{2m}^x \; (v_0^x \neq 0 \wedge \ldots), \\ x & \text{becomes} & \dfrac{(v_2^x \Leftrightarrow v_1^x) + \underline{\alpha}(v_4^x \Leftrightarrow v_3^x) + \cdots + \underline{\alpha}^{m-1}(v_{2m}^x \Leftrightarrow v_{2m-1}^x)}{v_0^x}, \\ \lambda & \text{becomes} & \text{the same fraction in new variables } v_0^\lambda, v_1^\lambda, \ldots, v_{2m}^\lambda. \end{array}$$

Writing $P(\iota, \vec{\lambda}, \vec{x})$ in the new variables as a rational expression and separating the common denominator, we get a polynomial $\tilde{P}(\iota, \vec{v}^{\lambda}, \vec{v}^{x}) \in \mathbb{Z}[\alpha][\iota, \vec{v}^{\lambda}, \vec{v}^{x}]$. Let us group the variables v_0 in another tuple. We substitute also $v^{\vec{\lambda}}, v_0^{\vec{\lambda}}$ with non-standard natural values $\underline{v^{\vec{\lambda}}}$ respectively denominators $\underline{v_0^{\lambda}} \neq 0$ which correspond to the fixed value of λ. All these numbers are not uniquely determined, so we fix again one choice. Then:

$$R^* \models \forall i < \mu \; \exists v^{\vec{x}}, v_0^{\vec{x}} \in \mathbb{N}^* \Big(\tilde{P}(i, v^{\vec{x}}, v_0^{\vec{x}}, \underline{v^{\vec{\lambda}}}, \underline{v_0^{\vec{\lambda}}}) = 0 \wedge \bigwedge_{\vec{x}} v_0^x \neq 0 \Big).$$

Next we represent the polynomial as linear combination of the powers of α and get new polynomials $\tilde{P}_1, \ldots, \tilde{P}_m$ with integral coefficients such that:

$$\tilde{P} = \tilde{P}_1 + \underline{\alpha}\tilde{P}_2 + \cdots + \underline{\alpha}^{m-1}\tilde{P}_m.$$

The set $\{1, \alpha, \ldots, \alpha^{m-1}\}$ being linearly independent over $\mathbb{Q}$, we can substitute $\tilde{P} = 0$ by the conjunction $\wedge_j \tilde{P}_j = 0$. As last remark:

$$\mathbb{N} \models t \neq 0 \iff \exists w \; t = w + 1.$$

We have reached our goal. The result of our reformulations is that:

$$\mathbb{N}^* \models \forall i < \mu \; \exists v^{\vec{x}}, v_0^{\vec{x}} \; \Big(\bigwedge_{j=1}^{m} \tilde{P}_j(i, v^{\vec{x}}, v_0^{\vec{x}}, \underline{v^{\vec{\lambda}}}, \underline{v_0^{\vec{\lambda}}}) = 0 \wedge \bigwedge_{\vec{x}} \; \exists w^x \; v_0^x = w^x + 1 \Big).$$

This relation will be called $E(\mu, v^{\vec{\lambda}}, v_0^{\vec{\lambda}})$. Now after Lemma 4.3,

$$\mathbb{N}^* \models E^*\Big(\eta(\mu), \eta(\underline{v^{\vec{\lambda}}}), \eta(\underline{v_0^{\vec{\lambda}}})\Big).$$

The only condition to check in order to follow the same steps in backwards is if for all the new parameters $\eta(\underline{v_0^{\lambda}}) \neq 0$. This is true because η is injective. Recalling that the restriction $\eta\,|_{\mathbb{N}^*}$ uniquely determines η on R^*, we are getting

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

For the rings of algebraic integers the proof is easier (we have not to worry about the denominators!) and works along the same pattern. Instead of the powers of the primitive element one should consider an integral base. □

Remark 4.5 *Lemmata 4.3 and 4.4 are also true for all formulas in prenex normal form whose prefixes consist of arbitrary sequences of existential $\exists x$ and restricted universal $\forall x < y$, $\forall x \leq y$ quantifiers. In the last cases, y may be a free variable or a bounded one.*

There are two ways to convince us about it. The first is to apply the Theorem of Matiyasevich in the extended form. Over $\mathbb{N}$ is the defined relation recursively enumerable, hence diophantine, and we repeat the proof of 4.3. Over R we apply the same algorithm to find an equivalent formula over $\mathbb{N}$ which is diophantine. The second way would be to use the two lemmata for making an induction on the number of restricted universal quantifiers. Anyway, situations like $\forall x \leq y\ \phi(x, y, \vec{\sigma})$ could be managed in the equivalent form $\forall x < y\ \phi(x, y, \vec{\sigma}) \wedge \phi(y, y, \vec{\sigma})$. η operates on all free variables which occur inside formulas or as bounds for the restricted quantifiers, and only on them. $\square$

4.3 A Natural Definition for $\mathbb{Z}$ in Polynomials

The third and last point of the preparation concerns the diophantine definability over polynomial rings. Apparently all that we have to do is to quote the following strong theorem of Alexandra Shlapentokh to which we have already refered in the proof of 2.14:

Theorem 4.6 (Alexandra Shlapentokh) *Let L be again the formal language of rings and Δ a domain of characteristic 0. Let $\underline{T}$ be a new constant interpreted as a transcendental T over Δ. Then $\mathbb{Z}$ is $L \cup \{\underline{T}\}$-diophantine in $\Delta[T]$.*

We have some reasons to reprove this result in a weaker form only for the number fields and rings. First these objects enable us to give an easier proof which displays just one occurrence of the Pell equation and seems to be more structural. We use an older idea of Jan Denef, see [Denef 1] and again our important Theorem 2.14. As second reason, our approach will permit us to stress a deeper similarity between the diophantine definability of $\mathbb{Z}$ in rings of algebraic integers and the Theorem of Matiyasevich. We start presenting Denef's result:

Lemma 4.7 (Jan Denef) *Let Δ be a domain of characteristic 0 such that there is a set A, $\mathbb{Z} \subset A \subset \Delta$, which is L-diophantine in $\Delta[T]$ with respect to any formal language L. Then $\mathbb{Z}$ is $L \cup \{\underline{T}\}$-diophantine in $\Delta[T]$.*

Sketch of proof: We consider the following Pell equation over $\Delta[T]$:

$$X^2 \Leftrightarrow (\underline{T}^2 \Leftrightarrow 1)Y^2 = 1,$$

and we observe that:

1. Its solutions in $\Delta[T]$ are exactly the pairs $(\pm X_n, \pm Y_n)_{n \in \mathbb{N}}$ defined by

$$X_n + Y_n\sqrt{T^2 \Leftrightarrow 1} = \left(T + \sqrt{T^2 \Leftrightarrow 1}\right)^n.$$

The proof is not trivial and uses the algebraic form of the Theorem of Riemann-Roch. All the solutions are already in $\mathbb{Z}[T]$. In particular,

$$Y_n(T) = \sum_{i=1,\ \text{odd}}^{n} \binom{n}{i} (T^2 \Leftrightarrow 1)^{\frac{i-1}{2}} T^{n-i}.$$

2. The evaluation $\pm Y_n(1) = \pm n$. So for all $x \in \mathbb{N}$ we get $T \Leftrightarrow 1 \,|\, Y_x \Leftrightarrow x$.

Finally, in $\Delta[T]$:

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

□

Lemma 4.8 *If R is a number field or its ring of algebraic integers, then $\mathbb{Z}$ is LT-diophantine in $R[T]$.*

Proof: Now, if $\Delta = R$ is a number field or ring, R is L-diophantine in $R[T]$ using Theorem 2.14. So we substitute in Denef's principial definition $x \in A$ by the L-diophantine formula defining $x \in R$, using only new bounded variables. □

4.4 The Diophantine Transfer

Our preparations reach here their end.

Theorem 4.9 (Transfer of Diophantine Definability) *Let R be a number field or its ring of algebraic integers and let L be the appropriate language for R. The following statements are equivalent:*

1. *$\mathbb{Z}$ is L-diophantine in R.*
2. *$\mathfrak{Res}_{R^*} : \mathfrak{End}_{R[T]}(R[T]^*) \to \mathfrak{End}_R(R^*)$ is surjective.*
3. *For all $d \in \mathbb{N}$ and relation $M \subseteq R^d$:*

$$M \text{ is } L \Leftrightarrow \text{diophantine in } R \Longleftrightarrow M \text{ is } LT \Leftrightarrow \text{diophantine in } R[T].$$

Proof: We remark that the third point refines the general transfer of definability stated in the third chapter saying when does it preserve the property to be existentially definable (in our case synonymous with diophantine). The second point says in fact that the embeddings $\eta \in \mathfrak{End}_R(R^*)$ are extendable to embeddings $\bar{\eta} \in \mathfrak{End}_{R[T]}(R[T]^*)$ such that $\mathfrak{Res}_{R^*}(\bar{\eta}) = \eta$.

We will make a circular proof starting with the trivial implications.

$\underline{2 \Rightarrow 3:}$

For proving the direction $\Rightarrow$ of the equivalence in question we remember again that R is L-diophantine in $R[T]$, so we must only relativize all variables (free and bounded) of the defining formula of M to R.

For the other direction $\Leftarrow$ we consider $\eta \in \mathfrak{End}_R(R^*)$ an arbitrary embedding and $\bar{\eta} \in \mathfrak{End}_{R[T]}(R[T]^*)$ an embedding which extends η. M is LT-diophantine in $R[T]$, so $\bar{\eta}(M^*) \subseteq M^*$, but $M \subseteq R$ and $\bar{\eta}\,|_{R^*} = \eta$, hence $\eta(M^*) \subseteq M^*$. The choice of η was arbitrary. Following 1.1 and 1.2, M is L-diophantine in R.

$\underline{3 \Rightarrow 1:}$

$\mathbb{Z}$ is LT-diophantine in $R[T]$ following 4.8. By point 3, $\mathbb{Z}$ should be L-diophantine in R.

$\underline{1 \Rightarrow 2:}$

This proof proceeds in the same steps as the similar one from Chapter 3. In order to better understand what happens, let us recall the extension of an automorphism. If $\varphi \in \mathfrak{Aut}_R(R^*)$, the action of its extension $\bar{\varphi}$ to $R[T]^*$ 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 $\eta \in \mathfrak{End}_R(R^*)$ is a not surjective external embedding. As positive facts we note that the naturals $\mathbb{N}$ and their ordering are diophantine in R, so $\eta(\mathbb{N}^*) \subseteq \mathbb{N}^*$ and $\eta|_{\mathbb{N}^*}$ is monotone. As negative facts, in general is $\eta([0,\nu]) \neq [0, \eta(\nu)]$ and not an internal set.

Suppose that the description of x has been done using a Gödel function which is L-diophantine in R. Its existence, under the assumption that $\mathbb{Z}$ was L-diophantine in R, which is now assumed, has been proven in 4.2. 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 like restriction of a standard function to an internal set.

What we have done was 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 $j \in [0, \eta(\nu)] \setminus \eta([0, \nu])$. We remember that η commutes with all diophantine functions, as the automorphisms did before with the definable functions. That fact has no more a central importance, being now too weak because of the new born elements. Its place will be taken by the results like 4.3, 4.4 and 4.5.

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 remember the convention about letters like i, j, k, l which should denote only (nonstandard) natural numbers. Suppose that we have encoded the sequence $(a_i)_{i=0}^{\nu}$ two times, using two not compulsory different diophantine Gödel functions $F_{1,2}$ and two coding parameters $\vec{\lambda}_{1,2}$. This means:

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

$F_{1,2}$ being both diophantine over R, all the used constants belong to L and designate standard elements. If we substitute the functions with their definitions we obtain a diophantine relation and like prefix a restricted universal quantifier on (nonstandard) naturals. This is exactly the situation from 4.4. We get directly:

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

(Like before the universal quantified variables remain η-free.)

