Charles University in Prague
Faculty of Mathematics and Physics

DOCTORAL THESIS

Petr Glivický

Study of Arithmetical Structures and Theories with Regard to Representative and Descriptive Analysis

Department of Theoretical Computer Science
and Mathematical Logic

Supervisor of the doctoral thesis: Doc. RNDr. Josef Mlček, CSc.

Study programme: Mathematics
Specialization: Algebra, Number Theory and Mathematical Logic

Prague 2013

I declare that I carried out this doctoral thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that the Charles University in Prague has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 paragraph 1 of the Copyright Act.

In Prague, June 12, 2013 Petr Glivický

Název práce: Studium aritmetických struktur a teorií s ohledem na reprezentační a deskriptivní analýzu

Autor: Mgr. Petr Glivický
Katedra teoretické informatiky a matematické logiky
Matematicko-fyzikální fakulta
Univerzita Karlova v Praze
Malostranské náměstí 25, 118 00 Praha 1
e-mail: petrglivicky@gmail.com

Vedoucí práce: Doc. RNDr. Josef Mlček, CSc.
Katedra teoretické informatiky a matematické logiky
Matematicko-fyzikální fakulta
Univerzita Karlova v Praze
Malostranské náměstí 25, 118 00 Praha 1
e-mail: josef.mlcek@mff.cuni.cz

Katedra: Katedra teoretické informatiky a matematické logiky
Matematicko-fyzikální fakulta
Univerzita Karlova v Praze
Malostranské náměstí 25, 118 00 Praha 1

Abstrakt:

Jsme motivováni otázkou vztahu lokálních a globálních vlastností operace o ve struktuře tvaru $\langle \mathcal{B}, o \rangle$ s ohledem na aplikaci pro studium modelů $\langle \mathcal{B}, \cdot \rangle$ Peanovy aritmetiky, kde $\mathcal{B}$ je model aritmetiky Presburgerovy. Zajímá nás zejména problém závislosti, který formulujeme jako otázku určení uzávěru závislosti

$$\mathrm{icl}^O(E) = \{\overline{d} \in B^n; (\forall o, o' \in O)(o \upharpoonright E = o' \upharpoonright E \Rightarrow o(\overline{d}) = o'(\overline{d}))\},$$

kde $\mathcal{B}$ je struktura, O množina n-árních operací na B a $E \subseteq B^n$. Ukážeme, že tento problém lze převést na otázku definovatelnosti v jisté expanzi $\mathcal{B}$. Speciálně, je-li $\mathcal{B}$ saturovaný model Presburgerovy aritmetiky a O množina všech (saturovaných) peanovských součinů na $\mathcal{B}$, dokážeme, že pro $a \in B$ je $\mathrm{icl}^O(\{a\} \times B)$ nejmenší možný, tj. obsahující právě ty dvojice $(d_0, d_1) \in B^2$, kde jedno z d_i je tvaru $p(a)$ pro nějaký polynom $p \in \mathbb{Q}[x]$.

Uvedená problematika úzce souvisí s deskriptivní analýzou lineárních teorií, což jsou (až na změnu jazyka) teorie jistých diskrétně uspořádaných modulů nad určitými diskrétně uspořádanými obory integrity. Dokážeme tvrzení o eliminaci kvantifikátorů v lineárních teoriích a nalezneme prvomodely jejich jednoduchých kompletních extenzí. Provedeme detailní analýzu definovatelných množin v modelu $\mathcal{A}$ lineární teorie a odvodíme, že každá definovatelná množina je sjednocením lineárních obrazů mnohostěnů v A^n pro nějaké $n \in \mathbb{N}$.

Zvláště důležitým příkladem lineární teorie je lineární aritmetika LA (přesněji její „$\mathbb{Z}$-verze" ZLA) – aritmetická teorie s plnou indukcí rozšiřující Presburgerovu aritmetiku o násobení jediným nestandardním prvkem. Jako důsledek výše uvedeného dokážeme, že LA je modelově kompletní (eliminační množina je tvořena primitivně pozitivními formulemi) a rozhodnutelná, nalezneme její jednoduché kompletní extenze a sestrojíme jejich prvomodely. Dokážeme též, že modely LA jsou až na elementární ekvivalenci právě nehlavní ultraprodukty struktur $\langle \mathbb{N}, 0, 1, +, \leq, n \cdot \_ \rangle$ s $n \in \mathbb{N}$.

Jako algebraickou aplikaci uvedených výsledků ukážeme, že prvomodely jednoduchých kompletních extenzí LA určují 2^ω různých oborů integrity R s $\mathbb{Z}[x] \subseteq R \subseteq \mathbb{Q}[x]$, které jsou ω-stage euklidovské, ale nejsou k-stage euklidovské pro žádné $0 < k \in \mathbb{N}$. To řeší problém položený G. E. Cookem v [Coo76].

Klíčová slova:

lineární aritmetika, eliminace kvantifikátorů, Peanova aritmetika, extenze Presburgerovy aritmetiky, kvazieuklidovské okruhy

Title: Study of arithmetical structures and theories with regard to representative and descriptive analysis

Author: Mgr. Petr Glivický
Dept. of Theoretical Computer Science and Mathematical Logic
Faculty of Mathematics and Physics
Charles University in Prague
Malostranské náměstí 25, 118 00 Praha 1
e-mail: petrglivicky@gmail.com

Supervisor: Doc. RNDr. Josef Mlček, CSc.
Dept. of Theoretical Computer Science and Mathematical Logic
Faculty of Mathematics and Physics
Charles University in Prague
Malostranské náměstí 25, 118 00 Praha 1
e-mail: josef.mlcek@mff.cuni.cz

Department: Dept. of Theoretical Computer Science and Mathematical Logic
Faculty of Mathematics and Physics
Charles University in Prague
Malostranské náměstí 25, 118 00 Praha 1

Abstract:

We are motivated by a problem of understanding relations between local and global properties of an operation o in a structure of the form $\langle \mathcal{B}, o \rangle$, with regard to an application for the study of models $\langle \mathcal{B}, \cdot \rangle$ of Peano arithmetic, where $\mathcal{B}$ is a model of Presburger arithmetic. We are particularly interested in a dependency problem, which we formulate as the problem of describing the dependency closure

$$\mathrm{icl}^O(E) = \{\overline{d} \in B^n; (\forall o, o' \in O)(o \restriction E = o' \restriction E \Rightarrow o(\overline{d}) = o'(\overline{d}))\},$$

where $\mathcal{B}$ is a structure, O a set of n-ary operations on B, and $E \subseteq B^n$. We show, that this problem can be reduced to a definability question in certain expansion of $\mathcal{B}$. In particular, if $\mathcal{B}$ is a saturated model of Presburger arithmetic, and O is the set of all (saturated) Peano products on $\mathcal{B}$, we prove that, for $a \in B$, $\mathrm{icl}^O(\{a\} \times B)$ is the smallest possible, i.e. it contains just those pairs $(d_0, d_1) \in B^2$ for which at least one of d_i equals $p(a)$, for some polynomial $p \in \mathbb{Q}[x]$.

We show that the presented problematics is closely connected to the descriptive analysis of linear theories. That are theories, models of which are – up to a change of the language – certain discretely ordered modules over specific discretely ordered integral domains. We prove a quantifier elimination result in linear theories, and we find the prime models of their simple complete extensions. We perform a detailed analysis of definable sets in a model $\mathcal{A}$ of a linear theory, and show that definable sets are unions of linear images of polyhedra in A^n, with $n \in \mathbb{N}$.

A particularly important example of linear theories is the linear arithmetic LA (more precisely, its "$\mathbb{Z}$-like" variant ZLA). That is an arithmetical theory with the full induction, which extends Presburger arithmetic by multiplication by a single nonstandard element. As a corollary of the results above, we show that LA is model-complete (elimination set consists of primitive positive formulas) and decidable, we find its simple complete extensions and construct their prime models. We also prove that models of LA are, up to elementary equivalence, exactly all non-principal ultraproducts of the structures $\langle \mathbb{N}, 0, 1, +, \leq, n \cdot \_ \rangle$, with $n \in \mathbb{N}$.

As an algebraic application of the presented results, we show that the prime models of the simple complete extensions of LA determine 2^ω different integral domains R, with $\mathbb{Z}[x] \subseteq R \subseteq \mathbb{Q}[x]$, which are ω-stage Euclidean, but not k-stage Euclidean, for any $0 < k \in \mathbb{N}$. This solves the problem posed by G. E. Cooke in [Coo76].

Keywords:

linear arithmetic, quantifier elimination, Peano arithmetic, extensions of Presburger arithmetic, quasi-Euclidean rings

Motto

Wir müssen wissen.
Wir werden wissen.

– David Hilbert

To everybody who will read with joy.

Acknowledgment

This thesis would not have been possible without support, advice and selfless help of many people. The following lines are devoted to them.

My deepest gratitude belongs to Josef Mlček, my advisor and the true mentor. That were many inspiring discussions with him, what have provoked my enthusiasm for the problematics presented in this thesis, and his willing support and guidance carried me through the process of its creation. His trans-disciplinary knowledge and interests combined with his friendly attitude caused that working with him has been constantly broadening my horizons.

I would like to express my thanks to my friend, colleague and everlasting badminton rival Jan Šaroch. His persistent interest in the research presented in this thesis has motivated me to keep working. He has also read large portions of the text and made many valuable comments. Jan's contribution was crucial especially for chapter 3. This chapter is almost identical to our joint paper [GŠ13], which was Jan's initiative and, from more than a half, his work.

I might have easily end up overwhelmed by the amount of administrative tasks connected to my study and work. The only reason I did not, was thanks to Mrs. Petra Novotná and her frequent, invaluable help.

A significant part of the research presented in the thesis was carried out within the project *Representative and Descriptive Analysis of Arithmetical Structures and Theories*, supported by the grant *GAUK 4372/2011* by the Grant Agency of the Charles University in Prague.

I made a considerable advance in the work during my short stay in the inspiring environment of the National University of Singapore. My thanks for providing me this opportunity belong to doc. Antonín Kučera. The visit was generously supported by the Asian Initiative for Infinity.

During the period of writing this thesis, I attended dozens of another conferences, workshops and summer or winter schools, which inspired me in my work. Part of the travel costs was financed by a number of governmental and privately funded organizations. All of them deserve my acknowledgment.

Last but not least, I would like to thank my family for their support, and Ria for being so tolerant and for letting me spend many hours and days with my work rather than with her.

In Prague, June 12, 2013 — Petr Glivický

Contents

Introduction

In this thesis, we are motivated by a problem of understanding relations between local and global properties of an operation o in a first-order structure of the form $\langle \mathcal{B}, o \rangle$, with a particular interest in the case where $\mathcal{B}$ is a model of Presburger arithmetic Pr and o is a "Peano product" on $\mathcal{B}$, i.e. $\langle \mathcal{B}, o \rangle$ is a model of Peano arithmetic P.

Dependency problem

The problem above may be specified as follows: Given a "background model" $\mathcal{B}$ and a set O of all n-ary operations on B satisfying certain global property (e.g. being a Peano product), we want to describe the *dependency closure*

$$\mathrm{icl}^O(E) = \{\overline{d} \in B^n; (\forall o, o' \in O)(o \restriction E = o' \restriction E \Rightarrow o(\overline{d}) = o'(\overline{d}))\},$$

for $E \subseteq B^n$ (see 2.1.1). We call this task the $(\mathcal{B}, O, E)$*-dependency problem.*

A *Peano dependency problem* is a $(\mathcal{B}, O, E)$-dependency problem where $\mathcal{B}$ is a (saturated) model of Pr and O is the set of all (saturated) Peano products on $\mathcal{B}$. Its solution may contribute to new constructions of models of arithmetic, different from the known methods (cuts, end-extensions, ultraproducts, …; see the historical remark at the end of the introduction).

Reduction to definability

A $(\mathcal{B}, O, E)$-dependency problem with saturated $\mathcal{B}$ may be solved by studying a definability problem in certain expansion of $\mathcal{B}$, called a *fixator*. This is formulated in the *DD-theorem* 2.1:2.

In chapter 2, Proposition 2.2:1 and Corollary 2.2:2, we completely solve an important case of the Peano dependency problem, for $E = E_a = \{a\} \times B$, with a nonstandard (an *"a-slice"*). We prove that, in this case, $\mathrm{icl}(E)$ is as small as possible, i.e. it contains only the trivially dependent points $\overline{d} = (d_0, d_1)$ where at least one of d_i equals $p(a)$, for some polynomial $p \in \mathbb{Q}[x]$.

By the DD-theorem, the key for the proof is understanding definability in the respective fixator. The fixator is a model of *linear arithmetic*[1] LA – an extension

[1] The name "linear arithmetic" is used somewhat vaguely and/or inconsistently through the literature. It denotes more different concepts where an important role is played by inequalities of "linear" combinations of "unknowns". In this thesis, linear arithmetic denotes the first order theory LA from section 1.1.4.1 (or an equivalent theory).

of Pr by multiplication by a nonstandard scalar, with the full induction scheme. The needed definability results follow from Corollary 1.4:7 1) of the *Main Theorem on Linear Theories* 1.3:4.

Peano products

Proposition 2.2:1, in particular, enables us to construct interesting examples of (Peano) products. The first of them are *meeting pairs of Peano products*, constructed in Corollary 2.3:1. Another is a construction of a Robinson product which satisfies a portion of induction (Proposition 2.3:2).

Corollary 2.4:2 solves the question of possible interpolation of a Peano product through a given point $\langle \bar{b}, d \rangle \in B^3$.

Linear theories

The mentioned fundamental Main Theorem on Linear Theories 1.3:4 is a result of the study of chapter 1 on linear theories – a class of theories which generalize the linear arithmetic LA. Models of linear theories are (up to a change of the language) certain (integrally-divisible) discretely ordered modules over specific (regularly quasi-Euclidean and with degrees) discretely ordered integral domains.

Linear theories are of its own interest, and a large part of this thesis is devoted to the analysis of them.

Besides a quantifier elimination result for linear theories, contained in the Main Theorem on Linear Theories 1.3:4, we perform a detailed analysis of terms (the *Harmonic Form Theorem* 1.3:6) and definable sets and functions in their models (corollaries of the *Bases Theorem* 1.3:8). In particular, we prove that every definable set in a model $\mathcal{A}$ of a linear theory is a finite union of linear images of polyhedra in A^k, for some $k \in \mathbb{N}$.

The theorems 1.3:4, 1.3:6 and 1.3:8 are proven in section 1.5. The proofs are based on three fundamental Propositions – S, H and B (1.5:2, 1.5:3 and 1.5:4) – and on a calculus which is a generalization of the calculus of continued fractions.

Let us note that linear theories can be understood as extending both of the following – the theory of $\mathbb{Z}$-groups (which is, in fact, the simplest linear theory) and the theory of modules over some associative ring (the first one is extended by allowing multiplication by some non-integer scalars, the second one by adding an ordering). From this point of view, our results on linear theories generalize the classical results of Mojżesz Presburger [Pre29] on $\mathbb{Z}$-groups (Presburger arithmetic) and, partially, the results of Walter Baur [Bau76] and Leonard Monk [Mon75] on modules.

Two-sorted quantifier elimination for ordered ring-modules

In section 1.6, we apply our method of proof of the Theorem 1.3:4 to generalize and strengthen known quantifier elimination results for two-sorted structures of the type "ring-module" (or "ordered ring-ordered module").

Our Corollary 1.6:2 of Theorem 1.6:1 states a quantifier elimination result for doded-modules (see 1.6) – certain two-sorted structures of the type "ordered ring-ordered module" (in fact, just two-sorted variants of models of linear theories). This is an ordered analogue of the quite well-known result by Lou van den Dries and Jan Holly in [vdDH92] for two-sorted unordered modules and it strengthens the result by Volker Weispfenning in [Wei97, Theorem 4.1] for two-sorted discretely ordered modules over the ring $\mathbb{Z}$ of integers (more precisely for the models of a two-sorted variant of Presburger arithmetic). See section 1.6 for more details.

Let us note that in [vdDH92] the problem of generalizing the results to ordered modules (even for the simplest case of the module $\mathbb{Z}$ of integers) is considered as "very interesting" but as one that "seems to be very hard".

Our proof of Corollary 1.6:2 requires substantially different methods than those used in [vdDH92] or [Wei97]. The absence of ordering in [vdDH92] is, clearly, a great simplification. In Remark 1.5:1, we point out the reasons why the general case stated in Corollary 1.6:2 is essentially more difficult than the Presburger case from [Wei97].

Properties of linear arithmetic

As an application of the Main Theorem on Linear Theories 1.3:4 and results from section 1.2, we find basic model-theoretic properties of LA (Corollary 1.4:7) – we prove that LA is decidable and model-complete (in fact, that every formula is in LA equivalent to a disjunction of primitive positive formulas), we describe all its simple complete extensions and construct their prime models. Models of LA are characterized as non-principal ultraproducts of definable expansions of the standard model $\langle \mathbb{N}, 0, 1, +, \leq \rangle$ (Corollary 1.4:8). It is also proven that LA is equivalent to a theory La (see 1.1.4.1) which arises from LA by replacing the induction scheme by the scheme of integral divisibility (see 1.1.2). All is done in section 1.4.2.

Although the properties of LA are similar to those of Pr, the proof is much more difficult. This is, as we will argue in Remark 1.5:1, mainly due to the fact that, for $n \in \mathbb{N}$, any remainder modulo n may be expressed as one of finitely many constant terms, while this is no more true for n non-standard.

The results on LA contribute to the ongoing research on extensions of Presburger arithmetic (see the survey paper [Bès01] for details concerning this problematic).

An application to the theory of quasi-Euclidean integral domains

Chapter 3 contains an interesting application of results from chapter 1 to the theory of quasi-Euclidean integral domains. We find 2^ω different integral domains R, with $\mathbb{Z}[x] \subseteq R \subseteq \mathbb{Q}[x]$, which are quasi-Euclidean but not k-stage Euclidean, for any $0 < k \in \mathbb{N}$. This solves an open question of George E. Cooke from [Coo76].

The domains R are constructed from the prime models of simple complete extensions of LA by taking their mirror "$\mathbb{Z}$-like" versions and endowing them with a natural ring structure.

Remark: Historical remark on constructions of models of Peano arithmetic

Nonstandard models of Peano arithmetic were implicitely found by Kurt Gödel as a consequence of his famous incompleteness theorems [Göd31], and were explicitely constructed (using an ultraproduct) by Thoralf Skolem only a few years later ([Sko33] and [Sko34]).

However, an enormous complexity of such models was apparent already in those days. By the incompleteness theorems, no class of elementary equivalent models of P can be recursively axiomatized. Moreover, Gödel's proof showed that each model of P contains such a complicated structure as a model of the finite set theory. These results were supported in late fifties by a theorem of Stanley Tennenbaum [Ten59], which stated that in every countable nonstandard model of P both, addition and multiplication, are non-recursive.

Despite of these facts, Robert MacDowell's and Ernst Specker's work on elementary end-extensions [MS61] showed that some constructions of interesting nonstandard models are possible. The results of Jeff Paris, Laurie Kirby and Leo Harrington ([Par78], [KP82] and [PH77]), obtained by methods of cuts and indicators, provided the first examples of natural combinatorial statements, true in the standard model but unprovable in P.

Chapter 1

Descriptive Analysis of Linear Theories

In this chapter, we are motivated by the problem of understanding the theory of linear arithmetic (LA). LA is an arithmetical theory in the language $L^{lin} = \langle 0, 1, +, \underline{a}, \leq \rangle$, where $\underline{a}$ is intended as multiplication by a single element (see 1.1.4.1 for the axiomatic). It is a theory with the full induction for its language, and as such it should be understood as standing between Presburger (Pr) and Peano (P) arithmetics.

Our study of LA is led not only by our interest in the problem itself; in chapter 2 we will use it to prove non-trivial results about the structure of Peano products on a fixed saturated model of Pr (a more direct approach to this can be found in [Gli09]).

Instead of the "$\mathbb{N}$-like" theory LA, we are going to work in its equivalent, but technically more pleasant, "$\mathbb{Z}$-like" variant, which is denoted ZLA (see 1.1.4.2). Similarly, the $\mathbb{Z}$-like variant of Presburger arithmetic (additive arithmetic AA; see 1.1.3.1) is the theory of $\mathbb{Z}$-groups ($\mathbb{Z}$-additive arithmetic; ZAA see 1.1.3.2).

The theories ZLA and ZAA are examples of what we call linear theories. That are theories, models of which are – up to a change of language – some (expansions by constants of) discretely ordered modules over certain discretely ordered integral domains. The module is required to be integrally-divisible over the domain (i.e. integer division works), and the domain needs to be regularly quasi-Euclidean (i.e. the regular Euclidean algorithm stops in finite time) and has to have degrees (such that $\deg(r) \leq \deg(q) \Leftrightarrow |r| \leq n|q|$ for some $n \in \mathbb{N}$); see section 1.3.1 for the detailed definitions. We consider the expansion

$$\mathcal{F} = \langle F, 0, 1, +, -, \leq, r, c, q^{-1} \rangle_{r \in \mathrm{D}_{\mathcal{F}}, c \in \mathrm{C}_{\mathcal{F}}, q \in {}^{+}\mathrm{D}_{\mathcal{F}}}$$

of a model described above by definitions of integral division q^{-1} by all positive scalars q from its integral domain $\mathsf{D}_{\mathcal{F}}$ and by some definable constants c, such that $\mathrm{C}_{\mathcal{F}}$ is the universe of a substructure of $\mathcal{F}$. Such an expansion $\mathcal{F}$ is called a lineal (see 1.3.1.3).

The main results of this chapter are the following three theorems, formulated in section 1.3.2: the Main Theorem on Linear Theories 1.3:4, the Harmonic Form Theorem 1.3:6 and the Bases Theorem 1.3:8.

The Main Theorem on Linear Theories states that in every lineal each nonempty set definable over parameters $\overline{a}$ contains the value $t(\overline{a})$ of a term t. Moreover, t may be chosen "almost uniformly" with respect to different lineals and different tuples $\overline{a}$; see concepts of solvability (1.2.2.1) and almost uniform solvability (1.2.2.3). As a corollary of the Main Theorem, we get a quantifier elimination result for linear theories; in particular, we will see that every lineal admits quantifier elimination. We also describe all simple complete extensions of a given linear theory T and their prime models (see Corollary 1.3:5).

Working in a fixed lineal, we show that every term can be, up to a "finite noise", equivalently written in harmonic form, i.e. as a linear combination of the basic harmonic functions r^{-1} (see 1.3.2.2.1), and every formula is equivalent to a harmonic one. This is the Harmonic Form Theorem 1.3:6. Moreover, we perform a detailed analysis of definable sets in a lineal $\mathcal{F}$ and give a geometric characterization of them as unions of linear images of polyhedra in F^k, for some $k \in \mathbb{N}$. A similar characterization of definable functions as "piecewise linear" is also stated (see Corollary 1.3:9 of the Bases Theorem 1.3:8). The last result justifies the name "linear theory".

As we mentioned in the Introduction chapter, the results above generalize the classical results of Presburger [Pre29] on $\mathbb{Z}$-groups and, partially, of Baur [Bau76] and Monk [Mon75] on modules.

We apply the Main Theorem on Linear Theories to determine basic properties of the $\mathbb{Z}$-linear arithmetic ZLA (see Theorem 1.4:5). It is shown that ZLA is model-complete (in fact, that every formula is in LA equivalent to a disjunction of primitive positive formulas) and decidable. The simple complete extensions of ZLA correspond to elements $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, where $\mathbb{P}$ denotes the set of prime numbers, and $\mathbb{J}_p$, for $p \in \mathbb{P}$, the set of all p-adic integers. The prime models of the complete extensions are constructed as structures $\mathcal{C}_\tau$, with $\mathbb{Z}[x] \subseteq \mathrm{C}_\tau \subseteq \mathbb{Q}[x]$. As a corollary, it is shown that the models of ZLA are, up to elementary equivalence, just ultraproducts $\mathcal{Z}_\mathcal{U} = (\prod_{n\in\mathbb{N}}\langle\mathbb{Z}, 0, 1, +, -, \underline{n}\cdot\_, \leq\rangle)/_\mathcal{U}$, where $\mathcal{U}$ is a non-principal ultrafilter on $\mathbb{N}$ (see Corollary 1.4:6).

Let us note that the sets C_τ, endowed with the structure of a ring, are examples of integral domains, which are ω-stage Euclidean but not k-stage Euclidean for any $k \in \mathbb{N}$. This answers the open question by G. E. Cooke from [Coo76]; see chapter 3 for more details on this topic.

The mentioned results about ZLA can be almost automatically translated to similar statements about LA (see Corollary 1.4:7) and understood as stating that LA is a theory typologically similar to Pr (and far away from P). Whether the same is true also for the theory LA^2 (extension of Pr by multiplication by two independent scalars; see 1.1.5.1), is posed as the Open question 1.

Our quantifier elimination and decidability results for LA contribute to the long and ongoing research on extensions of Presburger arithmetic. A good survey paper for this problematics is [Bès01]. [1]

Our proof of the three main theorems relies on a calculus of terms in a lineal. This calculus can be seen as a generalization of the calculus of continued fractions. Basic steps of the proof are sketched in 1.5.1.

In section 1.6, we formulate an easy consequence of the proof – a quantifier elimination result (Corollary 1.6:2 of Theorem 1.6:1) for certain two-sorted structures of the type "ordered ring-ordered module" (in fact, just for two-sorted variants of models of linear theories). As we already mentioned in the Introduction, this generalizes results by Lou van den Dries and Jan Holly in [vdDH92] for two-sorted unordered modules and by Volker Weispfenning in [Wei97] for two-sorted discretely ordered modules over the ring $\mathbb{Z}$ of integers (more precisely for the models of a two-sorted variant of Presburger arithmetic). See section 1.6 for more details.

1.1 Arithmetical theories

We state here a few axiomatics of theories which will play a role of important and motivating examples in our further explanation.

All the presented theories are "arithmetics" or "$\mathbb{Z}$-arithmetics", i.e. extensions of the basic additive arithmetic, in the language $L^{add} = \langle 0, 1, +, \leq \rangle$ or $L^{add}_{\mathbb{Z}} = \langle 0, 1, +, -, \leq \rangle$ respectively, by fragments of multiplication and the full induction scheme. As we already mentioned in the prologue of this chapter, this problematics is connected with the study of expansions of the structure $\langle \mathbb{N}, 0, 1, + \rangle$; we again refer to the survey article [Bès01] for more details.

All of our example theories are extensions of the additive arithmetic by multiplication by some fixed scalars (i.e. extensions by some "slices" of the full binary multiplication). They form a linearly ordered chain between Presburger (Pr) and Peano (P) arithmetics (which are its least and largest elements), where the ordering is given by the number of scalars.

Besides the "$\mathbb{N}$-like" and "$\mathbb{Z}$-like" versions of the theories, we will distinguish two equivalent but different axiomatics for each theory – the "inductive" one (based on the induction scheme for all formulas) and the "divisible" one (based on the scheme of integral-divisibility). All the axiomatics, we define, are summarized in the Table 1.1.

[1] It seems that no attention has been yet paid to the extensions of Pr by linear functions. The reason is, probably, that they are trivial when eximined in the standard model $\langle \mathbb{N}, 0, 1, + \rangle$. Even the quite general result of Semënov in [Sem84, Theorem 2, p.617] dismisses linear functions as trivial definable cases.

Level	$\mathbb{N}$-like ind.	$\mathbb{N}$-like div.	$\mathbb{Z}$-like ind.	$\mathbb{Z}$-like div.
additive	Pr=AA	Aa	ZAA	ZAa
linear	LA	La	ZLA	ZLa
κ-linear	LA$^\kappa$	–	ZLA$^\kappa$	–
Peano	P	–	ZP	–

Table 1.1: Arithmetical theories

1.1.1 Induction and $\mathbb{Z}$-induction

Let us remind that, for a formula φ in a language extending $\langle 0,1,+,\leq\rangle$, the *axiom of induction* for φ is the following formula:

$$I(\varphi):\ \ (\varphi(0)\,\&\,(\varphi(x)\rightarrow\varphi(x+1)))\rightarrow(\forall x)\varphi(x).$$

For a formula φ in a language extending $\langle 0,1,+,\leq\rangle$, the following is called the *axiom of $\mathbb{Z}$-induction* for φ:

$$I_{\mathbb{Z}}(\varphi):\ \ ((\exists z)\varphi(z)\,\&\,(\varphi(x)\leftrightarrow\varphi(x+1)))\rightarrow(\forall x)\varphi(x).$$

For a set Γ of formulas, $I(\Gamma)$ and $I_{\mathbb{Z}}(\Gamma)$ denote the sets of all axioms $I(\varphi)$ and $I_{\mathbb{Z}}(\varphi)$, for $\varphi\in\Gamma$, respectively. If Γ is the set of all L-formulas, we write $I(L)$, $I_{\mathbb{Z}}(L)$ instead of $I(\Gamma)$, $I_{\mathbb{Z}}(\Gamma)$.

1.1.2 Integral divisibility

Let α be an unary term in a language extending $\langle 0,1,+,\leq\rangle$. The formula

$$id(\alpha):\ \ (\exists y)(\alpha(y)\leq x<\alpha(y+1))$$

is called the *axiom of integral-divisibility* for α.

Let Λ be a set of unary terms. We define $id(\Lambda)=\{id(\alpha);\alpha\in\Lambda\}$.

1.1.3 Additive arithmetics

The following theories are just different axiomatics of Presburger arithmetic. We define them in order to introduce a consistent and systematic notation for all presented theories. We also want to specify the axioms we use for “Presburger arithmetic” since they vary through the literature.

1.1.3.1 AA and Aa

Additive arithmetic (AA) is a theory in the language $L^{add} = \langle 0, 1, +, \leq \rangle$. Its axioms are

$$\begin{array}{llll} \text{(A1)} & 0 \neq z+1 & \text{(A2)} & x+1 = y+1 \to x = y \\ \text{(A3)} & x+0 = x & \text{(A4)} & x+(y+1) = (x+y)+1 \end{array}$$

$$(\mathrm{D}_{\leq})\ x \leq y \leftrightarrow (\exists z)(x+z = y)$$

and the scheme $I(L^{add})$ of induction for all L^{add}-formulas. AA without the induction scheme is denoted AA^-.

The axiomatic Aa contains the following axioms:

$$\begin{array}{llll} \text{(a1)} & 0 \neq z+1 \,\&\, (x \neq 0 \to (\exists z)(x = z+1)) & \text{(a2)} & x+z = y+z \to x = y \\ \text{(a3)} & x+0 = x & \text{(a4)} & x+(y+z) = (x+y)+z \end{array}$$

$$\text{(a5)}\ x+y = y+x$$

$$(\mathrm{D}_{\leq})\ x \leq y \leftrightarrow (\exists z)(x+z = y)$$

and the scheme of integral-divisibility $id(\underline{n})$, for $0 < n \in \mathbb{N}$, where $\underline{n}(x)$ denotes $x + \cdots + x$, with n summands. We also write $\underline{0}(x) = 0$, $\underline{-n}(x) = -\underline{n}(x)$ and $\mathbf{z} = \underline{z}1$, for $z \in \mathbb{Z}$. Aa without the integral-divisibility scheme is denoted Aa^-.

1.1.3.2 ZAA and ZAa

$\mathbb{Z}$-additive arithmetic (ZAA) is the theory in the language $L^{add}_{\mathbb{Z}} = \langle 0, 1, +, -, \leq \rangle$ consisting of the axioms

$$\begin{array}{llll} \text{(ZA1)} & (\exists z)(x = z+1) & \text{(ZA2)} & x+1 = y+1 \to x = y \\ \text{(ZA3)} & x+0 = x & \text{(ZA4)} & x+(y+1) = (x+y)+1 \end{array}$$

$$(\mathrm{D}_{-})\ -x+x = 0$$

$$\text{(O1)}\quad (x = -1 \vee 0 \leq x) \leftrightarrow 0 \leq x+1 \quad \text{(OD)}\quad x \leq y \leftrightarrow 0 \leq -x+y$$

and the scheme $I_{\mathbb{Z}}(L^{add}_{\mathbb{Z}})$ of $\mathbb{Z}$-induction for all $L^{add}_{\mathbb{Z}}$-formulas. ZAA without the induction scheme is denoted ZAA^-. Note that (ZAi) is the same axiom as (Ai), for $i \neq 1$.

The axiomatic ZAa is given by the axioms

$$\begin{array}{llll} \text{(Za1)} & (\exists z)(x = z+1) & \text{(Za2)} & x+z = y+z \to x = y \\ \text{(Za3)} & x+0 = x & \text{(Za4)} & x+(y+z) = (x+y)+z \end{array}$$

$$\text{(Za5)}\ x+y = y+x$$

$$(\mathrm{D}_{-})\ -x+x = 0$$

$$\begin{array}{llll} \text{(o1)} & x \leq 0 \vee 0 \leq x & \text{(o2)} & (x \leq 0 \,\&\, 0 \leq x) \to x = 0 \\ \text{(o3)} & (0 \leq x \,\&\, 0 \leq y) \to 0 \leq x+y & \text{(o4)} & x \leq 0 \vee 1 \leq x \end{array}$$

$$\text{(oD)}\ x \leq y \leftrightarrow 0 \leq -x+y$$

and the scheme of integral-divisibility $id(\underline{n})$, for $0 < n \in \mathbb{N}$. ZAa without the integral-divisibility scheme is denoted ZAa$^-$.

Remark 1.1:1. It is not difficult to see that AA is an extension of Aa, and ZAA is an extension of ZAa. Later, we show that AA, Aa and ZAA, ZAa are both even equivalent (see Proposition 1.4:1). Moreover, ZAA is equivalent to the theory of $\mathbb{Z}$-groups, i.e. $Th(\langle \mathbb{Z}, 0, 1, +, -, \leq \rangle)$.

Lemma 1.1:2. *The following is provable in* ZAa*:*

1) the axioms of Abelian groups, i.e.

- *a)* $x + (y + z) = (x + y) + z$,
- *b)* $x + y = y + x$,
- *c)* $x + 0 = x$,
- *d)* $-x + x = 0$,

2) $\leq$ *is discrete linear ordering, with* 1 *as the least positive element, and compatible with* $+$, *i.e.*

- *a)* $\leq$ *is a linear ordering,*
- *b)* $0 < 1$, $x \leq 0 \vee 1 \leq x$,
- *c)* $(u \leq x \,\&\, v \leq y) \rightarrow u + v \leq x + y$.

Proof. Easy. □

1.1.4 Linear arithmetics

1.1.4.1 LA and La

Linear arithmetic (LA) is a theory in the language $L^{lin} = \langle 0, 1, +, \underline{a}, \leq \rangle$, where $\underline{a}$ is an unary functional symbol (with the intended meaning "multiplication by a scalar a"). The axioms of LA are

$$\begin{gathered} \text{all axioms of AA}^- \\ (\text{L1}) \quad \underline{a}(x+1) = \underline{a}x + \underline{a}1 \quad (\text{L2}) \quad 0 \leq \underline{a}1 \\ (\text{L0}) \; \underline{a}1 \neq n \text{ for all } n \in \mathbb{N} \end{gathered}$$

and the scheme $I(L^{lin})$ of induction for all L^{lin}-formulas. LA without the induction scheme is denoted LA$^-$.

