Master's Thesis

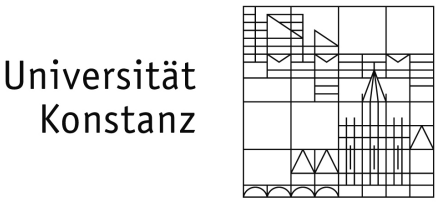
on the topic

Quantifier Elimination Tests and Examples

by

Magdalena Forstner

at



Fachbereich Mathematik und Statistik

supervised by

Dr. Panteleimon Eleftheriou

second corrector

Prof. Dr. Salma Kuhlmann

Konstanz, 2017

Acknowledgements

Foremost, I would like to express my sincere gratitude to my supervisor Pantelis Eleftheriou for the continuous support, for his patience, motivation, and for his most helpful comments. His guidance helped me in all the time of research and writing of this thesis.

A special thanks goes out to Deirdre Haskell for an interesting and motivating conversation, as well as for her helpful recommendations on Section 6.1 of this thesis.

Further, I owe my deep gratitude to Chris Miller for his highly valuable answers to my questions in reference to Section 7.3.

Last but not least, I would like to thank my proofreaders and my loved ones for their unconditional encouragement. I was continually amazed by their willingness to spend so much time and effort supporting me to finish this thesis.

Thank you to all of you!

Contents

1 Introduction **1**

2 Model Theoretical Background **3**

3 Basic Quantifier Elimination Criteria **11**
3.1 First Approach to Quantifier Elimination 11
3.2 Algebraically Closed Fields 15
3.3 Real Closed Fields 17

4 Quantifier Elimination by Algebraically Prime Models **23**
4.1 Algebraically Prime Models and Simple Closedness 23
4.2 Presburger Arithmetic 24

5 Quantifier Elimination by Types and Saturation **31**
5.1 Types and Saturated Models 31
5.2 Differentially Closed Fields 35

6 Quantifier Elimination by Lou van den Dries **43**
6.1 Extensions of Partial Embeddings 43
6.2 The Field of Reals with a Predicate for the Powers of Two 46

7 Applications **59**
7.1 One Geometric Consequence 59
7.2 Completeness and Decidability 60
7.3 Definable Sets 62

Bibliography **65**

1 Introduction

In 1927 and 1928 Alfred Tarski was in charge of the seminar on problems in logic at the University of Warsaw. He used this seminar to pursue a development of the method of quantifier elimination. A theory is said to admit quantifier elimination if every formula is equivalent, in all models of the theory, to a formula without any quantifiers. The term itself is due to Tarski as well as the following statement about it:

> *"It seems to us that the elimination of quantifiers, whenever it is applicable to a theory, provides us with direct and clear insight into both the syntactical structure and the semantical content of that theory—indeed, a more direct and clearer insight than the modern more powerful methods [...]."* [DoMoTa]

Indeed, quantifier elimination is a powerful method for a model theoretic investigation of algebraic structures. It helps not only in the questions of completeness and decidability but also for a better understanding of definable sets and the algebraic structure itself, since these studies are often made rather complicated by quantifiers.

Under his guidance, Tarski and his students at the Warsaw seminar achieved significant results. Tarski suggested to one of his students—his name was Mojzesz Presburger—to develop an elimination-of-quantifiers procedure for the additive theory of the integer numbers. The student succeded and submitted the result as his thesis for a master's degree. The theory became known as Presburger Arithmetic and will be subject in this present thesis as well.

Tarksi was able to apply the method of quantifier elimination to the ordered field of real numbers. In both of these cases, the method yielded a decision algorithm, that is an algorithm which decides whether a given sentence is true or false.

There are some equivalent formulations of quantifier elimination as well as many sufficient conditions that imply quantifier elimination. Such conditions are called quantifier elimination tests. One of the two general aims of this thesis at hand is to prove a few well-known tests and apply them afterwards to some theories. The second aim is to provide a proof of a particular quantifier elimination test that was introduced in 1985 by Lou van den Dries, but so far, no clear proof has been published. Lou van den Dries is a Dutch mathematician who has successfully been applying model theoretical methods to the field of real numbers, highly improving the understanding of the reals. He also laid the foundation to the concept of o-minimality which has since become a recognized branch within model theory. Information concerning his work can be found in [UoI]. We will meet the concept of o-minimality again in Theorem 7.10. In most of the tests that we are going to discuss in this thesis, one needs to show the existence of some specified element. The quantifier elimination test that van den Dries gave in [vdD] differs from other tests

as one is rather free in the choice of a particular element. This will become clear once we apply the test to the theory of the field of reals with a predicate for the powers of two.