Now we prove the independence of the definition of the choice of the representing sequence. We could have done it in the same time with the other independence, but we didn't do that from methodological reasons. Let us consider two $*$-finite internal sequences which represent the same nonstandard polynomial, being $\approx$-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 $\vec{\lambda}_{1,2}$. 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:

$$\begin{aligned} \forall i \leq \nu_2 \Leftrightarrow \nu_1 \Leftrightarrow 1 \qquad & F^*(\vec{\lambda_2}, \nu_1 + 1 + i) = 0, \\ \forall i \leq \eta(\nu_2) \Leftrightarrow \eta(\nu_1) \Leftrightarrow 1 \qquad & F^*(\eta(\vec{\lambda_2}), \eta(\nu_1) + 1 + i) = 0. \end{aligned}$$

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

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

Let $x, y \in R[T]^*$ 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 and diophantinely refined in 4.2. For $a_0 \in R^*$, 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 $(0, 1) \subset R$ is the shortest representing sequence for T and is encoded modulo F^* with the standard parameter $(1, \lambda) \in \mathbb{N}^2$:

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

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

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

Consider $x, y, z \in R[T]^*$ 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 the polynomial addition.

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

Using again 4.4 we find that $\mathcal{R}_+(\nu, \vec{\lambda}, \vec{\gamma}, \vec{\epsilon}) \Longrightarrow \mathcal{R}_+(\eta(\nu), \eta(\vec{\lambda}), \eta(\vec{\gamma}), \eta(\vec{\epsilon}))$ which means $\bar{\eta}(x) + \bar{\eta}(y) = \bar{\eta}(z)$.

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

We start again with $xy = w$ in $R[T]^*$. We use the same elements x and y which have been used for proving the additivity and their already displayed representing sequences. Like in the proof of 3.2, it is a standard fact over $R[T]^*$ that the product of two polynomials accepting both of them representing sequences of length ν accepts itself a representing sequence of length 2ν. Now we need a more accurate notation. We choose as diophantine Gödel function exactly the function defined in 3.1 and refined in 4.2. Let also:

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

We must model diophantinely over R 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:

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

We remark that $F^*(\vec{\theta}, k) \in R^* \subset R[T]^*$ and the relation of divisibility is meant in that last ring. For a complete description of the polynomial product we have to model now this relation of polynomial divisibility diophantinely over R^*. 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

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

which is an elementwise product of the finite sequence $\overleftrightarrow{a}$ with the reversed finite sequence $\overleftrightarrow{b'}$, where $a' = a\,|_{[0,k]}$ and the same 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 like:

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

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.

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

We need some more explanations. Our 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 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 modelling formula possible. Using the remark 4.5,

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

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:

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

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

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

As last we remark that we must 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 3.5, we state the following:

Corollary 4.10 (Diophantine elimination of T) *If R is a number ring or field, $\mathbb{Z}$ is L-diophantine in R iff all relations M which are LT-diophantine in $R[T]$ and consist of constant elements only are also L-diophantine in $R[T]$.*

Proof: Indeed, if $\mathbb{Z}$ is diophantine in R, any such relation M is L-diophantine in R. Its definition can be relativized to the L-definition of R in $R[T]$ given by the Theorem 2.14 leading to an L-diophantine definition of M in $R[T]$. On the other side if the diophantine elimination of T is possible, it may be applied to an LT-definition of $\mathbb{Z}$ in $R[T]$, for example that one which was given in 4.8. We claim that the obtained L-definition of $\mathbb{Z}$ in $R[T]$ defines already $\mathbb{Z}$ in R. Suppose its shape to be:

$$R[T] \models \quad X \in \mathbb{Z} \Longleftrightarrow \exists X_1, \ldots, X_n \; P(X, X_1, \ldots, X_n) = 0,$$

for a $P \in R[X, X_1, \ldots, X_n]$. If $X \in \mathbb{Z}$, we choose polynomials $X_1, \ldots, X_n$ which satisfy the definition and we evaluate them in $T \rightsquigarrow 0$, finding constant elements $X_1(0), \ldots, X_n(0) \in R$ which satisfy the definition. If $X \in R \setminus \mathbb{Z}$ then such polynomials do not exist, so elements in R which satisfy the definition do not exist anyway. $\square$

Chapter 5

On the Theorem of Matiyasevich

We intend to present an unexpected consequence of Theorem 4.9 in the case $\mathcal{O} = \mathbb{Z}$. The next Corollary is a first trivial consequence.

Corollary 5.1 *If L is the formal language of rings and LT its extension with the constant $\underline{T}$ representing the polynomial variable T, then for the ring $\mathbb{Z}$ the following are true:*

2. $\mathfrak{Res}_{\mathbb{Z}^*} : \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \to \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$ *is surjective.*

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

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

Proof: $\mathbb{Z}$ is trivially a diophantine subset of itself. Apply Theorem 4.9. □

5.1 Getting Back the Theorem of Matiyasevich

What we have used as nontrivial fact in proving Theorem 4.9 and of course Corollary 5.1 is just the Theorem of Matiyasevich. This very strong result has the draw back that its proof, arithmetic and combinatorial, is not really transparent for the structural algebraist. We have now the possibility to state an equivalent set-theoretical fact. Unfortunately, we cannot expect its proof to be easy in a pure set-theoretical way.

Theorem 5.2 *The fact that $\mathfrak{Res}_{\mathbb{Z}^*} : \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \to \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$ is surjective implies the Theorem of Matiyasevich.*

Proof: For the proof we make the same steps like in proving the Transfer Theorem 4.9. Keeping the facts stated in 5.1 as (2.) and (3.) and denoting the Theorem of Matiyasevich with (1'.), we repeat the circular argument. $1' \Rightarrow 2$ and $2 \Rightarrow 3$ have both the same proof as for Theorem 4.9. Now we prove:

$\underline{3 \Rightarrow 1' :}$

For this goal we have to introduce some definitions and a little historical background. In the 60's, before Yuri Matiyasevich prominently entered the scene, but after the joint work of Martin Davis, Hilary Putnam and Julia Robinson, it was already known that exponential diophantine equations are undecidable over $\mathbb{N}$, see [DPR], and that it would have been enough for a so called Julia Robinson predicate (relation with exponential increment) to be diophantine over $\mathbb{N}$ in order to allow all the recursively enumerable sets to be diophantine.

Definition: A **Julia Robinson predicate** $\rho(u, v)$ over $\mathbb{N}$ satisfies:

$$\begin{array}{llll} (\rho(u,v) & \Longrightarrow & v \leq u^u) & \text{and} \\ \forall k \in \mathbb{N} & \exists u, v \in \mathbb{N} & \rho(u,v) \ \wedge & v > u^k. \end{array}$$

It was 1963 when Martin Davis and Hilary Putnam proved the following:

Lemma 5.3 (Davis-Putnam) *There is a Julia Robinson predicate $\rho(u, v)$ over $\mathbb{N}$ which is LT-diophantine in $\mathbb{Z}[T]$. Moreover, all recursively enumerable relations over $\mathbb{N}$ are LT-diophantine in $\mathbb{Z}[T]$.*

Sketch of proof: First we have to recall that, given $a \in \mathbb{N}$ with $a \geq 2$, the Pell equation

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

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

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

Comparing them with the solutions of the polynomial Pell equation:

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

in $\mathbb{Z}[T]$ (see lemma 4.7), which are the pairs of polynomials $(\pm X_n, \pm Y_n)$ given by:

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

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 $a = 2$:

$$x^2 \Leftrightarrow 3y^2 = 1$$

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:**

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

Claim: ρ is a Julia Robinson predicate.

1.) $2_u < 4^u < u^u$.

2.) If there was 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 claim that:

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

Indeed, $T \Leftrightarrow 1 \,|\, Y \Leftrightarrow u \Leftrightarrow\rightarrow u = Y(1) \Leftrightarrow\rightarrow Y = Y_u \Leftrightarrow\rightarrow X = X_u \Leftrightarrow\rightarrow$

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

Recalling again the results of the joint work of Davis, Putnam and J. Robinson, we see that all the recursively enumerable relations over $\mathbb{N}$ are diophantine in $\mathbb{Z}[T]$, of course using T, because T has already been used in the definition of the Julia Robinson predicate. □

Corollary 5.4 *Let Δ be a domain of characteristic 0. Then there is a Julia Robinson predicate $\rho(u,v)$ over $\mathbb{N}$ which is LT-diophantine in $\Delta[T]$. Moreover, all recursively enumerable relations over $\mathbb{N}$ are LT-diophantine in $\Delta[T]$.*

Proof: This is a combination between the theorems of Alexandra Shlapentokh 4.8 and the classical theorem of M. Davis and H. Putnam 5.3. We do not use the Theorem of Matiyasevich at this point. □

Now we can go back to $\underline{3 \Rightarrow 1'}$:. We apply the transfer of definability to our predicate ρ and we get that ρ is L-diophantine over $\mathbb{Z}$. The same is true for all other recursively enumerable relations. □□

5.2 Comments

Before finishing the chapter, we sum up our principal results. For number rings and fields R we defined an application of natural restriction

$$\mathfrak{Res}_{R^*} : \mathfrak{End}_{R[T]}(R[T]^*) \Leftrightarrow\!\!\!\rightarrow \mathfrak{End}_R(R^*),$$

which is a homomorphism of monoids. Using it we have proven:

$$\begin{aligned} \text{Theorem of Matiyasevich} &\iff \mathfrak{Res}_{\mathbb{Z}^*} \text{ is surjective,} \\ \mathbb{Z} \text{ is } L\text{-diophantine in } \mathcal{O} &\iff \mathfrak{Res}_{\mathcal{O}^*} \text{ is surjective,} \\ \mathbb{Z} \text{ is } L\text{-diophantine in } K &\iff \mathfrak{Res}_{K^*} \text{ is surjective.} \end{aligned}$$

In all three cases this is further equivalent with a transfer of diophantine definability which completes the result of Chapter 2.

One should remark that, from a structural point of view, the problem to define $\mathbb{Z}$ diophantinely in an arithmetical ring is the same as that to define the exponential relation (a, b, a^b) diophantinely in $\mathbb{N}$ or $\mathbb{Z}$. All the essential cases of diophantine definitions of $\mathbb{Z}$ in rings of algebraic integers $\mathcal{O}_K$ which are known: [Denef 2] for rings corresponding to the quadratic fields K, [Denef-Lipshitz] for K totally real and [Pheidas] for the case when K has exactly two conjugate non-real embeddings in $\mathbb{C}$, have been proven adapting the proof of the Theorem of Matiyasevich in more sophisticated situations. They defined diophantinely exponential relations which contain all powers of well chosen elements of the $\mathcal{O}_K$ in question. Adding a quantifier, i.e. making a projection, we get the set of all exponents, which is a set between $\mathbb{N}$ and $\mathbb{Z}$.

This idea does not seem to work for other number rings. All cases proved so far show an important peculiarity: the multiplicative group of units in rings of integers belonging to several quadratic extensions of the given fields has relative free rank ≤ 1 over the multiplicative group of units of the given ring. It is not difficult to see [Sauerland] that the displayed cases are the only ones in which this fact takes place and that the behaviour of the Pell equation seems of no use in the remaining cases.

Hopefully a new proof of the Theorem of Matiyasevich or a set-theoretical (?) proof of the fact that $\mathfrak{Res}_{\mathbb{Z}^*}$ is surjective would be easier to generalize to all rings $\mathcal{O}$ of algebraic integers.