Remark 1.1:3. The name "linear arithmetic" is used somewhat vaguely and/or inconsistently through the literature. It denotes more different concepts where an important role is played by inequalities of "linear" combinations of "unknowns". Therefore, we stress that, for us, linear arithmetic means always the first order theory LA above.

The axiomatic La is given by

$$\begin{gathered}\text{all axioms of } \mathrm{Aa}^- \\ (\mathrm{l1}) \quad \underline{a}(x+y) = \underline{a}x + \underline{a}y \quad (\mathrm{l2}) \quad 0 \le x \to 0 \le \underline{a}x \\ (\mathrm{l0})\ \underline{a}1 \ne n \text{ for all } n \in \mathbb{N}\end{gathered}$$

and the scheme of integral divisibility $id(\underline{p})$, for every polynomial $0 < p \in \mathbb{Z}[a]$. Here, for $0 < p = \sum_{i<m} c_i a^i \in \mathbb{Z}[a]$, with $c_i \in \mathbb{Z}$, we denote $\underline{p}(x)$ the term $\sum_{i<m} \underline{c_i}(\underline{a}^i(x))$, where $\underline{a}^i(x) = \underline{a}(\ldots(\underline{a}(x))\ldots)$ with n occurances of $\underline{a}$. Moreover, for $r = \frac{p}{n} \in \mathbb{Q}[a]$, with $p \in \mathbb{Z}[a]$ and $0 < n \in \mathbb{N}$, we define $\underline{r}(x) = y \leftrightarrow \underline{p}(x) = \underline{n}(y)$. We write $\mathbf{r}$ for the constant term $\underline{r}(1)$.

La without the integral-divisibility scheme is denoted La$^-$.

Example 1.1:4. Let $\mathcal{A} = \langle A, 0, 1, +, \cdot, \le\rangle$ be a non-standard model of Peano arithmetic (see 1.1.6), and let $a \in A - \mathbb{N}$. Then $\mathcal{A}^a = \langle A, 0, 1, +, \underline{a}, \le\rangle$, where $\underline{a}(x) = a \cdot x$, is a model of LA. Moreover, if $\mathcal{A}$ is κ-saturated then $\mathcal{A}^a$ is as well.

1.1.4.2 ZLA and ZLa

$\mathbb{Z}$-linear arithmetic (ZLA) is the theory in the language $L^{lin}_{\mathbb{Z}} = \langle 0, 1, +, -, \underline{a}, \le\rangle$ with axioms

$$\begin{gathered}\text{all axioms of } \mathrm{ZAA}^- \\ (\mathrm{L1}) \quad \underline{a}(x+1) = \underline{a}x + \underline{a}1 \quad (\mathrm{L2}) \quad 0 \le \underline{a}1 \\ (\mathrm{L0})\ \underline{a}1 \ne n \text{ for all } n \in \mathbb{N}\end{gathered}$$

and the scheme $I_{\mathbb{Z}}(L^{lin}_{\mathbb{Z}})$ of $\mathbb{Z}$-induction for all $L^{lin}_{\mathbb{Z}}$-formulas. ZLA without the induction scheme is denoted ZLA$^-$.

The axiomatic ZLa consists of axioms

$$\begin{gathered}\text{all axioms of } \mathrm{ZAa}^- \\ (\mathrm{l1}) \quad \underline{a}(x+y) = \underline{a}x + \underline{a}y \quad (\mathrm{l2}) \quad 0 \le x \to 0 \le \underline{a}x \\ (\mathrm{l0})\ \underline{a}1 \ne n \text{ for all } n \in \mathbb{N}\end{gathered}$$

and the scheme of integral divisibility $id(\underline{p})$, for every polynomial $0 < p \in \mathbb{Z}[a]$.

ZLa without the integral-divisibility scheme is denoted ZLa$^-$.

1.1.5 κ-linear arithmetics

1.1.5.1 LA$^\kappa$

For a cardinal number κ, κ-linear arithmetic (LA$^\kappa$) is a theory in the language $L^{\kappa-lin} = \langle 0, 1, +, \underline{a}_\alpha, \le\rangle_{\alpha<\kappa}$, where $\underline{a}_\alpha$ are unary functional symbols (with the intended meaning "multiplication by a scalar a_α").

The axioms of LA^κ are

$$\text{all axioms of } \mathrm{AA}^-$$
$$(\kappa\mathrm{L1})\quad \underline{a}_\alpha(x+1)=\underline{a}_\alpha x+\underline{a}_\alpha 1 \quad (\kappa\mathrm{L2})\quad 0\le \underline{a}_\alpha 1 \quad (\kappa\mathrm{L3})\quad \underline{a}_\alpha(\underline{a}_\beta x)=\underline{a}_\beta(\underline{a}_\alpha x)$$
$$(\kappa\mathrm{L0})\ \text{“}\underline{a}_\alpha \text{ is not definable by any formula not containing } \underline{a}_\alpha\text{”},$$

for all $\alpha,\beta<\kappa$, and the scheme $I(L^{\kappa-lin})$ of induction for all $L^{\kappa-lin}$-formulas. LA^κ without the induction scheme is denoted $\mathrm{LA}^{\kappa-}$.

1.1.5.2 ZLA$^\kappa$

For a cardinal number κ, κ-$\mathbb{Z}$-linear arithmetic (ZLA^κ) is the theory in the language $L_{\mathbb{Z}}^{\kappa-lin}=\langle 0,1,+,-,\underline{a}_\alpha,\le\rangle_{\alpha<\kappa}$ with the axioms

$$\text{all axioms of } \mathrm{ZAA}^-$$
$$(\kappa\mathrm{L1})\quad \underline{a}_\alpha(x+1)=\underline{a}_\alpha x+\underline{a}_\alpha 1 \quad (\kappa\mathrm{L2})\quad 0\le \underline{a}_\alpha 1 \quad (\kappa\mathrm{L3})\quad \underline{a}_\alpha(\underline{a}_\beta x)=\underline{a}_\beta(\underline{a}_\alpha x)$$
$$(\kappa\mathrm{L0})\ \text{“}\underline{a}_\alpha \text{ is not definable by any formula not containing } \underline{a}_\alpha\text{”},$$

for all $\alpha,\beta<\kappa$, and the scheme $I_{\mathbb{Z}}(L_{\mathbb{Z}}^{\kappa-lin})$ of $\mathbb{Z}$-induction for all $L_{\mathbb{Z}}^{\kappa-lin}$-formulas. ZLA^κ without the induction scheme is denoted $\mathrm{ZLA}^{\kappa-}$.

Remark 1.1:5. The 0-linear arithmetic LA^0 is just the additive arithmetic AA, while the 1-linear arithmetic LA^1 is equivalent to the linear arithmetic LA.

1.1.6 Peano arithmetics

Peano arithmetic (P) is a theory in the language $L^{ar}=\langle 0,1,+,\cdot,\le\rangle$. Its axioms are

$$\text{all axioms of } \mathrm{AA}^-$$
$$(\mathrm{M1})\quad x\cdot 0=0 \quad (\mathrm{M2})\quad x\cdot(y+1)=x\cdot y+x$$

and the scheme $I(L^{ar})$ of induction for all L^{ar}-formulas. P without the induction scheme is denoted P^- (the Robinson arithmetic Q is the extension of P^- by $x\ne 0\to(\exists z)(x=z+1)$).

$\mathbb{Z}$-Peano arithmetic (ZP) is the theory in the language $L_{\mathbb{Z}}^{ar}=\langle 0,1,+,-,\cdot,\le\rangle$ given by the axioms

$$\text{all axioms of } \mathrm{ZAA}^-$$
$$(\mathrm{M1})\quad x\cdot 0=0 \quad (\mathrm{M2})\quad x\cdot(y+1)=x\cdot y+x$$

and the scheme $I_{\mathbb{Z}}(L_{\mathbb{Z}}^{ar})$ of induction for all $L_{\mathbb{Z}}^{ar}$-formulas. ZP without the induction scheme is denoted ZP^-.

Observation 1.1:6. *The following diagram, where $T \vdash S$ denotes that T is an extension of S, and where $1 < \kappa < \lambda$, holds:*

$$\begin{array}{ccccccc}
\mathrm{AA} & \vdash & \mathrm{Aa} & \qquad & \mathrm{ZAA} & \vdash & \mathrm{ZAa} \\
\perp & & \perp & & \perp & & \perp \\
\mathrm{LA} & \vdash & \mathrm{La} & & \mathrm{ZLA} & \vdash & \mathrm{ZLa} \\
\perp & & & & \perp & & \\
\mathrm{LA}^\kappa & & & & \mathrm{ZLA}^\kappa & & \\
\perp & & & & \perp & & \\
\mathrm{LA}^\lambda & & & & \mathrm{ZLA}^\lambda & &
\end{array}$$

1.1.7 Models of $\mathbb{N}$-like and $\mathbb{Z}$-like variants

Let T be one of the theories AA, Aa, LA, La, LA$^\kappa$, P, and ZT be the corresponding $\mathbb{Z}$-like variant of T. It can be easily shown that, for every model $\mathcal{A} = \langle A, 0, S, +, \leq, \ldots\rangle \models T$, its canonical "$\mathbb{Z}$-version" $\mathcal{A}^\pm = \langle A \cup -A, 0, 1, +, -, \leq, \ldots\rangle$ is a model of ZT. On the other side, the positive part $\mathcal{B}^+ = \langle B^+, 0, 1, +, \leq, \ldots\rangle$ of any model $\mathcal{B} \models ZT$ is a model of T.

For an $L(T)$-formula φ, the formula φ^+, created by replacing every quantification Qx in φ by $Qx \geq 0$, satisfies

$$\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{A}^\pm \models \varphi^+[\overline{a}], \tag{1.1}$$

for every $\overline{a} \in A$. Similarly, it is easy (but a bit more technical), for an $L(ZT)$-formula ψ, to construct an $L(T)$-formula $\psi^\pm$, such that it is

$$\mathcal{A} \models \psi^\pm[\overline{a}] \Leftrightarrow \mathcal{A}^\pm \models \psi[\overline{a}], \tag{1.2}$$

for every $\overline{a} \in A$.

1.2 Model-theoretical background

At this place, we formulate a theoretical background for our next explanation. The concepts presented in this section are simple and the proofs mostly elementary; the reason, why we introduce them, is that they show themselves very useful for formulating and proving the presented results.

1.2.1 Σ_1-separability and decidability

We prove an easy but useful equivalent for decidability of recursively axiomatizable theories (Proposition 1.2:1). This criterion is particularly useful for theories which have "well described" but uncountable (and thus not recursively enumerable) set of non-equivalent simple complete extensions.

In the following, by a theory we mean (a numeric presentation of) some axiomatic in a recursive language L. Then $Th(T)$ denotes the set of all L-sentences provable in T and $CS(T)$ the set of all L-sentences consistent with T.

1.2.1.1 Γ-separability

Let $\Gamma \subseteq \mathcal{P}(\mathbb{N})$. A theory T is Γ-*separable* if there is $\mathcal{S} \subseteq CS(T)$, $\mathcal{S} \in \Gamma$ and dense in $CS(T)$, i.e. such that for $\varphi \in CS(T)$ there is $\varphi' \in \mathcal{S}$ with $T, \varphi' \vdash \varphi$.

Proposition 1.2:1. *For a recursively axiomatizable theory T, the following are equivalent:*

1) T is decidable,

2) T is Δ_1-separable,

3) T is Σ_1-separable.

Proof. 1)⇒2): $CS(T)$ is Δ_1 and dense in itself.
2)⇒3): Clear.
3)⇒1): Let $\mathcal{S}$ be Σ_1 and dense in $CS(T)$. Then $\varphi \notin Th(T) \Leftrightarrow \neg\varphi \in CS(T) \Leftrightarrow$ there is $\varphi' \in \mathcal{S}$ such that $\neg\varphi \in Th(T, \varphi')$; therefore $\mathbb{N} - Th(T)$ is Σ_1. □

1.2.1.2 Γ-almost-completion

A binary relation $\mathcal{C} \subseteq \mathbb{N}^2$ is a Γ-*almost-completion* of a theory T if $\mathcal{C} \in \Gamma$, for each $n \in \mathrm{dom}(\mathcal{C})$ the set $\mathcal{C}[n]$ is a simple complete extension of T, and $\mathcal{C}$ is dense in the set of all simple complete extensions of T, i.e., for any $\varphi \in CS(T)$, there is $n \in \mathrm{dom}(\mathcal{C})$ such that $\varphi \in Th(\mathcal{C}[n])$.

Proposition 1.2:2. *If a recursively axiomatizable theory T has a Σ_1-almost-completion then it is decidable.*

Proof. If $\mathcal{C}$ is a Σ_1-almost-completion of T then $CS(T) = \bigcup_{n \in \mathrm{dom}(\mathcal{C})} Th(\mathcal{C}[n])$ is Σ_1. □

1.2.2 Solvable theories

We formulate a property of solvability of a theory T, which states that every non-empty definable set in a model of T contains a "solution" expressible as a value of a term. In Proposition 1.2:6, we show that solvability implies quantifier elimination. The property of solvability will prove itself very helpful for the detailed analysis of definable sets in models of linear theories, which we perform in section 1.3.1.

We also show that if a theory T satisfies a stronger condition of almost uniform solvability then every function definable in a model of T can be written as a "piecewise term".

1.2.2.1 Solvable and n-solvable theories

We define concepts of solvable and n-solvable theories. Although these can (and will) be defined in general, we will make use of solvability and 0-solvability only.

We say that a theory T is *[n-]solvable* [for $n \in \mathbb{N}$] if, for every model $\mathcal{M} \models T$, every L-formula $\varphi(x, \overline{y})$ [with $l(\overline{y}) \leq n$] and an $l(\overline{y})$-tuple $\overline{a}$ from M, it holds

$$\mathcal{M} \models (\exists x)\varphi(x, \overline{a}) \Rightarrow \mathcal{M} \models \varphi(t(\overline{a}), \overline{a}), \text{ for some } L_T\text{−term } t.$$

Remark 1.2:3. It easily follows from the proof of Lemma 1.2:5 that, in the definition of solvable theory, we could equivalently replace the arbitrary φ by a quantifier-free formula. However, this is not true for n-solvability. Let us also note that in both cases we may equivalently replace the single variable x by a tuple $\overline{x}$.

The following statement is a classical result:

Lemma 1.2:4. *Let T be an L-theory and $\varphi(\overline{x})$ an L-formula, such that $l(\overline{x}) > 0$, or L contains a constant symbol. Then the following are equivalent:*

1) There is a quantifier-free $\psi(\overline{x})$, such that $T \vdash \varphi \leftrightarrow \psi$.

2) For any $\mathcal{M}, \mathcal{N} \models T$ with a common substructure $\mathcal{C}$ and every $\overline{a} \in C$, it is

$$\mathcal{M} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{N} \models \varphi(\overline{a}). \tag{1.3}$$

Proof. Folklore. □

Lemma 1.2:5.
1) If a theory is solvable then it has quantifier elimination.

2) Suppose that $n > 0$, or L contains a constant symbol. If T is n-solvable then every $\varphi(\overline{x})$, with $l(\overline{x}) \leq n$, is equivalent to some quantifier-free $\psi(\overline{x})$.

Proof. 1): Suppose that a theory T is solvable and let $\mathcal{M}, \mathcal{N}$ and $\overline{a}$ be as in Lemma 1.2:4 2). Clearly, it is enough to prove (1.3) for a formula $(\exists x)\psi(x, \overline{y})$ with ψ quantifier-free. Let $\mathcal{M} \models (\exists x)\psi(x, \overline{a})$. Then, by solvability, $\mathcal{M} \models \psi(t(\overline{a}), \overline{a})$ for some term t, and since $t(\overline{a}) \in \mathcal{C} \subseteq \mathcal{N}$, we have $\mathcal{N} \models (\exists x)\psi(x, \overline{a})$.
2): By induction on the least number m of quantifiers in a prenex normal form of φ. The case $m = 0$ is trivial. For the induction step, we may suppose that φ is $(\exists x)\chi(x, \overline{y})$, for some χ such that $l(\overline{y}) \leq n$. Let $\mathcal{M}, \mathcal{N}, \overline{a}$ be as in Lemma 1.2:4 2), and suppose $\mathcal{M} \models \varphi(\overline{a})$. By n-solvability, there is a term t such that $\mathcal{M} \models \chi(t(\overline{a}), \overline{a})$. $\chi(t(\overline{y}), \overline{y})$ has at most n free variables, hence it is in T equivalent to a quantifier-free formula, by induction assumption. Therefore $\mathcal{N} \models \chi(t(\overline{a}), \overline{a})$, and φ is equivalent to a quantifier-free formula by Lemma 1.2:4. □

For a structure $\mathcal{M}$ and $X \subseteq M$, we denote $\mathcal{M}\langle X\rangle$ the substructure of $\mathcal{M}$ generated by X and $M\langle X\rangle$ its universe. $\mathcal{M}_{(X)}$ stands for the structure of all definable elements in $\mathcal{M}$ over X, and $M_{(X)}= \{a \in M; \{a\} \in \mathrm{Df}^1(X, \mathcal{M})\}$ denotes its universe.

Proposition 1.2:6. *For a theory T in a language with a constant symbol, it is equivalent:*

1) T is solvable.

2) T has quantifier elimination and is axiomatizable by open formulas.

3) T is model-complete and is axiomatizable by open formulas.

4) For $\mathcal{N} \subseteq \mathcal{M} \models T$, it is $\mathcal{N} \prec \mathcal{M}$.

5) For $\mathcal{M} \models T$, $X \subseteq M$, it is $M\langle X\rangle = M_{(X)}$, and it is a dense set (of all atoms) in $\mathrm{Df}^1(X, \mathcal{M})$.

Proof. 1)⇒2): T has quantifier elimination by Lemma 1.2:5. Let $\mathcal{M} \subseteq \mathcal{N} \models T$. Then, by the Tarski-Vaught test, it is $\mathcal{M} \prec \mathcal{N}$, and hence $\mathcal{M} \models T$. Indeed: For $\overline{a} \in M$, if $\mathcal{N} \models (\exists x)\varphi(x, \overline{a})$, there is, by solvability of T, a term $t(\overline{y})$ such that $\mathcal{N} \models \varphi(t(\overline{a}), \overline{a})$, and clearly $t(\overline{a}) \in M$.
2)⇒3): Clear.
3)⇒4): We get $\mathcal{N} \models T$, by open-axiomatizability of T, and thus $\mathcal{N} \prec \mathcal{M}$, by model-completeness.
4)⇒5): Let $\{a\} \in \mathrm{Df}^1(X, \mathcal{M})$, and $\varphi(x, \overline{b})$, with $\overline{b} \in X$, define $\{a\}$ in $\mathcal{M}$. Then, by $\mathcal{M}\langle X\rangle \prec \mathcal{M}$, there is exactly one $a' \in M\langle X\rangle$ such that $\mathcal{M}\langle X\rangle \models \varphi(a', \overline{b})$, and hence also $\mathcal{M} \models \varphi(a', \overline{b})$, which implies $a = a'$. Density of $M\langle X\rangle$: Let $\emptyset \neq D \in \mathrm{Df}^1(X, \mathcal{M})$. Then, by $\mathcal{M}\langle X\rangle \prec \mathcal{M}$, it is $D \cap M\langle X\rangle \neq \emptyset$.
5)⇒1): Let $\mathcal{M} \models T$, $\overline{a} \in M$, and $\psi(x, \overline{y})$ be an open formula such that it is $\mathcal{M} \models (\exists x)\psi(x, \overline{a})$. Then, by the assumptions, there is an atom of the form $\{t(\overline{a})\}$, with t a term, under $\{b; \mathcal{M} \models \psi(b, \overline{a})\}$, and clearly $\mathcal{M} \models \psi(t(\overline{a}), \overline{a})$. □

We formulate the following two strengthenings of solvability. Let us remind that, by Remark 1.2:3, in the definition of solvable theory, it suffices to verify the condition only for quantifier-free formulas.

1.2.2.2 Uniformly solvable theory

We say that a theory T is *uniformly solvable* if, for each quantifier-free formula $\psi(x, \overline{y})$, there is a term t such that

$$T \vdash (\exists x)\psi(x, \overline{y}) \rightarrow \psi(t(\overline{y}), \overline{y}).$$

Example 1.2:7. Let L be the language $\langle 0, 1, P\rangle$, where $0, 1$ are two constant symbols, and P is an unary predicate symbol. Then the theory

$$T = \{0 \neq 1, (\forall x)(x = 0 \vee x = 1), (\exists! x)P(x)\}$$

is solvable but not uniformly solvable.

1.2.2.3 Almost uniformly solvable theory

We say that a theory T is *almost uniformly solvable* if, for each quantifier-free formula $\psi(x,\overline{y})$, there are finitely many terms t_i, $i<n$, such that

$$T \vdash (\exists x)\psi(x,\overline{y}) \to \bigvee_{i<n} \psi(t_i(\overline{y}),\overline{y}).$$

By the following lemma, almost uniform solvability may be formulated as a seemingly weaker condition.

Lemma 1.2:8. *The following are equivalent:*

1) T is almost uniformly solvable.

2) For each quantifier-free formula $\psi(x,\overline{y})$ and $\mathcal{M} \models T$, there are finitely many terms t_i, $i<n$, such that $\mathcal{M} \models (\exists x)\psi(x,\overline{y}) \to \bigvee_{i<n} \psi(t_i(\overline{y}),\overline{y})$.

Proof. 1) $\Rightarrow$ 2) is clear.
2) $\Rightarrow$ 1): For a model $\mathcal{M} \models T$, we get $n^{(\mathcal{M})}$ and $t_j^{(\mathcal{M})}$, for $j < n^{(\mathcal{M})}$. We set $X = \{t_j^{(\mathcal{M})}; \mathcal{M} \models T, j < n^{(\mathcal{M})}\}$ and

$$S = T \cup \{(\exists x)\psi(x,\overline{c})\} \cup \{\textstyle\bigwedge_{t\in F} \neg\psi(t(\overline{c}),\overline{c}); F \subseteq X \text{ finite}\},$$

where $\overline{c}$ are new constant symbols with $l(\overline{c}) = l(\overline{y})$.

We prove that S is inconsistent. Otherwise it has a model $\langle \mathcal{M}, \overline{c}\rangle$ such that

$$\mathcal{M} \models (\exists \overline{y})((\exists x)\psi(x,\overline{y})\,\&\, \bigwedge_{j<n^{(\mathcal{M})}} \neg\psi(t_j^{(\mathcal{M})},\overline{y})),$$

and $\mathcal{M} \models T$; this contradicts the choice of the terms $t_j^{(\mathcal{M})}$. Hence, for some finite $F \subseteq X$, it is $T \vdash (\exists x)\psi(x,\overline{c}) \to \bigvee_{t\in F} \psi(t(\overline{c}),\overline{c})$, and thus

$$T \vdash (\exists x)\psi(x,\overline{y}) \leftrightarrow \bigvee_{t\in F} \psi(t,\overline{y}).$$

$\square$

1.2.2.4 Piecewise terms

An [open] *piecewise term*, or shortly an [open] *p-term*, is a tuple $\tau = (t_i,\psi_i)_{i=0}^{n-1}$, more suggestively written as a piecewise defined function

$$\tau(\overline{x}) = \Big\{ t_i(\overline{x}) \text{ if } \psi_i(\overline{x});\ i = 0,\ldots,n-1, \tag{1.4}$$

where $n>0$, t_i are terms, and ψ_i are [open] formulas such that, for every $\overline{a}$, exactly one of $\psi_i(\overline{a})$ holds. A subterm of a p-term $\tau = (t_i,\psi_i)_{i=0}^{n-1}$ is any subterm of some t_i or of some ψ_i.

The value of a term $\tau(\overline{x})$ from (1.4) at point $\overline{a} \in M$ in structure $\mathcal{M}$ is $t_i(\overline{a})$, where i is such that $\mathcal{M} \models \psi_i(\overline{a})$. We identify each term t with the p-term $(t,\top)$ (here $\top$ denotes "truth").

Proposition 1.2:9. *Let T be almost uniformly solvable, $\mathcal{M} \models T$ and $X \subseteq M$. Then every X-definable (in $\mathcal{M}$) function $f : M^n \to M$ is the realization of an open p-term $\tau(\overline{y}, \overline{a})$ with $\overline{a} \in X$.*

Proof. Clearly, T is solvable, hence it has quantifier elimination, by Proposition 1.2:6. Therefore we may suppose that f is defined in $\mathcal{M}$ by an open formula $\chi(x, \overline{y}, \overline{a})$, with $\overline{a} \in X$. By the almost uniform solvability of T, there are terms $t_i(\overline{y}, \overline{z})$, for $i < m$, such that $\mathcal{M} \models \bigvee_{i<m} \chi(t_i(\overline{y}, \overline{a}), \overline{y}, \overline{a})$.

Now, we may set $\tau = (t_i, \psi_i)_{i<m}$, where ψ_i is the formula

$$\chi(t_i(\overline{y}, \overline{a}), \overline{y}, \overline{a}) \mathbin{\&} \bigwedge_{j<i} \neg\chi(t_j(\overline{y}, \overline{a}), \overline{y}, \overline{a}).$$

□

1.2.3 Solvable extensions by definitions

In this section, we deal with theories which have solvable extensions by definitions. Proposition 1.2:11 provides a characterization of such theories.

Example 1.2:10. All arithmetical theories with the full induction, such as Pr, LA or P (see section 1.1 for definitions), can be extended by definitions of new functions in such a way that the resulting extensions are solvable. For each formula $\varphi(x, \overline{y})$, it suffices to define a function which, for given parameters $\overline{a}$, outputs the minimal element of the set defined by $\varphi(x, \overline{a})$ (if it is non-empty).

Let $L = L^{\mathcal{F}} \cup L^{\mathcal{R}}$ be a language containing the constant symbol 0, $L^{\mathcal{F}}$ be its algebraic part and $L^{\mathcal{R}}$ the relational part. For an L-formula $\varphi(\overline{x}, y)$, we denote

$cor(\varphi)$: the L-formula "φ is a correct defining formula of a function",
$\delta(\varphi)$: the conditional definition of $\underline{\varphi}$:
$(cor(\varphi) \mathbin{\&} \varphi(\overline{x}, \underline{\varphi}(\overline{x}))) \vee (\neg cor(\varphi) \mathbin{\&} \underline{\varphi}(\overline{x}) = 0)$,

where $\underline{\varphi}$ is a new $l(\overline{x})$-ary functional symbol. For $F \subseteq Fm_L$, we write

$$T^F = T \cup \{\delta(\varphi); \varphi \in F\}$$

for the extension of T by functions definable by formulas from F. For an L-structure $\mathcal{M}$, we denote $\mathcal{M}^F$ the corresponding expansion of $\mathcal{M}$ and L^F the respective extension of L. If s is a new symbol of T^F, we write $\dot{s}$ for the L-formula φ which defines s (i.e. such that $s = \underline{\varphi}$). When there is no danger of misunderstanding, we write just s instead of $\dot{s}$.

We say that T is *F-solvable* [*F-n-solvable*] if T^F is solvable [n-solvable]. Then $\emptyset$-solvable means just solvable and similarly for the n-solvability.

Proposition 1.2:11. *Let T be an L-theory and $n \in \mathbb{N}$. The following statements are equivalent:*

1) T is Fm_L-[n-]solvable.

2) For every $\mathcal{M} \models T$ and $X \subseteq M$ [with $|X| \leq n$], each non-empty X-definable set in $\mathcal{M}$ contains an X-definable element.

3) For every $\mathcal{M} \models T$ and $X \subseteq M$ [with $|X| \leq n$], it is $\mathcal{M}_{(X)} \prec \mathcal{M}$.

4) For every $\mathcal{M} \models T$ and $X \subseteq M$ [with $|X| \leq n$], the structure $\mathcal{M}_{(X)}$ is a prime model over X in $\mathcal{M}$.

Proof. 1) $\Rightarrow$ 2) is immediate.
2) $\Rightarrow$ 3) follows from the Tarski-Vaught test.
3) $\Rightarrow$ 1) is easy by observing that, for $b \in \mathcal{M}_{(\overline{a})}$, there is a $\emptyset$-definable function f with $f(\overline{a}) = b$.
3) $\Rightarrow$ 4): Let $\mathcal{N}$ be an L-structure and $f : M \to N$ a partial elementary map, with $\mathrm{dom}(f) = X$. Then f can be extended to an isomorphism between $\mathcal{M}_{(X)}$ and $\mathcal{N}_{(f[X])}$, by setting $f(a) = b$, where $b \in N$ is defined in $\mathcal{N}$ by the same L-formula as a in $\mathcal{M}$. Then, by 3), f is an elementary embedding.
4) $\Rightarrow$ 3): Clearly, the only elementary embedding of $\mathcal{M}_{(X)}$ into $\mathcal{M}$ extending the identity on X is the identity. $\square$

The following corollary states that the prime models and the simple complete extensions of F-0-solvable theories are at most as "complex" as F.

Corollary 1.2:12. *Let T be an L-theory and $F \subseteq Fm_L$ be such that T is F-0-solvable. Then, for $\mathcal{M} \models T$, it is:*

1) $\mathcal{M}_{(\emptyset)} = \mathcal{M}^F\langle\emptyset\rangle|L$ is the unique (even if $\|L\| > \omega$) prime model of $Th(\mathcal{M})$,

2) $Th(\mathcal{M})$ is equivalent to $T \cup OTh_L(\mathcal{M}^F)$ (equivalently to $T \cup OTh_L(\mathcal{M}^F\langle\emptyset\rangle)$),

where $OTh_L(\mathcal{N})$ denotes the set of canonical L-translations of open sentences true in $\mathcal{N}$.

Moreover, if T^F is open-complete then T is complete.

Proof. 1) $\mathcal{M}_{(\emptyset)} = \mathcal{M}^F\langle\emptyset\rangle|L$ is a trivial consequence of 0-solvability of T^F. $\mathcal{M}_{(\emptyset)}$ is a prime model by Proposition 1.2:11. The uniqueness is clear.
2): Let $\mathcal{N} \models T \cup OTh_L(\mathcal{M}^F)$. Then $\mathcal{M}^F\langle\emptyset\rangle \cong \mathcal{N}^F\langle\emptyset\rangle$, and thus $\mathcal{M} \equiv \mathcal{N}$, by 1).
"Moreover" follows from Lemma 1.2:5 2). $\square$

1.2.4 Syntactic presentation of prime models

In the previous section, we proved that prime models of simple complete extensions of a F-0-solvable L-theory can be seen as having universes consisting of (some) constant L^F-terms (see Corollary 1.2:12 1)). We, informally, call this presentation of the prime models "syntactic".

The way in which syntactic presentations of the prime models of different complete extensions of a theory T overlap, provides an interesting information about properties of T. In this section, we draft some possibilities of this method.

Let further T be an L-theory, and $F \subseteq Fm_L$ be such that T is F-0-solvable. For $\mathcal{M} \models T$, we denote $\mathcal{M}_{\bullet,F}$ the L^F-structure of constant terms of the theory $Th(\mathcal{M}^F)$; the realization $r_{\mathcal{M}}$ of a symbol $r \in L^{\mathcal{R}}$ in $\mathcal{M}_{\bullet,F}$ is given by

$$r_{\mathcal{M}}(\overline{s}) \Leftrightarrow \mathcal{M}^F \models r(\overline{s}), \tag{1.5}$$

for any tuple $\overline{s}$ of constant L^F-terms. By the formula (1.5) for r equal to $=$, we also define the equivalence $=_{\mathcal{M}}$ on the set of all constant L^F-terms.

For a constant L^F-term s, we write $cor(s)$ instead of $\bigwedge\{cor(\varphi); \underline{\varphi} \text{ occurs in } s\}$, and we denote $M_{c,F}= \{s; \mathcal{M} \models cor(s)\}$. Finally, we define the canonical structure of $Th(\mathcal{M})^F$ as $\mathcal{M}_{*,F}= \mathcal{M}_{\bullet,F}/{=_{\mathcal{M}}}$.

By Corollary 1.2:12 1), $\emptyset$-definable elements in $\mathcal{M}$ are just the values of constant L^F-terms, and they form the universe of the prime-model of $Th(\mathcal{M})$. Thus, we have the following:

Observation 1.2:13. *$\mathcal{M}_{*,F}|L \cong \mathcal{M}_{(\emptyset)}$ is the unique prime model of $Th(\mathcal{M})$, and thus*

$$\mathcal{M} \equiv \mathcal{N} \Leftrightarrow \mathcal{M}_{*,F} = \mathcal{N}_{*,F},$$

for $\mathcal{M}, \mathcal{N} \models T$.

It is easy to see that every equivalence-class $[s]_{=_{\mathcal{M}}} \in M_{*,F}$ contains some $s' \in M_{c,F}$. The set $M_{c,F}$ itself may carry some information about the structure $\mathcal{M}_{*,F}$. That is why we define the *F-correctness diagram* of $\mathcal{M}$:

$$\Delta^{cor}(\mathcal{M}, F) \;=\; \{cor(\varphi); \underline{\varphi} \in M_{c,F}\} \cup \{\neg cor(\varphi); \underline{\varphi} \notin M_{c,F}\}.$$

1.2.4.1 Completeness up to/in correctness

The two extremal cases, where $M_{c,F}$ carries the full and no information about $\mathcal{M}_{*,F}$, are considered in the following definitions.

A theory T is said to be *complete up to correctness w.r.t. F*, or shortly *F-cuc*, if, for every $\mathcal{M}, \mathcal{N} \models T$, it is $M_{c,F} = N_{c,F} \Rightarrow \mathcal{M}_{*,F} = \mathcal{N}_{*,F}$.

T is called *complete in correctness w.r.t. F*, or shortly *F-cic*, if, for every $\mathcal{M}, \mathcal{N} \models T$, it is $M_{c,F} = N_{c,F}$.

1.2.4.2 Compatibility

Two L-structures $\mathcal{M}, \mathcal{N}$ are said to be *F-compatible* if, for every $r \in L^{\mathcal{R}}$ or r being $=$, it is $r_{\mathcal{M}} = r_{\mathcal{N}}$ on the set $M_{c,F} \cap N_{c,F}$. T is *F-compatible* if every pair $\mathcal{M}, \mathcal{N} \models T$ is.

Observation 1.2:14. *The following implications hold:*

1) T is complete $\Leftrightarrow$ T is F-cuc and F-cic.

2) T is complete $\Rightarrow$ T is F-compatible $\Rightarrow$ T is F-cuc.

The following examples show that the implications in the Observation 1.2:14 2) can not be reversed.