There are until now no known examples of diophantine definitions of $\mathbb{Z}$ in number fields. It is even conjectured that $\mathbb{Z}$ is not diophantinely definable in $\mathbb{Q}$, see [B. Mazur]. On this problem we are giving just the following weak:

Remark 5.5 *If $\mathbb{Z}$ is not diophantine in $\mathbb{Q}$ then it is not diophantine in any number field K.*

Proof: Let $K = \mathbb{Q}(\alpha)$ and $\eta \in \mathfrak{End}_{\mathbb{Q}}(\mathbb{Q}^*)$ such that $\eta(\mathbb{Z}^*) \not\subset \mathbb{Z}^*$. We define the trivial extension $\eta' \in \mathfrak{End}_K(K^*)$:

$$\eta'(x) = \eta'(x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1}) = \eta(x_1) + \eta(x_2)\alpha + \cdots + \eta(x_n)\alpha^{n-1}.$$

Of course $\eta'(\mathbb{Z}^*) \not\subset \mathbb{Z}^*$ so $\mathbb{Z}$ is not diophantine in K even in its appropriate language. A clasical (standard) proof of this remark would be also very easy. $\square$

Chapter 6

The Isomorphism Theorem

The next theorem is maybe our best result:

Theorem 6.1 *The application of natural restriction:*

$$\mathfrak{Res}_{\mathbb{Z}^*} \ : \ \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \ \tilde{\Leftrightarrow} \ \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$$

is an isomorphism of monoids.

6.1 The Injectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$

The surjectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$ was shown in Chapter 5. For proving the injectivity we need some more notions and results.

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** $\mathbb{Z}[T]$. The recursive presentations were introduced by Michael Rabin in a general setting, see [Rabin]. He called them structures of recursive ring.

Our principal ingredient will be the following theorem of Jan Denef. For the proof, see in appendix or in the original paper [Denef 3].

Theorem 6.2 *Let LT be the appropriate language for the polynomial ring* $\mathbb{Z}[T]$. *For all recursive presentations* θ *of* $\mathbb{Z}[T]$ *the corresponding relation*

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

is LT-diophantine in $\mathbb{Z}[T]$.

We will call any relation $\mathcal{R}$ over $\mathbb{Z}[T]$ **recursively enumerable over** $\mathbb{Z}[T]$ iff its inverse image $\theta^{-1}(\mathcal{R})$ is recursively enumerable over $\mathbb{N}$ for some recursive presentation θ. The following corollary justifies why this definition does not depend on the choice of the recursive presentation θ.

Corollary 6.3 (Jan Denef) *A relation over $\mathbb{Z}[T]$ is LT-diophantine over $\mathbb{Z}[T]$ iff it is recursively enumerable.*

Sketch of proof: Let us fix a θ as in the theorem. 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 recursively enumerable θ^{-1} image over $\mathbb{N}$, this inverse image must be diophantine over $\mathbb{Z}[T]$ by Lemma 5.3 [Davis-Putnam]. θ is diophantine over $\mathbb{Z}[T]$, so the relation is itself diophantine over $\mathbb{Z}[T]$. □

We used for the corollary only the fact that θ is a diophantine bijection, thus it is also a recursive relation. The Theorem of Matiyasevich has not been used either in the proof of the Theorem of Denef in the restricted sense 6.2 nor in the proof of the Theorem of Denef in extended sense 6.3. The similarity between the Theorem of Denef in the extended sense 6.3 and the Theorem of Matiyasevich in the extended sense is evident. We will prove the existence of a deeper dualism between them.

Now we have all we need to prove the injectivity part of the Isomorphism Theorem6.1. 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 one $F \in \mathbb{Z}[T]^*$. θ is a bijective function, hence there is exactly one $n \in \mathbb{N}^*$ such that $\mathcal{R}^*_\theta(n, F)$. Since $\mathcal{R}_\theta$ is also diophantine,

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

due again to 1.1.

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

6.2 Getting Back the Theorem of Denef

What we have really used in proving the injectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$ was only the existence of a surjection : $\mathbb{N} \twoheadrightarrow \mathbb{Z}[T]$ which is diophantine over $\mathbb{Z}[T]$. However, we have just shown that

$$\text{Theorem of Denef} \implies \mathfrak{Res}_{\mathbb{Z}^*} \text{ is injective.}$$

As we have seen, the only not sophisticated applications of the Pell equation, which seem also to contain its pure principle, are the proofs presented for defining $\mathbb{Z}$ in polynomials in 4.8 and for defining a relation with exponential increment also in polynomials in 5.3. We have proven that assuming 5.3 the surjectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$ implies in a structural way the Theorem of Matiyasevich. We intend now to do the same thing for the Theorem of Denef.

Theorem 6.4 *The fact that $\mathfrak{Res}_{\mathbb{Z}^*} : \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*) \to \mathfrak{End}_{\mathbb{Z}}(\mathbb{Z}^*)$ is injective implies the Theorem of Denef 6.2.*

Proof: Let again θ be a recursive presentation of $\mathbb{Z}[T]$. Considering an embedding $\alpha \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$, it is to prove that for all $n \in \mathbb{N}^*$ and corresponding $F \in \mathbb{Z}[T]^*$:

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

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, hence $(\theta^*)^{-1} = (\theta^{-1})^*$. We define the following external function:

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

The definition makes sense because $\mathbb{N}$ is diophantine over $\mathbb{Z}$. We show stepwise 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 developping a machinery for extending embeddings which differs from this one used in the proof of Theorem 4.9. The role of the diophantine Gödel function is now taken by the diophantine 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. This supplementary remark will be useful for the Corollary 6.6.

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

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

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

is a recursive relation over $\mathbb{N}$. By lemma 5.3 (Davis-Putnam) $\mathcal{R}_{\mathfrak{op}}$ is diophantine over $\mathbb{Z}[T]$. We are avoid again the Theorem of Matiyasevich.

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:

Lemma 6.5 *The* **corestriction** *of* θ *on* $\mathbb{N}$*:*

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

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

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

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

Since $\mathcal{R}_+$ is recursive, $\oplus$ is algorithmically computable. We construct the following pairs: $(a,0)$, $(b,1)$, $(b \oplus b, 2)$, ... (n,m), $(n \oplus b, m+1)$, ... 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, see in appendix. □

In virtue of 5.3, $\mathfrak{theta}$ is diophantine in $\mathbb{Z}[T]$. So for $n, m \in \mathbb{N}^*$:

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

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 $\mathfrak{theta}^*(n,m)$. Take an arbitrary $m \in \mathbb{N}^*$.

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

hence 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:

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

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

6.3 Other Applications

We recall now that the group of invertible elements of the monoid of embeddings of a structure in itself is exactly the group of automorphisms of that structure. This gives a trivial corollary to the Isomorphism Theorem 6.1.

Corollary 6.6 *The application of natural restriction*

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

is an isomorphism of groups.

This result over $\mathbb{Z}$ is just a little bit stronger than the result we have got in the General Transfer Theorem3.4 for all number fields and rings. What model-theoretic importance does the supplementary information have?

Definition: A relation $M \subseteq \mathbb{N}^k$ is called **arithmetic** iff it is definable over $\mathbb{N}$. We call a relation $M \subseteq (\mathbb{Z}[T])^k$ **arithmetic** iff its reverse image under any recursive presentation θ of $\mathbb{Z}[T]$ is arithmetical over $\mathbb{N}$.

Corollary 6.7 *A relation over $\mathbb{Z}[T]$ is LT-definable iff it is arithmetic.*

If we remember Theorem 2.2 together with the Corollary 6.3, we get:

Corollary 6.8 *There is no recursive presentation θ of the ring $\mathbb{Z}[T]$ which is diophantine with respect to the formal language of rings L.*

Proof: $\mathbb{N}$ is L-diophantine in $\mathbb{Z}[T]$ following Theorem 2.14, and a complement of a point in $\mathbb{N}$ is also trivially L-diophantine, writing

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

If θ was L-diophantine, we could have defined $\mathbb{Z}[T] \setminus \{0\}$ L-diophantinely in $\mathbb{Z}[T]$. This contradicts Theorem 2.2. □

It is the time to look for less trivial applications. In Chapter 3 we developed a possible technique to extend embeddings. The injectivity of $\mathfrak{Res}_{\mathbb{Z}^*}$ tells us that any such extension must be unique.

Theorem 6.9 (Structure of Embeddings) *All $\eta \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$ 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 Theorem 4.9. Any recursive enumerable relation in $\mathbb{N}$ which might have been used for this extension is diophantine over $\mathbb{Z}[T]^*$ with Lemma 5.3, so we did not use the Theorem of Matiyasevich. 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. □□

We emphasize situations when we avoid to apply the Theorem of Matiyasevich because, whithout knowing the deep nature of the isomorphism in Theorem 6.1, we must make a procedural difference between injectivity and surjectivity. The Structure Theorem above has only apparently made use of the surjectivity. It represents in fact just the injectivity and the Theorem of Denef.

After the work of Matiyasevich, Julia Robinson and others we have a big collection of relations of mathematical interest which are diophantine over $\mathbb{N}$. In what follows we do not intend to do an analogous exhaustive work over $\mathbb{Z}[T]$. Some of our relations are easy to prove as recursively enumerable, so already diophantine after the Theorem of Denef 6.2. We want just to give some examples on the combinated power of the Structure Theorem 6.9 and the diophantine Theorem of Beth 2.9.

Theorem 6.10 *The following relations are LT-diophantine in* $\mathbb{Z}[T]$*:*

$$\begin{aligned}
\text{Deg}\ (F,n) &\iff n \in \mathbb{N} \ \wedge\ \text{degree}\ (F) = n.\\
\Pi\,(i,F,a) &\iff i \in \mathbb{N} \ \wedge\ a \in \mathbb{Z} \ \wedge\ \text{the i}^{\text{th}}\ \text{coefficient of}\ F\ :\ a_i = a.\\
\text{Monic}\ (F) &\iff a_n = 1.\\
\text{PowerT}\ (i,F) &\iff i \in \mathbb{N} \ \wedge\ F = T^i.\\
\text{Eisenstein}\ (p,F) &\iff p \in \mathbb{N} \ \wedge\ p\ \text{prime} \ \wedge\ p \not| a_n \ \wedge \forall i \in [0, n \Leftrightarrow 1]\ \ p \,|\, a_i\\
&\qquad \wedge\ p^2 \not| a_0.\\
\text{Cyclotomic}\ (F) &\iff \exists\, n \in \mathbb{N}\ \ n \geq 1 \ \wedge\ F = T^n \Leftrightarrow 1.
\end{aligned}$$

Proof: For any relation $\mathcal{R}$ from above one see immediately with the Structure Theorem that:

$$\mathcal{R}^*(\vec{F}) \implies \mathcal{R}^*(\eta(\vec{F}))$$

for all $\eta \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$. □□

We can now combine different methods in order to prove the diophantine character over $\mathbb{Z}[T]$ of several other relations, as in the next corollary:

Corollary 6.11 *The following two other relations are LT-diophantine:*

$$\begin{aligned}
&F \not| G \ \wedge\ F \text{ is monic.}\\
&\text{Composition}\ (F,G,H) \quad (:\iff\ F \circ G = H).
\end{aligned}$$

Proof: We write the first relation like:

$$\begin{aligned}\text{Monic}\ (F)\ \ &\wedge\ \ [(\text{degree}\ (F) > \text{degree}\ (G))\ \vee\ (\exists\, H, R\ G = FH + R\ \wedge \\ &\wedge\ \ \text{degree}\ (R) < \text{degree}\ (F)\ \wedge\ R \neq 0)].\end{aligned}$$

We must just remember that $R \neq 0$ is a diophantine relation, $\mathbb{Z}[T]$ being an adequate ring as in Theorem 2.15. It would have been a typical mistake to motivate this fact using the Structure Theorem followed by the new version of the Theorem of Beth. In fact, we may apply New Beth only because the ring is adequate.