Example 1.2:15.

a) Let $\mathrm{Pr}_c = \mathrm{Pr} \cup \{c > \underline{n}; n \in \mathbb{N}\}$, with c a new constant symbol, and F be the set of the canonical formulas formally defining fractions of the form $\frac{mc+n}{k}$, with $m, n, k \in \mathbb{Z}$, $k > 0$. Then Pr_c is F-0-solvable and F-compatible but not complete.

b) Let $\mathrm{Pr}_{c,d} = \mathrm{Pr} \cup \{c, d > \underline{n}; n \in \mathbb{N}\}$, with c, d new constant symbols, and F be the set of the canonical definitions of fractions of the form $\frac{mc+nd+i}{k}$, with $m, n, i, k \in \mathbb{Z}$, $k > 0$. The theory

$$T = \mathrm{Pr}_{c,d} \cup \{(2|c \,\&\, nc < d) \vee (\neg 2|c \,\&\, nd < c); n \in \mathbb{N}\}$$

is F-0-solvable and F-cuc but not F-compatible.

1.2.4.3 Prime-envelope

We show that all prime models of an F-compatible theory T can be "faithfully" embedded into a single structure – a prime-envelope of T.

An L^F-structure $\mathcal{Q}$ is called an *F-prime-envelope* of T if every $\mathcal{M}_{*,F}$, with $\mathcal{M} \models T$, is an $L^{F_{c,\mathcal{M}}}$-substructure (where $F_{c,\mathcal{M}} = \{\varphi \in F; \mathcal{M} \models cor(\varphi)\}$) of $\mathcal{Q}$, and $\mathcal{Q}$ is generated by $\bigcup_{\mathcal{M} \models T} M_{*,F}$.

Proposition 1.2:16. *Let $F \subseteq Fm_L$ be such that T is F-0-solvable. Then the following holds:*

1) T is F-cuc $\Leftrightarrow$ $Th(\mathcal{M})$ is equivalent to $T \cup \Delta^{cor}(\mathcal{M}, F)$, for every $\mathcal{M} \models T$.
$\Leftrightarrow$ $\bigcup_{\mathcal{M} \models T} \{\bigwedge \Gamma; \Gamma \subseteq \Delta^{cor}(\mathcal{M}, F)$ finite$\}$ is dense in the set $CS(T)$ of all sentences consistent with T.

2) T is F-cic $\Leftrightarrow$ $T \vdash \Delta^{cor}(\mathcal{M}, T)$, for every $\mathcal{M} \models T$.
$\Leftrightarrow$ $\Delta^{cor}(\mathcal{M}, F) = \Delta^{cor}(\mathcal{N}, F)$, for every $\mathcal{M}, \mathcal{N} \models T$.

3) *T is F-compatible* $\Leftrightarrow$ *T has an F-prime-envelope.*
$\Leftrightarrow$ *The theory $T \cup \{cor(\varphi); \varphi \in F'\}$ decides all atomic $L^{F'}$-sentences, for every finite $F' \subseteq F$.*

Proof. 1): The first "$\Leftrightarrow$" is an easy consequence of Observation 1.2:13. The second "$\Leftrightarrow$" is trivial.
2): Directly from definition.
3): The first equivalence: "$\Rightarrow$": We set $Q = \bigcup_{\mathcal{M} \models T} \mathcal{M}_{c,F}/_{=_\mathcal{Q}}$, where $=_\mathcal{Q}$ is the transitive closure of $\bigcup_{\mathcal{M} \models T}(=_\mathcal{M} \restriction M_{c,F})$. For each symbol $r \in L^\mathcal{R}$, we define $r_\mathcal{Q} = \bigcup_{\mathcal{M} \models T} r_\mathcal{M}/_{=_\mathcal{Q}}$ and $f_\mathcal{Q}(\overline{[q]_{=_\mathcal{Q}}}) = f_\mathcal{M}(\overline{[q]_{=_\mathcal{M}}})$, if $\overline{q} \in M_{c,F}$, and 0 otherwise. The definitions are correct, and $\mathcal{Q} = \langle Q, r_\mathcal{Q}, f_\mathcal{Q} \rangle$ is an F-prime-envelope of T.
"$\Leftarrow$" is immediate. The second equivalence is easy.

□

1.3 Analysis of lineals and linear theories

In this section, we define the key concepts of this chapter – the notions of a lineal and a linear theory – and formulate our main results concerning them; the proof of the results is postponed to section 1.5. We prove that ZAa and ZLa (defined in section 1.1) are examples of linear theories; in section 1.4, we will use the results of this section to perform a basic model-theoretic analysis of ZAa and ZLa.

1.3.1 Lineals and linear theories

As we allready stated in the prologue of this chapter, linear theories are, informatively (up to a change of the language), theories of some (expansions by constants of) discretely ordered modules over certain discretely ordered integral domains. More precisely, T is a linear theory if every model $\mathcal{A} \models T$ is equidefinable with certain expansion of a discretely ordered module (called lineal; see 1.3.1.3) over a domain which is a doded (see 1.3.1.2). Note that, by Corollary 1.3:5, every $\mathcal{A} \models T$ has quantifier elimination in the language of the corresponding lineal.

1.3.1.1 Notation

For a structure $\mathcal{M}$ in a language $L = \langle 0, 1, +, -, \leq, \ldots \rangle$, we denote ${}^+M$ the set of all non-negative elements from M.

For an unary increasing function f on M, f^{-1} denotes the integral inverse of f (if it exists), i.e. the function f^{-1} such that $f^{-1}(x)$ is the largest y with $f(y) \leq x$. For linear f, this is equivalent to

$$\langle \mathcal{M}, f, f^{-1} \rangle \models 0 \leq x - f(f^{-1}(x)) < f(1). \tag{1.6}$$

1.3.1.2 Doded

An ordered integral domain $\mathsf{D} = \langle \mathrm{D}, 0, 1, +, -, \cdot, \leq \rangle$ is called a *doded* if it

(R1) is discretely ordered by $\leq$, with 1 being the least positive element, i.e.

(R1-a) $\leq$ is a linear ordering of D,

(R1-b) $r \leq s \to r + t \leq s + t$,

(R1-c) $0 \leq r, s \to 0 \leq r \cdot s$,

(R1-d) $0 < 1 \,\&\, \neg(\exists r)(0 < r < 1)$,

(R2) is regularly quasi-Euclidean, i.e. the Euclidean algorithm in D (with one step given by $(q, r) \mapsto (r, q - rr^{-1}(q)))$ is correctly defined and always stops in finitely many steps (at some $(q', 0)$),

(R3) has degrees, i.e. there is a function $\deg : \mathrm{D} \to \mathbb{N} \cup \{-\infty\}$ such that $\mathrm{rng}(\deg)$ is a lower set in $\mathbb{N} \cup \{-\infty\}$, and $\deg r \leq \deg q \Leftrightarrow |r| \leq n|q|$, for some $n \in \mathbb{N}$.

Example 1.3:1.

a) The ordered ring of integers is a doded; the degree map is defined as $\deg z = 0$, for $0 \neq z \in \mathbb{Z}$, and $\deg 0 = -\infty$.

b) Let $\tau = \langle \tau_p \rangle \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$, where $\mathbb{P}$ is the set of all prime numbers, and $\mathbb{J}_p$, for $p \in \mathbb{P}$, is the ring of p-adic integers. Let $\mathbb{Z}[a] \subseteq \mathrm{D}_\tau \subseteq \mathbb{Q}[a]$ be defined as

$$\mathrm{D}_\tau = \left\{ \frac{r}{n} \in \mathbb{Q}[a]; 0 < n \in \mathbb{N}, r \in \mathbb{Z}[a], \text{ and } (\forall p \in \mathbb{P})\, \pi_{\mathrm{v}_p(n)}(r(\tau_p)) = 0 \right\}.$$

Here, v_p denotes the usual p-valuation, π_k the canonical projection of $\mathbb{J}_p$ to $\mathbb{Z}_{p^k}$. Further, τ_p is the pth projection of τ, and the substitution $r(\tau_p)$ is done inside $\mathbb{J}_p$, where $\mathbb{Z}$ is embedded via $z \mapsto (z \bmod p, z \bmod p^2, z \bmod p^3, \dots)$. See section 3.2 for details.

Equivalently:

$$\tfrac{r}{n} \in \mathrm{D}_\tau \Leftrightarrow n | r(a),$$

where a is such that $a \equiv_{p^k} \tau_p(k)$, for $p \in \mathbb{P}$ and $k \in \mathbb{N}$.

The ring D_τ is a doded: It is discretely (linearly) ordered since no $q \in \mathbb{Q}[a]$ with $0 < q < 1$ is in D_τ. The degree map is the usual degree of polynomials. D_τ is regularly quasi-Euclidean by Theorem 3.4:2.

1.3.1.3 Lineal

A lineal is any structure $\mathcal{F} = \langle F, 0, 1, +, -, \leq, r, c, q^{-1}\rangle_{r\in \mathrm{D}_\mathcal{F}, c\in \mathrm{C}_\mathcal{F}, q\in {}^+\mathrm{D}_\mathcal{F}}$ where

- $\mathrm{D}_\mathcal{F}$ is an universe of a doded $\mathsf{D}_\mathcal{F}$,
- $\mathcal{F}$ and $\mathcal{C}_\mathcal{F} = \mathcal{F} \restriction \mathrm{C}_\mathcal{F}$ are expansions of discretely ordered $\mathsf{D}_\mathcal{F}$-modules (with the least positive element 1) by constants c and integral inverses q^{-1}.

The definition above implicitly states that the functions q^{-1}, for $q \in {}^+\mathrm{D}_\mathcal{F}$, are all correctly defined, and $\mathrm{C}_\mathcal{F}$ is closed on all q^{-1}. Moreover, since, for given $q \in {}^+\mathrm{D}_\mathcal{F}$, the mapping $r \mapsto r1$ is an embedding of $\langle \mathrm{D}_\mathcal{F}, 0, 1, +, -, \leq, q \cdot \_\rangle$ into $\langle F, 0, 1, +, -, \leq, q\rangle$, and q^{-1} is defined in both these structures by the same formula (as in (1.6)), we get the following, for all $q, r \in \mathrm{D}_\mathcal{F}$, $q > 0$:

$$\mathcal{F} \models (q^{-1}r)1 = q^{-1}(r1).$$

This observation enables us to consider $\langle \mathrm{D}_\mathcal{F}, 0, 1, +, -, \leq, r \cdot \_, q^{-1}\rangle_{r\in \mathrm{D}_\mathcal{F}, q\in {}^+\mathrm{D}_\mathcal{F}}$ as a substructure of $\langle F, 0, 1, +, -, \leq, r, q^{-1}\rangle_{r\in \mathrm{D}_\mathcal{F}, q\in {}^+\mathrm{D}_\mathcal{F}}$ and to identify $r \in \mathrm{D}_\mathcal{F}$ with $r1 \in F$.

We extend the degree map $\deg : \mathrm{D}_\mathcal{F} \to \mathbb{N} \cup \{-\infty\}$ to the whole F by

$$\deg(x) = \min\{\deg(r); r \in \mathrm{D}_\mathcal{F}, |x| \leq r\}, \tag{1.7}$$

where $\min(\emptyset) = \infty$.

Example 1.3:2.

a) The structure $\langle \mathbb{Z}, 0, 1, +, -, \leq, \underline{z}, \mathbf{z}, \underline{n}^{-1}\rangle_{z\in\mathbb{Z}, 0<n\in\mathbb{N}}$ is a lineal (the ring of integers is a doded by Example 1.3:1 a)). More generally, for $\mathcal{A} \models \mathrm{ZAa}$, the structure $\mathcal{F}_\mathcal{A} = \langle A, 0, 1, +, -, \leq, \underline{z}, \mathbf{z}, \underline{n}^{-1}\rangle_{z\in\mathbb{Z}, 0<n\in\mathbb{N}}$ is a lineal.

b) Let us recall that, for a formula φ, we denote $cor(\varphi)$ the formula "φ is correct defining formula of a function", and if s is a symbol defined by φ, we write $\dot{s}$ for φ (see section 1.2.3).

   Let $\mathcal{A} = \langle A, 0, 1, +, -, \underline{a}, \leq\rangle \models \mathrm{ZLa}$. We set

$$\begin{aligned} \mathrm{C}_\mathcal{A} = \mathrm{D}_\mathcal{A} &= \{r \in \mathbb{Q}[a]; \mathcal{A} \models cor(\dot{\underline{r}})\} = \\ &= \{r \in \mathbb{Q}[a]; r = \tfrac{p}{n} \text{ with } p \in \mathbb{Z}[a],\ n \in \mathbb{N} \text{ and } \mathcal{A} \models \mathbf{n}|\mathbf{p}\} = \\ &= \mathbb{Q}[a] \cap A. \end{aligned}$$

   Clearly, $\mathbb{Z}[a] \subseteq \mathrm{D}_\mathcal{A} \subseteq \mathbb{Q}[a]$, and $\mathrm{D}_\mathcal{A}$ is closed under operations of the polynomial ring $\mathbb{Q}[a]$; we denote $\mathsf{D}_\mathcal{A}$ the ordered subring of the ordered polynomial ring $\mathbb{Q}[a]$ with the universe $\mathrm{D}_\mathcal{A}$.

   By Proposition 3.3:2 (it is easy to verify that the proof uses only properties of $\mathcal{A}$ provable in ZLa), the rings $\mathsf{D}_\mathcal{A}$, for $\mathcal{A} \models \mathrm{ZLa}$, correspond (not uniquely) to the rings D_τ from Example 1.3:1 b) and vice versa.

More precisely,

$$\mathrm{D}_\tau = \mathrm{D}_\mathcal{A} \Leftrightarrow \mathcal{A} \models p^k | \mathbf{a} - \pi_k(\tau_p) \text{ for all } p \in \mathbb{P},\ 0 < k \in \mathbb{N}.$$

The structure $\mathcal{F}_\mathcal{A} = \langle A, 0, 1, +, -, \leq, \underline{r}, \mathbf{p}, \underline{q}^{-1} \rangle_{r \in \mathrm{D}_\mathcal{A}, p \in \mathrm{C}_\mathcal{A}, q \in^+ \mathrm{D}_\mathcal{A}}$ is a lineal.

Proof: $\mathsf{D}_\mathcal{A}$ is a doded by Example 1.3:1 b). $\mathcal{F}_\mathcal{A}$ is an expansion of an ordered $\mathsf{D}_\mathcal{A}$-module by Lemma 1.1:2. To show that $\mathrm{C}_\mathcal{A}$ is a universe of a substructure of $\mathcal{F}_\mathcal{A}$, it suffices to show that it is closed under the functions $\underline{q}^{-1}$, for all $0 < q \in \mathrm{D}_\mathcal{A}$; this is proved in Lemma 3.4:1 (the proof can be done in ZLa).

c) Let $\mathcal{A} \models$ZAa^c= ZAa $\cup \{c \geq n; n \in \mathbb{N}\}$. We denote $\mathsf{D}_\mathcal{A}$ the ring of integers, and we set

$$\mathrm{C}_\mathcal{A} = \mathbb{Q}\langle c^A, 1\rangle \cap A = \left\{ \frac{ic^A + j}{l}; i, j, l \in \mathbb{Z},\ l > 0,\ \mathcal{A} \models l | ic + j \right\}.$$

Then the structure $\mathcal{F}_\mathcal{A} = \langle A, 0, 1, +, -, \leq, \underline{z}, k, \underline{n}^{-1} \rangle_{z \in \mathbb{Z}, k \in \mathrm{C}_\mathcal{A}, 0 < n \in \mathbb{N}}$ is a lineal. Indeed, it is enough to prove that $\mathrm{C}_\mathcal{A}$ is closed under the functions $\underline{n}^{-1}$, for $0 < n \in \mathbb{N}$: Let $k = \frac{ic+j}{l} \in \mathrm{C}_\mathcal{A}$ and $0 < n \in \mathbb{N}$. By integral divisibility in ZAa^c, there is $0 \leq m < n$ such that $n | k - m$. Then $\underline{n}^{-1} k = \frac{k-m}{n} = \frac{ic + (j - ml)}{nl} \in \mathrm{C}_\mathcal{A}$.

1.3.1.4 Linear theory, linealization

Let L be a language extending $L^z = \langle 0, 1, +, -, \leq \rangle$ (where $-$ is unary), T be an L-theory, and let $\mathrm{D}, \mathrm{C} \subseteq Fm_L$. A (D, C)-*linealization* of T is any map $\mathcal{A} \mapsto \mathcal{F}_\mathcal{A}$, for $\mathcal{A} \models T$, such that every $\mathcal{F}_\mathcal{A} = \langle A, 0, 1, +, -, \leq, r, c, q^{-1} \rangle_{r \in \mathrm{D}_{\mathcal{F}_\mathcal{A}}, c \in \mathrm{C}_{\mathcal{F}_\mathcal{A}}, q \in^+ \mathrm{D}_{\mathcal{F}_\mathcal{A}}}$ is a lineal equidefinable with $\mathcal{A}$, and the sets $\dot{\mathrm{D}}_{\mathcal{F}_\mathcal{A}}$, $\dot{\mathrm{C}}_{\mathcal{F}_\mathcal{A}}$ of definitions in $\mathcal{A}$ of functions from $\mathrm{D}_{\mathcal{F}_\mathcal{A}}$ and constants from $\mathrm{C}_{\mathcal{F}_\mathcal{A}}$ satisfy $\dot{\mathrm{D}}_{\mathcal{F}_\mathcal{A}} \subseteq \mathrm{D}$ and $\dot{\mathrm{C}}_{\mathcal{F}_\mathcal{A}} \subseteq \mathrm{C}$.

An L-theory T is a *linear theory* if it has an (Fm_L, Fm_L)-linealization.

Example 1.3:3.

a) Let $\dot{\mathbb{Z}}_1$ and $\dot{\mathbb{Z}}_0$ denote the sets of $L^{add}_\mathbb{Z}$-formulas $\dot{\underline{z}}$ and $\dot{\mathbf{z}}$ which define symbols $\underline{z}$ and $\mathbf{z}$, for $z \in \mathbb{Z}$, respectively. ZAa is a linear theory, and

$$\mathcal{A} \mapsto \mathcal{F}_\mathcal{A} = \langle A, 0, 1, +, -, \leq, \underline{m}, \mathbf{k}, \underline{n}^{-1} \rangle_{m \in \mathbb{Z}, k \in \mathbb{Z}, n \in \mathbb{N} - \{0\}},$$

for $\mathcal{A} \models$ ZAa, is its $(\dot{\mathbb{Z}}_1, \dot{\mathbb{Z}}_0)$-linealization.

b) Let $\dot{\mathbb{Q}}[a]_1$ and $\dot{\mathbb{Q}}[a]_0$ be the sets of all $L^{lin}_\mathbb{Z}$-formulas $\dot{\underline{r}}$ and $\dot{\mathbf{r}}$ which define symbols $\underline{r}$ or $\mathbf{r}$ respectively, for $r \in \mathbb{Q}[a]$. ZLa is a linear theory, and

$$\mathcal{A} \mapsto \mathcal{F}_\mathcal{A} = \langle A, 0, 1, +, -, \leq, \underline{r}, \mathbf{p}, \underline{q}^{-1} \rangle_{r \in \mathrm{D}_\mathcal{A}, p \in \mathrm{C}_\mathcal{A}, q \in^+ \mathrm{D}_\mathcal{A}},$$

for $\mathcal{A} \models$ ZAa, is its $(\dot{\mathbb{Q}}[a]_1, \dot{\mathbb{Q}}[a]_0)$-linealization.

c) Let $\dot{\mathbb{Q}}\langle c,1\rangle_0$ denotes the set of all formulas $\dot{k}$ which define constants $k \in \mathbb{Q}\langle c,1\rangle$ (see Example 1.3:2 c)). The theory ZAa^c from Example 1.3:2 c) is a linear theory, and

$$\mathcal{A} \mapsto \mathcal{F}_{\mathcal{A}} = \langle A, 0, 1, +, -, \leq, \underline{m}, k, \underline{n}^{-1}\rangle_{m\in\mathbb{Z}, k\in \mathrm{C}_{\mathcal{A}}, n\in\mathbb{N}-\{0\}},$$

for $\mathcal{A} \models$ ZAa^c, is its $(\dot{\mathbb{Z}}_1, \dot{\mathbb{Q}}\langle c,1\rangle_0)$-linealization.

We further identify $\mathrm{D}_{\mathcal{F}_{\mathcal{A}}}$ with the set $\dot{\mathrm{D}}_{\mathcal{F}_{\mathcal{A}}} \subseteq Fm_L$ of L-definitions of functions $r \in \mathrm{D}_{\mathcal{F}_{\mathcal{A}}}$ and similarly for $\mathrm{C}_{\mathcal{F}_{\mathcal{A}}}$. When a linealization is fixed, we often write $\mathrm{D}_{\mathcal{A}}$, $\mathrm{C}_{\mathcal{A}}$ instead of $\mathrm{D}_{\mathcal{F}_{\mathcal{A}}}$, $\mathrm{C}_{\mathcal{F}_{\mathcal{A}}}$.

Also, for a set $D \subseteq Fm_L$ of definitions of unary functions, by D^{-1} we denote the set of definitions of their integral inverses (see section 1.3.1.1).

1.3.2 Main results

At this place, we state our three main theorems on linear theories and lineals (1.3:4, 1.3:6 and 1.3:8) and their important corollaries. The Main Theorem on Linear Theories 1.3:4 is essential for our descriptive analysis of linear theories, the other two theorems are its refinements, which help us to provide a detailed characterization of definable functions and sets in models of linear theories.

1.3.2.1 Solvability and quantifier elimination

The following is a fundamental statement concerning descriptive complexity of (models of) linear theories. The concept of solvability is defined in section 1.2.2; see also section 1.2.3 for the explanation of the notation T^F.

Theorem 1.3:4 (Main Theorem on Linear Theories)**.** *Let T be a linear theory in a language L, $\mathcal{A} \mapsto \mathcal{F}_{\mathcal{A}}$ be a (D,C)-linealization, and $E = \mathrm{D} \cup \mathrm{C} \cup \mathrm{D}^{-1}$. Then*

1) T^E is almost uniformly solvable.

2) T^{C} is 0-solvable.

From Theorem 1.3:4 2), it follows that, for every $\mathcal{A} \models T$, the set $\mathrm{C}_{\mathcal{A}}$ is the universe of a substructure of $\mathcal{A}$; we set $\mathcal{C}_{\mathcal{A}} = \mathcal{A} \restriction \mathrm{C}_{\mathcal{A}}$.

Corollary 1.3:5.

1) T^E admits quantifier elimination and is axiomatizable by open formulas.

2) For $\mathcal{A} \models T$, the structure $\mathcal{C}_{\mathcal{A}}$ is the unique prime model of $Th(\mathcal{A})$.

3) For $\mathcal{A} \models T$, the theory $Th(\mathcal{A})$ is equivalent to $T \cup OTh_L(\mathcal{A}^{\mathrm{C}})$ (or equivalently to $T \cup OTh_L({\mathcal{C}_{\mathcal{A}}}^{\mathrm{C}})$),

where $OTh_L(\mathcal{N})$ is the canonical L-translation of the set of all open sentences true in $\mathcal{N}$.

Proof. 1) follows from Proposition 1.2:6, 2) and 3) from Corollary 1.2:12. □

1.3.2.2 Harmonic forms

We prove that every term or formula can be, in a given lineal, equivalently written in "harmonic form", i.e. as composed solely of linear combinations of expressions of the form $r^{-1}x$, where x is a variable. Let, further, $\mathcal{F}$ be a fixed lineal. We write D and C instead of $\mathrm{D}_{\mathcal{F}}$ and $\mathrm{C}_{\mathcal{F}}$.

1.3.2.2.1 Harmonic term We say that a term $t(\overline{x})$ is *harmonic* (or equivalently *in harmonic form*) if

$$t(\overline{x}) = \sum_{i=0}^{N-1} \underline{q_i}\,\underline{r_i}^{-1}(x_{f(i)}) + \underline{c},$$

for some $q_i, r_i \in \mathrm{D}$, $c \in \mathrm{C}$ and $f : N \to l(\overline{x})$. A formula or a p-term (see 1.2.2.4) is harmonic if all its maximal subterms are.

1.3.2.2.2 Almost-term The following special case of a p-term is worth to be named. A p-term τ is called an *almost-term* if it is of the form

$$\tau(\overline{x}) = \Big\{ s(\overline{x}) + c_i \text{ if } \psi_i(\overline{x}),\ i < n,$$

where $s(\overline{x})$ is a term, and $c_i \in \mathrm{C}$, for $i < n$. We write $\mathrm{core}(\tau)$ for s and $\mathrm{cond}(\tau)$ for the set of all "conditions" ψ_i, $i < n$.

Theorem 1.3:6 (Harmonic Form Theorem)**.** *Let $\mathcal{F}$ be a lineal.*

1) For every term $t(\overline{x})$, there is an open harmonic almost-term $\tau(\overline{x})$ such that $\mathcal{F} \models t(\overline{x}) = \tau(\overline{x})$.

2) For every formula $\varphi(\overline{x})$, there is an open harmonic formula $\psi(\overline{x})$ such that $\mathcal{F} \models \varphi(\overline{x}) \leftrightarrow \psi(\overline{x})$.

Remark 1.3:7*.* Our proof of Theorem 1.3:6, in fact, proves more than stated – the equivalent harmonic forms can be found not only for each lineal $\mathcal{F}$ separately but at once for a given linear theory. However, proving this explicitely would cause that all the statements and subproofs of our proof would be recognizably longer and more complicated.

1.3.2.3 Bases and definable functions and sets in lineals

The machinery, we are going to develop for the proof of the Main Theorem 1.3:4, enables us to perform a detailed analysis of definable functions and sets in a lineal $\mathcal{F}$. In particular, we prove that every definable set $D \subseteq F^n$ is a union of linear images of polyhedra in F^m, for some $m \in \mathbb{N}$ (see Corollary 1.3:9 2)).

1.3.2.3.1 Divisor Let α be a formula or a p-term in harmonic form. A scalar $r \in \mathrm{D}$ is called an *x-divisor* [*divisor*] of α if α contains a subterm of the form $r^{-1}x$ [for some variable x]. The set of all x-divisors [divisors] in α is denoted $\mathrm{Div}_x(\alpha)$ [$\mathrm{Div}(\alpha)$]. α is said to be *over* a set $S \subseteq \mathrm{D}$ [in x] if $\mathrm{Div}(\alpha) \subseteq S$ [$\mathrm{Div}_x(\alpha) \subseteq S$]. If $\mathrm{Div}_{[x]}(\alpha) = \emptyset$, we call α *linear* [in x].

1.3.2.3.2 Basis Let $d \leq e \leq \omega$ and $B \subseteq {}^+\mathrm{D}$. We say that B is a *$[d, e]$-basis* if there is an enumeration $B = \langle b_i \rangle_{d \leq i < e}$ such that $\deg b_i = i$. $[0, \omega]$-basis is often called just *basis*.

Theorem 1.3:8 (Bases Theorem)**.** *Let $\overline{\delta} \in F^n$, $C_p(\overline{\delta}) = \prod_{i<n}[\delta_i, \delta_i + p - 1] \subseteq F^n$ be a cube with edges of scalar length $p \in \mathrm{D}$, $e = \deg(p)$, and B be a $[0, e]$-basis. Let $l(\overline{x}) = n$. Then the following holds:*

1) Every term $t(\overline{x})$ is on $C_p(\overline{\delta})$ equal to a harmonic almost-term $\tau(\overline{x})$ which is over mB for some $m \in \mathbb{N}$.

2) Every formula $\varphi(\overline{x})$ is on $C_p(\overline{\delta})$ equivalent to an open harmonic formula $\psi(\overline{x})$ which is over mB for some $m \in \mathbb{N}$.

Moreover:

- *m can be chosen as any number sufficiently large with respect to divisibility.*
- *If t or φ contain parameters from a set X then τ and ψ contain only parameters from $X \cup \overline{\delta}$.*

1.3.2.3.3 Box, polyhedron For $0 < \overline{a} \in F^n$, we denote

$$K(\overline{a}) = \prod_{i=0}^{n-1}[0, a_i - 1]$$

the n-dimensional *box* with edges $\overline{a}$. Let $Y \subseteq F^n$ and $\overline{\beta} \in F$. A set $P \subseteq Y \subseteq F^n$ is called a *polyhedron* in Y over parameters from $X \subseteq F$ if P is the set of all solutions $\overline{x} \in Y$ of a system of inequalities of the form $L(\overline{x}) \leq s(\overline{\beta})$, where s is a term, $\overline{\beta} \in X$ are parameters, and L is a linear form (in $\mathcal{F}$, i.e. with coefficients from D).

1.3.2.3.4 Linear coordination of F^n Let $\overline{\delta} = (\delta_0, \ldots, \delta_{n-1}) \in F^n$, $m = a_0 \in \mathbb{N}$, and let $\overline{a} = (a_0, a_1, \ldots, a_N)$ and p be scalars such that $\deg(a_i) = 1$, for $1 \leq i \leq N$, $\deg(p) = N$, and $mb_N \geq p$, where $b_0 = 1$, $b_j = \prod_{1 \leq i \leq j} a_i$ (then $\langle b_j \rangle_{0 \leq j \leq N}$ is a $[0, N+1]$-basis).

We define $g' : K(\overline{a}) \times F \to F$ as

$$g'(\overline{\alpha}, u) = \alpha_0 + \sum_{j=0}^{N-1} m b_j \alpha_{j+1} + pu \tag{1.8}$$

and $g : (K(\overline{a}) \times F)^n \to F^n$ as $g = (g' + \delta_0, \ldots, g' + \delta_{n-1})$, i.e.

$$g((\overline{\alpha_i}, u_i)_{i<n}) = (g'(\overline{\alpha_i}, u_i) + \delta_i)_{i<n}. \tag{1.9}$$

We call such a g the *(linear)* $(\overline{\delta}, \overline{a}, p)$*-coordination* of F^n.

Obviously, g is surjective, thanks to $mb_N \geq p$. If $mb_N = p$ then g is a bijection.

We set

$$P_g = \{(\overline{\alpha_i}, u_i)_{i<n}; \bigwedge_{i<n} \alpha_{i,0} + \sum_{j=0}^{N-1} mb_j \alpha_{i,j+1} < p\}.$$

It is easy to see that $g \restriction P_g : P_g \to F^n$ is a bijection.

An important property of a coordination is that, for $x = g'(\overline{\alpha}, 0)$, $(mb_i)^{-1} x$ is a linear combination of $\overline{\alpha}$:

$$(mb_i)^{-1} x = \sum_{j=i}^{N-1} \frac{b_j}{b_i} \alpha_{j+1}, \tag{1.10}$$

where $b_i | b_j$, for $i \leq j$.

Corollary 1.3:9. *Let $\mathcal{F}$ be a lineal, $\overline{\delta} = (\delta_0, \ldots, \delta_{n-1}) \in F^n$, $\langle a_i \rangle_{i=1}^{\infty}$ be scalars with* $\deg(a_i) = 1$, *for all i, and let $X \subseteq F$ be a set of parameters. Then the following holds:*

1) Every X-definable (in $\mathcal{F}$) function $f : F^n \to F$ is given by a formula

$$f \circ g = \lambda \text{ on } P_g,$$

i.e. $f(g((\overline{\alpha_i}, u_i)_{i<n})) = \lambda((\overline{\alpha_i}, u_i)_{i<n})$ for $((\overline{\alpha_i}, u_i)_{i<n}) \in P_g$, where the map $g : (K(\overline{a}) \times F)^n \to F^n$ is a $(\overline{\delta}, \overline{a}, p)$-coordination of F^n, with $a_0 = m \in \mathbb{N}$, $\overline{a} = (a_0, \ldots, a_N)$ and p a scalar, and $\lambda((\overline{\alpha_i}, u_i)_{i<n})$ is a linear p-term over parameters from $X \cup \overline{\delta}$.

In a particular case when f is a term, λ can be chosen as a linear almost-term.

2) Every set $D \subseteq F^n$ X-definable in $\mathcal{F}$ can be written as

$$D = \bigcup_{i<k} g[P_i],$$

where $g : (K(\overline{a}) \times F)^n \to F^n$ is a $(\overline{\delta}, \overline{a}, p)$-coordination of F^n, with $a_0 = m \in \mathbb{N}$, $\overline{a} = (a_0, \ldots, a_N)$ and p a scalar, and $P_i \subseteq P_g$, for $i < k$, are finitely many polyhedra in $(K(\overline{a}) \times F)^n$ over parameters from $X \cup \overline{\delta}$.

Moreover, $a_0 = m$ and p may be chosen as any elements sufficiently large with respect to divisibility (the choice of m depends on p).

Proof. 1): By Proposition 1.2:9, f is the realization of a p-term τ with parameters from X. Therefore it is enough to prove the statement for $f = t(\overline{x})$ where t is a term (with parameters from X). We may also suppose $\overline{\delta} = \overline{0}$ (the general result may be then obtained by setting $t'(\overline{y}) = t(\overline{y} + \overline{\delta})$).

Let $t(\overline{x})$ be a term and $\overline{\delta} = \overline{0}$. There is a scalar p which is a linear period of t, i.e. there are scalars $\overline{\gamma}$ such that $t(\overline{x} + p\overline{u}) = t(\overline{x}) + \overline{\gamma u}$ holds for all $\overline{x}, \overline{u}$. We set $N = \deg(p)$, $b_0 = 1$, $b_j = \prod_{1 \leq i \leq j} a_i$ (then $\langle b_j \rangle_{0 \leq j \leq N}$ is a $[0, N+1]$-basis) and take $a_0 = m \in \mathbb{N}$ such that $mb_N \geq p$ and such that there is an almost-term $\tau(\overline{x})$ over $\langle mb_j \rangle_{j<N}$ with $\tau(\overline{x}) = t(\overline{x})$, for $0 \leq \overline{x} < p$ (this can be achieved by Theorem 1.3:8; τ is with parameters from X). Let g be the $(\overline{0}, \overline{a}, p)$-coordination of F^n.

Every $\overline{x} \in F^n$ can be uniquely written in the form $\overline{x} = g((\overline{\alpha_i}, u_i)_{i<n})$, with $(\overline{\alpha_i}, u_i)_{i<n} \in P_g$. Set $h(\overline{\alpha_i}) = \alpha_{i,0} + \sum_{j=0}^{N-1} mb_j \alpha_{i,j+1}$. Then it is

$$t(g((\overline{\alpha_i}, u_i)_{i<n})) = t((h(\overline{\alpha_i}))_{i<n}) + \overline{\gamma u} = \tau((h(\overline{\alpha_i}))_{i<n}) + \overline{\gamma u}.$$

By (1.10), it is $\tau((h(\overline{\alpha_i}))_{i<n}) + \overline{\gamma u} = \lambda((\overline{\alpha_i}, u_i)_{i<n})$, for some linear almost-term λ.

The "moreover" part of the statement is clear from our choice of p and m.

2): Let D be defined by a formula $\varphi(\overline{x})$ with parameters from X. By Corollary 1.3:5 1), we may suppose that φ is open.

For every atomic subformula $t(\overline{x}) \leq 0$ of φ, let λ_t be a linear almost-term and g_t a $(\delta, \overline{a}, p)$-coordination such that $t \circ g_t = \lambda_t$ (this is possible by 1)). By the "moreover" part of the statement, we may suppose that all g_t are mutually equal and denote them just g. Every $\overline{x} \in F^n$ can be uniquely written in the form $\overline{x} = g((\overline{\alpha_i}, u_i)_{i<n})$, with $(\overline{\alpha_i}, u_i)_{i<n} \in P_g$. Then $t(\overline{x}) \leq 0 \Leftrightarrow \lambda_t((\overline{\alpha_i}, u_i)_{i<n}) \leq 0$. The last inequality defines a finite union of polyhedra in $(K(\overline{a} \times F))^n$ with parameters $X \cup \overline{\delta}$. This proves the theorem.