The relation:

$$\text{Evaluation}\ (F, a, b) \iff a \in \mathbb{Z}\ \wedge\ b \in \mathbb{Z}\ \wedge\ T \Leftrightarrow a \,|\, F \Leftrightarrow b$$

is a particular case of the relation Composition (F, G, H). It is diophantine and we have already used it many times. Now:

$$\text{Composition}\ (F, G, H) \iff$$

$$\begin{array}{lllllll}\exists d \Big(& d \in \mathbb{N} & \wedge & d = \text{degree}\ H & \wedge & d = \text{degree}\ F & \text{degree}\ G \wedge \\ & \forall i & \leq d+1 & \exists a, b \in \mathbb{Z} & [& T \Leftrightarrow i \,|\, H \Leftrightarrow a & \wedge \\ & & \wedge & T \Leftrightarrow i \,|\, G \Leftrightarrow b & \wedge & T \Leftrightarrow b \,|\, F \Leftrightarrow a &] \Big).\end{array}$$

This formula is true because a polynomial of degree d is uniquely determined by $d+1$ of its values. It is also diophantine, being recursively enumerable over $\mathbb{Z}[T]$. □

To sum up: we have found an isomorphism which is a structural fact about objects whose construction can be done in a pure set-theoretical way. Its existence is equivalent to the logical conjunction of the theorems of Matiyasevich and Denef. The equivalence used only the classical result of Davis and Putnam, which has a clear algebraic nature. The original proofs of these two difficult results are based on many special properties of the Pell equation and on very complex combinatorial constructions and are not really iluminating for the structural algebraist. A direct structural proof of the Isomorphism Theorem will mean a symultaneous (?) proof of the two big results. Of course we may not be very optimistic about this speculation, because a direct proof of the Isomorphism Theorem seems in this moment entirely inaccessible.

Chapter 7

Other Isomorphism Theorems

We put the question if other rings of algebraic integers $\mathcal{O} \neq \mathbb{Z}$ have the property that the application of natural restriction $\mathfrak{Res}_{\mathcal{O}^*}$ is an isomorphism of monoids. That's why we prove some equivalences which are for many reasons dual to the Diophantine Transfer 4.9. For example, as Theorem 4.9 used in proof the Theorem of Matiyasevich, uses the proof of Theorem 7.1 the analogous Theorem of Denef 6.2.

The question if there is a form of Theorem 7.1 valid also in the case of number fields is unfortunately still open.

7.1 $\mathbb{Z}[T]$ as a Subring

Theorem 7.1 *For a ring of algebraic integers $\mathcal{O}$ the following assertions are equivalent:*

1. *There is a surjective function $\lambda : \mathbb{N} \twoheadrightarrow \mathcal{O}[T]$ which is diophantine in $\mathcal{O}[T]$ using the language LT.*
2. *$\mathfrak{Res}_{\mathcal{O}^*} : \mathfrak{End}_{\mathcal{O}[T]}(\mathcal{O}[T]^*) \twoheadrightarrow \mathfrak{End}_{\mathcal{O}}(\mathcal{O}^*)$ is injective.*
3. *All recursive presentations $\theta : \mathbb{N} \twoheadrightarrow \mathcal{O}[T]$ are LT-diophantine in $\mathcal{O}[T]$.*
4. *All relations M over $\mathcal{O}[T]$ are LT-diophantine in $\mathcal{O}[T]$ iff they are recursively enumerable with respect to some recursive presentation θ of $\mathcal{O}[T]$.*
5. *$\mathbb{Z}[T]$ is LT-diophantine in $\mathcal{O}[T]$.*

Proof: There are a lot of possibilities to prove this theorem. For the convenience of the reader we choosed a short circular proof.

$\underline{1 \Longrightarrow 2}$: The same proof as for the Isomorphim Theorem 6.1.

$\underline{2 \Longrightarrow 3}$: The same proof as for the reciprocal of 6.1: Theorem 6.4.

$\underline{3 \Longrightarrow 4}$: The same proof as for Corollary 6.3.

$\underline{4 \Longrightarrow 5}$:

$\mathbb{Z}[T]$ is LT-diophantine in $\mathcal{O}[T]$ according to the hypothesis because there is a recursive presentation λ of $\mathcal{O}[T]$ such that $\mathbb{Z}[T]$ is a recursively enumerable set with respect to λ.

We construct such a λ. Let us fix a recursive presentation $\theta : \mathbb{N} \to \mathbb{Z}[T]$ and an integral basis $\{\alpha_1, \ldots, \alpha_m \,|\, \alpha_1 = 1\}$ of $\mathcal{O}$ over $\mathbb{Z}$. We choose and fix also a bijection between $\mathbb{N}$ and $\mathbb{N}^m$ which is birecursive over $\mathbb{N}$, i.e. the function itself and all the projections of the inverse function are recursive. Iterations of the pairing function of Cantor are such functions. We denote the function by $k = (k_1, \ldots, k_m)$. We define $\lambda : \mathbb{N} \to \mathcal{O}[T]$ to be:

$$\lambda(k) = \sum_{i=1}^{m} \theta(k_i)\alpha_i,$$

where the k's are in the displayed relation over $\mathbb{N}$. The function λ is trivially bijective. We must show that it transfers the ring operations of $\mathcal{O}[T]$ in recursive relations over $\mathbb{N}$. We choose for these relations an operational notation as follows: $\theta^{-1}(+_{\mathbb{Z}[T]}) = \oplus_{\mathbb{Z}}$, $\theta^{-1}(\cdot_{\mathbb{Z}[T]}) = \otimes_{\mathbb{Z}}$, $\lambda^{-1}(+_{\mathcal{O}[T]}) = \oplus_{\mathcal{O}}$, $\lambda^{-1}(\cdot_{\mathcal{O}[T]}) = \otimes_{\mathcal{O}}$. An operation of substraction is uniquely determined by the addition and will play an auxiliary role. It will be always denoted by $\ominus$. We see already that:

$$\begin{aligned} k \oplus_{\mathcal{O}} l = n \iff\ & k = (k_1, \ldots, k_m) \ \wedge\ l = (l_1, \ldots, l_m) \ \wedge \\ & \wedge\ n = (k_1 \oplus_{\mathbb{Z}} l_1, \ldots, k_m \oplus_{\mathbb{Z}} l_m). \end{aligned}$$

The corresponding formula for the multiplication depends explicitly of the considered number ring. In order to avoid sophisticated notations we prefer to ilustrate the idea giving an example. If $\mathcal{O} = \mathbb{Z}$[i], then:

$$\begin{aligned} k \otimes_{\mathcal{O}} l = n \iff\ & k = (k_1, k_2) \ \wedge\ l = (l_1, l_2) \ \wedge \\ & \wedge\ n = (\, k_1 \otimes_{\mathbb{Z}} l_1 \ominus_{\mathbb{Z}} k_2 \otimes_{\mathbb{Z}} l_2 \ ,\ k_1 \otimes_{\mathbb{Z}} l_2 \oplus_{\mathbb{Z}} k_2 \otimes_{\mathbb{Z}} l_1 \,). \end{aligned}$$

The formulas use the classical order of operations. It became evident that $\oplus_{\mathcal{O}}$ and $\otimes_{\mathcal{O}}$ are recursive functions over $\mathbb{N}$ because they are compositions of recursive functions.

We have shown that λ is a recursive presentation of $\mathcal{O}[T]$. Let us denote as in Lemma 6.5 $\theta^{-1}(0)$ by a. Then:

$$\lambda^{-1}(\mathbb{Z}[T]) = \{k \in \mathbb{N} \,|\, \exists k_1 \leq \varphi(k)\ k = (k_1, a, \ldots, a)\},$$

where the bound $\varphi(k)$ is a known recursive function which depends of the m-tuple coding. For the pairing function of Cantor and its iterations the bound $\varphi(k) = 2^{m-1}k$ is always sufficient.

So $\lambda^{-1}(\mathbb{Z}[T])$ is a recursively enumerable subset of $\mathbb{N}$.

$\underline{5 \Longrightarrow 1}$:

We assume to have quantified equations with free variables, which define diophantinely:

- A bijection $k = (k_1, \ldots, k_m)$ between $\mathbb{N}$ and $\mathbb{N}^m$, over $\mathbb{N}$. The k^{th} iteration of the pairing function of Cantor may be used again.

-The relation $\mathcal{R}_{\theta,\mathbb{Z}[T]}$ corresponding to a recursive presentation of $\mathbb{Z}[T]$, inside $\mathbb{Z}[T]$. Its diophantine character is assured by Denef's Theorem, which is used only in this point.

-$\mathbb{Z}[T]$ inside $\mathcal{O}[T]$. Such an equation exists by hypothesis.

We recall that $\mathbb{Z}$ and $\mathbb{N}$ are diophantine in $\mathcal{O}[T]$. We will write a diophantine definition of the structure of recursive ring λ which has been constructed in the last proof. We introduce an analogous notation:

$$\begin{aligned} \mathcal{R}_{\theta,\mathbb{Z}[T]}(n,F) &\iff n \in \mathbb{N} \ \wedge \ \theta(n) = F, \\ \mathcal{R}_{\lambda,\mathcal{O}[T]}(n,F) &\iff n \in \mathbb{N} \ \wedge \ \lambda(n) = F. \end{aligned}$$

Now we finally write:

$$\begin{aligned} \mathcal{R}_{\lambda,\mathcal{O}[T]}(k,F) \iff & \exists k_1, \ldots, k_m, P_1, \ldots, P_m \\ & k \in \mathbb{N} \ \wedge \ k_1 \in \mathbb{N} \ \wedge \cdots \wedge \ k_m \in \mathbb{N} \ \wedge \\ & P_1 \in \mathbb{Z}[T] \ \wedge \cdots \wedge \ P_m \in \mathbb{Z}[T] \ \wedge \\ & k = (k_1, \ldots, k_m) \ \wedge \\ & \mathcal{R}_{\theta,\mathbb{Z}[T]}(k_1, P_1) \ \wedge \cdots \wedge \mathcal{R}_{\theta,\mathbb{Z}[T]}(k_m, P_m) \ \wedge \\ & F = \underline{\alpha_1} P_1 + \cdots + \underline{\alpha_m} P_m. \end{aligned}$$

We should not forget to relativize all equations to their natural domains and to use at any step new variables. The function λ is in particular a surjection from $\mathbb{N}$ onto $\mathcal{O}[T]$, diophantinely defined in $\mathcal{O}[T]$ using the appropriate language LT. □□

7.2 Other Isomorphism Theorems

From the five statements of Theorem 7.1, the statement which looks more atractive is the LT-diophantine definability of $\mathbb{Z}[T]$ in $\mathcal{O}[T]$. A natural remark like

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

leads to an easy proof of the following:

Proposition 7.2 *For every ring of algebraic integers $\mathcal{O}$, the complement $\mathcal{O}[T] \setminus \mathbb{Z}[T]$ is LT-diophantine in $\mathcal{O}[T]$.*

Proof: $\mathbb{Z}$ is diophantine in $\mathcal{O}[T]$ by Corollary 4.8, and $\mathcal{O} \setminus \mathbb{Z}$ is diophantine in $\mathcal{O}[T]$ by adapting the proof of Lemma 4.1. Translating the remark above, we get the following definition:

$$F \in \mathcal{O}[T] \setminus \mathbb{Z}[T] \Longleftrightarrow \exists a, b \;\; a \in \mathbb{Z} \wedge b \in \mathcal{O} \setminus \mathbb{Z} \;\wedge\; \underline{T} \Leftrightarrow a \,|\, F \Leftrightarrow b.$$

□

Of course this does not mean that $\mathbb{Z}[T]$ is not diophantine in $\mathcal{O}[T]$, but it may mean that such a definition would be difficult to find. On the other hand it means that $\mathbb{Z}[T]$ is always LT-definable in $\mathcal{O}[T]$. Together with results like Theorem 3.2 and Corollary 6.6, Proposition 7.2 leads to the following weak isomorphisms:

Corollary 7.3 *For all rings of algebraic integers $\mathcal{O}$, the application of natural restriction*

$$\mathfrak{Res}_{\mathcal{O}^*} \;:\; \mathfrak{Aut}_{\mathcal{O}[T]}(\mathcal{O}[T]^*) \Leftrightarrow\!\!\!\!\rightarrow \mathfrak{Aut}_{\mathcal{O}}(\mathcal{O}^*)$$

is an isomorphism of groups. Both groups are isomorphic with $\mathfrak{Aut}(\mathbb{N}^*)$ through the canonical applications $\mathfrak{Res}_{\mathbb{N}^*}$.