□

Remark 1.3:10. The statement of the Corollary 1.3:9 2) can be understood as stating that the Boolean algebra of definable sets (over parameters X) in $\mathcal{F}$ is isomorphic to the algebra generated by polyhedra over X in $K(\overline{a})$.

The similar statement for the Lindenbaum algebra of a linear theory can be proven as well. However, we do not do that for the same reasons which we already explained in the Remark 1.3:7.

Remark 1.3:11. Let us note that, alternatively, linear theories may be defined as two sorted ("ordered ring-ordered module") theories. In that case the proof of the Main Theorem on Linear Theories 1.3:4 yields a quantifier elimination statement for ordered modules with scalar variables – see section 1.6 for details. This problem has been studied in [vdDH92] for unordered modules and in [Wei97] for discretely ordered modules over the ring $\mathbb{Z}$ of integers (more precisely for the two-sorted variant of Presburger arithmetic).

1.4 Application of the main results

We use the Main Theorem on Linear Theories 1.3:4 to examine basic model-theoretic properties of linear theories ZAa and ZLa (and consequently of their $\mathbb{N}$-like versions Aa and La).

The results are stated in Propositions 1.4:1 and Theorem 1.4:5, respectively, and in their corollaries.

1.4.1 Properties of ZAa and Aa

The theory ZAa (which is only a $\mathbb{Z}$-like version of Presburger arithmetic Pr) is well-explored. In this section, we mostly reprove long-known results. We do that in order to show the possibilities of our method and to give the reader an opportunity to become more familiar with concepts we defined. If the reader feels confident in understanding our previous definitions, he or she may safely skip this section.

In Example 1.3:3 a), we showed that ZAa is a linear theory and we described its linealization. Let us remind that $\dot{\mathbb{Z}}_1$ and $\dot{\mathbb{Z}}_0$ stand for the sets of $L^{add}_{\mathbb{Z}}$-formulas $\dot{\underline{z}}$ and $\dot{\mathbf{z}}$ which define symbols $\underline{z}$ and $\mathbf{z}$, for $z \in \mathbb{Z}$, respectively. We denote $\dot{\mathbb{Z}} = \dot{\mathbb{Z}}_1 \cup \dot{\mathbb{Z}}_0 \cup {}^+\dot{\mathbb{Z}}_1^{-1}$, where ${}^+\dot{\mathbb{Z}}_1^{-1}$ denotes the set of definitions of integral inverses of positive scalars $\underline{z}$. It is easy to see that all formulas from $\dot{\mathbb{Z}}$ are in ZAa equivalent to existential ones.

The Main Theorem on Linear theories 1.3:4 and the results from section 1.2 make it easy to prove the following properties of the theory ZAa:

Proposition 1.4:1 (Properties of ZAa)**.**

1) $\mathrm{ZAa}^{\dot{\mathbb{Z}}}$ *is almost uniformly solvable,* $\mathrm{ZAa}^{\dot{\mathbb{Z}}_0}$ *is* 0*-solvable.*
Hence: ZAa *is model-complete.*
Moreover: Every formula is in ZAa *equivalent to a disjunction of primitive positive formulas, i.e. to a formula of the form* $\bigvee_{i<n}(\exists \overline{z})\psi_i$*, where each* ψ_i *is a system of linear inequalities.*

2) ZAa *is decidable, complete, and* $\langle \mathbb{Z}, 0, 1, +, -, \leq \rangle$ *is its prime model.*

3) Theories ZAa*,* ZAA *and* $Th(\langle \mathbb{Z}, 0, 1, +, -, \leq \rangle)$ *are equivalent.*

Proof. 1) is a corollary of Theorem 1.3:4 and the fact that each formula from $\dot{\mathbb{Z}}$ is equivalent to a disjunction of primitive positive formulas.
2): $\langle \mathbb{Z}, 0, 1, +, -, \leq \rangle$ is the prime model of every $Th(\mathcal{A})$ with $\mathcal{A} \models$ ZAa, by Corollary 1.3:5 2), hence it is the prime model of ZAa. Completeness and decidability are immediate consequences.
3): Clearly, ZAA and $Th(\langle \mathbb{Z}, 0, 1, +, -, \leq \rangle)$ are extensions of ZAa; the statement then follows from 2). $\square$

Let $\dot{\mathbb{N}}_1$ and $\dot{\mathbb{N}}_0$ be the sets of L^{add}-formulas $\dot{\underline{n}}$ and $\dot{\mathbf{n}}$ which define symbols $\underline{n}$ and $\mathbf{n}$, for $n \in \mathbb{N}$, respectively. We denote $\dot{\mathbb{N}} = \dot{\mathbb{N}}_1 \cup \dot{\mathbb{N}}_0 \cup {}^{+}\dot{\mathbb{N}}_1^{-1}$, where ${}^{+}\dot{\mathbb{N}}_1^{-1}$ denotes the set of definitions of integral inverses of positive scalars $\underline{n}$.

Corollary 1.4:2 (Properties of Aa)**.**

1) $\mathrm{Aa}^{\dot{\mathbb{N}}}$ *is almost uniformly solvable,* $\mathrm{Aa}^{\dot{\mathbb{N}}_0}$ *is* 0*-solvable.*
Hence: Aa *is model-complete.*
Moreover: Every formula is in Aa *equivalent to a disjunction of primitive positive formulas, i.e. to a formula of the form* $\bigvee_{i<n}(\exists \overline{z})\psi_i$*, where each* ψ_i *is a system of linear inequalities.*

2) Aa *is decidable, complete, and* $\langle \mathbb{N}, 0, 1, +, \leq \rangle$ *is its prime model.*

3) Theories Aa*,* AA *and* $Th(\langle \mathbb{N}, 0, 1, +, \leq \rangle)$ *are equivalent.*

Proof. The statements follow easily from Proposition 1.4:1, by using relations (1.1) and (1.2) from 1.1.7. □

1.4.2 Properties of ZLa and La

We state here basic properties of ZLa – we show its elimination set of formulas, describe its simple complete extensions including their prime models and prove its decidability (see Theorem 1.4:5). Moreover, we provide a characterization of models of ZLa as non-principal ultraproducts of definable expansions of the standard model $\langle \mathbb{Z}, 0, 1, +, \leq \rangle$ (see Corollary 1.4:6). As a corollary, we get similar results also for La (Corollaries 1.4:7 and 1.4:8).

The results can be interpreted as stating that LA is model-theoretically very similar to Pr and far away from P (although the proof of the properties for LA is much more difficult than the same for Pr; we will discuss that in section 1.5). Whether this is true also for LA_κ with $\kappa \geq 2$, is posed as the Open question 1.

Let us remind that $\dot{\mathbb{Q}}[a]_1$ and $\dot{\mathbb{Q}}[a]_0$ are the sets of all $L^{lin}_{\mathbb{Z}}$-formulas $\dot{\underline{r}}$ and $\dot{\mathbf{r}}$ which define symbols $\underline{r}$ or $\mathbf{r}$ respectively, for $r \in \mathbb{Q}[a]$. The following lemma states that ZLa proves the "full" scheme of integral-divisibility (see 1.1.2 for definition).

Lemma 1.4:3. ZLa $\vdash$ *cor*$(\dot{\underline{r}}) \to$ *id*$(\underline{r})$*, for* $0 < r \in \mathbb{Q}[a]$*.*

Proof. Let $r = \frac{p}{n}$, with $p \in \mathbb{Z}[a]$, $0 < n \in \mathbb{N}$. Further, we work in a fixed $\mathcal{A} \models$ ZLa.

Suppose that $\mathcal{A} \models$ *cor*$(\dot{\underline{r}})$, i.e. $\mathbf{n}|\mathbf{p}$ in $\mathcal{A}$. By id($\underline{\mathrm{p}}$), there is y such that $0 \leq \underline{n}x - \underline{p}y < \underline{p}1$; then $0 \leq x - \underline{r}y < \underline{r}1$. □

In Example 1.3:3 b), we showed that ZLa is a linear theory, and we described its linealization. In order to formulate the consequences of the Main Theorem on Linear Theories 1.3:4 for ZLa, we need to introduce some notation.

1.4.2.1 Extensions ZLa_τ, structures $\mathcal{C}_\tau$

Motivated by the Example 1.3:2 b), we define ZLa_τ, for $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, to be the extension of ZLa by axioms expressing $\mathbf{p^k}|\mathbf{a} - \pi_k(\tau_p)$, for all $p \in \mathbb{P}$, $0 < k \in \mathbb{N}$.

We also set $\mathcal{C}_\tau = \langle \mathrm{D}_\tau, 0, 1, +, -, \leq, \underline{a}\rangle$, where $\underline{a}$ is the unary function of multiplication by the variable a (i.e. $\mathcal{C}_\tau$ is an $L^{lin}_{\mathbb{Z}}$-structure, which is a restriction of D_τ as a module over itself).

1.4.2.2 Syntactic presentation of $\mathrm{D}_\mathcal{A}$

For $\mathcal{A} \models \mathrm{ZLa}$, we identify the set $\mathrm{D}_\mathcal{A}$ (see Example 1.3:2 b)) with the set $A_{*,\dot{\mathbb{Q}}[a]_0}$ of all equivalence-classes of correct constant terms of $\mathcal{A}^{\dot{\mathbb{Q}}[a]_0}$ ($A_{*,\dot{\mathbb{Q}}[a]_0}$ is the universe of the canonical structure of $Th(\mathcal{A})^{\dot{\mathbb{Q}}[a]_0}$; see section 1.2.4 for details). This is possible since $\mathcal{A} \models \mathbf{r} \neq \mathbf{r}'$, for two different elements $r, r' \in \mathrm{D}_\mathcal{A}$.

Lemma 1.4:4. *The naturally defined $L^{\dot{\mathbb{Q}}[a]_0}$-structure $\mathcal{Q}$ with the universe $\mathbb{Q}[a]$ is a $\dot{\mathbb{Q}}[a]_0$-prime-envelope of* ZLa*. Therefore,* ZLa *is $\dot{\mathbb{Q}}[a]_0$-compatible and $\dot{\mathbb{Q}}[a]_0$-cuc.*

Proof. It is $A_{*,\dot{\mathbb{Q}}[a]_0} = \mathrm{D}_\mathcal{A} \subseteq \mathbb{Q}[a]$, for every $\mathcal{A} \models \mathrm{ZLa}$. Hence, $\mathcal{Q}$ is a $\dot{\mathbb{Q}}[a]_0$-prime-envelope of ZLa. The rest of the statement follows from Proposition 1.2:16 and Observation 1.2:14. □

1.4.2.3 Properties of ZLa

Denote $\dot{\mathbb{Q}}[a] = \dot{\mathbb{Q}}[a]_1 \cup \dot{\mathbb{Q}}[a]_0 \cup {}^+\dot{\mathbb{Q}}[a]_1^{-1}$, where ${}^+\dot{\mathbb{Q}}[a]_1^{-1}$ denotes the set of definitions of integral inverses of positive scalars $\underline{q}$. It is easy to see that all formulas from $\dot{\mathbb{Q}}[a]$ are in ZLa equivalent to existential formulas.

Theorem 1.4:5 (Properties of ZLa)**.**

1) $\mathrm{ZLa}^{\dot{\mathbb{Q}}[a]}$ *is almost uniformly solvable,* $\mathrm{ZLa}^{\dot{\mathbb{Q}}[a]_0}$ *is* 0*-solvable.*
Hence: ZLa *is model-complete.*
Moreover: Every formula is in ZLa *equivalent to a disjunction of primitive positive formulas, i.e. to a formula of the form $\bigvee_{i<n}(\exists \overline{z})\psi_i$, where each ψ_i is a system of linear inequalities.*

2) ZLa_τ*, for $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, are all simple complete extensions of* ZLa*.*
For $\mathcal{A}, \mathcal{B} \models \mathrm{ZLa}$, it is $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \mathbf{a}^\mathcal{A} \equiv \mathbf{a}^\mathcal{B} \mod n$, for all $0 < n \in \mathbb{N}$.

3) $\mathcal{C}_\tau$ *is the unique prime model of* ZLa_τ*, for $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$.*

4) ZLa *is decidable.*
ZLa_τ *is decidable if and only if τ is recursive.*

5) Theories ZLa *and* ZLA *are equivalent.*

Proof. 1) is a corollary of Theorem 1.3:4 and the fact that each formula from $\dot{\mathbb{Q}}[a]$ is equivalent to a disjunction of primitive positive formulas.

2): By Example 1.3:2 b), every model $\mathcal{A} \models$ ZLa is a model of some ZLa_τ, with $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$. ZLa is $\dot{\mathbb{Q}}[a]_0$-cuc, by Lemma 1.4:4. Now, by Proposition 1.2:16, it is enough to prove that for $\mathcal{A}, \mathcal{B} \models \mathrm{ZLa}_\tau$ it is $\mathrm{D}_\mathcal{A} = \mathrm{D}_\mathcal{B}$. This is true since $\frac{r}{n} \in \mathrm{D}_\mathcal{A} \Leftrightarrow \mathcal{A} \models \mathbf{n}|\mathbf{r}$, and the last is decided by the new axioms of ZLa_τ. The characterization of models up to elementary equivalence is an immediate consequence.

3) follows from 2) and Corollary 1.3:5 2).

4): The set $\{\bigwedge_{p_0>p\in\mathbb{P},k<k_0} \mathbf{a} \equiv_{p^k} \tau(p,k); p_0 \in \mathbb{P}, k_0 \in \mathbb{N}, \tau : (\mathbb{P} \cap p_0) \times k_0 \to \mathbb{N}$ such that $\tau(p,k') \equiv_{p^k} \tau(p,k) < p^k$, for all $k \le k' < k_0, p_0 > p \in \mathbb{P}\}$ is dense in $CS(\mathrm{ZLa})$, and it is easy to verify that it is Σ_1. Therefore, ZLa is Σ_1-separable and hence decidable, by Proposition 1.2:1.

ZLa_τ is decidable if and only if it is recursively axiomatizable.

5): For each $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, the theory ZLA_τ is a simple extension of ZLa_τ, and therefore these theories are equivalent, by 2). Then ZLA and ZLa have the same simple complete extensions, thus are equivalent. □

Corollary 1.4:6. *Up to elementary equivalence, models of* ZLa *are exactly all ultraproducts*

$$\mathcal{Z}_\mathcal{U} = (\prod_{n\in\mathbb{N}} \langle \mathbb{Z}, 0, 1, +, -, \underline{n}, \le \rangle)/_\mathcal{U},$$

where $\mathcal{U}$ *is a non-principal ultrafilter on* $\mathbb{N}$*, i.e.* $\mathcal{U} \in \beta\mathbb{N} - \mathbb{N}$.

Proof. 1) Let $\mathcal{U} \in \beta\mathbb{N} - \mathbb{N}$. We show that $\mathcal{Z}_\mathcal{U} \models$ ZLa.

All axioms of ZLa, except the axioms $\underline{a}1 \ne m$, are true in all structures $\langle \mathbb{Z}, 0, 1, +, -, \underline{n}, \le \rangle$. The axiom $\underline{a}1 \ne m$ holds in all $\langle \mathbb{Z}, 0, 1, +, -, \underline{n}, \le \rangle$ with $n > m$, and $\{n; n > m\} \in \mathcal{U}$ since $\mathcal{U}$ is non-principal. Therefore, $\mathcal{Z}_\mathcal{U} \models$ ZLa.
2) Let ZLa_τ, with $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, be a simple complete extension of ZLa. We find $\mathcal{U} \in \beta\mathbb{N} - \mathbb{N}$ such that $\mathcal{Z}_\mathcal{U} \models \mathrm{ZLa}_\tau$.

Let $\mathcal{S}_\tau = \{[m, \infty); m \in \mathbb{N}\} \cup \{\pi_m(\tau_p) + p^m \cdot \mathbb{N}; p \in \mathbb{P},\ 0 < m \in \mathbb{N}\}$. By the Chinese Remainder Theorem, finite intersections of elements from $\mathcal{S}$ are non-empty, hence there is an ultrafilter $\mathcal{U} \supseteq \mathcal{S}$. Clearly, $\mathcal{U}$ is non-principal and $\mathcal{Z}_\mathcal{U} \models \mathrm{ZLa}_\tau$. □

1.4.2.4 Properties of La

Let ${}^+\dot{\mathbb{Q}}[a]_1$ and ${}^+\dot{\mathbb{Q}}[a]_0$ be the sets of all L^{lin}-formulas $\dot{\underline{r}}$ and $\dot{\mathbf{r}}$ which define symbols $\underline{r}$ or $\mathbf{r}$ respectively, for $0 \le r \in \mathbb{Q}[a]$. Denote ${}^+\dot{\mathbb{Q}}[a] = {}^+\dot{\mathbb{Q}}[a]_1 \cup {}^+\dot{\mathbb{Q}}[a]_0 \cup {}^+\dot{\mathbb{Q}}[a]_1{}^{-1}$, where ${}^+\dot{\mathbb{Q}}[a]_1{}^{-1}$ denotes the set of definitions of integral inverses of positive scalars $\underline{q}$.

We define La_τ, for $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, to be the extension of La by axioms expressing $\mathbf{p^k}|\mathbf{a} - \pi_k(\tau_p)$, for all $p \in \mathbb{P}$, $0 < k \in \mathbb{N}$. We also set $\mathcal{C}^+_\tau = \langle {}^+\mathrm{D}_\tau, 0, 1, +, -, \leq, \underline{a}\rangle$, where $\underline{a}$ is the unary function of multiplication by the variable a.

Corollary 1.4:7 (Properties of La)**.**

1) $\mathrm{La}^{+\dot{\mathbb{Q}}[a]}$ *is almost uniformly solvable,* $\mathrm{La}^{+\dot{\mathbb{Q}}[a]_0}$ *is* 0*-solvable.*
   Hence: La *is model-complete.*
   Moreover: Every formula is in La *equivalent to a disjunction of primitive positive formulas, i.e. to a formula of the form* $\bigvee_{i<n}(\exists \overline{z})\psi_i$*, where each* ψ_i *is a system of linear inequalities.*

2) La_τ*, for* $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$*, are all simple complete extensions of* La*.*
   For $\mathcal{A}, \mathcal{B} \models \mathrm{La}$*, it is* $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \mathbf{a}^{\mathcal{A}} \equiv \mathbf{a}^{\mathcal{B}} \mod n$*, for all* $0 < n \in \mathbb{N}$*.*

3) $\mathcal{C}^+_\tau$ *is the unique prime model of* La_τ*, for* $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$*.*

4) La *is decidable.*
   La_τ *is decidable if and only if* τ *is recursive.*

5) *Theories* La *and* LA *are equivalent.*

Proof. Follows easily from Theorem 1.4:5, by using relations (1.1) and (1.2) from 1.1.7. □

Corollary 1.4:8. *Up to elementary equivalence, models of* La *are exactly all ultraproducts*

$$\mathcal{N}_{\mathcal{U}} = (\prod_{n\in\mathbb{N}} \langle \mathbb{N}, 0, 1, +, -, \underline{n}, \leq\rangle)/_{\mathcal{U}},$$

where $\mathcal{U}$ *is a non-principal ultrafilter on* $\mathbb{N}$*, i.e.* $\mathcal{U} \in \beta\mathbb{N} - \mathbb{N}$*.*

Proof. Similarly, as for Corollary 1.4:2. □

As we have already noted, the theories LA^κ, with κ cardinal, form an ascending chain of theories between Pr and P. We have also remarked that Corollary 1.4:7 can be understood as stating that $\mathrm{LA} = \mathrm{LA}^1$ is model-theoretically similar to $\mathrm{Pr} = \mathrm{LA}^0$ and different from P. In particular, no model of P is definable in a model of LA. Therefore, it is natural to ask the following:

Open question 1.

a) *Are model-theoretical properties of* LA^κ*, with* $\kappa \geq 2$*, still similar to those of* Pr*? In particular, are theories* LA^κ*, with* $\kappa \geq 2$*, model-complete and decidable?*

b) *Could be some model of* P *definable in a model of* LA^κ*?*

1.5 Proofs

In this section, we prove Theorems 1.3:4, 1.3:6 and 1.3:8. For reader's convenience, we sketch the key steps of the proofs here.

1.5.1 Proof prologue

In section 1.5.2, we derive the theorems from three crucial propositions, denoted S, H and B. All these propositions are statements considering a single lineal. Therefore we fix a lineal $\mathcal{F}$ with universe F and denote the sets $\mathrm{D}_{\mathcal{F}}$ and $\mathrm{C}_{\mathcal{F}}$ of scalars and constants of $\mathcal{F}$ shortly as D and C.

We prove the Propositions S, H, and B in the following steps. First, in Proposition 1.5:12, we manage to decompose every "basic non-harmonic" term $\begin{bmatrix} q \\ r \end{bmatrix}(x) = r^{-1}\underline{q}x$ into a sum of simpler terms. We use this result to show that we can get rid of non-harmonic terms completely (Proposition H, 1.5:3). This will enable us to prove Proposition B 1.5:4 and finally use its special case for a base $\langle b_i \rangle_{i<\omega}$ with $b_i | b_{i+1}$, to deduce Proposition S 1.5:2, too.

Our method of proof relies on a calculus of terms in $\mathcal{F}$, which is a generalization of the calculus of continued fractions.

Remark 1.5:1. The problem of descriptive analysis for linear theories (such as ZLA) turns out to be considerably harder than the same task for similar theories, e.g. the theory of $\mathbb{Z}$-groups (ZAA) – which is the simplest linear theory – or the theory of modules over an associative ring R. In fact, linear theories can be seen as generalizing both these cases.

The reason of greater complexity of definable sets in ZLA, compared to the theory of modules, lies, of course, in the presence of the ordering. The difference between ZLA and ZAA can be better understood by considering the following example:

Let $\varphi(x)$ be the formula $r^{-1}(qx) - \frac{q}{r}x \leq c$, where q, r are scalars and c is a constant.

The set D defined by φ is, clearly, r-periodical. In ZAA, it is $r \in \mathbb{Z}$, therefore D can be written as a union of finitely many arithmetical progressions. Nevertheless, in ZLA, r may be non-standard. That is why the finite decomposition trick does not work and D needs to be examined in detail.

1.5.2 Main propositions

Here, we state three propositions, denoted S, H and B, which form three pillars of our proof of the theorems 1.3:4, 1.3:6 and 1.3:8. We prove the propositions in the following sections. In this section, we derive the theorems from them.

The following proposition is the crucial step in the proof of the Main Theorem on Linear Theories 1.3:4.

Proposition 1.5:2 (Proposition S)**.** *Let $\psi(x, \overline{y})$ be an open formula. There are finitely many terms $t_i(\overline{y})$, $i < n$, such that*

$$(\exists x)\psi \leftrightarrow \bigvee_{i<n} \psi(t_i, \overline{y}).$$

The proposition below proves the Harmonic Forms Theorem 1.3:6.

Proposition 1.5:3 (Proposition H)**.** *Every term $t(\overline{x})$ is equivalent to a harmonic almost-term $\tau(\overline{x})$.*

Moreover, if a variable x does not occur in any subterm of the form $r^{-1}s$ (where s is a term) in t then the same is true in τ.

The following proposition states the key step for the proof of the Bases Theorem 1.3:8.

Proposition 1.5:4 (Proposition B)**.** *Let $\delta \in F$, $p, r \in {}^{+}\mathrm{D}$ be scalars, $e = \deg(p)$, $d = \deg(r)$, and $B = \langle b_i \rangle_{d \leq i < e}$ be a $[d, e]$-basis. Then $r^{-1}x$ is on $[\delta, \delta + p - 1]$ equal to a harmonic almost-term $\tau(x)$ (possibly with parameter δ) which is over $mB = \langle mb_i \rangle_{d \leq i < e}$, for some $m \in \mathbb{N}$.*

Moreover, m can be chosen as any number sufficiently large with respect to divisibility.

The proof of the Propositions S, H and B occupies a significant portion of this text. At this place, we derive the theorems 1.3:4, 1.3:6 and 1.3:8 from them.

1.5.2.1 Proof of the Main Theorem on Linear Theories

Theorem 1.3:4 (Main Theorem on Linear Theories)**.** *Let T be a linear theory in a language L, $\mathcal{A} \mapsto \mathcal{F}_{\mathcal{A}}$ be a (D, C)-linealization, and $E = \mathrm{D} \cup \mathrm{C} \cup \mathrm{D}^{-1}$. Then*

1) T^E is almost uniformly solvable.

2) T^{C} is 0-solvable.

Proof. 1): By Lemma 1.2:8, it is enough to prove that

$$\mathcal{A}^E \models (\exists x)\psi(x, \overline{y}) \to \bigvee_{i<n} \psi(t_i(\overline{y}), \overline{y}), \tag{1.11}$$

for every $\mathcal{A} \models T$, quantifier-free L^E-formula ψ and some L^E-terms t_i, $i < n$, depending on $\mathcal{A}$, ψ. In fact, we prove (1.11) even for arbitrary L^E-formula ψ and with t_i, $i < n$, $L(\mathcal{F}_{\mathcal{A}})$-terms.

Note that $\mathcal{A}^E$ is an expansion of the lineal $\mathcal{F}_{\mathcal{A}}$. Let ψ be an L^E-formula. By easy translation, ψ is in $\mathcal{A}^E$ equivalent to an $L(\mathcal{F}_{\mathcal{A}})$-formula φ. By Proposition S

(1.5:2), $Th(\mathcal{F}_\mathcal{A})$ is almost uniformly solvable, hence solvable and admits quantifier elimination, by Proposition 1.2:6. Therefore,

$$\mathcal{F}_\mathcal{A} \models (\exists x)\varphi(x,\overline{y}) \to \bigvee_{i<n} \varphi(t_i(\overline{y}),\overline{y}),$$

for some $L(\mathcal{F}_\mathcal{A})$-terms t_i, $i<n$. Then, clearly, (1.11) holds for these t_i, $i<n$.
2): Let ψ be an L^{C}-sentence. In 1), we proved that there are constant $L(\mathcal{F}_\mathcal{A})$-terms t_i, $i<n$, such that (1.11) holds. By the definition of lineal (see 1.3.1.3), every t_i is equal in $\mathcal{F}_\mathcal{A}$ to some constant $c_i \in \mathrm{C}_\mathcal{A}$. □

1.5.2.2 Proof of the Harmonic Form Theorem

Theorem 1.3:6 (Harmonic Form Theorem)**.** *Let $\mathcal{F}$ be a lineal.*

1) *For every term $t(\overline{x})$, there is an open harmonic almost-term $\tau(\overline{x})$ such that $\mathcal{F} \models t(\overline{x}) = \tau(\overline{x})$.*

2) *For every formula $\varphi(\overline{x})$, there is an open harmonic formula $\psi(\overline{x})$ such that $\mathcal{F} \models \varphi(\overline{x}) \leftrightarrow \psi(\overline{x})$.*

Proof. 1) is an immediate consequence of the Proposition H 1.5:3. We may suppose that τ is open, thanks to Corollary 1.3:5 1) of Theorem 1.3:4.
2) follows from 1), by replacing all maximal subterms in φ by their harmonic equivalents. □

1.5.2.3 Proof of the Bases Theorem

Theorem 1.3:8 (Bases Theorem)**.** *Let $\overline{\delta} \in F^n$, $C_p(\overline{\delta}) = \prod_{i<n}[\delta_i, \delta_i + p - 1] \subseteq F^n$ be a cube with edges of scalar length $p \in \mathrm{D}$, $e = \deg(p)$, and B be a $[0,e]$-basis. Let $l(\overline{x}) = n$. Then the following holds:*

1) *Every term $t(\overline{x})$ is on $C_p(\overline{\delta})$ equal to a harmonic almost-term $\tau(\overline{x})$ which is over mB for some $m \in \mathbb{N}$.*

2) *Every formula $\varphi(\overline{x})$ is on $C_p(\overline{\delta})$ equivalent to an open harmonic formula $\psi(\overline{x})$ which is over mB for some $m \in \mathbb{N}$.*

Moreover:

- *m can be chosen as any number sufficiently large with respect to divisibility.*
- *If t or φ contain parameters from a set X then τ and ψ contain only parameters from $X \cup \overline{\delta}$.*

Proof. 1): By Proposition H 1.5:3, $t(\overline{x})$ is equivalent to a harmonic almost-term $\sigma(\overline{x})$. Now it suffices to replace every subterm $r^{-1}(x_i)$ of σ by its equivalent from Proposition B 1.5:4.
2) follows directly from 1), by replacing all maximal subterms of φ by their equivalents. □

1.5.3 Preliminaries of the proof

From now on, we are heading towards the proof of the Propositions S, H and B (see section 1.5.2).

We consider all the new symbols defined in the rest of this section just as abbreviations, i.e. we do not add them formally to the language. Elements from D (and their realizations in $\mathcal{F}$) are further often called just scalars, elements from C are referred to as constants. For a scalar r, we denote the constant $r1$ also as r.

For better clarity of our formulas, we also freely use fractions with denominators from $\mathrm{D}-\{0\}$; expressions as $\frac{x}{r}$ or x/r always denote fractions, while the integer division is strictly denoted as $r^{-1}x$.

The following Lemma is easy:

Lemma 1.5:5. *Let $q, r, r' \in \mathrm{D}$. Then the following holds:*

a) $\deg(q) < \deg(r) \Rightarrow |q| < |r|$

b) $\deg(r) = 0 \Leftrightarrow r \in \mathbb{Z} - \{0\}$

c) For $q \neq 0$ it is $\deg(r') < \deg(r) \Leftrightarrow \deg(qr') < \deg(qr)$

d) $\deg(q + r) \leq \max(\deg(q), \deg(r))$

e) $\deg(qr) \geq \deg(q) + \deg(r)$

Proof. We prove only e); the other statements are trivial. We show that it is $\deg(qr) \geq \deg(q) + \deg(r)$, for a fixed q, by induction on $\deg(r)$. The case $\deg(r) = 0$ follows from b). For the induction step, we have, for all r' with $\deg(r') < \deg(r)$, the following: $\deg(qr) > \deg(qr') \geq \deg(q) + \deg(r')$. Hence, $\deg(qr) \geq \deg(q) + \deg(r)$. □

For $0 < q \in \mathrm{D}$, we define the remainder function for division by q:

$$\mu_q(x) = x - qq^{-1}x.$$

Moreover, we write shortly $\mu_{r_1,\ldots,r_n}(x)$ instead of $\mu_{r_1}(\mu_{r_2}(\ldots(\mu_{r_n}(x))\ldots))$.

The following is easy to prove:

Lemma 1.5:6. *For all scalars $r, q > 0$ and $x \in F$, it is:*

a) $r^{-1}q^{-1}x = (rq)^{-1}x = q^{-1}r^{-1}x,$

b) $(qr)^{-1}(qx) = r^{-1}x,$

c) $0 \leq \mu_r(x) < r,$

d) $r^{-1}x = \frac{x-\mu_r(x)}{r},$

e) $r^{-1}(x + y) = r^{-1}x + r^{-1}y + i_{r,x,y}$*, where* $i_{r,x,y} = 0$ *if* $\mu_r(x) + \mu_r(y) < r$*, and* $i_{r,x,y} = 1$*, otherwise.*

1.5.4 Continued fractions

We start to build the calculus of terms in $\mathcal{F}$. It is based on and generalizes the calculus of continued fractions.

For scalars $a_1, \ldots, a_n \in \mathrm{D}$, where $a_i > 0$ for $i > 1$, we denote

$$[a_1, \ldots, a_n] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n}}}$$

the *continued fraction* with coefficients $a_1, \ldots, a_n$.

The axiom (R2) from the definition of doded (see 1.3.1.2) ensures that for every $q, r \in \mathrm{D}$, with $r > 0$, there are $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \mathrm{D}$ such that $q/r = [a_1, \ldots, a_n]$. Indeed, we may define $a_i = {t_i}^{-1} s_i$, where (s_i, t_i) is the partial result after the $(i-1)$-th step of the Euclidean algorithm, starting from (q, r), i.e.

$$\begin{aligned} s_1 &= q, & t_1 &= r, \\ s_{i+1} &= t_i, & t_{i+1} &= \mu_{t_i}(s_i). \end{aligned}$$

By (R2), the algorithm stops after $n+1$ steps, for some $n \in \mathbb{N}$. We define the nominators q_i and denominators r_i of the partial continued fractions $[a_1, \ldots, a_i]$, for $1 \le i \le n$. For technical purposes, we also set $q_{-1} = r_0 = 0$, $q_0 = r_{-1} = 1$. Further, we fix this notation, i.e. unless stated otherwise, given the pair $q, r \in \mathrm{D}$, $r > 0$, the symbols n, a_i, q_i and r_i are defined for q, r as above.

Lemma 1.5:7. *Let $q, r \in \mathrm{D}$, and $1 \le j \le n$. For $i < j$, we set $x_i = [a_{i+1}, \ldots, a_j]$. Then*

a) $q_j = a_j q_{j-1} + q_{j-2}$, $r_j = a_j r_{j-1} + r_{j-2}$,

b) $q_{j-1} r_j - q_j r_{j-1} = (-1)^{j+1}$,

c) If $i + 1 < j$ *then* $x_i = a_{i+1} + \frac{1}{x_{i+1}}$,

d) $\frac{q_j}{r_j} = \frac{q_i x_i + q_{i-1}}{r_i x_i + r_{i-1}}$,

e) $q/r = [a_1, \ldots, a_n] = q_n/r_n$, *and* q_n, r_n *are co-prime.*

Proof. Easy. $\square$

1.5.5 Bracket $\begin{bmatrix} q \\ r \end{bmatrix}$ and its decomposition

We introduce an useful concept of a bracket function $\begin{bmatrix} q \\ r \end{bmatrix}(x)$, for scalars q, r, $r > 0$, as a cornerstone for our calculus of terms.

Brackets $\begin{bmatrix}1\\r\end{bmatrix} = r^{-1}$ should be understood as "basic harmonic functions", while $\begin{bmatrix}q\\r\end{bmatrix}$, with $q \neq 1$, as non-harmonic ones, where the rate of non-harmonicity roughly corresponds to the complexity of the continued fraction of q/r. In this section, we prove that the graph of $\begin{bmatrix}q\\r\end{bmatrix}$ is a curve parametrized by a pair of linear forms defined on a "spiraloid" (see Proposition 1.5:12 1)). As a consequence, every bracket $\begin{bmatrix}q\\r\end{bmatrix}$ can be decomposed into a sum of "more harmonic" terms (Proposition 1.5:12 2)).

1.5.5.1 Bracket $\begin{bmatrix}q\\r\end{bmatrix}$

Let q, r be two scalars, $r > 0$. We define the *bracket*

$$\begin{bmatrix}q\\r\end{bmatrix}(x) = r^{-1}qx.$$

If q, r are not coprime, and q', r' are coprime and such that $\frac{q}{r} = \frac{q'}{r'}$ then, clearly, $\begin{bmatrix}q\\r\end{bmatrix}(x) = \begin{bmatrix}q'\\r'\end{bmatrix}(x)$, for all x, by Lemma 1.5:6 b). Further, let q, r be be fixed coprime scalars, $r > 0$, $[a_1, \ldots, a_n]$ (where $a_1 < 0$ if $q < 0$) be the continued fraction of $\frac{q}{r}$ and q_i, r_i the nominators and denominators of the partial continued fractions (for instance, $q_n = q$ and $r_n = r$).

For the proof of Proposition 1.5:12, we will need the following lemmas.

Lemma 1.5:8. *For $i = 0, \ldots, n-1$, let $m_i = r_i \cdot [a_{i+1}, \ldots, a_n] + r_{i-1}$. Then the following holds for any $z_i \in F$:*

$$\frac{q_n}{r_n} \cdot r_i z_i = q_i z_i + \frac{(-1)^{i+1}}{m_i} z_i.$$

Proof. Denote $x_i = [a_{i+1}, \ldots, a_n]$. Then, by Lemma 1.5:7,

$$\begin{aligned}
\frac{q_n}{r_n} \cdot r_i z_i &= \frac{q_i x_i r_i z_i + q_{i-1} r_i z_i}{r_i x_i + r_{i-1}} = \\
&= \frac{(q_i x_i r_i z_i + q_i z_i r_{i-1}) + (q_{i-1} r_i z_i - q_i z_i r_{i-1})}{r_i x_i + r_{i-1}} = \\
&= q_i z_i + \frac{q_{i-1} r_i - q_i r_{i-1}}{r_i x_i + r_{i-1}} \cdot z_i = \\
&= q_i z_i + \frac{(-1)^{i+1}}{r_i x_i + r_{i-1}} z_i.
\end{aligned}$$

□

Lemma 1.5:9. *Let* $\overline{z} = (z_1, \ldots, z_{n-1}) \in [0; a_2 - 1] \times \prod_{i=2}^{n-1}[0; a_{i+1}]$, *and let* m_i *denotes* $r_i \cdot [a_{i+1}, \ldots, a_n] + r_{i-1}$. *Then*

$$\sum_{i=1}^{n-1} \frac{z_i}{m_i} \leq 1 - \frac{1}{r_n}.$$

Moreover, the bound is tight.

Proof. Clearly, it is enough to prove

$$\sum_{i=1}^{n-1} \frac{a_{i+1}}{m_i} - \frac{1}{m_1} = 1 - \frac{1}{r_n}. \tag{1.12}$$

Denote $x_i = [a_{i+1}, \ldots, a_n]$ as in the previous proof. At first, we express all m_i's in terms of x_j's. For $i < m - 1$, it is, by Lemma 1.5:7 c),

$$m_i = r_i x_i + r_{i-1} = (r_i a_{i+1} + r_{i-1}) + \frac{r_i}{x_{i+1}} = r_{i+1} + \frac{r_i}{x_{i+1}} = \frac{m_{i+1}}{x_{i+1}},$$

$$m_0 = r_0 x_0 + r_{-1} = 0 \cdot x_0 + 1 = 1.$$

Hence,

$$m_i = \prod_{j=1}^{i} x_j. \tag{1.13}$$

Let $x_i = \frac{s_i}{t_i}$, where s_i, t_i are relatively prime. For $i = 0, \ldots, n-2$, using Lemma 1.5:7 c), we can get $\frac{s_i}{t_i} = \frac{a_{i+1}s_{i+1}+t_{i+1}}{s_{i+1}}$ and thus (since $a_{i+1}s_{i+1} + t_{i+1}$ and s_{i+1} are, clearly, relatively prime)

$$s_{i+1} = t_i \tag{1.14}$$

and

$$\begin{aligned} a_{i+1}s_{i+1} &= s_i - t_{i+1}, \\ a_{i+1}t_i &= s_i - t_{i+1}. \end{aligned} \tag{1.15}$$

For $i = n-1$, we have $t_{n-1}a_n = 1 \cdot a_n = s_{n-1}$.

From (1.14), we get

$$m_i \overset{(1.13)}{=} \prod_{j=1}^{i} = \frac{s_1}{t_1} \cdot \frac{s_2}{t_2} \cdot \cdots \cdot \frac{s_i}{t_i} = \frac{s_1}{t_i}, \tag{1.16}$$

and further,

$$\sum_{i=1}^{n-1} \frac{a_{i+1}}{m_i} \overset{(1.16)}{=} \sum_{i=1}^{n-1} \frac{t_i a_{i+1}}{s_1} \overset{(1.15)}{=} \frac{\sum_{i=1}^{n-2}(s_i - t_{i+1}) + s_{n-1}}{s_1} \overset{(1.14)}{=} \frac{s_1 + s_2 - t_{n-1}}{s_1}. \tag{1.17}$$

Since, obviously, $s_1 = r_n$, $s_2 = t_1$, $t_{n-1} = 1$, $m_1 = \frac{s_1}{t_1}$, we have

$$\sum_{i=1}^{n-1} \frac{a_{i+1}}{m_i} - \frac{1}{m_1} \overset{(1.17)}{=} \frac{r_n + t_1 - 1}{r_n} - \frac{t_1}{r_n} = 1 - \frac{1}{r_n}.$$

□

1.5.5.2 $\mathcal{C}_r^q$, forms f_r, f_q

We define the "cuboid" $\mathcal{C}_r^q$ and linear forms $f_r, f_q \colon \mathcal{C}_r^q \to F$ as

$$\mathcal{C}_r^q = [0; a_2 - 1] \times \prod_{i=2}^{n-1} [0; a_{i+1}] \times (\leftarrow; \rightarrow),$$

$$f_r(\overline{z}) = \sum_{i=1}^{n} (-1)^{i+1} r_i z_i, \quad f_q(\overline{z}) = \sum_{i=1}^{n} (-1)^{i+1} q_i z_i.$$

The following lemma states that the form f_r gives a "cuboid parametrization" of F.

Lemma 1.5:10. *The form f_r is surjective and (≤ 2)-to-1.*

Proof. Easy. □

Remark 1.5:11. Let $\mathcal{S}_r^q \subseteq \mathcal{C}_r^q$ be the set of all $\leq_{Lex}$-maximal elemets of $\sim_{q,r}$-factor classes (where $\leq_{Lex}$ is the lexicographical order of $\mathcal{C}_r^q$, and the equivalence $\sim_{q,r}$ is defined by $\overline{z} \sim_{q,r} \overline{z'} \Leftrightarrow f_r(\overline{z}) = f_r(\overline{z'})$).

It is easy to see that the form $f_r \restriction \mathcal{S}_r^q$ is an isomorphism of $\langle \mathcal{S}_r^q, \leq_{Lex} \rangle$ and $\langle F, \leq^F \rangle$. Hence, $\langle F, \leq^F \rangle$ can be imagined as a spiral "wrapped around" $\mathcal{S}_r^q$, that is why we call $\mathcal{S}_r^q$ a "spiraloid".

Proposition 1.5:12 (cuboid decomposition of $\begin{bmatrix} q \\ r \end{bmatrix}$)**.** *Let q, r be scalars, $r > 0$. Then the following holds:*

1) $\begin{bmatrix} q \\ r \end{bmatrix} \circ f_r = f_q$ on $\mathcal{C}_r^q$.

2) Let $s_{q,r} = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} r_{2i} a_{2i+1}$, $t_{q,r} = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} q_{2i} a_{2i+1}$. *Then, for all $x \in F$,*

$$\begin{bmatrix} q \\ r \end{bmatrix}(x) = \sum_{i=1}^{n} q_i \cdot {r_i}^{-1} \mu_{r_{i+1},\ldots,r_n}(x + s_{q,r}) - t_{q,r}. \tag{1.18}$$

We call the expression on the right side of (1.18) the *cuboid decomposition* of the bracket $\begin{bmatrix} q \\ r \end{bmatrix}(x)$.

Proof. (of Proposition 1.5:12)
1) Denote $x = f_r(\overline{z}) = \sum_{i=1}^{n}(-1)^{i+1} r_i z_i$, for fixed $\overline{z} \in \mathcal{C}_r^q$. Then we have

$$\begin{aligned}\begin{bmatrix} q \\ r \end{bmatrix}(x) &= \left\lfloor \frac{q_n}{r_n} x \right\rfloor \overset{Lemma 1.5:8}{=} \left\lfloor \sum_{i=1}^{n}(-1)^{i+1} q_i z_i + \sum_{i=1}^{n-1} \frac{z_i}{m_i} \right\rfloor = \\ &= \sum_{i=1}^{n}(-1)^{i+1} q_i z_i + \left\lfloor \sum_{i=1}^{n-1} \frac{z_i}{m_i} \right\rfloor \overset{Lemma 1.5:9}{=} \sum_{i=1}^{n}(-1)^{i+1} q_i z_i = f_q(\overline{z}).\end{aligned}$$

2) is a corollary of 1) via a change of coordinates. Let $x \in F$ be given. By Lemma 1.5:10, we can choose coordinates $\overline{z} \in \mathcal{C}_r^q$ such that $x = \sum_{i=1}^{n}(-1)^{i+1} r_i z_i$. Set

$$z_i' = \begin{cases} a_{i+1} - z_i & i < n \text{ even}, \\ z_i & i < n \text{ odd}, \\ (-1)^{n+1} z_n & i = n. \end{cases}$$

Then

$$x + s_{q,r} = \sum_{i=1}^{n} r_i z_i' = \sum_{i=1}^{n} r_i z_i'', \tag{1.19}$$

where $\overline{z''} \in \mathcal{S}_r^q$. By 1), we get also

$$\sum_{i=1}^{n} q_i z_i' = \sum_{i=1}^{n} q_i z_i'', \tag{1.20}$$

and, by maximality of $\overline{z''}$ and (1.19),

$$z_i'' = {r_i}^{-1} \mu_{r_{i+1},\dots,r_n}(x + s_{q,r}). \tag{1.21}$$

Finaly, we can compute

$$\begin{aligned}\begin{bmatrix} q \\ r \end{bmatrix}(x) &\overset{1)}{=} \sum_{i=1}^{n}(-1)^{i+1} q_i z_i = \sum_{i=1}^{n} q_i z_i' - t_{q,r} \overset{(1.20)}{=} \sum_{i=1}^{n} q_i z_i'' - t_{q,r} \overset{(1.21)}{=} \\ &\overset{(1.21)}{=} \sum_{i=1}^{n} q_i \cdot {r_i}^{-1} \mu_{r_{i+1},\dots,r_n}(x + s_{q,r}) - t_{q,r}.\end{aligned}$$

□

1.5.6 Harmonization

In this subsection, we prove the Proposition H 1.5:3. That is, we show that every term in $\mathcal{F}$ can be (up to a "noise") expressed as a linear combination of basic "harmonic" functions r^{-1}, and, consequently, any open formula is equivalent to one with all terms harmonic (see 1.3.2.2.1).

We are going to develop a calculus of brackets $\begin{bmatrix} q \\ r \end{bmatrix}$ (see 1.5.5.1 for definition). For the reason of simplicity, we will write

$$\begin{bmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \end{bmatrix}$$

instead of

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \circ \dots \circ \begin{bmatrix} a_n \\ b_n \end{bmatrix}.$$

1.5.6.1 Harmonic terms

We rewrite here the definition of harmonic term (see 1.3.2.2.1) in the bracket notation: A term $t(\overline{x})$ is *harmonic* (or equivalently *in harmonic form*) if it is a sum of expressions of the form $\begin{bmatrix} A & 1 \\ 1 & B \end{bmatrix}(x_i)$, with $A, B \in \mathrm{D}$, and possibly a scalar $r \in \mathrm{D}$.

1.5.6.2 Convention

The rest of this subsection is devoted to the proof of Proposition H 1.5:3. For the purpose of this proof, we further consider (the so far abbreviations) binary minus (-) and $\mu_r(\_)$ to be symbols in our language. On the other hand, we forbid the unary minus (it can be replaced using multiplication by the scalar -1). (Formally, we get a modification L' of our original language $L(\mathcal{F})$. But the difference between $L(\mathcal{F})$ and L' is of purely technical character, since there is a simple translation between these two languages.) In the rest of this subsection, the word "term" means L'-term and similarly for almost-term and formula.

The idea of the proof is to lower the "non-harmonicity" of a term (almost-term) by decomposing its "strings" $\begin{bmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \end{bmatrix}$, using Proposition 1.5:12 and "almost-distributivity" of strings over addition (see Lemma 1.5:16 below). The non-harmonicity of newly created strings needs to be controled during the proces. For these purposes, we introduce a few new concepts.

1.5.6.3 Strings

Let t be a term. In the tree of subterms of t, vertices correspond to subterms (root to t, leafs to variables and constants) and edges to symbols.

Example 1.5:13. Let $t = q(r_0 s^{-1}x - r_1(y + t^{-1}r_2c))$ be a term, with x, y variables, c a constant and q, r_0, r_1, r_2, s, t scalars. The corresponding tree of subterms of t is

$$\begin{tikzcd}
 & t \arrow[d, "q"] & & \\
 & r_0s^{-1}x - r_1(y+t^{-1}r_2c) \arrow[dl, "+"'] \arrow[dr, "-"] & & \\
r_0s^{-1}x \arrow[d, "r_0"] & & r_1(y+t^{-1}r_2c) \arrow[d, "r_1"] & \\
s^{-1}x \arrow[d, "s^{-1}"] & & y+t^{-1}r_2c \arrow[dl, "+"'] \arrow[dr, "+"] & \\
x & y & & t^{-1}r_2c \arrow[d, "t^{-1}"] \\
 & & & r_2c \arrow[d, "r_2"] \\
 & & & c
\end{tikzcd}.$$

Any sequence of symbols from edges and the leaf of a branch in the tree of subterms of t, in the ascending order from the root to the leaf, in which we omit all edges corresponding to symbols $+, -$, is called a *string* of t. The string is a $+$-*string* [$-$-*string*] if the number of omitted symbols $-$ was even [odd]. The set of all strings [$+$-strings,$-$-strings] of t is denoted $\mathrm{str}(t)$ [$\mathrm{str}^+(t)$, $\mathrm{str}^-(t)$]. The set of strings of an p-term τ [formula φ] (denoted $\mathrm{str}(\tau)$ [$\mathrm{str}(\varphi)$]) is the union of the sets $\mathrm{str}(t)$, over all maximal subterms t of τ [φ].

Example 1.5:14. Let $t = q(r_0s^{-1}x - r_1(y + t^{-1}r_2c))$ be a term, as in Example 1.5:13. There are three strings of t: $\alpha_0 = \langle q, r_0, s^{-1}, x\rangle$, $\alpha_1 = \langle q, r_1, y\rangle$ and $\alpha_2 = \langle q, r_1, t^{-1}, r_2, c\rangle$. Two of them, α_1 and α_2, are $-$-strings, while α_0 is a $+$-string.

The *reduced string* $\tilde{\alpha}$ arises from a string α by removing the maximal initial segment of α consisting only of scalar multiplications. We denote the set of reduced strings of t as $\tilde{\mathrm{str}}(t)= \{\tilde{\alpha}; \alpha \in \mathrm{str}(t)\}$ and similarly for $\tilde{\mathrm{str}}(\tau)$ and $\tilde{\mathrm{str}}(\varphi)$.

Example 1.5:15. Let $\alpha_0 = \langle q, r_0, s^{-1}, x\rangle$, $\alpha_1 = \langle q, r_1, y\rangle$ and $\alpha_2 = \langle q, r_1, t^{-1}, r_2, c\rangle$ be the strings from Example 1.5:14. Their reduced versions are $\tilde{\alpha_0} = \langle s^{-1}, x\rangle$, $\tilde{\alpha_1} = \langle y\rangle$ and $\tilde{\alpha_2} = \langle t^{-1}, r_2, c\rangle$.

1.5.6.4 Notation $T \to T'$, $[\![T]\!]_S$, $\alpha \sqsubseteq_n \beta$ and $\alpha \sqsubseteq \beta$

The following notation will help us to keep the complexity of almost-terms under control, during the proof of Proposition H.

For two strings α, β and $n \in \omega$, we write $\alpha \sqsubseteq_n \beta$ if there are at most n symbols $f_0, \ldots, f_{i-1}$ such that $\beta = \langle f_0, \ldots, f_{i-1}\rangle\smallsmile\alpha$. We write $\alpha \sqsubseteq \beta$ if $\alpha \sqsubseteq_n \beta$, for some $n \in \omega$.

For two sets of terms T, S, we denote $[\![T]\!]_S$ the set of all almost-terms τ with $\mathrm{core}(\tau) \in T$ and such that all maximal subterms in $\mathrm{cond}(\tau)$ are of the form $\sum_i q_i \cdot s_i + r$, where $r, q_i \in \mathrm{D}$ and $s_i \in S$. We will often write $[\![t]\!]_S$ instead of $[\![\{t\}]\!]_S$. We will also write $[\![t]\!]_\square$ instead of $[\![t]\!]_{\{\alpha;\exists\beta\in\tilde{\mathrm{str}}(t)(\alpha\square\beta)\}}$, where $\square$ stands for any symbol $\sqsubseteq, \sqsubseteq_n$. We will sometimes write $[\![t]\!]$ instead of $[\![t]\!]_{\sqsubseteq_0}$ and $[\![t]\!]_=$ instead of $[\![t]\!]_{\{t\}}$. We may also use abbreviations with obvious meaning such as $[\![t]\!]_{\sqsubseteq_i\cup=}$.

Let T, T' be two sets of almost-terms. We say that T reduces to T' and denote it $T \to T'$ if every almost-term $\tau \in T$ is equivalent to some $\tau' \in T'$. We will often write $\tau \to T'$ instead of $\{\tau\} \to T'$ and similarly on the right side.

We say that a term t is *distributed* if it is a sum of strings. A p-term [a formula] is distributed if all its maximal subterms are.

Lemma 1.5:16. *Let t, s be terms and $r \in \mathrm{D}$, $r > 0$. Then*

a) $r^{-1}(t \pm s) \to [\![r^{-1}t \pm r^{-1}s]\!]_{\{t,s,r^{-1}t,r^{-1}s\}}$

b) $\mu_r(t \pm s) \to [\![\mu_r(t) \pm \mu_r(s)]\!]_{\{\mu_r(t),\mu_r(s)\}}$

c) $t \to [\![\sum \mathrm{str}^+(t) - \sum \mathrm{str}^-(t)]\!]_\sqsubseteq$

d) Every almost-term is equivalent to a distributed one.

Proof.
a) It is easy to see that

$$r^{-1}x + y = \begin{cases} r^{-1}x + r^{-1}y & \text{if } \mu_r(x) + \mu_r(y) < r, \\ r^{-1}x + r^{-1}y + 1 & \text{if } \mu_r(x) + \mu_r(y) \geq r, \end{cases}$$

and similarly for $x - y$.
b) Similarly as a).
c) Follows from a) and b), by induction on the maximal depth of occurrence of $+, -$ in t.
d) Easy consequence of a) and b). □

The following lemma lists basic techniques of complexity reduction, which we are going to use throughout our proof.

Here and further on, we use notation $s(\overline{T})$, where s is a term, and T_i are sets of terms, to denote the set of all terms $s(\bar{t})$, where $t_i \in T_i$. Let S be a set of terms. Then $\mathrm{sTm}(S)$ denotes the set of all subterms of terms from S.

Lemma 1.5:17. *Let t_i, t, s be terms, T, S, U, V, W, T_i, S_i sets of terms and X_i, Y_i sets of almost-terms.*

1) a) Relation $\to$ is a preorder on $\mathcal{P}(aTm)$, where aTm stands for the set of all almost-terms.

b) If $X_i \to Y_i$ then $s(X_0, \ldots, X_{n-1}) \to s(Y_0, \ldots, Y_{n-1})$.

c) If $t \to [\![s]\!]_S$ then $[\![t]\!]_T \to [\![s]\!]_{T\cup S}$.

d) If $T \to [\![S]\!]_V$ and $U \to [\![W]\!]_W$ then $[\![T]\!]_U \to [\![S]\!]_{V\cup W}$.

2) a) The following holds

$$s\left([\![t_0]\!]_{T_0}, \ldots, [\![t_{n-1}]\!]_{T_{n-1}}\right) \to [\![s(t_0, \ldots, t_{n-1})]\!]_{\bigcup_{i=0}^{n-1} T_i \cup \mathrm{sTm}(s)(\bar{t})}.$$

Moreover, if s does not contain divs nor mods then

$$s\left([\![t_0]\!]_{T_0}, \ldots, [\![t_{n-1}]\!]_{T_{n-1}}\right) \to [\![s(t_0, \ldots, t_{n-1})]\!]_{\bigcup_{i=0}^{n-1} T_i}.$$

b) $[\![t]\!]_T \circ ([\![s_0]\!]_{S_0}, \ldots, [\![s_n]\!]_{S_n}) \to [\![t \circ \bar{s}]\!]_{\bigcup_{i=0}^{n-1} S_i \cup \mathrm{sTm}(t,T)\circ\bar{s}}$.

Proof. 1): Easy verification.
2) a): By induction on complexity of s. In the induction steps for r^{-1} and μ_r, Lemma 1.5:16 a) and b) is used.
2) b): Follows directly from 2) a).

□

By the Proposition 1.5:12 2), every bracket $\begin{bmatrix} q \\ r \end{bmatrix}$ can be expressed in a cuboid form

$$\begin{bmatrix} q \\ r \end{bmatrix}(x) = \sum_{i=1}^{n} q_i \cdot \left(\begin{bmatrix} 1 \\ r_i \end{bmatrix} \mu_{r_{i+1},\ldots,r_n}(x+s)\right) - t, \tag{1.22}$$

where $q_i, r_i \in \mathrm{D}$ are the nominator and the denominator of the i-th partial continued fraction of $\frac{q}{r}$, and $s, t \in \mathrm{C}$. In the following series of lemmas, we will reduce $\begin{bmatrix} q \\ r \end{bmatrix}$ to a simpler form. For the reason of simplicity, we often use functional notation for terms, i.e. we write, for example, μ_r instead of $\mu_r(x)$ or id instead of x.

Lemma 1.5:18. *Let $b_0 \le \ldots \le b_{k-1}$, with $k > 1$, be scalars having the same degree (in the doded D). Then*

a) $\mu_{b_1,\ldots,b_{k-1}} \to [\![\mu_{b_{k-1}}]\!]$,

b) $\begin{bmatrix} 1 \\ b_0 \end{bmatrix} \mu_{b_1,\ldots,b_{k-1}} \to [\![0]\!]_{\mu_{b_{k-1}}}$.

Proof. We will prove both statements, (a) and (b), of the Lemma simultaneously by induction on k.

For $k=2$, (a) is trivial. To prove (b), consider $\begin{bmatrix}1\\b_0\end{bmatrix}\mu_{b_1}(x)$. We have

$$\mu_{b_1}(x) < b_1 \leq m \cdot b_0,$$

for some $m \in \omega$ (since $\deg(b_0) = \deg(b_1)$). Then

$$\begin{bmatrix}1\\b_0\end{bmatrix}\mu_{b_1}(x) = \Big\{ i \text{ if } \psi_i;\ i < m+1,$$

where $\psi_i(x) \doteq ib_0 \leq \mu_{b_1}(x) < (i+1)\cdot b_0$. Clearly, the later is an almost-term in $[\![0]\!]_{\mu_{b_1}}$.

For the induction step in (a), we have

$$\begin{aligned}\mu_{b_1,\dots,b_{k-1}} &= \mu_{b_1} \circ \mu_{b_2,\dots,b_{k-1}} = \\ &= \mu_{b_2,\dots,b_{k-1}} - \begin{bmatrix}b_1 & 1\\ 1 & b_1\end{bmatrix} \circ \mu_{b_2,\dots,b_{k-1}} \to \\ &\to [\![\mu_{b_{k-1}}]\!] - [\![0]\!]_{\mu_{b_{k-1}}} \to [\![\mu_{b_{k-1}}]\!],\end{aligned}$$

where the first arrow follows from the induction assumptions and Lemma 1.5:17 1b), 2a) and the second from 2a). The induction step for (b):

$$\begin{bmatrix}1\\b_0\end{bmatrix}\mu_{b_1,\dots,b_{k-1}} \to \begin{bmatrix}1\\b_0\end{bmatrix}[\![\mu_{b_{k-1}}]\!] \to \left[\!\!\left[\begin{bmatrix}1\\b_0\end{bmatrix}\mu_{b_{k-1}}\right]\!\!\right]_{\sqsubseteq} \to [\![0]\!]_{\mu_{b_{k-1}}},$$

where the first arrow follows from (a), the second one from Lemma 1.5:17 2a), and the third one from the induction assumption for $k=2$ and Lemma 1.5:17 1d). $\square$

Lemma 1.5:19. *Let $b_0 \leq \ldots \leq b_{k-1}$, $k>0$, be scalars. For any finite set $F \subseteq \omega$, we take an enumeration $F = \{f_0, \ldots, f_{|F|-1}\}$ such that $f_0 < \ldots < f_{|F|-1}$.*

a) Then

$$\mu_{b_1,\dots,b_{k-1}} \to \left[\!\!\left[\sum_{F\subseteq\{1,\dots,k-1\}} (-1)^{|F|}\begin{bmatrix} b_{f_0} & b_{f_1} & \ldots & b_{f_{|F|-1}} & 1\\ 1 & b_{f_0} & \ldots & b_{f_{|F|-2}} & b_{f_{|F|-1}}\end{bmatrix}\right]\!\!\right],$$

b) and

$$\begin{bmatrix}1\\b_0\end{bmatrix}\mu_{b_1,\dots,b_{k-1}} \to \left[\!\!\left[\sum_{F\subseteq\{1,\dots,k-1\}} (-1)^{|F|}\begin{bmatrix} b_{f_0} & b_{f_1} & \ldots & b_{f_{|F|-1}} & 1\\ b_0 & b_{f_0} & \ldots & b_{f_{|F|-2}} & b_{f_{|F|-1}}\end{bmatrix}\right]\!\!\right]_{\sqsubseteq_1}.$$

Proof. By simultaneous induction on k. The case $k = 1$ is trivial. Let $k = 2$.
a): $\mu_{b_1} = id - \begin{bmatrix} b_1 & 1 \\ 1 & b_1 \end{bmatrix} \in \left[\!\left[\sum_{F\subseteq\{1\}}(-1)^{|F|}\begin{bmatrix} b_{f_0} & 1 \\ 1 & b_{f_0} \end{bmatrix} \right]\!\right]$.
b): $\begin{bmatrix} 1 \\ b_0 \end{bmatrix}\mu_{b_1} = \begin{bmatrix} 1 \\ b_0 \end{bmatrix}\left(id - \begin{bmatrix} b_1 & 1 \\ 1 & b_1 \end{bmatrix}\right) \to \left[\!\left[\begin{bmatrix} 1 \\ b_0 \end{bmatrix} - \begin{bmatrix} b_1 & 1 \\ b_0 & b_1 \end{bmatrix} \right]\!\right]_{\sqsubseteq_1}$, where the arrow follows from Lemma 1.5:16 a).

Induction step: a):

$$\mu_{b_1,\dots,b_{k-1}} = \mu_{b_2,\dots,b_{k-1}} - \begin{bmatrix} b_1 & 1 \\ 1 & b_1 \end{bmatrix}\mu_{b_2,\dots,b_{k-1}}. \tag{1.23}$$

By induction assumptions on a) and b), we get

$$\begin{aligned} \mu_{b_2,\dots,b_{k-1}} &\to \left[\!\left[\sum_{F\subseteq\{2,\dots,k-1\}}(-1)^{|F|}\begin{bmatrix} b_{f_0} & b_{f_1} & \dots & b_{f_{|F|-1}} & 1 \\ 1 & b_{f_0} & \dots & b_{f_{|F|-2}} & b_{f_{|F|-1}} \end{bmatrix} \right]\!\right], \\ \begin{bmatrix} b_1 & 1 \\ 1 & b_1 \end{bmatrix}\mu_{b_2,\dots,b_{k-1}} &\to \left[\!\left[\sum_{F\subseteq\{2,\dots,k-1\}}(-1)^{|F|}\begin{bmatrix} b_1 & b_{f_0} & b_{f_1} & \dots & b_{f_{|F|-1}} & 1 \\ 1 & b_1 & b_{f_0} & \dots & b_{f_{|F|-2}} & b_{f_{|F|-1}} \end{bmatrix} \right]\!\right]_{\sqsubseteq_1}. \end{aligned}$$

For the string $\beta = \begin{bmatrix} b_1 & b_{f_0} & b_{f_1} & \dots & b_{f_{|F|-1}} & 1 \\ 1 & b_1 & b_{f_0} & \dots & b_{f_{|F|-2}} & b_{f_{|F|-1}} \end{bmatrix}$, there are only two strings $\alpha \sqsubseteq_1 \tilde{\beta}$, namely β itself and $\begin{bmatrix} b_{f_0} & b_{f_1} & \dots & b_{f_{|F|-1}} & 1 \\ 1 & b_{f_0} & \dots & b_{f_{|F|-2}} & b_{f_{|F|-1}} \end{bmatrix}$. That is why we get from (1.23) and Lemma 1.5:17 2a) the following:

$$\mu_{b_1,\dots,b_{k-1}} \to \left[\!\left[\sum_{F\subseteq\{1,\dots,k-1\}}(-1)^{|F|}\begin{bmatrix} b_{f_0} & b_{f_1} & \dots & b_{f_{|F|-1}} & 1 \\ 1 & b_{f_0} & \dots & b_{f_{|F|-2}} & b_{f_{|F|-1}} \end{bmatrix} \right]\!\right].$$

To prove b), consider

$$\begin{aligned} \begin{bmatrix} 1 \\ b_0 \end{bmatrix}\mu_{b_1,\dots,b_{k-1}} &\to \left[\!\left[\begin{bmatrix} 1 \\ b_0 \end{bmatrix}\sum_F(-1)^{|F|}\begin{bmatrix} b_{f_0} & b_{f_1} & \dots & b_{f_{|F|-1}} & 1 \\ 1 & b_{f_0} & \dots & b_{f_{|F|-2}} & b_{f_{|F|-1}} \end{bmatrix} \right]\!\right]_{(\sqsubseteq_1\cup=)} \to \\ &\to \left[\!\left[\sum_F(-1)^{|F|}\begin{bmatrix} b_{f_0} & b_{f_1} & \dots & b_{f_{|F|-1}} & 1 \\ b_0 & b_{f_0} & \dots & b_{f_{|F|-2}} & b_{f_{|F|-1}} \end{bmatrix} \right]\!\right]_{\sqsubseteq_1}, \end{aligned}$$

where the first arrow follows from a) and Lemma 1.5:17 2a), and the second one from Lemma 1.5:16 a) and Lemma 1.5:17 1d). □

Lemma 1.5:20. *Let* $\frac{q}{r} = [a_1, \ldots, a_n]$ *and* i *is maximal such that* $\deg(a_i) > 0$ *(*$i = 0$ *if all* $a_i \in \mathbb{Z}$*). Then*

$$\begin{bmatrix} q \\ r \end{bmatrix} \to \left[\!\!\left[\sum_{j=1}^{i-1} \sum_{F \subseteq \{j+1,\ldots,i-1\} \cup \{n\}} (-1)^{|F|} \begin{bmatrix} q_j & r_{f_0} & r_{f_1} & \ldots & r_{f_{|F|-1}} & 1 \\ 1 & r_j & r_{f_0} & \ldots & r_{f_{|F|-2}} & r_{f_{|F|-1}} \end{bmatrix} + \begin{bmatrix} q_n & 1 \\ 1 & r_n \end{bmatrix} \right]\!\!\right].$$

In particular,

$$\begin{bmatrix} q \\ r \end{bmatrix} \to \left[\!\!\left[\sum_j s_j \right]\!\!\right]_{S_r},$$

where $s_j \in S_r$*, and* S_r *is the set of all strings* $\begin{bmatrix} a_1 & a_2 & \ldots & a_{l-1} & 1 \\ 1 & b_2 & \ldots & b_{l-1} & b_l \end{bmatrix}$ *such that* $\deg(b_i) < \deg(r)$*, for* $i < l$*, and* $\deg(b_l) \le \deg(r)$*.*

Proof. At first, observe that

$$0 = \deg r_1 \le \ldots \le \deg(r_{i-1}) < \deg(r_i) = \ldots = \deg(r_n) = \deg(r). \tag{1.24}$$

In particular, if $i = 0, 1$ then $r_j \in \mathbb{N}$, for all j. Indeed, by Lemma 1.5:7, it is $r_j = a_j \cdot r_{j-1} + r_{j-2}$. Since $\deg(a_i) > 0$, we have $\deg(r_i) > \deg(r_{i-1})$. Due to maximality of i, we get $\deg(r_j) = \deg(r_i)$, for $j \ge i$.

By substitution $y = x + s$ into the cuboid form (1.22) of $\begin{bmatrix} q \\ r \end{bmatrix}$, we get

$$\begin{bmatrix} q \\ r \end{bmatrix}(x) = \sum_{j=1}^{n} q_j \cdot \left(\begin{bmatrix} 1 \\ r_j \end{bmatrix} \mu_{r_{j+1},\ldots,r_n}(y) \right) - t = \sum_{j=1}^{n} q_j \cdot t_j(y) - t, \tag{1.25}$$

where $t \in \mathrm{D}$, and $t_j = \begin{bmatrix} 1 \\ r_j \end{bmatrix} \mu_{r_{j+1},\ldots,r_n}$.