As before in 6.7, we may conclude that the relations which are definable over $\mathcal{O}[T]$ are exactly the arithmetic relations.

What can we say about the monoids $\mathfrak{End}_{\mathcal{O}[T]}(\mathcal{O}[T]^*)$? A long time I had not enough evidence to support my conjectures. But when I was prepairing the text to be published, I received some good news from Gent (Belgium). Karim Zahidi proved in his Thesis the following generalization of the Theorem of Denef 6.2, see [Zahidi]:

Theorem 7.4 (K. Zahidi) *Let K be a totally real number field and $\mathcal{O}$ its ring of algebraic integers. Then there is a recursive presentation $\theta : \mathbb{N} \to \mathcal{O}[T]$ which is LT-diophantine in $\mathcal{O}[T]$.*

According to our Theorem of Characterization 7.1, it is true for these rings that $\mathbb{Z}[T]$ is LT-diophantine in $\mathcal{O}[T]$ and that the application of natural restriction $\mathfrak{Res}_{\mathcal{O}^*} : \mathfrak{End}_{\mathcal{O}[T]}(\mathcal{O}[T]^*) \Leftrightarrow\!\!\!\!\rightarrow \mathfrak{End}_{\mathcal{O}}(\mathcal{O}^*)$ is injective. On the other hand, all these rings $\mathcal{O}$ have the property that $\mathbb{Z}$ is L-diophantine in $\mathcal{O}$, see [Denef-Lipshitz], so according with our Diophantine Transfer Theorem 4.9 is $\mathfrak{Res}_{\mathcal{O}^*}$ also surjective. If we put all this information together, we get the following strong isomorphisms:

Theorem 7.5 *If $\mathcal{O}$ is the ring of algebraic integers of some totally real number field, then the application of natural restriction*

$$\mathfrak{Res}_{\mathcal{O}^*} \;:\; \mathfrak{End}_{\mathcal{O}[T]}(\mathcal{O}[T]^*) \Leftrightarrow\!\!\!\!\rightarrow \mathfrak{End}_{\mathcal{O}}(\mathcal{O}^*)$$

is an isomorphism of monoids. Both monoids are isomorphic with $\mathfrak{End}(\mathbb{N}^*)$ through the canonical applications $\mathfrak{Res}_{\mathbb{N}^*}$.

In the same way as already shown in Chapter 6, all conclusions and applications of the Isomorphism Theorem for $\mathbb{Z}$ are still true for the totally real number rings $\mathcal{O}$. In particular, a relation is LT-diophantine in $\mathcal{O}[T]$ iff it is recursively enumerable, and the elements of $\mathfrak{End}_{\mathcal{O}[T]}(\mathcal{O}[T]^*)$ are described by a corresponding Structure Theorem.

7.3 Comments

Coming back to the diophantine problem of defining $\mathbb{Z}[T]$ in $\mathcal{O}[T]$, we get a last negative result in the same spirit as of Theorem 2.2:

Theorem 7.6 *If L is the appropriate language for a number ring $\mathcal{O}$ then $\mathbb{Z}[T]$ is not L-diophantine in $\mathcal{O}[T]$.*

Proof: Suppose that there was a polynomial $P \in \mathcal{O}[X, X_1, \ldots, X_n]$ such that:

$$\mathcal{O}[T] \models \quad X \in \mathbb{Z}[T] \iff \exists X_1, \ldots, X_n \;\; P(X, X_1, \ldots, X_n) = 0.$$

We recall that without a name for T the polynomial ring $\mathcal{O}[T]$ is no more an adequate ring, but is still conjunctive and disjunctive, so a diophantine definition may be contracted in one quantified equation.

Of course $T \in \mathbb{Z}[T]$, so we may choose and fix polynomials $X_1, \ldots, X_n \in \mathcal{O}[T]$ such that:

$$\mathcal{O}[T] \models \quad P(\underline{T}, X_1(\underline{T}), \ldots, X_n(\underline{T})) = 0.$$

Considering this polynomial identity over $\mathcal{O}$, we see that $\underline{T}$ is a new constant which doesn't belong to L and has no interpretation as element in $\mathcal{O}$. It may be substituted by any constant term over the appropriate language L for getting a true proposition over $\mathcal{O}$. We choose a constant term representing an element $\epsilon \in \mathcal{O} \setminus \mathbb{Z}$.

$$\mathcal{O} \models \quad P(\epsilon, X_1(\epsilon), \ldots, X_n(\epsilon)) = 0.$$

The values $x_i := X_i(\epsilon) \in \mathcal{O} \subset \mathcal{O}[T]$, so it is true that:

$$\mathcal{O}[T] \models \quad \exists X_1, \ldots, X_n \;\; P(\epsilon, X_1, \ldots, X_n) = 0.$$

Applying our hypothesis we get $\epsilon \in \mathbb{Z}[T]$, so $\epsilon \in \mathbb{Z}[T] \cap \mathcal{O} = \mathbb{Z}$, which is in contradiction with the choice of ϵ. □□

Observing that the rank of $\mathcal{O}$ as $\mathbb{Z}$-module coincides with the rank of $\mathcal{O}[T]$ as $\mathbb{Z}[T]$-module, one could ask if it is possible to find a simultaneous diophantine definition for $\mathbb{Z}$ in $\mathcal{O}$ and $\mathbb{Z}[T]$ in $\mathcal{O}[T]$. The last Theorem 7.6 implicitly gives a negative answer to this question.

As a final conclusion, we repeat two of our equivalences for a ring of algebraic integers $\mathcal{O}$:

$$\begin{aligned} \mathfrak{Res}_{\mathcal{O}^*} \text{ surjective} &\iff \mathbb{Z} \text{ is } L\not\Leftrightarrow\text{diophantine in } \mathcal{O}, \\ \mathfrak{Res}_{\mathcal{O}^*} \text{ injective} &\iff \mathbb{Z}[T] \text{ is } LT\not\Leftrightarrow\text{diophantine in } \mathcal{O}[T]. \end{aligned}$$

We put again the problem of proving Isomorphism Theorems in a general setting and without using already available results on definability, **in order** to get structural proofs of the corresponding definability results which would be independent of the search after ad-hoc definitions.

Here are two out of the many open questions which we may use for a happy-end: Does every ring of algebraic integers $\mathcal{O}$ satisfy an Isomorphism Theorem? Are these results true over other finitely generated domains of characteristic 0?

Chapter 8

Appendix

8.1 Some Finite Rings

This part is an appendix to Chapter 2. Its main goal is to exemplify the behaviour of two notions introduced there, conjunctive and disjunctive rings, in the exotic case of commutative rings which are not domains. In order to make something that could be still significant for Number Theory we have chosen the rings of classes of division rests of $\mathbb{Z}$. The author thanks Prof. M. Ziegler, Prof. S. Basarab and Dr. M. Nüsken for interesting preliminary discussions over the topics contained in this appendix. The "only if" half of the next theorem has been done together with M. Nüsken.

All results of this section deal with the rings of rest-classes $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ and seem to be new. Along the section we understand through the language L an extension with constants of the formal language of rings.

Definition: We recall that a ring R was considered **disjunctive** with respect to a language L iff the binary relation $x = 0 \vee y = 0$ could be defined over R by an L-formula of the form $\exists\, x_1, \ldots, x_n\ P(x, y, x_1, \ldots, x_n) = 0$, where $P \in R[x, y, x_1, \ldots, x_n]$.

Theorem 8.1 *The commutative ring $\mathbb{Z}_n$ is disjunctive iff $n = p^k$ is a prime power.*

Proof: First we prove necessity. Let $p, q \in \mathbb{Z}$ be relatively prime (but not necessarily prime) and suppose that there exists a polynomial $P \in \mathbb{Z}[x, y, \vec{x}]$ such that:

$$\mathbb{Z}_{pq} \models \exists\, \vec{x}\ \tilde{P}(x, y, \vec{x}) = 0 \Longleftrightarrow x = 0 \ \vee \ y = 0.$$

where $\tilde{P} = P \bmod pq$. We prefer to work in the language of the congruences. The pairs $(0, q)$ and $(p, 0)$ must satisfy the diophantine definition. That's why in $\mathbb{Z}$ the following are true:

$$\begin{aligned} &\exists\, b_1, \ldots, b_n \quad P(0, q, b_1, \ldots, b_n) \equiv 0 \mod(pq), \\ &\exists\, c_1, \ldots, c_n \quad P(p, 0, c_1, \ldots, c_n) \equiv 0 \mod(pq). \end{aligned}$$

This implies:

$$\begin{aligned} \exists\, b_1, \ldots, b_n \quad & P(0, q, b_1, \ldots, b_n) \equiv 0 \mod(p), \\ \exists\, c_1, \ldots, c_n \quad & P(p, 0, c_1, \ldots, c_n) \equiv 0 \mod(q). \end{aligned}$$

We choose and fix such solutions b_i and c_i. As a direct application of the Chinese Remainder Theorem, possible because $(p, q) = 1$, we find $a_i \in \mathbb{Z}$ such that:

$$\begin{aligned} a_i &\equiv b_i \mod (p), \\ a_i &\equiv c_i \mod (q). \end{aligned}$$

Preserving the congruences we may substitute now the b_i's and the c_i's with the a_i's. Moreover we may substitute the 0's with the respective modulo p and q. We get:

$$\begin{aligned} P(p, q, a_1, \ldots, a_n) &\equiv 0 \mod(p), \\ P(p, q, a_1, \ldots, a_n) &\equiv 0 \mod(q). \end{aligned}$$

Using again the fact that p and q are relatively prime, we get:

$$P(p, q, a_1, \ldots, a_n) \equiv 0 \mod (pq).$$

This means of course that:

$$\mathbb{Z}_{pq} \models \exists\, \vec{x}\ \tilde{P}(p, q, \vec{x}) = 0,$$

which is in fact the contradiction $p = 0 \ \vee \ q = 0$ in $\mathbb{Z}_{pq}$.