For $1 \le j \le i-1$, we have

$$t_j = \begin{bmatrix} 1 \\ r_j \end{bmatrix} \mu_{r_{j+1},\ldots,r_{i-1}} \circ \mu_{r_i,\ldots,r_n}.$$

By (1.24) and Lemmas 1.5:18 and 1.5:19, it is

$$\begin{aligned} \mu_{r_i,\ldots,r_n} &\to [\![\mu_{r_n}]\!] \to \left[\!\!\left[id - \begin{bmatrix} r_n & 1 \\ 1 & r_n \end{bmatrix} \right]\!\!\right], \\ \begin{bmatrix} 1 \\ r_j \end{bmatrix} \mu_{r_{j+1},\ldots,r_{i-1}} &\to \left[\!\!\left[\sum_{F \subseteq \{j+1,\ldots,i-1\}} (-1)^{|F|} \begin{bmatrix} r_{f_0} & r_{f_1} & \ldots & r_{f_{|F|-1}} & 1 \\ r_j & r_{f_0} & \ldots & r_{f_{|F|-2}} & r_{f_{|F|-1}} \end{bmatrix} \right]\!\!\right]_{\sqsubseteq_1}. \end{aligned}$$

Then, by Lemma 1.5:17 2b), we get

$$t_j \to \left[\!\!\left[\sum_{F\subseteq\{j+1,\dots,i-1\}} (-1)^{|F|} \begin{bmatrix} r_{f_0} & r_{f_1} & \dots & r_{f_{|F|-1}} & 1 \\ r_j & r_{f_0} & \dots & r_{f_{|F|-2}} & r_{f_{|F|-1}} \end{bmatrix} \left(id - \begin{bmatrix} r_n & 1 \\ 1 & r_n \end{bmatrix} \right) \right]\!\!\right]_{\sqsubseteq} \to$$

$$\to \left[\!\!\left[\sum_{F\subseteq\{j+1,\dots,i-1\}\cup\{n\}} (-1)^{|F|} \begin{bmatrix} r_{f_0} & r_{f_1} & \dots & r_{f_{|F|-1}} & 1 \\ r_j & r_{f_0} & \dots & r_{f_{|F|-2}} & r_{f_{|F|-1}} \end{bmatrix} \right]\!\!\right]_{\sqsubseteq}. \tag{1.26}$$

For $i \leq j < n$, it is

$$t_j \to [\![0]\!]_{\mu_{r_n}} \to [\![0]\!]_{\left\{id, \begin{bmatrix} 1 \\ r_n \end{bmatrix}\right\}}. \tag{1.27}$$

Finally, for $j = n$, we get

$$t_j = \begin{bmatrix} 1 \\ r_n \end{bmatrix}. \tag{1.28}$$

Combining (1.26) – (1.28) with (1.25), we obtain

$$\begin{aligned} \begin{bmatrix} q \\ r \end{bmatrix}(x) \to & \left(\sum_{j=1}^{i-1} q_j \cdot \left[\!\!\left[\sum_{F\subseteq\{j+1,\dots,i-1\}\cup\{n\}} (-1)^{|F|} \begin{bmatrix} r_{f_0} & r_{f_1} & \dots & r_{f_{|F|-1}} & 1 \\ r_j & r_{f_0} & \dots & r_{f_{|F|-2}} & r_{f_{|F|-1}} \end{bmatrix} \right]\!\!\right]_{\sqsubseteq} + \right. \\ & \left. + \sum_{j=i}^{n-1} q_j \cdot [\![0]\!]_{\left\{id, \begin{bmatrix} 1 \\ r_n \end{bmatrix}\right\}} + \begin{bmatrix} q_n & 1 \\ 1 & r_n \end{bmatrix} \right)(y) \to \\ \to & \left[\!\!\left[\left(\sum_{j=1}^{i-1} \sum_{F\subseteq\{j+1,\dots,i-1\}\cup\{n\}} (-1)^{|F|} \begin{bmatrix} q_j & r_{f_0} & \dots & 1 \\ 1 & r_j & \dots & r_{f_{|F|-1}} \end{bmatrix} + \begin{bmatrix} q_n & 1 \\ 1 & r_n \end{bmatrix} \right)(y) \right]\!\!\right]_{\sqsubseteq} \to \\ \to & \left[\!\!\left[\left(\sum_{j=1}^{i-1} \sum_{F\subseteq\{j+1,\dots,i-1\}\cup\{n\}} (-1)^{|F|} \begin{bmatrix} q_j & r_{f_0} & \dots & 1 \\ 1 & r_j & \dots & r_{f_{|F|-1}} \end{bmatrix} + \begin{bmatrix} q_n & 1 \\ 1 & r_n \end{bmatrix} \right)(x) \right]\!\!\right]_{\sqsubseteq}, \end{aligned}$$

where the last arrow is by substitution $x + s$ for y and Lemma 1.5:16 c).

Finally, it is easy to see that if $\alpha \sqsubseteq \begin{bmatrix} q_j & r_{f_0} & \dots & 1 \\ 1 & r_j & \dots & r_{f_{|F|-1}} \end{bmatrix}$, for some j, then $\tilde{\alpha} \sqsubseteq_0 \tilde{\beta}$, where $\beta = \begin{bmatrix} q_{j'} & r_{f_0} & \dots & 1 \\ 1 & r_{j'} & \dots & r_{f_{|F|-1}} \end{bmatrix}$, for some j'. Therefore, in the last expression, the symbol $\sqsubseteq$ can be replaced by $\sqsubseteq_0$.

The "in particular" follows directly from (1.24). □

The following lemma is the first step in the inductive proof of Proposition H 1.5:3.

Lemma 1.5:21. *Let a_i, b_i, $i = 1, \ldots, n$ be scalars such that* $\deg(b_i) = 0$, *for all* i. *Then*

$$\left[\begin{array}{ccc} a_1 & \ldots & a_n \\ b_1 & \ldots & b_n \end{array}\right] \to \left[\!\left[\left[\begin{array}{cc} \prod_{i=1}^n a_i & 1 \\ 1 & \prod_{i=1}^n b_i \end{array}\right]\right]\!\right]_{\sqsubseteq 1}.$$

Proof. Set $p_j = \prod_{i=1}^j b_i \in \mathbb{N}$, $g_j = \prod_{i=1}^j a_i$. Denote $f_n = \left[\begin{array}{ccc} a_1 & \ldots & a_n \\ b_1 & \ldots & b_n \end{array}\right]$. We prove that

$$f_n(x + p_n k) = f_n(x) + g_n k$$

by induction on n. If $n = 1$, it is clear.

For the induction step, we have

$$\begin{aligned} f_n(x + p_n k) &= f_{n-1}\left(\begin{bmatrix} a_n \\ b_n \end{bmatrix}(x) + p_{n-1} a_n \cdot k\right) = \\ &= f_{n-1}\left(\begin{bmatrix} a_n \\ b_n \end{bmatrix}(x)\right) + g_{n-1} \cdot a_n \cdot k = \\ &= f_n(x) + g_n k, \end{aligned}$$

where the first equality is due to $b_n | p_n$, and the second one is by the induction assumption.

Now,

$$\begin{aligned} f_n(x) &= f_n\left(\mu_{p_n}(x) + p_n \cdot \begin{bmatrix} 1 \\ p_n \end{bmatrix}(x)\right) = f_n\left(\mu_{p_n}(x)\right) + g_n \cdot \begin{bmatrix} 1 \\ p_n \end{bmatrix}(x) = \\ &= \left\{ \begin{bmatrix} g_n & 1 \\ 1 & p_n \end{bmatrix}(x) + f_n(i) \text{ if } \mu_{p_n}(x) = i;\ i = 0, \ldots, p_n - 1\ . \right. \end{aligned}$$

□

Now, we are ready for our proof of Proposition H 1.5:3.

Proposition 1.5:3 (Proposition H)**.** *Every term $t(\overline{x})$ is equivalent to a harmonic almost-term $\tau(\overline{x})$.*

Moreover, if a variable x does not occur in any subterm of the form $r^{-1}s$ (where s is a term) in t then the same is true in τ.

Proof. Let t be a term. By Lemma 1.5:16 d), t is equivalent to a distributed almost-term σ. We may assume that σ does not contain binary minus nor any symbol μ_r. Then it is, clearly, enough to prove that every string

$$\alpha = \left[\begin{array}{ccc} a_1 & \ldots & a_n \\ b_1 & \ldots & b_n \end{array}\right] \tag{1.29}$$

is equivalent to an almost-term in harmonic form.

Let assign to any string α of the form (1.29) the triple

$$I_\alpha = (d_\alpha, N_\alpha, K_\alpha)$$

where $d_\alpha = \max \deg b_i$, $N_\alpha = |\{i; \deg b_i = d_\alpha\}|$, and $K_\alpha = \min\{n-i; \deg b_i = d_\alpha\}$. We prove the previous statement by induction on $I_\alpha \in \langle \mathbb{N}^3, \leq_{\mathrm{Lex}} \rangle$. We will denote the only free variable in α as x, but we will often omit writing it.

If $d_\alpha = 0$, the statement follows from Lemma 1.5:21. Otherwise, let α be a string as in (1.29). Denote $d_\alpha, N_\alpha, K_\alpha$ just d, N, K, and set $J = n - K$ (then b_J is the rightmost b_i with $\deg b_i = d$). Then

$$\begin{bmatrix} a_J \\ b_J \end{bmatrix} \to \left[\!\!\left[\sum_j s_j \right]\!\!\right]_{S_{b_J}},$$

with $s_j \in S_{b_J}$, according to Lemma 1.5:20. By Lemmas 1.5:16 and 1.5:17, then

$$\alpha \to \left[\!\!\left[\sum_j \begin{bmatrix} a_1 & \dots & a_{J-1} \\ b_1 & \dots & b_{J-1} \end{bmatrix} \circ s_j \circ \begin{bmatrix} a_{J+1} & \dots & a_n \\ b_{J+1} & \dots & b_n \end{bmatrix} \right]\!\!\right]_{\sqsubseteq}.$$

Denote the j-th summand in the previous expression as α_j, and let $\beta \sqsubseteq \alpha_j$. We complete the proof by showing that β is equivalent to a string β' with $I_{\beta'} < I_\alpha$.

By the definition of S_{b_J}, it is $d_{s_j} \leq \deg b_J = d_\alpha$. If $d_{s_j} < d_\alpha$ then, clearly, also $I_\beta \leq I_{\alpha_j} < I_\alpha$. Otherwise, $s_j = \begin{bmatrix} u_1 & \dots & 1 \\ 1 & \dots & v_l \end{bmatrix}$, where $\deg v_i < d_\alpha$, for $i < l$, and $\deg v_l = d_\alpha$. Suppose that $J < n$. Then

$$\alpha_j = \begin{bmatrix} a_1 & \dots & a_{J-1} & u_1 & \dots & 1 & a_{J+1} & \dots & a_n \\ b_1 & \dots & b_{J-1} & 1 & \dots & v_l & b_{J+1} & \dots & b_n \end{bmatrix},$$

and, since $\begin{bmatrix} 1 & a_{J+1} \\ v_l & b_{J+1} \end{bmatrix} = \begin{bmatrix} a_{J+1} \\ v_l \cdot b_{J+1} \end{bmatrix} = \begin{bmatrix} 1 & a_{J+1} \\ b_{J+1} & v_l \end{bmatrix}$, any $\beta \sqsubseteq \alpha_j$ is equivalent to some β' such that

$$\beta' \sqsubseteq \alpha'_j = \begin{bmatrix} a_1 & \dots & a_{J-1} & u_1 & \dots & 1 & a_{J+1} & \dots & a_n \\ b_1 & \dots & b_{J-1} & 1 & \dots & b_{J+1} & v_l & \dots & b_n \end{bmatrix},$$

or

$$\beta' \sqsubseteq \begin{bmatrix} a_{J+1} & \dots & a_n \\ b_{J+1} & \dots & b_n \end{bmatrix}.$$

Again, it is easy to verify that $I_{\beta'} \leq I_{\alpha'_j} < I_\alpha$. Finally, if $J = n$ then

$$\alpha_j = \begin{bmatrix} a_1 & \dots & a_{J-1} & u_1 & \dots & 1 \\ b_1 & \dots & b_{J-1} & 1 & \dots & v_l \end{bmatrix} = \begin{bmatrix} a_1 & \dots & a_{J-1} & u_1 & \dots & u_{l-1} \\ b_1 & \dots & b_{J-1} & 1 & \dots & v_{l-1} \end{bmatrix}(y),$$

where $y = y^{(j)} = \begin{bmatrix} 1 \\ v_l \end{bmatrix} = \begin{bmatrix} 1 \\ v_l^{(j)} \end{bmatrix}$, and any $\beta \sqsubseteq \alpha_j$ is equivalent to some $\beta'(y)$ such that

$$\beta' \sqsubseteq \alpha'_j = \begin{bmatrix} a_1 & \dots & a_{J-1} & u_1 & \dots & u_{l-1} \\ b_1 & \dots & b_{J-1} & 1 & \dots & v_{l-1} \end{bmatrix}.$$

Clearly, $I_{\beta'} \le I_{\alpha'_j} < I_\alpha$.

By the induction assumption, α is equivalent to an almost-term $\tau(x, \overline{y})$ in harmonic form. After substituting $y^{(j)} = \begin{bmatrix} 1 \\ v_l^{(j)} \end{bmatrix}$, we get a term $\tau'(x)$ in harmonic form, equivalent to α. □

1.5.7 Bases

In this subsection, we prove Proposition B 1.5:4. The proposition implies that every p-term or open formula can be on any interval $[Q, R]$, with $Q, R \in \mathrm{D}$, equivalently written over a multiple of a given basis. Bases $\langle b_i \rangle_{i<\omega}$ with $b_i | b_{i+1}$ will be of special importance, in particular, for the proof of Proposition S 1.5:2.

We will need the following lemmas.

Lemma 1.5:22. *Let* $0 < R < r \in \mathrm{D}$, $0 \ne n \in \mathbb{N}$. *Then*

a) $r^{-1}x = \{ n \cdot (nr)^{-1}(x) + i$ if $ir \le \mu_{nr}(x) < (i+1)r;\ i = 0, \dots, n-1$,

b) $$r^{-1}x = \begin{cases} \begin{bmatrix} R & 1 \\ r & R \end{bmatrix}(x) & \text{if } r\left(\begin{bmatrix} R & 1 \\ r & R \end{bmatrix}(x) + 1\right) \ge x, \\ \begin{bmatrix} R & 1 \\ r & R \end{bmatrix}(x) + 1 & \text{otherwise.} \end{cases}$$

Proof. Direct computation. □

Lemma 1.5:23. *Let* $0 < R, r \in \mathrm{D}$ *such that* $\deg R \le \deg r$, *and* $0 \ne n \in \mathbb{N}$.

a) There is a harmonic almost-term $\tau(x)$ *over* $\{nr\}$, *equivalent to* $r^{-1}x$.

b) There is a harmonic almost-term $\tau(x)$ *over the set* $\{r'; R|r'\}$, *equivalent to* $r^{-1}x$.

Proof. a) Directly from Lemma 1.5:22 a).

b) By a), we may suppose that $R < r$ (there is $n \in \mathbb{N}$ such that $nr > R$). Denote $\beta = R^{-1}x$. Then, by Lemma 1.5:22 a), we have:

$$r^{-1}x = \begin{cases} \begin{bmatrix} R \\ r \end{bmatrix}(\beta) & \text{if } r \cdot \left(\begin{bmatrix} R \\ r \end{bmatrix}(\beta) + 1\right) \ge x, \\ \begin{bmatrix} R \\ r \end{bmatrix}(\beta) + 1 & \text{otherwise.} \end{cases}$$

Consider now β as a variable. By Proposition H 1.5:3, there is an almost-term $\tau'(\beta, x)$ in harmonic form, equivalent to $r^{-1}x$ and such that $\mathrm{Div}_x(\tau') = \emptyset$. After substituting $\beta = R^{-1}x$ into τ', we get an almost-term $\tau(x)$ in harmonic form such that each $r' \in \mathrm{Div}_x(\tau)$ is a multiple of R.

□

Now, we are ready for a proof of Proposition B 1.5:4.

Proposition 1.5:4 (Proposition B)**.** *Let $\delta \in F$, $p, r \in {}^+\mathrm{D}$ be scalars, $e = \deg(p)$, $d = \deg(r)$, and $B = \langle b_i \rangle_{d \le i < e}$ be a $[d, e]$-basis. Then $r^{-1}x$ is on $[\delta, \delta + p - 1]$ equal to a harmonic almost-term $\tau(x)$ (possibly with parameter δ) which is over $mB = \langle mb_i \rangle_{d \le i < e}$, for some $m \in \mathbb{N}$.*

Moreover, m can be chosen as any number sufficiently large with respect to divisibility.

Proof. Observe, first, that it is enough to prove the statement for $\delta = 0$. Indeed, $r^{-1}(y+\delta)$ is, by Lemma 1.5:6 e), equivalent to an almost-term $\sigma(y)$ with $\mathrm{Div}(\sigma) = \{r\}$, and hence, by the proposition's case $\delta = 0$, on $[0, p-1]$ equivalent to a harmonic almost-term $\tau'(y)$, with $\mathrm{Div}_y(\tau') \subseteq \{m \cdot b_i; d \le i < e\}$, for a given m. By substitution $y = x - \delta$, we then have $r^{-1}x$ equivalent to $\tau'(x-\delta)$ on $[\delta, \delta+p-1]$ and $\tau'(x-\delta)$ (again by Lemma 1.5:6 e)) equivalent to an almost-term $\tau(x)$ in harmonic form, with $\mathrm{Div}_x(\tau) = \mathrm{Div}_y(\tau') \subseteq \{m \cdot b_i; \deg r \le i < e\}$.

Further, suppose $\delta = 0$. It is enough to prove that $r^{-1}x$ is on $[0, p-1]$ equivalent to a harmonic almost-term $\tau'_r(x)$ with

$$\mathrm{Div}(\tau'_r) \subseteq \{m' \cdot b_i; 0 < m' \in \mathbb{N}, \deg r \le i < e\}. \tag{1.30}$$

Then we are done almost immediately: We choose m_S to be the least common multiple of all such $m' \in \mathbb{N}$ that $m'b_i \in \mathrm{Div}(\tau'_r)$, for some i. Now, if $0 < m \in \mathbb{N}$ is a multiple of m_S then $\tau'_r(x)$ is equivalent to a harmonic almost-term $\tau_r(x)$ with $\mathrm{Div}(\tau_r) \subseteq \{m \cdot b_i; \deg r \le i < e\}$, according to Lemma 1.5:23 a).

Now, we find τ'_r such that (1.30) holds. We proceed by backwards induction on d. When $d \ge e$, there is $n \in \mathbb{N}$ such that $nr > p$. Then $r^{-1}x$ is on $[0, p-1]$ equivalent to

$$\tau'_r(x) = \big\{ l \text{ if } lr \le x < (l+1)r;\ l = 0, \ldots, n-1.$$

Suppose that $d < e$ and that the statement holds for all r' with $\deg r' > d$. Then $r^{-1}x$ is, by Lemma 1.5:23 b), equivalent to an almost-term $\sigma(x)$ with all $r' \in \mathrm{Div}(\sigma)$ divisible by $b_d \in B$. For $r' \in \mathrm{Div}(\sigma)$, it is either $r' = m'b_d$, for some $m' \in \mathbb{N}$, or $\deg r' > d$. Denote τ'_r the almost-term created from σ by replacing all ${r'}^{-1}x$ with $\deg r' > d$ by the respective almost-terms $\tau'_{r'}$ from the induction assumption; τ'_r has, clearly, the demanded properties. □

1.5.8 Solvability

Using the Proposition B 1.5:4 for $B = \langle b_i \rangle_{i<\omega}$ with $b_i | b_{i+1}$, we may now prove the last of the three main propositions – Proposition S 1.5:2.

1.5.8.1 Linear period and linear growth

A scalar $p \in \mathrm{D}$ is called a *linear period* of a term $t(x, \overline{y})$ in (a variable) x if $t(pu + v, \overline{y})$ is affine in u, for every $v, \overline{y} \in F$, i.e. for every $v, \overline{y} \in F$, there is $\gamma_{x,p}$=$\gamma_{x,p}(v, \overline{y})$$\in \mathrm{D}$ such that

$$t(pu + v, \overline{y}) = \gamma_{x,p} \cdot u + t(v, \overline{y}) \tag{1.31}$$

holds for all $u \in F$. It is not hard to see that the *linear growth* $\gamma_{x,p}(v, \overline{y})$ does not depend on v nor $\overline{y}$; we denote it $\gamma_{x,p}(t)$ (this follows from the easy observation that if P is the product of all occurances of x-divisors in $s(x, v, \overline{y})$ then $s(Pu, v, \overline{y}) = s'(Pu) + s''(v, \overline{y})$, for some terms s', s'').

We say that $p \in \mathrm{D}$ is a *linear period* of an open formula ψ [p-term τ] if it is a linear period of every maximal subterm of ψ [τ].

1.5.8.2 Balanced form

We say that an open harmonic formula ψ is *balanced* [in x] (in a *balanced form* [in x]) if there is an enumeration $\langle r_i \rangle_{i<n}$ of $\mathrm{Div}(\psi)$ [$\mathrm{Div}_x(\psi)$] such that $r_i | r_{i+1}$. Similarly, we define balanced form for an open harmonic p-term. If ψ is harmonic and balanced in x then, clearly, the maximal x-divisor in ψ is a linear period of ψ in x.

Lemma 1.5:24. *Let $\psi(v, \overline{y})$ be an open formula, and $0 < P \in \mathrm{D}$. Then there is an open harmonic $\chi(v, \overline{y})$, having a linear period p in v with $\deg(p) < \deg(P)$, and such that*

$$(\forall \overline{y})(\forall 0 \leq v < P)(\psi(v, \overline{y}) \leftrightarrow \chi(v, \overline{y})).$$

Proof. We apply the Proposition B 1.5:4 to (every maximal subterm of) ψ, the interval $[0, P]$ and a $[0, \deg(P)]$-basis $B = \langle b_i \rangle_{i<\deg(P)}$ such that $b_i | b_{i+1}$. The resulting formula χ is harmonic and over mB in v, for some $m \in \mathbb{N}$, hence balanced in v, and therefore its maximal v-divisor p ($p = 1$ if there are no v-divisors) is a linear period of χ in v. It is $p = mb_i$, for some $i < \deg(P)$, and thus $\deg(p) = i < \deg(P)$. $\square$

The following lemma proves Proposition S 1.5:2 for the case $\mathrm{Div}_x(\psi) = \emptyset$. The algorithm it contains is known as the *Fourier-Motzkin elimination.*

Lemma 1.5:25 ("Fourier-Motzkin elimination")**.** *Suppose that* $\psi(x, \overline{y})$ *is open and such that* $\mathrm{Div}_x(\psi) = \emptyset$*. Then there are finitely many terms* $t_j(\overline{y})$*,* $j < n \in \mathbb{N}$*, such that*

$$(\exists x)\psi(x, \overline{y}) \leftrightarrow \bigvee_{j<n} \psi(t_j, \overline{y}).$$

Proof. Without loss of generality, we can assume that ψ is a system of linear inequalities of the form $a_i x - s_i \leq 0$, where $a_i \in \mathrm{D}$ and s_i are terms with all their variables among $\overline{y}$. Denote I^+ $[I^-, I^0]$ the set of all indices i for witch $a_i > 0$ $[a_i < 0, a_i = 0]$. Then

$$\psi \leftrightarrow \bigwedge_{i \in I^0} s_i \leq 0 \,\&\, \bigwedge_{i \in I^-} x \geq \frac{s_i}{a_i} \,\&\, \bigwedge_{j \in I^+} x \leq \frac{s_j}{a_j}.$$

If both I^+ and I^- are empty then we can set $n = 1$ and $t_0 = 0$. Suppose that $I^+ \neq \emptyset$ (the other case is symetric). Then

$$(\exists x)\psi(x, \overline{y}) \leftrightarrow \bigvee_{j \in I^+} \psi({a_j}^{-1} s_j, \overline{y}).$$

$\square$

Now, we are going to prove Proposition S 1.5:2.

Proposition 1.5:2 (Proposition S)**.** *Let* $\psi(x, \overline{y})$ *be an open formula. There are finitely many terms* $t_i(\overline{y})$*,* $i < n$*, such that*

$$(\exists x)\psi \leftrightarrow \bigvee_{i<n} \psi(t_i, \overline{y}).$$

Proof. The case $\mathrm{Div}_x(\psi) = \emptyset$ follows immediately from Lemma 1.5:25; assume further $\mathrm{Div}_x(\psi) \neq \emptyset$. We may also suppose that ψ is harmonic (thanks to Proposition H 1.5:3). Let P be a linear period of ψ in x of the least degree; we prove the statement by induction on $\deg(P)$.

We denote $\tilde{\psi}(u, v, \overline{y})$ the formula created from ψ by replacing its each maximal subterm $t(x, \overline{y})$ with $\gamma_{x,P}(t) \cdot u + t(v, \overline{y})$. By (1.31) we have

$$\psi(Pu + v, \overline{y}) \leftrightarrow \tilde{\psi}(u, v, \overline{y}). \tag{1.32}$$

Since $\mathrm{Div}_u(\tilde{\psi}) = \emptyset$, by Lemma 1.5:25, there are terms $t'_j(v, \overline{y})$, $j < n'$, such that

$$(\exists x)\psi(x, \overline{y}) \leftrightarrow (\exists 0 \leq v < P) \bigvee_{j<n'} \tilde{\psi}(t'_j, v, \overline{y}) \leftrightarrow (\exists 0 \leq v < P) \bigvee_{j<n'} \psi(t''_j, \overline{y}),$$

where $t''_j(v,\overline{y}) = P \cdot t'_j + v$. Here, the first equivalence follows from (the unique) representability of x as $x = Pu + v$ with $0 \leq v < P$, and the second equivalence from (1.32).

If $\deg(P) = 0$ then the last formula is equivalent to $\bigvee_{j<n',m<P} \psi(t_{j,m},\overline{y})$, where $t_{j,m}(\overline{y}) = t''_j(\underline{m},\overline{y})$, which is what we wanted to prove.

Let $\deg(P) > 0$. By Lemma 1.5:24, there is $\chi(v,\overline{y})$ with a linear period p in v such that $\deg(p) < \deg(P)$ and

$$\bigvee_{j<n'} \psi(t''_j,\overline{y}) \leftrightarrow \chi(v,\overline{y}),$$

for $0 \leq v < P$. Denote χ' the formula $\chi \,\&\, (0 \leq v < P)$. By the induction assumption, there are terms $s_i(\overline{y})$, $i < k$, such that

$$(\exists x)\psi(x,\overline{y}) \leftrightarrow (\exists v)\chi'(v,\overline{y}) \leftrightarrow \bigvee_{i<k} \chi'(s_i,\overline{y}).$$

Denote $t_{i,j}(\overline{y}) = t''_j(s_i(\overline{y}),\overline{y})$. Then

$$(\exists x)\psi(x,\overline{y}) \leftrightarrow \bigvee_{i<k,j<n'} \psi(t_{i,j},\overline{y}).$$

$\square$

1.6 Two-sorted solvability

The proof of Theorems 1.3:4, 1.3:6 and 1.3:8 from section 1.5 proves, in fact, more than we stated so far: For example, in the statement of Proposition S 1.5:2 (and consequently also in Theorem 1.3:4), all scalars which occur in terms t_i can be constructed from scalars occuring in ψ by ring operations and integer division.

This observation may be formulated as solvability (or quantifier elimination) for so called doded-modules – structures in a two-sorted language of the type "ordered ring-ordered module" (i.e. in a language with a special sort for scalar variables), which are just two-sorted variants of models of linear theories. This is stated in Theorem 1.6:1 and its Corollary 1.6:2.

These results are an ordered analogues of the quite well-known results by Lou van den Dries and Jan Holly in [vdDH92] for two-sorted unordered modules and strengthen the result by Volker Weispfenning in [Wei97, Theorem 4.1] for two-sorted discretely ordered modules over the ring $\mathbb{Z}$ of integers (more precisely for the models of a two-sorted variant of Presburger arithmetic).

The results from [vdDH92] are generalized by adding an ordering to the language but for a price of restricting ourselves only to modules over rings which are dodeds (see 1.3.1.2) (and adding another order-related conditions). Let us note that in [vdDH92] the problem of generalizing the results to ordered modules (even for the simplest case of the module $\mathbb{Z}$ of integers) is considered as "very interesting" but as one that "seems to be very hard".

The Weispfenning's result is strengthened in two directions: first, we admit the universe of the ring sort to be not only the ring $\mathbb{Z}$ of integers but an arbitrary doded (see Example 1.3:1 for examples of dodeds); second, we give a strictly smaller elimination set of formulas than Weispfenning's "scalar bounded formulas" (see Remark 1.6:3).

Let $\mathbb{L}$ denote the two-sorted language of the type "ordered ring-ordered module", i.e. $\mathbb{L}$ consists of

- the ordered ring sort R with a language $\langle 0, 1, +, -, \cdot, \leq\rangle$,
- the ordered group sort M with a language $\langle 0, 1, +, -, \leq\rangle$ (the symbol 1 is intended for the least positive element),
- a binary function symbol $\cdot : R \times M \to M$ (scalar multiplication).

Further on, unless stated otherwise, symbols x, y, z denote M-variables while symbols p, q, r stand for R-variables. We also refer to R-variables as scalar variables and to quantification of those variables as scalar quantification.

A doded-module is a (two-sorted) $\mathbb{L}$-structure $\mathcal{A} = \langle \mathcal{R}, \mathcal{M}, \cdot\rangle$ such that

1) $\mathcal{R}$ is a doded (see 1.3.1.2),

2) $\langle \mathcal{M}, r \cdot \_\rangle_{r\in R}$ is a discretely ordered (with 1 being the least positive element), integrally-divisible (i.e. $(\forall x)(\exists y)(\exists 0 \leq z < r{\cdot}1)(x = r{\cdot}y{+}z)$ holds) $\mathcal{R}$-module.

We denote $\mathbb{L}'$ the extension of $\mathbb{L}$ by

- a binary function symbol ${}^{-1} : R^2 \to R$ (scalar integer-division),
- a binary function symbol ${}^{-1} : R \times M \to M$ (integer-division).

Usually, we write $r^{-1}q$ or $r^{-1}x$ instead of ${}^{-1}(r, q)$ or ${}^{-1}(r, x)$.

For a doded-module $\mathcal{A}$, we write $\mathcal{A}'$ for its $\mathbb{L}'$-expansion by definitions:

- $0 \leq q - r \cdot (r^{-1}q) < r$,
- $0 \leq x - r \cdot (r^{-1}x) < r \cdot 1$.

Now, we are ready to formulate the main result of this section. The following theorem may be understood as stating that every doded-module is "M-almost uniformly M-solvable".

Theorem 1.6:1. *Let $\mathcal{A} = \langle \mathcal{R}, \mathcal{M}, \cdot \rangle$ be a doded-module, $\varphi(\overline{r}, \overline{y}, x)$ be an $\mathbb{L}'$-formula without scalar quantifiers, and $\overline{\rho} \in R^{l(\overline{r})}$ be scalars. Then there are finitely many $\mathbb{L}'$-terms $t_i(\overline{r}, \overline{y})$, for $i < n$, with $n \in \mathbb{N}$, such that*

$$\mathcal{A}' \models (\exists x)\varphi(\overline{\rho}, \overline{y}, x) \leftrightarrow \bigvee_{i<n} \varphi(\overline{\rho}, \overline{y}, t_i(\overline{\rho}, \overline{y})).$$

Proof. First observe that, for fixed scalars $\overline{\rho} \in R^{l(\overline{r})}$, the formula $\varphi(\overline{\rho}, \overline{y}, x)$ can be written naturally as a formula in the language of the (one-sorted) lineal which corresponds to the (two-sorted) doded-module $\mathcal{A}$.

Then it is enough to check that the proof of Proposition S 1.5:2 (which occupies most of section 1.5) constructs terms t_i which contain only scalars expressible from the scalars occuring in ψ only by ring operations and the operation $^{-1}$ of scalar integer division (i.e. $\mathbb{L}'$-scalar-operations).

This is obvious with only two exceptions:

a) In Lemma 1.5:24, we used an arbitrary balanced basis B. By doing that we can only assure scalars in formula χ to be expressible by $\mathbb{L}'$-scalar-operations from the scalars occuring in ψ and scalars from the basis B.

b) In the final part of the proof of Proposition S 1.5:2, we defined P to be the linear period of ψ of the least degree. Again, it is not clear that such P is expressible by $\mathbb{L}'$-scalar-operations from the scalars occuring in ψ.

Both these problems can be easily resolved:

a) Instead of taking an arbitrary balanced basis and applying Proposition B 1.5:4, we may use the backwards induction idea from the proof of Proposition B directly with a simple modification: At the induction step do not use Lemma 1.5:23 b) to get all divisors be divisible by b_d but use the same lemma to get all divisors be divisible by the maximal divisor q such that all divisors $q' \leq q$ are up to multiplication by some $m \in \mathbb{N}$ linearly ordered by divisibility.

Then we get a balanced formula χ with all scalars expressible by $\mathbb{L}'$-scalar-operations from the scalars occuring in ψ.

b) It is enough to take P to be the least common multiple of all x-divisors in ψ.

$\square$

Corollary 1.6:2. *Let $\mathcal{A}$ be a doded-module. Every scalar-quantifier-free $\mathbb{L}'$-formula is in $\mathcal{A}'$ equivalent to a quantifier-free $\mathbb{L}'$-formula.*

Remark 1.6:3. To compare Corollary 1.6:2 with [Wei97, Theorem 4.1], let us note that any quantifier-free $\mathbb{L}'$-formula can be easily equivalently rewritten as a scalar bounded (i.e. with all quantifiers of the form $(\exists x,\ |x| \leq r \cdot 1)$ with r a scalar term) formula in the language $\mathbb{L} \cup \langle ^{-1}, \equiv \rangle$, where $^{-1}$ is the scalar integer-division, and $\equiv$ is a ternary $R \times M^2$ congruence relation, defined as $x \equiv_r y \leftrightarrow (\exists z)(r \cdot z = x - y)$.

Indeed, this is easy since $r^{-1}x = y \leftrightarrow (\exists z,\ |z| \leq (r-1) \cdot 1)(z \equiv_r x \,\&\, y = \frac{x-z}{r})$.

Chapter 2

Structure of Peano Products

In this chapter, we deal with a problem of understanding relations between local and global properties of an operation o in a first-order structure of the form $\langle \mathcal{B}, o \rangle$, with a particular interest in the case where $\mathcal{B}$ is a model of Presburger arithmetic Pr and o is a "Peano product" on $\mathcal{B}$, i.e. $\langle \mathcal{B}, o \rangle$ is a model of Peano arithmetic P.

This problem may be specified as follows: Given a "background model" $\mathcal{B}$ and a set O of all n-ary operations on B satisfying certain global property (e.g. being a Peano product), we want to describe the dependency closure

$$\mathrm{icl}^O(E) = \{\overline{d} \in B^n; (\forall o, o' \in O)(o \restriction E = o' \restriction E \Rightarrow o(\overline{d}) = o'(\overline{d}))\},$$

for $E \subseteq B^n$. We call this task the $(\mathcal{B}, O, E)$-dependency problem.

Illustratively speaking, a point $\overline{d}$ lies in the dependency closure $\mathrm{icl}^O(E)$ of the set E if the value $o(\overline{d})$ of any operation $o \in O$ is uniquely determined by its values on E.

Our particular interest is in the Peano dependency problem – a $(\mathcal{B}, O, E)$-dependency problem where $\mathcal{B}$ is a model of Pr and O is the set of all (saturated) Peano products on $\mathcal{B}$. Both, the general dependency problem and the Peano dependency problem, may be further modified and specified by various modifications of the dependency closure (see the more general definition 2.1.1).

A $(\mathcal{B}, O, E)$-dependency problem with saturated $\mathcal{B}$ may be solved by studying a definability problem (regarding almost-uniform definability; see 2.1.3) in certain expansion of $\mathcal{B}$, called a *fixator* (2.1.4). This is formulated in the *DD-theorem* 2.1:2.

In Proposition 2.2:1, we completely solve two important cases of the Peano dependency problem – for $E = \emptyset$ (which is easy) and for $E = E_a = \{a\} \times B$, with a nonstandard (an *"a-slice"*). We prove that, in these cases, $\mathrm{icl}(E)$ is as small as possible, i.e. it contains only the trivially dependent points (for $E = E_a$ that are points $\overline{d} = (d_0, d_1)$ where at least one of d_i equals $p(a)$, for some polynomial $p \in \mathbb{Q}[x]$).

By the DD-theorem, the key for the proof is understanding definability in the respective fixators. The fixators are models of Presburger arithemetic Pr (1.1.3.1) and linear arithmetic LA (1.1.4.1), respectively. We use here the descriptions of elimination sets of formulas for the fixators which we provided in Corollaries 1.4:2 and 1.4:7, respectively, in chapter 1.

An important special case of Proposition 2.2:1 proves the existence of pairs of Peano products $(\cdot, \circ)$ which coincide on an "a-slice" $E_a = \{a\} \times B$, with $a \in B - \mathbb{N}$, but differ in some $\overline{d} < a$ and in some $\overline{d'} > a$. We call such a couple a meeting pair of Peano products. By "piecing together" a meeting pair, it is possible to obtain a new "Robinson product" on $\mathcal{B}$, which satisfies certain portion of induction. In section 2.3, we put these ideas into the context of possible further research on constructions of models of Peano arithmetic.

Finally, section 2.4 contains a summary of our partial results regarding the problem of interpolating a given set of points in B^3 by the graph of some Peano product.

2.1 Dependency and definability

Given a saturated structure $\mathcal{B}$ (background-model) and a set O of n-ary operations on B, we want to know whether, for an operation $o \in O$, its value in a point $\overline{d} \in B^n$ is determined by its values on a set $E \subseteq B^n$; this question is precised in a concept of dependency in 2.1.1. The main result of this section, the DD-theorem 2.1:2, provides an equivalent for dependency in terms of definability in an expansion $\mathcal{A}$ of $\mathcal{B}$, called fixator (see 2.1.4 for definition).

Throughout this section, $\mathcal{A}$ denotes a saturated expansion of a background-model $\mathcal{B}$, $n > 0$ is an integer, $\overline{d} \in B^n$ and $E \subseteq B^n$. Further, all considered operations on $A = B$ are n-ary.

2.1.1 Dependency and marriages

Let $\sim$ be an equivalence relation on a set O of n-ary operations on B, $o \in O$. We say that a point $\overline{d} \in B^n$ $\sim$-depends *on* $E \subseteq B^n$ *[for o]* if, for $o', o'' \in O$ such that $o' \sim o''[= o]$ and $o' \restriction E = o'' \restriction E$, it is $o'(\overline{d}) = o''(\overline{d})$. The set

$$\mathrm{icl}^{\sim}_{[o]}(E) = \{\overline{d} \in B^n; \overline{d} \ \sim\text{-depends on } E \text{ [for } o]\}$$

is called the $\sim$-*dependency closure* of E [for o]. It is easy to see that it is

$$\mathrm{icl}^{\sim}(E) = \bigcap_{o \in O} \mathrm{icl}^{\sim}_{o}(E).$$

A pair (o, o') of operations on B is called a $(\overline{d}, E)$-*marriage* if $o \restriction E = o' \restriction E$, and $o(\overline{d}) \neq o'(\overline{d})$. The purpose of marriages is to witness that a point $\overline{d}$ does not belong to the dependency closure of a set E.

2.1.2 Conjugation

We are going to construct marriages as pairs (o, o^g), where $o^g = g^{-1}og$, for an appropriate automorphism g of $\mathcal{B}$. Clearly, it is $\langle \mathcal{B}, o^g \rangle \cong \langle \mathcal{B}, o \rangle$, via g, and

$$o^g(\overline{x}) = o(\overline{x}) \Leftrightarrow og(\overline{x}) = go(\overline{x}), \tag{2.1}$$

for all $\overline{x} \in B^n$.

Instead of $\langle \mathcal{B}, o' \rangle \cong \langle \mathcal{B}, o \rangle$ [via g], we write shortly $o' \cong o$ [via g].

2.1.3 Almost uniform definability

An useful criterion for dependency can be formulated using the concept of almost uniform definability, which we state at this place.

Two sequences ε, ε' of elements of A are said to be *indistinguishable* in $\mathcal{A}$ if they have the same complete type over $\emptyset$ in $\mathcal{A}$.

We say that a pair $(c, c') \in A^2$ is *equidefinable* from parameters $(\langle b_i \rangle_{i \in I}, \langle b'_i \rangle_{i \in I})$ in $\mathcal{A}$ if there is an $L(\mathcal{A})$-formula $\varphi(\overline{x}, y)$ which *equidefines* (c, c') in $\mathcal{A}$ from $(\langle b_i \rangle_{i \in I}, \langle b'_i \rangle_{i \in I})$; i.e. there is $\{i_j; j < l(\overline{x})\} \subseteq I$ such that φ defines c from $\langle b_{i_j} \rangle_{j < l(\overline{x})}$ and c' from $\langle b'_{i_j} \rangle_{j < l(\overline{x})}$.

An operation o is in $\mathcal{A}$ *almost-uniformly definable (a.u.-definable)* at a point $\overline{d} \in A^n$ over a set $E \subseteq A^n$ if, for all $\langle \overline{e}', \overline{d}' \rangle_{\overline{e} \in E}$ such that $\varepsilon = \sqcup \langle \overline{e}, o(\overline{e}), \overline{d} \rangle_{\overline{e} \in E}$ and $\varepsilon' = \sqcup \langle \overline{e}', o(\overline{e}'), \overline{d}' \rangle_{\overline{e} \in E}$ are indistinguishable in $\mathcal{A}$, the pair $(o(\overline{d}), o(\overline{d}'))$ is equidefinable from $(\varepsilon, \varepsilon')$ in $\mathcal{A}$.

Lemma 2.1:1. *Let o be an operation on A and $\varepsilon = \langle a_i, \overline{d} \rangle_{i \in I}$, $\varepsilon' = \langle a'_i, \overline{d}' \rangle_{i \in I}$ be two indistinguishable (in $\mathcal{A}$) systems of elements from A, with $|I| < |A|$, $l(\overline{d}) = l(\overline{d}') = n$. Then the following statements are equivalent:*

1) $(o(\overline{d}), o(\overline{d}'))$ is equidefinable in $\mathcal{A}$ from parameters $(\varepsilon, \varepsilon')$.

2) For every $g \in \mathrm{Aut}(\mathcal{A})$ such that $g(a_i) = a'_i$ and $g(\overline{d}) = \overline{d}'$, it is $og(\overline{d}) = go(\overline{d})$.

Moreover, the implication "1) $\Rightarrow$ 2)" is true even for a non-saturated $\mathcal{A}$.

Proof. 1) $\Rightarrow$ 2): Easy.
2) $\Rightarrow$ 1): Suppose $(o(\overline{d}), o(\overline{d}'))$ is not equidefinable from $(\varepsilon, \varepsilon')$. Define $g(a_i) = a'_i$, $g(\overline{d}) = \overline{d}'$ and $g(o(\overline{d})) = e$, where $e \neq o(\overline{d}') = og(\overline{d})$ is such that $\varepsilon \smile \langle o(\overline{d}) \rangle$ and $\varepsilon' \smile \langle e \rangle$ are indistinguishable (we construct such e later); then g can be extended to an automorphism of $\mathcal{A}$ contradicting 2).

Existence of e: Let $p(x) = \{\varphi(x, \varepsilon'); \mathcal{A} \models \varphi(o(\overline{d}), \varepsilon)\} \cup \{x \neq o(\overline{d}')\}$. Since $(o(\overline{d}), o(\overline{d}'))$ is not equidefinable from $(\varepsilon, \varepsilon')$, $p(x)$ is a type. Any e realizing $p(x)$ has the demanded properties. □

2.1.4 Fixators and DD-theorem

Let $G \subseteq \mathrm{Aut}(\mathcal{B})$ be a subgroup, o an n-ary operation on B, and $E \subseteq B^n$. We say that a saturated expansion $\mathcal{A}$ of $\mathcal{B}$ is a (G, E)-*fixator* for o if

$$g \in \mathrm{Aut}(\mathcal{A}) \Leftrightarrow g \in G, \text{ and } og(\overline{x}) = go(\overline{x}) \text{ for all } \overline{x} \in E.$$

For $o, o' \in O$, we write $o \sim^G o'$ if $o \cong o'$ via some $g \in G$. Clearly, $\sim^G$ is an equivalence on O.

Proposition 2.1:2 (DD-theorem). *Let o be an n-ary operation on B, $\overline{d} \in B^n$, and $E = E_s \cup E_f \subseteq B^n$, where $|E_s| < |B|$, and suppose that there is a saturated (G, E_f)-fixator $\mathcal{A}$ for o, with $G \subseteq \mathrm{Aut}(\mathcal{B})$. Then the following statements are equivalent:*

1) $\overline{d} \in \mathrm{icl}_o^{\sim^G}(E)$,

2) o is a.u.-definable at $\overline{d}$ over E_s in $\mathcal{A}$.

Proof. We have the following:

$\overline{d} \in \mathrm{icl}_o^{\sim^G}(E)$ $\Leftrightarrow$ For all $o' \cong o$, via some $g \in G$ such that $o' \restriction E = o \restriction E$, it is $o'(\overline{d}) = o(\overline{d})$.

$\Leftrightarrow$ For all $g \in G$ and $\overline{d'}, \overline{e'}$ with $\overline{e} \in E$, if $g(\overline{d}) = \overline{d'}$, and $g(\overline{e}) = \overline{e'}$, $g(o(\overline{e})) = o(\overline{e'})$, for $\overline{e} \in E$, then $g(o(\overline{d})) = o(\overline{d'})$.

$\Leftrightarrow$ o is a.u.-definable at $\overline{d}$ over E_s in $\mathcal{A}$.

Above, the first $\Leftrightarrow$ is the definition of $\mathrm{icl}_o^{\sim^G}(E)$, the second $\Leftrightarrow$ is by setting $o' = o^g$ and by (2.1), and the third $\Leftrightarrow$ follows by Lemma 2.1:1 and the definition of a (G, E_f)-fixator. $\square$

2.2 Dependency of Peano products

In this section, $\mathcal{B}$ will be a fixed saturated model of Presburger arithmetic[1] and O the set $\mathsf{sPP}(\mathcal{B})$ of all saturated Peano products on $\mathcal{B}$. Note that, up to an isomorphism, there are all saturated models of Peano arithmetic of size $|B|$ among the structures $\langle \mathcal{B}, \cdot \rangle$, where $\cdot \in \mathsf{sPP}(\mathcal{B})$.

We are going to prove the following proposition, which describes $\mathrm{icl}^{\mathsf{sPP}(\mathcal{B})}(E)$ for two particular cases: $E = \emptyset$ and $E = E_a = \{a\} \times B$, with $a \in B - \mathbb{N}$.

[1] Let us note that existence of saturated models is, in general, not provable in ZFC. However, a saturated model of Presburger aritmhetic of size κ exists provided that $\omega < \kappa = \kappa^{<\kappa}$. In particular, under the assumption of continuum hypothesis, there is such a model of size 2^ω. Here and further on, we therefore assume continuum hypothesis (which even implies that every countable structure in a countable language has a saturated elementary extension of size 2^ω).

For $a \in B - \mathbb{N}$, let us denote

$$D_a = \left\{ \frac{p}{n}; p \in {}^{+}\mathbb{Z}[a],\ 0 < n \in \mathbb{N} \text{ and } \mathcal{B} \models n|p \right\} = \mathbb{Q}[a] \cap B$$

(compare to $\mathrm{D}_{\mathcal{A}}$ from Example 1.3:2 b)). We also write $\circ \cong_{[a]} \cdot$ if there is an isomorphism f of $\langle \mathcal{B}, \circ \rangle$ and $\langle \mathcal{B}, \cdot \rangle$ [such that $f(a) = a$].

Proposition 2.2:1. *Let $a \in B - \mathbb{N}$. The following holds:*

1) $\mathrm{icl}_{\cdot}^{\cong}(\emptyset) = (\mathbb{N} \times B) \cup (B \times \mathbb{N})$, *for every* $\cdot \in \mathsf{sPP}(\mathcal{B})$,
$\mathrm{icl}^{\cong}(\emptyset) = (\mathbb{N} \times B) \cup (B \times \mathbb{N})$,

2) $\mathrm{icl}_{\cdot}^{\cong_a}(E_a) = (D_a \times B) \cup (B \times D_a)$, *for every* $\cdot \in \mathsf{sPP}(\mathcal{B})$,
$\mathrm{icl}^{\cong_a}(E_a) = (D_a \times B) \cup (B \times D_a)$.

Let $\mathsf{P}(\mathcal{B})$ denote the set of all commutative, associative and distributive Robinson products on $\mathcal{B}$ and $\mathsf{PP}(\mathcal{B})$ the set of all Peano products on $\mathcal{B}$. We get the following easy corollary:

Corollary 2.2:2. *Let $a \in B - \mathbb{N}$. The following holds:*

1) $\mathrm{icl}^{\mathsf{P}(\mathcal{B})}(\emptyset) = \mathrm{icl}^{\mathsf{PP}(\mathcal{B})}(\emptyset) = \mathrm{icl}^{\mathsf{sPP}(\mathcal{B})}(\emptyset) = (\mathbb{N} \times B) \cup (B \times \mathbb{N})$,

2) $\mathrm{icl}^{\mathsf{P}(\mathcal{B})}(E_a) = \mathrm{icl}^{\mathsf{PP}(\mathcal{B})}(E_a) = \mathrm{icl}^{\mathsf{sPP}(\mathcal{B})}(E_a) = (D_a \times B) \cup (B \times D_a)$.

Proof. The inclusions "$\subseteq$" follow from Proposition 2.2:1.

The opposite inclusions in 1) are trivial. In 2) they follow easily from commutativity, associativity and distributivity of the products. $\square$

Remark 2.2:3. Let us note that for the case $|E| < |B|$ the dependency problem is not difficult. Indeed, by the DD-theorem 2.1:2, $\overline{d} \in \mathrm{icl}_o^{\cong}(E) \Leftrightarrow o$ is a.u.-definable at $\overline{d}$ over E in $\mathcal{B}$ (because, clearly, $\mathcal{B}$ is an $(\mathrm{Aut}(\mathcal{B}), \emptyset)$-fixator for any operation o on B). But $\mathcal{B} \models \mathrm{Pr}$, hence the definability problem can be easily solved.

Nevertheless, if $|E| = |B|$, the relevant fixator may be more complex structure than $\mathcal{B}$. For example, in the next section, we will see that for $E = E_a$ the respective fixator is a model of LA.

2.2.1 Fixators for Peano products

We will prove Proposition 2.2:1 using the DD-theorem 2.1:2. That is why we need to know the respective fixators:

Observation 2.2:4.

a) $\mathcal{B}$ *is an* $(\mathrm{Aut}(\mathcal{B}), \emptyset)$*-fixator for any operation o on B.*

b) $\mathcal{B}_{a,\cdot} = \langle \mathcal{B}, a \cdot \_ \rangle$ *is an* (S_a, E_a)*-fixator for* $\cdot \in \mathsf{sPP}(\mathcal{B})$*, where S_a is the stabilizer of a under the action of* $\mathrm{Aut}(\mathcal{B})$.

Let us note that $\mathcal{B} \models \mathrm{Aa}$ and $\mathcal{B}_a \models \mathrm{La}$. We are going to prove both cases of Theorem 2.2:1 at once. Further, we work in one of the following settings, which we fix:

- $\mathcal{A} = \mathcal{B}$, $G = \mathrm{Aut}(\mathcal{B})$, $E = \emptyset$,
- $\mathcal{A} = \mathcal{B}_{a,\cdot}$ $G = S_a$, $E = E_a$, where $a \in B - \mathbb{N}$ and $\cdot \in \mathsf{sPP}(\mathcal{B})$.

In both cases, we have the following properties:

(*a) $\mathcal{A}$ is saturated,

(*b) every formula is in $\mathcal{A}$ equivalent to $\bigvee_{i<n}(\exists \overline{z})\psi_i$, where ψ_i, with $i < n$, are systems of linear inequalities,

(*c) the substructure $\mathcal{A}_{(\emptyset)}$ of all elements definable without parameters in $\mathcal{A}$ is an elementary substructure of $\mathcal{A}$.

This follows from Corollary 1.4:2 or Corollary 1.4:7, respectively.

The following Lemma is an adaptation of an idea by Jan Šaroch.

Lemma 2.2:5 (J. Šaroch)**.** *Let $p(\overline{x})$ be a complete type over $\emptyset$ in $\mathcal{A}$. Then $U = \{\overline{u}; \mathcal{A} \models p(\overline{u})\}$ is closed under the operation $\overline{u}, \overline{v} \mapsto \frac{\overline{u}+\overline{v}}{2}$.*

Proof. Let $\overline{u}, \overline{v} \in U$ and $\varphi(\overline{x}) \in p$. We prove $\varphi(\frac{\overline{u}+\overline{v}}{2})$.

By (*b), we may suppose that φ is of the form $\bigvee_{i<n}(\exists \overline{z})\psi_i$, where ψ_i, with $i < n$, are systems of linear inequalities. Since $\overline{u}$ and $\overline{v}$ have the same complete type, there is $i < n$ and $\overline{\pi} \in {}^{l(z)}2$ such that $(\exists \overline{z} \equiv_2 \overline{\pi})\psi_i$ holds for both $\overline{u}$ and $\overline{v}$. Then $(\exists \overline{z})\psi_i$ holds for $\frac{\overline{u}+\overline{v}}{2}$, as well. □

Lemma 2.2:6. *Let $\overline{u} \in A^2$ and $U = \{\overline{u}' \in A^2; tp(\overline{u}) = tp(\overline{u}')\}$. Then the following are equivalent:*

a) None of u_0, u_1 is $\emptyset$-definable in $\mathcal{A}$.

b) U contains $\overline{u}'$ and $\overline{u}''$ such that $u'_i \neq u''_i$, for $i = 0, 1$.

Proof. "b)⇒a)" is trivial.
"a)⇒b)": Set

$$\begin{aligned} U_0 &= \{v_1; (u_0, v_1) \in U\}, \\ U_1 &= \{v_0; (v_0, u_1) \in U\}. \end{aligned}$$

We show that each of U_0, U_1 has at least two elements. Then there are $v_0 \neq u_0$ and $v_1 \neq u_1$ such that $(u_0, v_1), (v_0, u_1) \in U$, and, by Lemma 2.2:5, the point $(u'_0, u'_1) = (\frac{u_0+v_0}{2}, \frac{u_1+v_1}{2}) \in U$ is different from (u_0, u_1) in both coordinates.

Suppose that $U_0 = \{u_1\}$. Then, by (*a), u_1 is definable from u_0, and thus it is $U = \{(u', f(u')); u' \in \mathrm{dom}(U)\}$, for some definable function f. By our assumption, $f(u') = u_1$, for all $u' \in \mathrm{dom}(U)$. Therefore, again by (*a), there is $\varphi \in tp(\overline{u})$ such that $\mathcal{A} \models \varphi(\overline{x}) \to f(x_0) = u_1$. By (*c), there is a $\emptyset$-definable $\overline{w} \in A^2$ such that $\varphi(\overline{w})$, and hence $u_1 = f(w_0)$ is $\emptyset$-definable.

The case $U_1 = \{u_0\}$ is symmetric. $\square$

Now, we are ready to prove Proposition 2.2:1.

Proposition 2.2:1. *Let $a \in B - \mathbb{N}$. The following holds:*

1) $\mathrm{icl}^{\cong}_{\cdot}(\emptyset) = (\mathbb{N} \times B) \cup (B \times \mathbb{N})$, *for every* $\cdot \in \mathsf{sPP}(\mathcal{B})$,
$\mathrm{icl}^{\cong}(\emptyset) = (\mathbb{N} \times B) \cup (B \times \mathbb{N})$,

2) $\mathrm{icl}^{\cong_a}_{\cdot}(E_a) = (D_a \times B) \cup (B \times D_a)$, *for every* $\cdot \in \mathsf{sPP}(\mathcal{B})$,
$\mathrm{icl}^{\cong_a}(E_a) = (D_a \times B) \cup (B \times D_a)$.

Proof. We need to prove that $\mathrm{icl}^{\sim^G}_{\cdot}(E) = (A_{(\emptyset)} \times A) \cup (A \times A_{(\emptyset)})$. The inclusion "$\supseteq$" is trivial. The opposite one is, by the DD-theorem 2.1:2 and Lemma 2.2:6, equivalent to the statement

$\cdot$ is a.u.-definable at $\overline{d}$ over $\emptyset$ in $\mathcal{A}$ $\Rightarrow$ $U = \{\overline{u}; tp(\overline{u}) = tp(\overline{d})\}$ does not contain $\overline{u}'$ and $\overline{u}''$ such that $u'_i \neq u''_i$, for $i = 0, 1$.

Suppose that $\cdot$ is a.u.-definable at $\overline{d}$ over $\emptyset$ in $\mathcal{A}$ by a formula φ and that it is $\overline{u}', \overline{u}'' \in U$. Then $U' = \{(\overline{u}, u_0 \cdot u_1); \overline{u} \in U\}$ is the set of all realizations of the type $tp(\overline{d}) \cup \{\varphi(\overline{x}, y)\}$. Therefore, by Lemma 2.2:5, $(\frac{\overline{u}'+\overline{u}''}{2}, \frac{u'_0 \cdot u'_1 + u''_0 \cdot u''_1}{2}) \in U'$, and hence $\frac{u'_0 \cdot u'_1 + u''_0 \cdot u''_1}{2} = \frac{u'_0 + u''_0}{2} \cdot \frac{u'_1 + u''_1}{2}$. This implies $u'_0 = u''_0$ or $u'_1 = u''_1$. $\square$

2.3 Meeting pairs of Peano products

Let $\mathcal{B}$ be a fixed saturated model of Presburger arithmetic, as in section 2.2. For $a \in B - \mathbb{N}$, we denote $E_a = \{a\} \times B$ the "slice" of B at a.

2.3.1 Meeting pair

Let $a \in B - \mathbb{N}$. A pair $(\cdot, \circ)$ of Peano products on $\mathcal{B}$ is called an *a-meeting pair* if it is $\cdot \restriction E_a = \circ \restriction E_a$, and $d_0 \cdot d_1 \neq d_0 \circ d_1$, $d'_0 \cdot d'_1 \neq d'_0 \circ d'_1$, for some $d_0, d_1 < a < d'_0, d'_1$. The following is an easy consequence of Proposition 2.2:1:

Corollary 2.3:1. *Let $a \in B - \mathbb{N}$, and $\cdot \in \mathsf{sPP}(\mathcal{B})$ be a saturated Peano product on $\mathcal{B}$. Then there is $\circ \in \mathsf{sPP}(\mathcal{B})$ such that $(\cdot, \circ)$ is an a-meeting pair of Peano products on $\mathcal{B}$. Moreover, $\circ$ can be chosen in such a way that $\cdot \cong_a \circ$.*

Proof. By Proposition 2.2:1, there are points $\overline{d}, \overline{d'} \notin \mathrm{icl}^{\cong_a}(E_a)$ with $\overline{d} < a < \overline{d'}$. Let $\bullet, \bullet'$ be witnesses for $\overline{d}, \overline{d'}$ respectively, i.e. $\bullet \cong_a \cdot \cong_a \bullet'$ coincide with $\cdot$ on E_a, but $d_0 \cdot d_1 \neq d_0 \bullet d_1$, $d'_0 \cdot d'_1 \neq d'_0 \bullet' d'_1$.

Suppose that neither $(\cdot, \bullet)$ nor $(\cdot, \bullet')$ is an a-meeting pair, then $(\bullet, \bullet')$ is one. Since $\bullet \cong_a \cdot$, via some g, we get $\bullet' \cong_a \circ$, via g (where $\circ = \bullet'^g$ is the "g-conjugate" of $\bullet'$; see section 2.1.2), and $(\cdot, \circ)$ is an a-meeting pair. □

Having a meeting pair $(\cdot, \circ)$, we construct a product $\times : B^2 \to B$, different from both $\cdot$ and $\circ$, such that $\langle \mathcal{B}, \times \rangle \models T$, where T is an extension of Robinson arithmetic Q by a set of induction axioms. This is stated as Proposition 2.3:2.

2.3.2 LB_x and LcB_x formulas

We denote LB_x [LcB_x] the set of formulas $\varphi(x, \overline{y})$ in the language of arithmetic $L^{ar} = \langle 0, S, +, \cdot, \leq \rangle$ such that every occurrence of multiplication in φ has the form $x \cdot z$ or $z \cdot x$, where z is a variable which is bound by a quantifier $Qz \leq x$ [$Qz \geq x$].

The L^{ar}-theory ILB [ILcB] is the extension of Robinson arithmetic Q by the scheme of induction $I(\mathrm{LB}_x)$ [$I(\mathrm{LcB}_x)$] for all formulas φ from LB_x [LcB_x] (here, x is the "induction variable").

Proposition 2.3:2. *Let $a \in B - \mathbb{N}$, and $(\cdot, \circ)$ be an a-meeting pair of Peano products on $\mathcal{B}$.*

1) For $\times = \cdot \restriction [0, a]^2 \cup \circ \restriction (B^2 - [0, a]^2)$, it is $\langle \mathcal{B}, \times \rangle \models$ ILB.

2) For $\times' = \cdot \restriction [a, \infty)^2 \cup \circ \restriction (B^2 - [a, \infty)^2)$, it is $\langle \mathcal{B}, \times' \rangle \models$ ILcB.

Proof. 1): Clearly, $\langle \mathcal{B}, \times \rangle \models$ Q. Let $\varphi(x, \overline{y}) \in \mathrm{LB}_x$. Then the following holds:

$$\langle \mathcal{B}, \times \rangle \models \varphi[b, \overline{c}] \quad \Leftrightarrow \quad \langle \mathcal{B}, \cdot \rangle \models \varphi[b, \overline{c}], \text{ for } b \leq a, \overline{c} \in B, \tag{2.2}$$
$$\langle \mathcal{B}, \times \rangle \models \varphi[b, \overline{c}] \quad \Leftrightarrow \quad \langle \mathcal{B}, \circ \rangle \models \varphi[b, \overline{c}], \text{ for } b \geq a, \overline{c} \in B. \tag{2.3}$$

We prove that the axiom of induction for φ holds in $\langle \mathcal{B}, \times \rangle$. Suppose that it is $\langle \mathcal{B}, \times \rangle \models \varphi[0, \overline{c}]$. Then, by (2.2) and by induction in $\langle \mathcal{B}, \cdot \rangle \models$ P, we get $\langle \mathcal{B}, \times \rangle \models \varphi[b, \overline{c}]$, for all $b \leq a$. Then, similarly, by (2.3) and by induction in $\langle \mathcal{B}, \circ \rangle \models$ P, we prove $\langle \mathcal{B}, \times \rangle \models \varphi[b, \overline{c}]$, for any $b \geq a$.
2) can be proven similarly. □

We ask the following, a bit vague, open question:

Open question 2. *Is it possible, by using similar methods, to construct Robinson products $\times$ which satisfy $I(\Gamma)$ for other sets $\Gamma \subseteq Fm_{L^{ar}}$? In particular, is it possible to construct Peano products this way?*

2.4 Peano interpolations

Let us remind that $\mathcal{B}$ stands for a fixed saturated model of Pr, and O denotes a fixed set of n-ary operations on B. In this section, we deal with a more subtle problem connected with dependency: Given points $(\bar{b}_i, d_i) \in B^{n+1}$, for $i \in I$, is there an operation $o \in O$ such that $o(\bar{b}_i) = d_i$, for all $i \in I$?

We are going to prove the following partial answer:

Proposition 2.4:1. *Let $o : B^n \to B$ satisfies*

$$o(\bar{b}) > \mathbb{N} \cdot \bar{b}, \text{ for all } \bar{b} > \mathbb{N}, \tag{2.4}$$

and $\mathbb{N} < \bar{b}, d \in B$ be such that

i) $d > \mathbb{N} \cdot \bar{b}$,

ii) $d \equiv o(\bar{b}) \mod n$, *for all* $0 < n \in \mathbb{N}$.

Then there is $o' \cong o$ such that $o'(\bar{b}) = d$.

Moreover, if $\bar{b} \equiv \bar{b'} \mod n \Rightarrow o(\bar{b}) \equiv o(\bar{b'}) \mod n$, for all $b \in B$ and $0 < n \in \mathbb{N}$, then the other implication holds as well.

Proof. Since $\mathcal{B}$ is saturated, it is enough to show that, for a formula $\varphi(\bar{x}, y)$, with $l(x) = n$, it is

$$\mathcal{B} \models \varphi[\bar{b}, d] \Rightarrow \mathcal{B} \models \varphi[\bar{b'}, o(\bar{b'})], \text{ for some } \bar{b'} \in B. \tag{2.5}$$

Indeed, in that case we can find an automorphism g of $\mathcal{B}$ (as in the proof of Lemma 2.1:1) such that $g(\bar{b'}) = \bar{b}$ and $g(o(\bar{b'})) = d$, for some $\bar{b'} \in B$. Then $o^g(\bar{b}) = d$.

We prove (2.5). By Corollary 1.4:2 1), we may suppose that φ is a conjunction of formulas $t = 0$, $t > 0$ and $n|t$, where t is of the form $\sum_i k_i x_i + ly + m$, with $k_i, l, m \in \mathbb{Z}$, and $0 < n \in \mathbb{N}$. Further, we work in $\mathcal{B}$.

Let φ be $t = 0$, and suppose $\varphi(\bar{b}, d)$. Then, by i), it is $l = 0$, and hence also $\varphi(\bar{b}, o(\bar{b}))$. Let φ be $t > 0$. If $\varphi(\bar{b}, d)$ holds then either $l > 0$, or $l = 0$. In both cases, we get $\varphi(\bar{b}, o(\bar{b}))$; in the first case, we use (2.4). Finally, let φ be $n|t$, and, again, suppose $\varphi(\bar{b}, d)$. Then $\varphi(\bar{b}, o(\bar{b}))$ holds, by ii).

The "moreover statement" is easy. $\square$

The following is an immediate consequence of Proposition 2.4:1.

Corollary 2.4:2. *Let $\mathbb{N} < b_0, b_1, d \in B$. There is a Peano product $\circ$ on $\mathcal{B}$ such that $b_0 \circ b_1 = d$ if and only if*

i) $d > \mathbb{N} \cdot b_i$, *for* $i < 2$,

ii) "$d \equiv b_0 \cdot b_1 \mod n$", *for all* $0 < n \in \mathbb{N}$.

(In ii), "$\cdots$" means the obvious additive equivalent of $\cdots$.)

Moreover, $\circ$ may be chosen to be isomorphic to any given Peano product $\cdot$.

Chapter 3

Quasi-Euclidean Subrings of $\mathbb{Q}[x]$[1]

We present an algebraic connection of the material introduced in the previous chapters.

We show that the rings D_τ from Example 1.3:1 b) are quasi-Euclidean subrings of $\mathbb{Q}[x]$ which are not k-stage Euclidean for any norm and positive integer k. These subrings can be either PID or non-UFD, depending on the choice of τ. In both cases, there are 2^ω such domains up to ring isomorphism. This solves the question of G. E. Cooke from [Coo76], where he asked whether there is an example of quasi-Euclidean domain, which is not 2-stage Euclidean.

The quasi-Euclidean property of the rings D_τ is proved in Theorem 3.4:2. The fact, that D_τ's are not k-stage Euclidean for any $0 < k \in \mathbb{N}$, is showed in Theorem 3.4:9.

This chapter stands aside the chapters 1 and 2 as an independent part, and the connections to the previous chapters are rather loose. In order to keep the material of this chapter completely self-contained, we do not presume anything from chapters 1 and 2. This includes also a change in notation: Domains D_τ from Example 1.3:1 b) are denoted R_τ in this chapter, as this fits better the conventions of algebraic texts.

3.1 Introduction

Although Euclidean and principal ideal domains have been intensively studied for almost a century, examples of non-Euclidean PIDs are still rather scattered throughout the literature, and thought of as more or less singular, non-frequent objects. The oldest of these examples are arguably the rings of integers of $\mathbb{Q}(\sqrt{d})$ for $d = -19, -43, -67, -163$. However, these are the only cases for negative d's,

[1]This chapter is joint work with Jan Šaroch, and is essentially identical to the paper [GŠ13]. The authors would like to thank Josef Mlček and Jan Trlifaj for reading parts of this text and giving several valuable comments.

and the results from [Wei73] and [Har04] indicate that it is almost surely the case of positive values of d, too.

Another type of examples was given by Samuel in his famous paper [Sam71]. Leutbecher (in [Leu78]) capitalized on his approach several years later, and proved that there are non-Euclidean PIDs which are even quasi-Euclidean (this was not the case of the four rings of integers mentioned above, as Cohn observed in [Coh66]).

Throughout this paper, by a *quasi-Euclidean domain*, we mean a commutative domain R for which there is a function $\phi : R^2 \to \omega$ such that, for all $(a, b) \in R^2$ with $b \neq 0$, there exists $q \in R$ with $\phi(b, a - bq) < \phi(a, b)$. The definition is similar to the one of classical Euclidean norm, with the important difference that by the norm function here, we do not measure elements of the ring but pairs of those. Also, ω can be equivalently replaced by some/any infinite ordinal in the definition; see Preliminaries section (in particular Proposition 3.2:1) for this and further equivalent definitions of quasi-Euclidean domain, and related concepts.

There are a few more published results on non-Euclidean PIDs. Unfortunately, they do not usually present a coherent class of these domains, or some sort of characterization of rings which are non-Euclidean PIDs in some distinguished class of domains. Nice attempts in this direction can be found in [And88] and [EH73].

In this text, we present a parametric construction which is in some sense a generalization of the approach used in [EH73]. We show that there are many discretely ordered non-Euclidean (even non-k-stage Euclidean in the sense of Cooke [Coo76]) subrings of $\mathbb{Q}[x]$ which are quasi-Euclidean. In fact, for each $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, where $\mathbb{J}_p$ denotes the ring of p-adic integers, we define one such subring. Moreover, we observe that the set $\prod_{p\in\mathbb{P}} \mathbb{J}_p$ splits into two parts of full cardinalities, depending on whether the resulting ring is PID or non-UFD. Since each quasi-Euclidean ring is Bézout (Proposition 3.2:1), there are no inbetween cases, i.e. non-PID and UFD at the same time.

3.2 Preliminaries

Throughout this chapter, all rings are (commutative integral) domains. Further, we denote by $\mathbb{P}$ the set of all primes in $\mathbb{N}$. For each $p \in \mathbb{P}$, $\mathbb{J}_p$ stands for the ring of p-adic integers, while $\mathbb{Z}_p$ denotes the field $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{J}_p \cong \varprojlim \mathbb{Z}_{p^k}$, we shall view $\mathbb{J}_p$ as a subring of $\prod_{k=1}^{\infty} \mathbb{Z}_{p^k}$, and denote, for a positive integer k, by π_k the canonical projection from $\mathbb{J}_p$ to $\mathbb{Z}_{p^k}$. It will not cause any confusion that the notation π_k does not reflect the prime p. Moreover, for technical reasons, we put $\pi_0 : \mathbb{J}_p \to \{0\}$; again, regardless of the prime p.

If we deal with elements from the ring $\mathbb{Q}[x]$, we define $\deg 0 = -1$, and we denote by $\operatorname{lc}(q)$ the leading coefficient of a polynomial q.