Now, let us see why the case $n = p^k$ is always disjunctive. We prove that:

$$\mathbb{Z}_{p^k} \models \quad x = 0 \vee y = 0 \iff \exists z\ z^{p^k - p^{k-1}} x + (1 \Leftrightarrow z^{p^k - p^{k-1}}) y = 0.$$

Indeed, if $x = 0$ we take $z = 1$ and if $y = 0$ we take $z = 0$. For proving the other direction, we recall that the multiplicative group of units of $\mathbb{Z}_{p^k}$ contains exactly the division classes of numbers which are not divisible by p and has cardinality $p^k \Leftrightarrow p^{k-1}$. For p prime and $k \geq 1$ one has $p^k \Leftrightarrow p^{k-1} \geq k$, thus

$$\begin{aligned} z^{p^k - p^{k-1}} = 0 &\Leftrightarrow z \in p\mathbb{Z}_{p^k}, \\ z^{p^k - p^{k-1}} = 1 &\Leftrightarrow z \in \mathbb{Z}_{p^k} \setminus p\mathbb{Z}_{p^k}. \end{aligned}$$

For any solution (x, y, z) of the equation, it reduces to $x = 0$ or to $y = 0$, so we are done. □□

As next topic we will explore which $\mathbb{Z}_n$ is conjunctive.

Definition: We recall that a ring R was considered **conjunctive** with respect to a language L iff the binary relation $x = 0 \wedge y = 0$ could be defined over R by an L-formula of the form $\exists\, x_1, \ldots, x_n\ P(x, y, x_1, \ldots, x_n) = 0$, where $P \in R[x, y, x_1, \ldots, x_n]$.

As before, we will get as answer more than the finite fields $\mathbb{Z}_p$. The set of the conjunctive $\mathbb{Z}_n$'s is also structurally dual with that of the disjunctive rings $\mathbb{Z}_n$.

Theorem 8.2 *The commutative ring $\mathbb{Z}_n$ is conjunctive iff $n = p_1 \dots p_s$ is square-free.*

Proof: We present a proof which consists of several small steps.

Lemma 8.3 *Let L be an extension with constants of the formal language of rings. If a commutative ring is conjunctive with respect to the language L, then there is an extension L' of L, with finitely many constants, such that the relation $x = 0 \wedge y = 0$ accepts a strongly diophantine quantifier-free L'-definition.*

This is just a trivial remark. If a diophantine L-definition has the form:

$$R \models\ x = 0 \wedge y = 0 \ \Leftrightarrow\ \exists\, x_1, \dots, x_n\ P(x, y, x_1, \dots, x_n) = 0,$$

then we fix $x'_1, \dots, x'_n \in R$ such that $P(0, 0, x'_1, \dots, x'_n) = 0$. We enlarge if necessary the language L to a language L' by adding constant symbols for the chosen elements and we denote $P(x, y, x'_1, \dots, x'_n) =: Q(x, y)$. So we have got the L'-definition:

$$R \models\ x = 0 \wedge y = 0 \ \Leftrightarrow\ Q(x, y) = 0.$$

In our case all elements are definable as constant terms which are sums of ones, so it is nothing to care about the language. □

Lemma 8.4 *The fields $\mathbb{Z}_p$ are conjunctive.*

This is another trivial remark. If $p > 2$ is an odd prime, there is some $D \in \mathbb{Z}_p$ which is not a quadratic rest modulo p. Then:

$$\mathbb{Z}_p \models\ x = 0 \wedge y = 0 \ \Leftrightarrow\ x^2 \Leftrightarrow Dy^2 = 0.$$

If $p = 2$, the following definition works:

$$\mathbb{Z}_2 \models\ x = 0 \wedge y = 0 \ \Leftrightarrow\ x + y + xy = 0.$$

Lemma 8.5 *The rings $\mathbb{Z}_{p^k}$ are not conjunctive for $k \geq 2$.*

Suppose that $\mathbb{Z}_{p^k}$ was conjunctive. After our first lemma, one should have a definition like this:

$$\mathbb{Z}_{p^k} \models\ x = 0 \wedge y = 0 \ \Leftrightarrow\ Q(x, y) = 0.$$

But $Q(0, 0) = 0$, thus $Q(x, y) = S(x, y) + ax + by$, where all monomials in S have degree ≥ 2. Now, if we suppose that $b \in p\mathbb{Z}_{p^k}$, say $b = pc$, then:

$$Q(0, p^{k-1}) = S(0, p^{k-1}) + cp^k = 0,$$

because the monomials which contain only y have degree ≥ 2 and $2k \Leftrightarrow 2 \geq k$ iff $k \geq 2$. But $p^{k-1} \neq 0$ in $\mathbb{Z}_{p^k}$, so we have got a contradiction. With an identical argument we conclude that $a, b \in \mathbb{Z}_{p^k} \setminus p\mathbb{Z}_{p^k} := \mathcal{U}(\mathbb{Z}_{p^k})$. In this case it is easy to see that the polynomial $Q(a^{-1}x, b^{-1}y)$ defines the same relation $x = 0 \wedge y = 0$ if $Q(x, y)$ does, so we may assume that $Q(x, y) = S(x, y) + x + y$. But in this case,

$$Q(p^{k-1}, \Leftrightarrow p^{k-1}) = S(p^{k-1}, \Leftrightarrow p^{k-1}) = 0,$$

again because of the fact that S collected monomials of degree ≥ 2. This last evident contradiction proves the lemma. □

Now we are ready to make the final step in proving the nontrivial half of our theorem. It is contained in the following:

Lemma 8.6 *If $n = p_1^{k_1} \dots p_s^{k_s}$ and $\mathbb{Z}_n$ is conjunctive, then all the s rings $\mathbb{Z}_{p_1^{k_1}}$, $\dots$, $\mathbb{Z}_{p_s^{k_s}}$ are also conjunctive.*

Indeed, we can read the Chinese Remainder Theorem as the existence of an isomorphism of rings:

$$\varphi : \mathbb{Z}_n \tilde{\Leftrightarrow} \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}}.$$

We call $\pi_i : \mathbb{Z}_n \to \mathbb{Z}_{p_i^{k_i}}$ the corresponding canonical projections. It is easy to see: if $Q(x, y) = 0$ defines $(0, 0)$ in $\mathbb{Z}_n$ then $\pi_i(Q)(x, y) = 0$ defines $(0, 0)$ in $\mathbb{Z}_{p_i^{k_i}}$. □

Since now we have proven that $\mathbb{Z}_n$ conjunctive $\Rightarrow$ n square-free. For proving the easier reciprocal, we consider a square-free $n = p_1 p_2 \dots p_s$ and the corresponding isomorphism:

$$\varphi : \mathbb{Z}_n \tilde{\Leftrightarrow} \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \dots \oplus \mathbb{Z}_{p_s}.$$

We notice that over $\mathbb{Z}_2$, $x + y + xy = x^2 + y^2 + xy$. For all odd primes p we fix an element $D_p \in \mathbb{Z}_p$ which is not a quadratic rest modulo p and we consider the polynomial $x^2 + 0 \cdot xy \Leftrightarrow D_p y^2$. To unify notations, we consider polynomials $Q_p \in \mathbb{Z}_p[x, y]$, of the form $Q_p(x, y) := x^2 + b_p xy + c_p y^2$ given by the conditions:

$$b_p := \begin{cases} 1, & \text{if } p = 2, \\ 0, & \text{if } p \text{ is odd.} \end{cases} \quad ; \quad c_p := \begin{cases} 1, & \text{if } p = 2, \\ \Leftrightarrow D_p, & \text{if } p \text{ is odd.} \end{cases}$$

We get now:

$$\mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \dots \oplus \mathbb{Z}_{p_s} \models \vec{x} = (0, \dots, 0) \wedge \vec{y} = (0, \dots, 0) \Leftrightarrow$$

$$\Leftrightarrow \vec{x}^{\,2} + (b_{p_1}, \dots, b_{p_s})\, \vec{x}\, \vec{y} + (c_{p_1}, \dots, c_{p_s})\, \vec{y}^{\,2} = 0,$$

where the operations are done componentwise. That is:

$$\mathbb{Z}_n \models x = 0 \wedge y = 0 \iff x^2 + bxy + cy^2 = 0,$$

with $b := \varphi^{-1}(b_{p_1}, \dots, b_{p_s})$ and $c := \varphi^{-1}(c_{p_1}, \dots, c_{p_s})$. □□

The following Corollary is now evident:

Corollary 8.7 *A ring $\mathbb{Z}_n$ is disjunctive and conjunctive iff $n = p$ is a prime.*

Profesor S. Basarab remarked in a personal communication that one can get analogous results if one studies the more general class of finite quotients of Dedekind rings instead of the class $(\mathbb{Z}_n)_{n\in\mathbb{N}\setminus\{0\}}$ of the finite quotients of $\mathbb{Z}$. Then, inside of this class, the disjunctive rings are exactly the "local" rings, the conjunctive rings are exactly the products of fields and for rings which are simultaneously disjunctive and conjunctive we get the class of all finite commutative fields.

The goals of this appendix have been reached: we characterized disjunctivity and conjunctivity for a class of finite rings. Now we will show just two variations for the sake of entertainment.

First we remark that all the rings $\mathbb{Z}_n$ are adequate, because the relation $t \neq 0$ can be represented as a finite disjunction:

$$\mathbb{Z}_n \models\ t \neq 0\ \Leftrightarrow\ t = 1 \wedge t = 2 \wedge \cdots \wedge t = n \Leftrightarrow 1.$$

We remark that this relation can be defined using just one quantified equation in the case that $\mathbb{Z}_n$ is disjunctive.

Definition: We call a ring R **strongly adequate** with respect to a language L iff the unary relation $t \neq 0$ can be defined in R using an L-formula of the form $\exists\, x_1, \ldots, x_n\ P(t, x_1, \ldots, x_n) = 0$, where $P \in R[t, x_1, \ldots, x_n]$. In other words, the unary relation $t \neq 0$ is strongly L-diophantine in R.

The natural question to put is if there are other strongly adequate rings $\mathbb{Z}_n$ in addition to the disjunctive rings. The answer is negative:

Theorem 8.8 *A ring $\mathbb{Z}_n$ is strogly adequate iff $n = p^k$ is a prime power.*

Proof: We have already shown that these rings are strongly adequate, being disjunctive. Now let $n = pq$ be a product of relatively prime natural numbers (again not necessarily prime numbers) such that the ring $\mathbb{Z}_n$ is strongly adequate. That is, $(p, q) = 1$ and there is a polynomial $\tilde{P} \in \mathbb{Z}_{pq}[t, x_1, \ldots, x_n]$ such that:

$$\mathbb{Z}_{pq} \models\ t \neq 0\ \Leftrightarrow\ \exists\, x_1, \ldots, x_n\ \tilde{P}(t, x_1, \ldots, x_n) = 0.$$

We prefer again the language of congruences. Let $P \in \mathbb{Z}[t, x_1, \ldots, x_n]$ be a polynomial which projects on $\tilde{P}$ through the canonical epimorphism $\mathbb{Z} \to \mathbb{Z}_{pq}$. In $\mathbb{Z}_{pq}$ is true that $p \neq 0$ and $q \neq 0$, so over $\mathbb{Z}$ is it true that:

$$\begin{aligned} &\exists\, b_1, \ldots, b_n \quad P(q, b_1, \ldots, b_n) \equiv 0 \mod(pq), \\ &\exists\, c_1, \ldots, c_n \quad P(p, c_1, \ldots, c_n) \equiv 0 \mod(pq). \end{aligned}$$

This implies:

$$\begin{aligned} &\exists\, b_1, \ldots, b_n \quad P(q, b_1, \ldots, b_n) \equiv 0 \mod(q), \\ &\exists\, c_1, \ldots, c_n \quad P(p, c_1, \ldots, c_n) \equiv 0 \mod(p). \end{aligned}$$

This is already a difference between this proof and the other on disjunctive rings. We choose and fix such solutions b_i and c_i. As a direct application of the Chinese Remainder Theorem, possible because $(p,q)=1$, we find $a_i \in \mathbb{Z}$ so that for all i:

$$\begin{aligned} a_i &\equiv b_i \mod (q), \\ a_i &\equiv c_i \mod (p). \end{aligned}$$

Preserving the congruences we may substitute now the b_i's and the c_i's with the a_i's. Moreover we may substitute in both congruences p and q with 0's. We get:

$$\begin{aligned} P(0,a_1,\ldots,a_n) &\equiv 0 \mod (p), \\ P(0,a_1,\ldots,a_n) &\equiv 0 \mod (q). \end{aligned}$$

Using again the fact that p and q are relatively prime, we get:

$$P(0,a_1,\ldots,a_n) \equiv 0 \mod (pq).$$

This means of course that:

$$\mathbb{Z}_{pq} \models \exists\, \vec{x}\ \tilde{P}(0,\vec{x}) = 0,$$

which is in fact the contradiction $\mathbb{Z}_{pq} \models 0 \neq 0$. □□

We can give a general quantified equation to define $t \neq 0$ in $\mathbb{Z}_{p^k}$. Unfortunately it needs so many terms and variables, that it has at most a theoretical interest. We claim that over $\mathbb{Z}_{p^k}$ the existential formula

$$\exists\, x_1, x_2, \ldots, x_{p^k-2}\ \sum_{i=1}^{p^k-2} x_i^{p^k-p^{k-1}} + 1 + t = 0,$$

is equivalent with $t \neq 0$. We recall that over $\mathbb{Z}_{p^k}$ the following are true:

$$\begin{aligned} z^{p^k-p^{k-1}} = 0 &\Leftrightarrow z \in p\mathbb{Z}_{p^k}, \\ z^{p^k-p^{k-1}} = 1 &\Leftrightarrow z \in \mathcal{U}(\mathbb{Z}_{p^k}). \end{aligned}$$

If $t=0$ then:

$$\Big\{ \sum_{i=1}^{p^k-2} x_i^{p^k-p^{k-1}} + 1 \mid x_i \in \mathbb{Z}_{p^k} \Big\} = \{1,\ldots,p^k \Leftrightarrow 1\} \not\ni 0,$$

so the equation hasn't solutions. If $t=1$ one can choose the solution $x_1 = \cdots = x_{p^k-2} = 1$. In general, if $t = m \in \{1,\ldots,p^k \Leftrightarrow 1\}$ the solution $x_1 = \cdots = x_{p^k-m-1} = 1$ and $x_{p^k-m} = \cdots = x_{p^k-2} = 0$ satisfies our equation. The claim has been proved.

Our last example on finite rings is motivated by the following natural question: How strong must a condition on diophantine definability be in order to be satisfied only by the fields $\mathbb{Z}_p$? We have already seen that the fields $\mathbb{Z}_p$ are the only rings $\mathbb{Z}_n$ which are simultaneously disjunctive and conjunctive, but these are of course two conditions. The relation which should be strongly diophantine is the following:

Definition: Given any set M, we define the **Symbol of Kronecker** to be the function $\delta : M^2 \to \{0,1\}$ defined by:

$$\delta(x,y) := \begin{cases} 1, & \text{if } x = y, \\ 0, & \text{if } x \neq y. \end{cases}$$

Definition: A ring R will be called a **Kronecker ring** with respect to a language L if the Symbol of Kronecker (with 0 and 1 interpreted as elements of R) is strongly L-diophantine.

In the last definition we understood again by L an extension with constants of the formal language of rings. Because of the last theorem on the complement of 0 one could believe that the rings $\mathbb{Z}_n$ which are Kronecker are again those with $n = p^k$, but this is not true.

Theorem 8.9 *$\mathbb{Z}_n$ is a Kronecker ring iff $n = p$ is a prime.*

Proof: It is easy to see that the fields $\mathbb{Z}_p$ are Kronecker. The following definition is a quantifier-free equation and works also for $p = 2$:

$$\mathbb{Z}_p \models \delta(x,y) = z \;\Leftrightarrow\; z + (x \Leftrightarrow y)^{p-1} \Leftrightarrow 1 = 0.$$

For proving the other direction, let $\mathbb{Z}_n$ be a Kronecker ring. That is, for a polynomial $P \in \mathbb{Z}_n[x, y, z, x_1, \ldots, x_n]$:

$$\mathbb{Z}_n \models \delta(x,y) = z \;\Leftrightarrow\; \exists\, x_1, \ldots, x_n \; P(x, y, z, x_1, \ldots, x_n) = 0.$$

We observe that for all $x, y \in \mathbb{Z}_n$, $\delta(x,y) = \delta(0, x \Leftrightarrow y)$. If $Q(u, z, x_1, \ldots, x_n) := P(0, u, z, x_1, \ldots, x_n)$, we get that:

$$u \neq 0 \;\Leftrightarrow\; \exists\, x_1, \ldots, x_n \; Q(u, 0, x_1, \ldots, x_n) = 0.$$

We have just prove that a Kronecker ring must be strongly adequate with respect to the same language. In our case it means that $n = p^k$ is a power of prime. The behaviour of Q is described as follows:

$$\exists\, x_1, \ldots, x_n \; Q(u, z, x_1, \ldots, x_n) = 0 \;\Leftrightarrow\; (u = 0 \wedge z = 1) \vee (u \neq 0 \wedge z = 0).$$

Denote further $S(u, z, x_1, \ldots, x_n) := Q(u, 1 \Leftrightarrow z, x_1, \ldots, x_n)$. We get:

$$\exists\, x_1, \ldots, x_n \; S(u, z, x_1, \ldots, x_n) = 0 \;\Leftrightarrow\; (u = 0 \wedge z = 0) \vee (u \neq 0 \wedge z = 1).$$

We use this polynomial in order to show that our ring $\mathbb{Z}_{p^k}$ must be also conjunctive. If we do this, we are done, because the only square-free powers of primes are the primes themselves. We consider the following relation:

$$\mathcal{R}(x,y) \;\Leftrightarrow\; \exists\, x_1,\ldots,x_n \; S(x^{p^k-p^{k-1}}y \Leftrightarrow x \Leftrightarrow y, y^{p^k-p^{k-1}} \Leftrightarrow y, x_1,\ldots,x_n) = 0.$$

It implies that $y^{p^k-p^{k-1}} \Leftrightarrow y \in \{0,1\}$. If $y^{p^k-p^{k-1}} \Leftrightarrow y = 1$ and $y \in \mathcal{U}(\mathbb{Z}_{p^k})$ then one gets $1 \Leftrightarrow y = 1$, $y = 0$, which is a contradiction. If $y \in p\mathbb{Z}_{p^k}$ then $\Leftrightarrow y = 1 \in p\mathbb{Z}_{p^k}$, which is a new contradiction. So $y^{p^k-p^{k-1}} \Leftrightarrow y$ must be 0, which implies $y \in \{0,1\}$.

On the other hand the fact that the second coordinate of the solution for $S = 0$ is 0 implies that the first coordinate must be 0 too. That is, $x^{p^k-p^{k-1}}y \Leftrightarrow x \Leftrightarrow y = 0$. If $y = 1$, we get $x^{p^k-p^{k-1}} \Leftrightarrow 1 = x$, the same as $x^{p^k-p^{k-1}} \Leftrightarrow x = 1$. We had already this equation (in y!) and we know that it has no solution in $\mathbb{Z}_{p^k}$.

So y must be $= 0$, and it implies from $x^{p^k-p^{k-1}}y \Leftrightarrow x \Leftrightarrow y = 0$ that $x = 0$ too. We observe also that $\mathcal{R}(0,0)$ is true. We have proven that

$$\mathcal{R}(x,y) \;\Leftrightarrow\; (x = 0 \;\wedge\; y = 0).$$

So the ring $\mathbb{Z}_{p^k}$ in question accepts a diophantine definition for the relation $x = 0 \;\wedge\; y = 0$ which consists of only one quantified equation, i.e. the ring is also conjunctive. □□

8.2 The Theorems of Matiyasevich and Denef

We present the proofs for the well known Theorems of Matiyasevich and Denef. One reason to do this is to give a complete proof of the Isomorphism Theorem 6.1. The other is to show what kind of combinatorial complexity could be substituted by structural facts like the Isomorphism Theorem.

We prove the Theorem of Matiyasevich in the restricted form which was already suggested in 5.2:

Theorem 8.10 *There exists a Julia Robinson predicate $\rho(u,v)$ over $\mathbb{N}$ which is L-diophantine over $\mathbb{N}$ and $\mathbb{Z}$.*

We remember that the pairs of solutions for the Pell equation:

$$P_2: \quad v^2 \Leftrightarrow (2^2 \Leftrightarrow 1)y^2 = 1$$

have been denoted by $(2_u, 2'_u)$ respecting the tradition of Davis and Putnam. The Julia Robinson predicate was:

$$\rho(u,v) \longleftrightarrow v = 2_u \ \wedge \ u > 3.$$

For the readability we will change notations. We call the general solution of P_2 : $(2_u, \delta_u)$. Moreover, for the equation P_T given over $\mathbb{N}$ by a **number** $T \in \mathbb{N},\ T > 2$:

$$P_T: \quad v^2 \Leftrightarrow (T^2 \Leftrightarrow 1)y^2 = 1$$

we denote the solution by (T_u, θ_u). We made this choice in order to emphasize some similarities with Theorem 5.2. The following auxiliary facts on the Pell equation can be proved by induction and are exposed in many books which present the Theorem of Matiyassevich:

Lemma 8.11 *The solutions of the Pell equations have the following properties:*

Congruence (C)

$$\begin{aligned} T_n &\equiv 2_n \mod (T \Leftrightarrow 2), \\ \theta_n &\equiv \delta_n \mod (T \Leftrightarrow 2), \\ \theta_n &\equiv n \mod (T \Leftrightarrow 1). \end{aligned}$$

First Step Down (F)

$$\begin{aligned} \delta_m \,|\, \delta_n \quad &\Longleftrightarrow \quad m \,|\, n, \\ \delta_m^2 \,|\, \delta_n \quad &\Longleftrightarrow \quad m\delta_m \,|\, n. \end{aligned}$$

Second Step Down (S)

$$\delta_i \equiv \delta_j \mod (2_n) \Longrightarrow \begin{cases} i \equiv j \mod (2n) & \vee \text{ (or)} \\ i \equiv \Leftrightarrow j \mod (2n). \end{cases}$$

Inequality (I)

$$2n \leq \delta_n.$$

The lemma is true also if we substitute the equation P_2 by an arbitrary $P_a,\ a \neq T$.

Now we start the proof of the theorem. Our goal is to prove that the relation $v = 2_u$ is diophantine. We tried to make the proof shorter by not displaying the defining equations and using embeddings. That proof in its original form comes from Martin Davis and was presented also by Smorynski, see [Smorynski].