3.2.1 Quasi-Euclidean and k-stage Euclidean domains

Various generalizations of the concept of a Euclidean domain were proposed and studied in the past. The one we find very natural, is the concept of quasi-Euclidean (used in [Leu78] and [Bou80]) or the equivalent notion of ω-stage Euclidean domain (used by Cooke in [Coo76]).

Given a ring R and a partial order $\leq$ on R^2, we say that $\leq$ is *quasi-Euclidean* if it has the descending chain condition (dcc), and for any pair $(a,b) \in R^2$ with $b \neq 0$, there exists an element q in R such that $(b, a-bq) < (a,b)$. We call R *quasi-Euclidean* provided there exists a quasi-Euclidean partial order on R^2.

Let $(a,b) \in R^2$ and k be a non-negative integer. A *k-stage division chain* starting from the pair (a,b) is a sequence of equations in R

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k. \end{aligned}$$

Such a division chain is called *terminating* if the last remainder r_k is 0 (r_{k-1} is then easily seen to be the GCD of a and b). Notice that a k-stage division chain is determined by its starting pair and the sequence of quotients $q_1, \ldots, q_k$. For the sake of compactness, in what follows, we shall denote this chain also by

$$\left(\begin{array}{c|ccc} a & q_1 & \ldots & q_k \\ b & r_1 & \ldots & r_k \end{array} \right).$$

Given such a division chain, we define its 0-th remainder r_0 as b.

In the following proposition, On denotes the class of all ordinal numbers.

Proposition 3.2:1. ([Bou80], [Coo76], [Leu78]) *For a commutative domain R, the following conditions are equivalent:*

1. *There exists a function $\phi : R^2 \to On$ (with $Rng(\phi) \subseteq \omega$) such that, for all $(a,b) \in R^2$ with $b \neq 0$, there exists $q \in R$ such that $\phi(b, a-bq) < \phi(a,b)$.*

2. *R is quasi-Euclidean.*

3. *R is a Bézout domain, and the group $\mathrm{GL}_2(R)$ of regular 2×2 matrices over R is generated by matrices of elementary transformations.*

4. *Every pair $(a,b) \in R^2$ with $b \neq 0$ has a terminating k-stage division chain for some positive integer k.*

Proof. (1) $\Longrightarrow$ (2) is trivial, we just put $(a, b) < (a', b')$ if $\phi(a, b) < \phi(a', b')$.

(2) $\Longrightarrow$ (4) follows directly by the dcc.

The equivalence of (3) and (4) was proved already in [O'M64, 14.3].

(4) $\Longrightarrow$ (1): We put $\phi(a, 0) = 0$ for all $a \in R$. If $b \neq 0$, we define $\phi(a, b)$ as the minimal $k \in \omega$ for which the pair (a, b) has a terminating k-stage division chain. (So we even manage to find ϕ with the range in ω.) $\square$

Notice that no notion of a norm is involved in the definition of a quasi-Euclidean domain. However, given a norm N on R (i.e. a function $N : R \to \mathbb{N}$ with $N(a) = 0$ iff $a = 0$), we can measure how far N is from being Euclidean: as in [Coo76], for $0 < k \leq \omega$, we say that R is a *k-stage Euclidean domain with respect to* N provided that, for every $(a, b) \in R^2$ with $b \neq 0$, there exists a positive integer $l \leq k$ such that for some l-stage division chain starting from (a, b) it is $N(r_l) < N(b)$. As usual, we say that R is *k-stage Euclidean* if there exists such a norm N on R. So, in our notation, 1-stage Euclidean means Euclidean (in the classic sense). On the other hand, by Proposition 3.2:1, R is ω-stage Euclidean (with respect to some/any norm) if and only if it is quasi-Euclidean.

Finally, observe that a quasi-Euclidean domain, being Bézout, is UFD if and only if it is PID. An example of non-UFD 2-stage Euclidean domain was given already by Cooke in [Coo76], at the end of §1. It is at this place, where he admits that he does not know of any example of quasi-Euclidean domain which is not 2-stage Euclidean. Interestingly, all examples, we are going to construct, have got this property.

3.2.2 Peano arithmetic and weak saturation

Although our construction will be purely algebraic, we are going to give also a description derived from a nonstandard model of Peano arithmetic (PA). There are several reasons to do this: the description is very natural, only basic logical tools are needed, and it sheds more light at the entire situation.

Our models of PA are thought of as models in the language of arithmetic $L = (0, 1, +, \cdot, \leq)$. The fact that it is an extension of the language of rings will make it more convenient for us to work with. In particular, we can immediately say that any model of PA is a (discretely ordered) commutative semiring with 0 and 1.

We will say that $\mathcal{M} \models \text{PA}$ is *weakly saturated* if every 1-type in $\mathcal{M}$ without parameters is realized in $\mathcal{M}$, i.e. given any set $Y = \{\varphi_i(x) \mid i \in I\}$ of L-formulas with one free variable x, there is $m \in M$ such that $\mathcal{M} \models \varphi_i[m]$ for all $i \in I$, provided that, for each finite subset S of I, one has $\mathcal{M} \models (\exists x) \bigwedge_{i \in S} \varphi_i(x)$. Indeed, weakly saturated models of PA exist, we can even take an appropriate elementary extension of $\mathbb{N}$, however, as we shall see, for such a model $\mathcal{M}$, it is necessarily $|M| \geq 2^\omega$.

3.3 Examples

3.3.1 Logical description

Let us fix a weakly saturated model $\mathcal{M}$. Then, as mentioned above, $\mathcal{M}$ forms a commutative semiring. Formally adding negative elements, we turn $\mathcal{M}$ into a commutative domain containing $\mathbb{Z}$ as a subring. We will denote this domain $\mathcal{M}^{\pm}$. Notice that $\mathcal{M}^{\pm}$ shares several basic properties with $\mathbb{Z}$, namely it is a discretely ordered GCD domain; also for every q, r with $r \neq 0$, there exists $0 \leq t < |r|$ such that r divides $q + t$ (where $|\_|$ is the usual absolute value). However, unlike $\mathbb{Z}$, $\mathcal{M}^{\pm}$ is not Noetherian.

Let a be a nonstandard element of $\mathcal{M}$, i.e. $a \in M \setminus \mathbb{N}$. We define a subring R_a of $\mathcal{M}^{\pm}$ in the following way:

$$R_a = \{m \in M^{\pm} \mid (\exists n \in \mathbb{N})(\exists h \in \mathbb{Z}[x])\, n \neq 0 \;\&\; n \cdot m = h(a)\}.$$

It is easily seen that R_a is a ring. It can be naturally approached if we, in the first step, take a subring of $\mathcal{M}^{\pm}$ generated by a (which is nothing else than $\mathbb{Z}[a] \cong \mathbb{Z}[x]$), and then allow division by nonzero integers in case it is possible in $\mathcal{M}^{\pm}$. We immediately observe that R_a is isomorphic to

$$R'_a = \left\{ \frac{h}{n} \in \mathbb{Q}[x] \;\middle|\; n \in \mathbb{N} \setminus \{0\}, h \in \mathbb{Z}[x], \text{ and } n \,|\, h(a) \text{ in } \mathcal{M}^{\pm} \right\}.$$

Remark 3.3:1.

1. Regardless of a, we have $R'_a \cap \mathbb{Q} = \mathbb{Z}$.

2. Notice that $R_a = R_{a+1}$ (for any nonstandard $a \in M$) but $R'_a \neq R'_{a+1}$ since precisely one of these two rings contains $x/2$. On the other hand, as we shall see later, it is possible that we have nonstandard $a, b \in M$ such that $R_a \neq R_b$ but $R'_a = R'_b$.

3. For our considerations, we do not need the full strength of PA. In fact, instead of binary multiplication, it is enough to have an endomorphism $a\cdot$ of the monoid $(M, +, 0)$ such that $a \cdot 1 \notin \mathbb{N}$, and the induction for all formulas in the language $(0, 1, +, a\cdot, \leq)$; so the resulting theory can be viewed as an extension of Presburger arithmetic rather than weakening of PA (see the theory LA from 1.1.4.1).

3.3.2 Algebraic description

As we have seen above, the definitions of R_a and R'_a rely on the fixed model $\mathcal{M}$ of PA. However, there is only a little amount of information about $a \in M$ that we actually need. This makes it possible—as we are going to demonstrate—to manage without refering to any Peano model. For $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$, we define a subring R_τ of $\mathbb{Q}[x]$.

$$R_\tau = \left\{ \frac{h}{n} \in \mathbb{Q}[x] \;\middle|\; n \in \mathbb{N} \setminus \{0\}, h \in \mathbb{Z}[x], \text{ and } (\forall p \in \mathbb{P})\, \pi_{\mathrm{v}_p(n)}(h(\tau_p)) = 0 \right\}.$$

Here, v_p denotes the usual p-valuation. Further, τ_p is the pth projection of τ, and the substitution $h(\tau_p)$ is done inside $\mathbb{J}_p$ where $\mathbb{Z}$ is canonically embedded via $z \mapsto (z \bmod p, z \bmod p^2, z \bmod p^3, \dots)$. We will use this substitution several times in the next section.

It follows easily from the definition that $\sigma \neq \tau$ implies $R_\sigma \neq R_\tau$. The correspondence between the rings R'_a and R_τ is made precise by Proposition 3.3:2.

Proposition 3.3:2. *Let $\mathcal{M}$ be a weakly saturated model of PA. Then:*

1. *For each nonstandard $a \in M$ there exists precisely one $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$ such that $R'_a = R_\tau$.*

2. *For each $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$ there is at least one nonstandard $a \in M$ such that $R'_a = R_\tau$.*

Proof. (1) There is even a ring homomorphism $\psi : \mathcal{M}^\pm \to \prod_{p\in\mathbb{P}} \mathbb{J}_p$ which assigns to $m \in M^\pm$ an element τ such that $\tau_p = (m \bmod p, m \bmod p^2, m \bmod p^3, \dots)$ for each $p \in \mathbb{P}$. It is a matter of straightforward verification that $R'_a = R_{\psi(a)}$ for any nonstandard $a \in M$.

(2) Let us consider the set Y consisting of all congruences $x \equiv_{p^k} \tau_p(k)$ and inequalities $x > k$, where $k \in \mathbb{N} \setminus \{0\}$ and $p \in \mathbb{P}$. Then Y is a 1-type in $\mathcal{M}$ (without parameters—positive integers are just constant terms in the language L) since any finite subset of Y has a solution in $\mathbb{N} \subset M$ by Chinese Remainder Theorem. So there is a global solution, $a \in M$, of all congruences and inequalities from Y, using the weak saturation of $\mathcal{M}$. (Now, it is clear that $|M| \geq 2^\omega$.) The inequalities assure that a is nonstandard, and checking the definitions, we immediately see that $R'_a = R_\tau$. $\square$

In the following section, we will freely use the fact (implicitly proved above) that, for every τ, the ring R_τ inherits the discrete ordering from $\mathcal{M}^\pm$ via isomorphism with R_a for some/any a.

3.4 Properties of the examples

3.4.1 Terminating division chains

We are going to show that, for every τ, the ring R_τ is quasi-Euclidean. So let τ be fixed for a while, put $R = R_\tau$, and let us denote by R^+ the subsemiring of R

consisting of polynomials with nonnegative leading coefficients. First, we prove the following auxiliary result.

Lemma 3.4:1. *Let $q, r \in R^+$ with $r \neq 0$, then there are (unique) $p, s \in R^+$ such that $q = pr + s$ and $s < r$.*

Moreover: Let $\tilde{p}, \tilde{s} \in \mathbb{Q}[x]$ be such that $q = \tilde{p}r + \tilde{s}$ and $\deg \tilde{s} < \deg r$. Further let $\tilde{p} = p'/m$ where $p' \in \mathbb{Z}[x]$, $m \in \mathbb{N} \setminus \{0\}$ and $0 \leq k < m$ such that $(p' - k)/m \in R^+$. Then the pair (p, s) satisfies

$$(p, s) = \begin{cases} (\tilde{p} - 1, \tilde{s} + r) & \text{for } k = 0 \ \& \ \mathrm{lc}(\tilde{s}) < 0, \\ \left(\frac{p' - k}{m}, \tilde{s} + \frac{k}{m} r\right) & \text{otherwise.} \end{cases}$$

Proof. Straightforward verification. □

If we look at R_a (for a with $R'_a = R$), there is only one pair (p, s) in the model $\mathcal{M}$ satisfying the properties from Lemma 3.4:1, namely the pair $(q \text{ div } r, q \text{ mod } r)$. Here, div stands for the binary operation of integer division. Thus in particular, we have that R^+ as a subsemiring of $\mathcal{M}$ is closed under binary operations div and mod.

Consequently, we say that a division chain $\left(\begin{array}{c|ccc} r_{-1} & q_1 & \dots & q_n \\ r_0 & r_1 & \dots & r_n \end{array} \right)$ in R^+ with $r_{-1}, r_0 > 0$ is *quasi-Euclidean* if $q_{i+1} = r_{i-1} \text{ div } r_i$ and $r_{i+1} = r_{i-1} \text{ mod } r_i$, for $i \geq 0$. A consequence of the proof of the following theorem is that, for any nonzero $a, b \in R^+$, there exists a positive integer n such that the quasi-Euclidean chain of length n starting from the pair (a, b) is terminating.

Theorem 3.4:2. *R is a quasi-Euclidean domain . In particular, it is Bézout.*

Proof. We will show that the condition (1) from Proposition 3.2:1 is satisfied. For this sake, we define $\phi : R^2 \to (2 \times \mathbb{N}^4, lex)$ by the formula $\phi(q, r) = (0, 0, 0, 0, 0)$ for $r = 0$, and

$$\phi(q, r) = (\delta_{q,r}, \deg q + 1, \deg r, n_{q,r}, n_{q,r} \cdot |\mathrm{lc}(q)|)$$

otherwise. Here, $\delta_{q,r}$ is 1 if $|q| \leq |r|$, and 0 otherwise; $n_{q,r} \in \mathbb{N}$ denotes the least common denominator of q, r. In the rest of the proof, we assume that $q > r > 0$. The other cases follow easily. (Notice that $\phi(q, r) = \phi(|q|, |r|)$.)

Since $\mathbb{Q}[x]$ is a Euclidean ring with the norm $\deg(-) + 1$, there are $\tilde{p}, \tilde{s} \in \mathbb{Q}[x]$ such that $q = \tilde{p}r + \tilde{s}$ and $\deg \tilde{s} < \deg r$. By Lemma 3.4:1, we get $p, s \in R^+$ satisfying $s < r$ and $q = pr + s$.

Suppose $s \neq 0$. We need to show that $\phi(r, s) < \phi(q, r)$ in the lexicographic order of $2 \times \mathbb{N}^4$. Since $0 < s < r$, we have $\delta_{r,s} = 0 = \delta_{q,r}$. We may assume $\deg q = \deg r = \deg s$ (otherwise, we are done immediately). Then $p \in \mathbb{N}$. Further, we have $q, r \in \frac{\mathbb{Z}[x]}{n_{q,r}}$, and hence $s = q - pr \in \frac{\mathbb{Z}[x]}{n_{q,r}}$. Therefore $n_{r,s} \leq n_{q,r}$. Moreover, from $r < q$, we have $\mathrm{lc}(r) \leq \mathrm{lc}(q)$.

Assume $n_{r,s} = n_{q,r}$ and $\mathrm{lc}(r) = \mathrm{lc}(q)$. Then, from the definition of $\tilde{p}$, we have $\tilde{p} = 1$, and thus $p' = 1 = m$, $k = 0$ in Lemma 3.4:1. The first case in the definition of (p, s) leads to a contradiction, since we get $p = 0$ (and so $q = s < r$). So it must be that $p = \tilde{p} = 1$ and $s = \tilde{s}$. In particular, we see that $\deg s = \deg \tilde{s} < \deg r$ which also contradicts one of our assumptions.

Finally, R is Bézout by Proposition 3.2:1. $\square$

3.4.2 Separating the PID cases

In the following few paragraphs, we distinguish the choices of τ which imply that R_τ is a PID. We also show that there are 2^ω pairwise nonisomorphic domains among the rings R_τ which are PID, and the same cardinality of those which are not PID. The next lemma will be useful.

Lemma 3.4:3. *Let $\tau \in \prod_{p\in\mathbb{P}} \mathbb{J}_p$. Then R_τ is a PID if and only if, for each nonzero $h \in \mathbb{Z}[x]$, the set $S_h = \{(p, k) \in \mathbb{P} \times (\mathbb{N} \setminus \{0\}) \mid \pi_k(h(\tau_p)) = 0\}$ is finite.*

Proof. Assume that S_h is infinite for some nonzero $h \in \mathbb{Z}[x]$. Then either the set $\{p \in \mathbb{P} \mid h/p \in R_\tau\}$ is infinite, or there exists a prime p such that $h/p^k \in R_\tau$ for any $k \in \mathbb{N}$. In the first case, we fix an enumeration $\{p_1, p_2, p_3, \dots\}$ of that set, and—using the definition of R_τ—we see that $(h/p_1, h/(p_1p_2), h/(p_1p_2p_3), \dots)$ is an infinite descending (with respect to divisibility) sequence of elements in R_τ; thus R_τ is not a UFD. In the second case, we use the same argument for the sequence $(h/p, h/p^2, h/p^3, \dots)$.

If R_τ is not a PID, then (since it is Bézout by Theorem 3.4:2) there has to be an infinite sequence of elements in R_τ descending in divisibility $(h_1/n_1, h_2/n_2, \dots)$; here $h_i \in \mathbb{Z}[x]$ and n_i are positive integers coprime with h_i in $\mathbb{Z}[x]$, for all $i > 0$. The polynomials h_i will eventually have the same degree ($\mathbb{Q}[x]$ is Euclidean) and absolute value of the leading coefficient ($\mathbb{Z}$ is Noetherian), and so we may w.l.o.g. assume that all the polynomials h_i are equal to a single nonzero $h \in \mathbb{Z}[x]$. It directly follows that, for this h, the set S_h is infinite. $\square$

Let us take a representative subset J of $\prod_{p\in\mathbb{P}} \mathbb{J}_p$ in the sense that, for each ρ, there is a $\tau \in J$ such that $R_\tau \cong R_\rho$, and for all $\tau, \sigma \in J$, $\tau \neq \sigma$, we have $R_\tau \ncong R_\sigma$. Then J is a disjoint union of the sets A and B, where $A = \{\tau \in J \mid R_\tau \text{ is a PID}\}$ and $B = \{\tau \in J \mid R_\tau \text{ is not a UFD}\}$.

Proposition 3.4:4. $|A| = |B| = 2^\omega$.

Proof. Let us assume that $|A| < 2^\omega$. For each $p \in \mathbb{P}$, we define $\tau_p \in \mathbb{J}_p$ in such a way that:

1. $\pi_1(\tau_p) = \lfloor \log p \rfloor$,
2. $n \cdot \tau_p \notin \{h(\sigma_p) \mid \sigma \in A \;\&\; h \in \mathbb{Z}[x]\}$, for every positive integer n,
3. τ_p is not a root in $\mathbb{J}_p$ of a nonzero polynomial from $\mathbb{Z}[x]$.

This is clearly possible since the first two conditions are satisfied by 2^ω different elements of $\mathbb{J}_p$. Let $\tau = \prod_{p\in\mathbb{P}} \tau_p$. We claim that R_τ is a PID which leads immediately to a contradiction (by (2), there cannot be $\sigma \in A$ with $R_\tau \cong R_\sigma$).

To prove this, we use Lemma 3.4:3. Let us fix a nonzero $h \in \mathbb{Z}[x]$. Then, using the limit comparison of h and log, we deduce that, for all sufficiently large primes p, we have $0 < |h(\lfloor \log p \rfloor)| < p$ which further implies $\pi_1(h(\tau_p)) \neq 0$. Together with the condition (3), we get that S_h is finite. This finishes the proof that $|A| = 2^\omega$.

To see that $|B| = 2^\omega$, it is enough to fix a $\sigma \in A$, and for each nonzero subset P of $\mathbb{P}$ define $\tau^P \in B$ by setting $\tau^P_p = (0,0,0,\dots)$ for $p \in P$, and $\tau^P_p = \sigma_p$ otherwise. $\square$

3.4.3 Keeping distance from Euclidean domains

Here, we prove that no R_τ is a k-stage Euclidean domain, whatever positive integer k we take. From now on, we work in a fixed ring R_τ. We start with two slightly technical lemmas [2].

Lemma 3.4:5. *Let* $Q = \left(\begin{array}{c|ccc} a & q_1 & \dots & q_k \\ b & r_1 & \dots & r_k \end{array}\right)$ *be a division chain starting from* (a,b) *with* $a,b,k > 0$. *There is a division chain* $Q' = \left(\begin{array}{c|ccc} a & q'_1 & \dots & q'_l \\ b & r'_1 & \dots & r'_l \end{array}\right)$ *with* $q'_i > 0$ *for* $i > 1$ *such that* $|r_k| = |r'_l|$ *and* $l \leq 2k-1$.

Proof. Denote T_1, T_2 the following two transformations on the set of all division chains starting from (a,b):

$$T_1 : \left(\begin{array}{c|ccc} a & q_1 & \dots & q_k \\ b & r_1 & \dots & r_k \end{array}\right) \mapsto$$

$$\left(\begin{array}{c|cccccccc} a & q_1 & \dots & q_{i-1} & q_i - 1 & 1 & -(q_{i+1}+1) & -q_{i+2} & \dots & -q_k \\ b & r_1 & \dots & r_{i-1} & r_i + r_{i-1} & -r_i & (-1)^2 r_{i+1} & (-1)^3 r_{i+2} & \dots & \pm r_k \end{array}\right)$$

where i is the first index such that $q_{i+1} < 0$ (T_1 is identity if there is no such i) and $\pm$ stands for $(-1)^{k-i+1}$;

$$T_2 : \left(\begin{array}{c|ccc} a & q_1 & \dots & q_k \\ b & r_1 & \dots & r_k \end{array}\right) \mapsto \left(\begin{array}{c|cccccc} a & q_1 & \dots & q_{i-1} & q_i + q_{i+2} & q_{i+3} & \dots & q_k \\ b & r_1 & \dots & r_{i-1} & r_{i+2} & r_{i+3} & \dots & r_k \end{array}\right)$$

where i is the first index such that $q_{i+1} = 0$ (T_2 is identity if there is no such i).

We will show a little bit more than stated; instead of $l \leq 2k-1$, we prove even that $l \leq k + n$ where $n = \max\{k - i + 1; i > 1 \,\&\, q_i < 0\}$ ($n = 0$ if there is no

[2] Lemma 3.4:5 is a modified version of a classical result on continued fractions by Perron (see [Per13, §37]).

such i). Put $Q = \left(\begin{array}{c|ccc} a & q_1 & \dots & q_k \\ b & r_1 & \dots & r_k \end{array}\right)$ and denote the corresponding pair (n,k) as $p_Q = (n_Q, k_Q)$. We prove the statement by induction on the pairs (n_Q, k_Q) with lexicographic ordering. The case $p_Q = (0,1)$ is trivial.

If there is i such that $q_{i+1} = 0$, we get $p_{T_2(Q)} \leq_{lex} (n_Q, k_Q - 2)$, and the induction assumption gives some Q'. It is easy to verify that this Q' meets all the requirements. (Note that in the case $i+1 = k$ we get $T_2(Q) = \left(\begin{array}{c|ccc} a & q_1 & \dots & q_{i-1} \\ b & r_1 & \dots & r_{i-1} \end{array}\right)$ and $r_{i-1} = r_{i+1}$.)

Otherwise, we have $q_i \neq 0$ whenever $i > 1$, and using T_1 we get

$$p_{T_1(Q)} \leq_{lex} (n_Q - 1, k_Q + 1).$$

Again, the Q' given by the induction assumption is what we wanted. □

Lemma 3.4:6. *Let* $\left(\begin{array}{c|ccc} a & q_1 & \dots & q_k \\ b & r_1 & \dots & r_k \end{array}\right)$ *be a division chain starting from* (a,b) *such that* $a, b, q_i > 0$ *for* $i > 1$, *and let* $\left(\begin{array}{c|ccc} a & e_1 & \dots & e_m \\ b & f_1 & \dots & 0 \end{array}\right)$ *be the quasi-Euclidean division chain in* R_τ *starting from* (a,b). *Assume* $m \geq k$.

Then $|r_k| \geq f_{k+1}$, *and in particular* $\deg(r_k) \geq \deg(f_{k+1})$ *(we put* $f_{k+1} = 0$ *if* $m = k$*).*

Proof. Take the least l such that $q_l \neq e_l$ (if there is no such, we are done since (f_i) is decreasing). By an inductive argument, it is easy to observe that the following holds (recall that we put $f_0 = r_0 = b$):

$$\text{If } q_l < e_l \text{ then } \begin{cases} r_{l+2i} \geq r_{l-1} \text{ for } i \geq 0, \\ r_{l+2i+1} \leq -r_{l-1} \text{ for } i \geq 1, \\ r_{l+1} \leq -r_{l-1} \text{ or } r_{l+1} = -f_l; \end{cases}$$

$$\text{and if } q_l > e_l \text{ then } \begin{cases} r_{l+2i} < -r_{l-1} \text{ for } i \geq 1, \\ r_{l+2i+1} > r_{l-1} \text{ for } i \geq 0, \\ r_l \leq -r_{l-1} \text{ or } (m > k \;\&\; r_l \leq -f_{l+1}). \end{cases}$$

The statement follows since $r_{l-1} = f_{l-1}$ and (f_i) is decreasing. □

Combining both lemmas together, we obtain the following corollary which gives us a bound on the speed of decrease of remainders in a division chain, compared to the quasi-Euclidean one. By letting a, b be any two consecutive Fibonacci numbers, one can see that the bound is optimal.

Corollary 3.4:7. *Given* $a, b > 0$, *let* $\left(\begin{array}{c|ccc} a & e_1 & \dots & e_n \\ b & f_1 & \dots & 0 \end{array}\right)$ *be the quasi-Euclidean division chain starting from* (a,b), *and* $\left(\begin{array}{c|ccc} a & q_1 & \dots & q_k \\ b & r_1 & \dots & r_k \end{array}\right)$ *be an arbitrary division chain. Then, for* $l \leq \min(k, n/2)$, *we have* $|r_l| \geq f_{2l}$.

Now, we have all the tools for proving that no R_τ is k-stage Euclidean domain, independently of the choice of $k > 0$. For the sake of better readability, we state the key step of the proof as a separate lemma.

Lemma 3.4:8. *Let k be a positive integer and $0 < b \in R_\tau$ such that $\deg(b) \geq 1$. Then there is $0 < a \in R_\tau$ such that every division chain $\left(\begin{array}{c|ccc} a & q_1 & \dots & q_l \\ b & r_1 & \dots & r_l \end{array}\right)$ of length $l \leq k$ starting from (a, b) satisfies $\deg(r_l) \geq \deg(b)$.*

Proof. By Corollary 3.4:7, it is enough to prove the statement for the quasi-Euclidean division chain instead of an arbitrary one.

Set $a = \frac{c}{d}(b - \beta)$ where $c, d \in \mathbb{N}$ are such that no division chain in $\mathbb{Z}$ of length $l \leq k$ starting from (c, d) is terminating (such c, d exist since Corollary 3.4:7 holds also in $\mathbb{Z}$) and $0 \leq \beta < d$ is such that $d|(b - \beta)$ in R_τ.

For a contradiction, let the quasi-Euclidean division chain

$$\left(\begin{array}{c|ccc} a & e_1 & \dots & e_l \\ b & f_1 & \dots & f_l \end{array}\right)$$

starting from (a, b) satisfy $\deg(f_l) < \deg(b)$. We may w.l.o.g. assume $\deg(f_{l-1}) = \deg(b)$; then we have $e_i \in \mathbb{Z}$ for all $i = 1, 2, \dots, l$.

Define the operation $\hat{}: R_\tau \to \mathbb{Q}$ as $\hat{r} = \mathrm{lc}(dr)/\mathrm{lc}(b)$. Easily $\hat{a}, \hat{b} \in \mathbb{Z}$, and therefore also $\hat{f}_i \in \mathbb{Z}$, for all $i \neq l$. Hence,

$$\left(\begin{array}{c|cccc} \hat{a} & e_1 & \dots & e_{l-1} & e_l \\ \hat{b} & \hat{f}_1 & \dots & \hat{f}_{l-1} & 0 \end{array}\right)$$

is a division chain in $\mathbb{Z}$ starting from $(\hat{a}, \hat{b}) = (c, d)$, a contradiction. $\square$

Theorem 3.4:9. *Let $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$ be arbitrary. Then the ring R_τ is not k-stage Euclidean for any positive integer k.*

Proof. Assume the contrary and let N be a norm such that R_τ is k-stage Euclidean with respect to N. To get a contradiction, we construct an infinite sequence $(b_0, b_1, \dots)$ of elements from R_τ with $N(b_i) > N(b_{i+1})$ and such that $\deg b_{i+1} \geq \deg b_i \geq 1$, for all $i \in \mathbb{N}$.

As the first step, put $b_0 = x \in R_\tau$. Now assume we have defined b_i for all $i \leq j \in \mathbb{N}$. Suppose $b_j > 0$. For b_j we find some a_j using Lemma 3.4:8. By the k-stage Euclidean property, there is an l-stage division chain $\left(\begin{array}{c|ccc} a_j & q_1 & \dots & q_l \\ b_j & r_1 & \dots & r_l \end{array}\right)$ with $l \leq k$ starting from the pair (a_j, b_j) such that $N(r_l) < N(b_j)$. So we can set $b_{j+1} = r_l$. By Lemma 3.4:8, we know that $\deg b_{j+1} \geq \deg b_j \geq 1$.

The case $b_j < 0$ is similar. For $-b_j$ find $-a_j$ by Lemma 3.4:8, take a division chain $\left(\begin{array}{c|ccc} a_j & q_1 & \dots & q_l \\ b_j & r_1 & \dots & r_l \end{array}\right)$ with $N(r_l) < N(b_j)$ and set $b_{j+1} = r_l$. If it were

$\deg r_l < \deg b_j$, we would have the division chain $\left(\begin{array}{c|ccc} -a_j & q_1 & \dots & q_l \\ -b_j & -r_1 & \dots & -r_l \end{array}\right)$ with $\deg -r_l < \deg -b_j$, contradicting the choice of $-a_j$. $\square$

We conclude this chapter by the following

Open question 3. *Is there an example of a k-stage Euclidean domain which is not $(k-1)$-stage Euclidean, for $k > 2$?*

Bibliography

[And88] D. D. Anderson, *An existence theorem for non-Euclidean PID's*, Communications in Algebra **16** (1988), no. 6, 1221–1229.

[Bau76] W. Baur, *Elimination of quantifiers for modules*, Israel Journal of Mathematics **25** (1976), 64–70.

[Bès01] A. Bès, *A survey of arithmetical definability*, Bulletin of the Belgian Mathematical Society – Simon Stevin (2001), 1–54, suppl.

[Bou80] B. Bougaut, *Algorithme explicite pour la recherche du P.G.C.D. dans certain anneaux principaux d'entiers de corps de nombres*, Theoretical Computer Science **11** (1980), 207–220.

[Coh66] P. M. Cohn, *On the structure of the* GL_2 *of a ring*, Publications mathématiques de l'I.H.É.S. **30** (1966), 5–53.

[Coo76] G. E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory. I*, Journal für die reine und angewandte Mathematik **282** (1976), 133–156.

[EH73] P. Eakin and W. Heinzer, *More noneuclidean PID's and Dedekind domains with prescribed class group*, Proceedings of the American Mathematical Society **40** (1973), 66–68.

[Gli09] P. Glivický, *Modely aritmetických a bohatých teorií*, Master's thesis, Faculty of Mathematics and Physics, Charles University in Prague, 2009, in Czech.

[Göd31] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik **38** (1931), 173–198.

[GŠ13] P. Glivický and J. Šaroch, *Quasi-euclidean subrings of* $\mathbb{Q}[x]$, Communications in Algebra **41** (2013), to appear, most likely in issue 8.

[Har04] M. Harper, $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Canadian Journal of Mathematics **56** (2004), 55–70.

[KP82] L. Kirby and J. Paris, *Accessible independence results for Peano arithmetic*, Bulletin of the London Mathematical Society **14** (1982), 285–293.

[Leu78] A. Leutbecher, *Euklidisher Algoritmus und die Gruppe GL_2*, Mathematische Annalen **231** (1978), 269–285.

[Mon75] L. Monk, *Elementary-recursive decision procedures*, Ph.D. thesis, University of California, Berkeley, 1975.

[MS61] R. MacDowell and E. Specker, *Modelle der Arithmetik*, Infinistic Methods. Proceedings of the Symposium on Foundations of Mathematics, Warsaw, 2-9 September 1959 (Oxford), Pergamon, 1961, pp. 257–263.

[O'M64] O. T. O'Meara, *On the finite generation of linear groups over Hasse domains*, Journal für die reine und angewandte Mathematik **217** (1964), 79–128.

[Par78] J. Paris, *Some independence results for Peano arithmetic*, Journal of Symbolic Logic **43** (1978), no. 4, 725–731.

[Per13] O. Perron, *Die Lehre von den Kettenbrüchen*, B. G. Teubner, Leipzig und Berlin, 1913.

[PH77] J. Paris and L. Harrington, *A mathematical incompleteness in Peano arithmetic*, Handbook of Mathematical Logic, Studies in Logic and the Foundations of Mathematics, North-Holland P. C., 1977, pp. 1133–1142.

[PJ91] M. Presburger and D. Jabcquette, *On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation*, History and Philosophy of Logic **12** (1991), no. 2, 225–233.

[Pre29] M. Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes Rendus du 1er congrès de Mathématiciens des Pays Slaves (1929), 92–101, English translation [PJ91].

[Sam71] P. Samuel, *About Euclidean rings*, Journal of Algebra **19** (1971), 282–301.

[Sem84] A. L. Semënov, *Logical theories of one-place functions on the set of natural numbers*, Mathematics of the USSR-Izvestiya **22** (1984), no. 3, 587–618.

[Sko33] Th. Skolem, *Über die Unmöglichkeit einer vollständigen Charakterisierung der Zahlenreihe mittels eines endlichen Axiomensystems*, Norsk Matematisk Forenings Skrifter **10** (1933), 73–82.

[Sko34] ______, *Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzhlbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen*, Fundamenta Mathematicae **23** (1934), 150–161.

[Ten59] S. Tennenbaum, *Non-archimedean models for arithmetic*, Notices of the American Mathematical Society **6** (1959), 270.

[vdDH92] L. van den Dries and J. Holly, *Quantifier elimination for modules with scalar variables*, Annals of Pure and Applied Logic **57** (1992), 161–179.

[Wei73] P. Weinberger, *Euclidean rings of algebraic numbers*, Proceedings of Symposia in Pure Mathematics **24** (1973), 321–332.

[Wei97] V. Weispfenning, *Complexity and uniformity of elimination in Presburger arithmetic*, Universität Passau, ACM Press, 1997, pp. 48–53.

Index

Index of Symbols