First we make an auxiliary construction. We write $y = \delta_u$. Of course $u\delta_u \mid u\delta_u$, so we may apply **F** to get:

$$\delta_u^2 \mid \delta_{u\delta_u} = \delta_{uy}.$$

Being solution of a Pell equation, the numbers 2_{uy} and δ_{uy} are relatively prime. We apply the Chinese Remainder Theorem and find a number $T \in \mathbb{N}$ such that:

$$\begin{aligned} T &\equiv 2 \mod (2_{uy}), \\ T &\equiv 1 \mod (\delta_{uy}). \end{aligned}$$

The number T defines the Pell equation P_T and we consider its solution (T_u, θ_u). We apply **C** to get:

$$\begin{aligned} T \Leftrightarrow 2 \ &| \ \theta_u \Leftrightarrow \delta_u, \\ T \Leftrightarrow 1 \ &| \ \theta_u \Leftrightarrow u. \end{aligned}$$

To sum up, the considered numbers satisfy the following divisibility relations:

$$\begin{array}{ccccccc} \delta_u^2 & | & \delta_{uy} & | & T \Leftrightarrow 1 & | & \theta_u \Leftrightarrow u, \\ & & 2_{uy} & | & T \Leftrightarrow 2 & | & \theta_u \Leftrightarrow \delta_u. \end{array}$$

The auxiliary construction is ready. Suppose that we have done it in the non-standard extension $\mathbb{N}^*$ of $\mathbb{N}$. Now we operate on the considered numbers with an embedding $\eta \in \mathfrak{End}(\mathbb{N}^*)$. The images of $(2_u, \delta_u)$ and $(2_{uy}, \delta_{uy})$ are still solutions of P_2, because $\eta(2) = 2$. We denote these images by $(2_k, \delta_k)$ and $(2_m, \delta_m)$ respectively, where $k, m \in \mathbb{N}^*$. Denote $\eta(T)$ by $\bar{T}$. The image of the pair (T_u, θ_u) is any solution of the equation $P_{\bar{T}}$ over $\mathbb{N}^*$. We denote it by $(\bar{T}_n, \bar{\theta}_n)$, again for an $n \in \mathbb{N}^*$.

The relation of divisibility is also diophantine and will be preserved by η. Our new situation is:

$$\begin{array}{cccccc} \delta_k^2 & | & \delta_m & | & \bar{T} \Leftrightarrow 1 & | & \bar{\theta}_n \Leftrightarrow \eta(u), \\ & & 2_m & | & \bar{T} \Leftrightarrow 2 & | & \bar{\theta}_n \Leftrightarrow \delta_k. \end{array}$$

Using **C** we get that $\bar{T} \Leftrightarrow 2 \,|\, \bar{\theta}_n \Leftrightarrow \delta_n$. Together with $2_m \,|\, \bar{T} \Leftrightarrow 2$ it means $2_m \,|\, \bar{\theta}_n \Leftrightarrow \delta_n$. From our array we read $2_m \,|\, \bar{\theta}_n \Leftrightarrow \delta_k$. We make the substraction of the two last relations and we write down the result like a congruence: $\delta_n \equiv \delta_k \mod (2_m)$. We apply **S** to get:

$$n \equiv \pm k \mod (2m).$$

From our array we read $\delta_k^2 \,|\, \delta_m$. We apply **F** in the other direction, it implies $k\delta_k \,|\, m$. So $k\delta_k \,|\, 2m \,|\, n \mp k$. We have got:

$$n \equiv \pm k \mod (\delta_k).$$

We get again from the array $\delta_k \,|\, \bar{T} \Leftrightarrow 1$. Comparing with the new instance of **C**: $\bar{\theta}_n \equiv n \mod (\bar{T} \Leftrightarrow 1)$, we obtain $\delta_k \,|\, \bar{\theta}_n \Leftrightarrow n$. Consulting the array for a last time, we get $\delta_k \,|\, \bar{\theta}_n \Leftrightarrow \eta(u)$. It implies:

$$n \equiv \eta(u) \mod (\delta_k).$$

Putting the last two more important relations together and applying the associativity, we reach finally:

$$\eta(u) \equiv \pm k \mod (\delta_k)$$

As last step we consider two instances of **I**. First $2k \leq \delta_k$. On the similar instance $2u \leq \delta_u$ we operate with η. We know already that the order on $\mathbb{N}$ is diophantine definable, that's why all embeddings are monotonly increasing. So $2\eta(u) \leq \delta_k$. Being both of $\eta(u)$ and k positive, if $\eta(u) \equiv \Leftrightarrow k \mod (\delta_k)$ we should have:

$$\delta_k \,|\, \eta(u) + k \leq 2 \max(\eta(u), k) \leq \delta_k,$$

which is possible just if $\eta(u) = k$. In the other case $\eta(u) \equiv k \mod (\delta_k)$ and are both of them $< \delta_k$, so anyway $\eta(u) = k$. We have got $\eta(\delta_u) = \delta_{\eta(u)}$, so $\eta(2_u) = 2_{\eta(u)}$ and:

$$v = 2_u \Leftrightarrow\!\!\rightarrow \eta(v) = 2_{\eta(u)}.$$

Using 1.1 and the fact that $\mathbb{N}$ is a diophantine algebraic structure, we have shown that $\rho(u, v)$ is a diophantine relation in $\mathbb{N}$. We have chosen the notations such that some similarities with Theorem 5.3 would be emphasized. □□

Let us speak now about the Theorem of Denef. We present the original proof from [Denef 3].

We remember first to have denoted by $Y_m(T)$ the second component of a solution (X, Y) for the Pell equation P_T:

$$X^2 \Leftrightarrow (T^2 \Leftrightarrow 1)Y^2 = 1$$

over any polynomial ring, and the fact that the relation $m \in \mathbb{N} \wedge F = Y_m$ is diophantine over $\mathbb{Z}[T]$ is equivalent with:

$$m \in \mathbb{N} \wedge X^2 \Leftrightarrow (T^2 \Leftrightarrow 1)Y^2 = 1 \wedge T \Leftrightarrow 1 \mid Y \Leftrightarrow m.$$

The last divisibility represents the evaluation of Y in 1. Evaluation (F, k, n) is also a diophantine relation over $\mathbb{Z}[T]$. Not so trivial is the following lemma:

Lemma 8.12 (Yves Pourchet) *The predicate*

$$\mathcal{P}(F) :\Longleftrightarrow \forall x \in \mathbb{R} \quad F(x) \geq 0.$$

is L-diophantine in $\mathbb{Z}[T]$.

The Theorem of Pourchet, see [Pourchet], says that all positive definite polynomial in $\mathbb{Q}[T]$ is the sum of five squares in $\mathbb{Q}[T]$. Using a common denominator, we translate this fact easily to a diophantine definition in $\mathbb{Z}[T]$.

Now let $\theta : \mathbb{N} \to \mathbb{Z}[T]$ be a recursive presentation of $\mathbb{Z}[T]$. We have to prove the following:

Theorem 8.13 (Jan Denef) *All the recursive presentations* $\theta : \mathbb{N} \to \mathbb{Z}[T]$ *are LT-diophantine over* $\mathbb{Z}[T]$.

Like for the Theorem of Matiyasevich, we start with an auxiliary construction. Consider an arbitrary $n \in \mathbb{N}$ and its image $\theta(n)$. We denote $d =$ degree $(\theta(n))$. We know that degree $(Y_{d+2}) = d + 1$, so we can be sure to find a $c \in \mathbb{N}$ such that:

$$\forall x \in \mathbb{R} \quad \theta(n)(x)^2 \leq Y_{d+2}^2(x) + c.$$

We recall the convention to denote with i, j, k just variables which vary through finite intervals of natural numbers. There is a number $b \in \mathbb{N}$ such that:

$$\forall i \leq d \qquad Y_{d+2}^2(i) < b.$$

As last step of the construction, we denote:

$$v = \theta(n)(2b + 2c + d).$$

We remark that $v \in \mathbb{Z}$. The set $\{(n, d, c, b, v)\}$ of all the possible 5-tuples obtained as above is a recursively enumerable relation over $\mathbb{Z}$, so it is diophantine over $\mathbb{Z}[T]$ following the Theorem of Davis and Putnam 5.3. Now we consider the construction to be done over $\mathbb{Z}[T]^*$ and we operate on it with an arbitrary

embedding $\eta \in \mathfrak{End}_{\mathbb{Z}[T]}(\mathbb{Z}[T]^*)$. We denote $\eta(a) := \bar{a}$. The set of all 5-tuples is a diophantine relation, hence we get at once:

$$(\bar{n}, \bar{d}, \bar{c}, \bar{b}, \bar{v}).$$

All this information concerns $\theta^*(\bar{n})$. About $\overline{\theta^*(n)}$ we may say only that:

$$\begin{aligned} \forall x \in \mathbb{R}^* \quad & \overline{\theta^*(n)}^2(x) \leq Y^2_{\bar{d}+2}(x) + \bar{c}, \\ & \bar{v} = \overline{\theta^*(n)} \ \ (2\bar{b} + 2\bar{c} + \bar{d}). \end{aligned}$$

From the first relation, we may already deduce degree $(\overline{\theta^*(n)}) \leq \bar{d} + 1$ because degree $(Y_{n+1}) = n$. From the corresponding information contained in the 5-tuple, one has degree $(\theta^*(\bar{n})) \leq \bar{d} + 1$. To conclude:

$$\text{degree } (\overline{\theta^*(n)} \Leftrightarrow \theta^*(\bar{n})) \leq \bar{d} + 1.$$

It is easy to see that:

$$(\overline{\theta^*(n)} \Leftrightarrow \theta^*(\bar{n})) \ (2\bar{b} + 2\bar{c} + \bar{d}) = 0.$$

The constant b was chosen depending only on the Davis-Putnam polynomials Y_n, so we can dominate the inequalities in the following way: For all $0 \leq i \leq \bar{d}$,

$$\begin{aligned} |\, \theta^*(\bar{n})(i) \,| \ &\leq \ |\, \theta^*(\bar{n})^2(i) \,| \ < \ \bar{b} + \bar{c}, \\ |\, \overline{\theta^*(n)}(i) \,| \ &\leq \ |\, \overline{\theta^*(n)}^2(i) \,| \ < \ \bar{b} + \bar{c}. \end{aligned}$$

Substracting, we get: For all $0 \leq i \leq \bar{d}$,

$$|\, (\overline{\theta^*(n)} \Leftrightarrow \theta^*(\bar{n})) \ (i) \,| \ < \ 2\bar{b} + 2\bar{c}.$$

Now we have got enough information to prove that this polynomial is in fact identically 0. Suppose that it was not. Then we must have a polynomial $S \in \mathbb{Z}[T]^*$, $S \neq 0$ such that:

$$\overline{\theta^*(n)} \Leftrightarrow \theta^*(\bar{n}) \ = \ (2\bar{b} + 2\bar{c} + \bar{d} \Leftrightarrow T)S.$$

There must be a k, $0 \leq k \leq \bar{d}$, with $S(k) \neq 0$ because a polynomial of degree $\leq \bar{d}$ which is not identically 0 can not have $d + 1$ zeroes. We remark that the set of zeros of a nonstandard polynomial is a $*$-finite internal set, which is subject of the standard operator **Cardinality**, with values in $\mathbb{N}^*$. It respects the length of the nonstandard intervals. Hence:

$$|\, (\overline{\theta^*(n)} \Leftrightarrow \theta^*(\bar{n})) \ (k) \,| \ \geq \ 2\bar{b} + 2\bar{c} + \bar{d} \Leftrightarrow k \ \geq \ 2\bar{b} + 2\bar{c},$$

which is a contradiction. In conclusion, for an arbitrary $n \in \mathbb{N}^*$,

$$\overline{\theta^*(n)} \ = \ \theta^*(\bar{n}),$$

which means that the recursive presentation θ is diophantine in $\mathbb{Z}[T]$ after the new version of the Theorem of Beth 1.1.

□□

Bibliography

[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, 1963

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

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

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

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

[Denef-Lipshitz] **Jan Denef, Leonhard Lipshitz**: *Diophantine sets over some Rings of Algebraic Integers* The Journal of the London Mathematical Society 18.3, 1978

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

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

[Lipshitz] **Leonhard Lipshitz**: *Diophantine correct models of Arithmetic* Procedings of the A.M.S. 73(1), 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, 1980

[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, 1988

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

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

[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, 1959

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

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

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

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

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

[Zahidi] **Karim Zahidi**: *to appear in* Proceedings of the A.M.S.