This shall be enough of history and on the significance of quantifier elimination. Let us give a brief outline of the present thesis.

In the following Chapter 2 we will review some basic notation from mathematical logic and recall some fundamental model theory which is going to be used in later chapters. At the end of Chapter 2 we will give a formal definition of quantifier elimination.

In Chapter 3 we will provide a simple, yet useful quantifier elimination test which we will then apply to the theory of algebraically closed fields and to the theory of real closed fields. For the latter we first develop some theory on real closed fields, whereas for algebraically closed fields we assume the reader to be already familiar with the topic.

Chapter 4 starts with the notion of algebraically prime models and simple closedness. The quantifier elimination test in this chapter follows very quickly. As already promised, we will then deal with Presburger Arithmetic. All results on this theory given here are due to Presburger, although the specific proof of quantifier elimination given in Section 4.2 is due to van den Dries.

In Chapter 5 we introduce types and saturated models. This is a large realm of model theory itself. We only provide the theory that we need for another quantifier elimination test. It follows some background on differential fields. Differential algebra is the study of algebraic structures equipped with a derivation. Model theory has proven quite useful in this area as the definition of differential closure is surprisingly more complex than the analogous notions of algebraic closure or real closure, see [Sac72a]. Once we have set the necessary background, we will prove quantifier elimination for differentially closed fields.

The main work for this thesis was Chapter 6. This is based on van den Dries' paper [vdD], in which the author only stated the quantifier elimination test without giving a proof. By finding some useful properties of extensions of partial embeddings, we succeded in proving the test. In the subsequent section we present a detailed proof of quantifier elimination for the ordered field of real numbers with a predicate for the powers of two.

Finally, in Chapter 7 we conclude this thesis by giving some applications of quantifier elimination. We hereby focus on completeness and decidability as well as on the understanding of definable sets. We will give one geometric consequence, namely the Differential Nullstellensatz, which is the analogue of Hilbert's Nullstellensatz for algebraically closed fields in differential algebra.

2 Model Theoretical Background

This chapter will give a brief introduction to model theoretic preliminaries which are necessary for the following chapters. It pursues the goal of explaining terminology and repeating some theory that we are going to use several times throughout this thesis. We will assume that the reader is already familiar with basic notions of mathematical logic. We follow the introductory chapters of [Mar02], [Pre86] and [Pre98].

Because in mathematical logic the formal language itself becomes an object of our investigation, one always needs to deal with two languages: On the one hand there is the formal language which is the object of our study, and on the other hand we have the metalanguage in which we talk about this formal language. The latter is the mathematical colloquial language. The former, however, the object language, depends on the subject being considered at the time and needs to be carefully defined.

Let I, J and K be arbitrary (possibly empty) index sets and $\mu : I \to \mathbb{N}$ and $\lambda : J \to \mathbb{N}$ two functions. For every $i \in I$ let f_i be a $\mu(i)$-ary function symbol, for every $j \in J$ let R_j be a $\lambda(j)$-ary relation symbol, and for every $k \in K$ let c_k be a constant symbol. The function μ assigns to each $i \in I$ the "arity" (i.e. number of arguments) $\mu(i)$ of the function symbol f_i, whereas the function λ assigns to each $j \in J$ the arity $\lambda(j)$ of the relation symbol R_j. Then,

$$\mathcal{L} = \langle (f_i)_{i\in I} \,;\, (R_j)_{j\in J} \,;\, (c_k)_{k\in K} \rangle$$

is called a *language*. For a fixed language $\mathcal{L}$, an *$\mathcal{L}$-structure*

$$\mathcal{M} = \big(M \,;\, (f_i^{\mathcal{M}})_{i\in I} \,;\, (R_j^{\mathcal{M}})_{j\in J} \,;\, (c_k^{\mathcal{M}})_{k\in K}\big)$$

consists of a nonempty set M, called the *universe* of $\mathcal{M}$, a $\mu(i)$-ary function $f_i^{\mathcal{M}} : M^{\mu(i)} \to M$ for each $i \in I$, a $\lambda(j)$-ary relation $R_j^{\mathcal{M}} \subseteq M^{\lambda(j)}$, and a fixed element $c_k^{\mathcal{M}} \in M$ for each $k \in K$. The superscript "$\mathcal{M}$" denotes the interpretation of the symbols in M. We will usually name structures by calligraphic letters and their universe by the corresponding Latin letters, i.e. if $\mathcal{M}, \mathcal{N}, \mathcal{A}, \mathcal{B}$ are $\mathcal{L}$-strucutres, then we will refer to their underlying universes by M, N, A, and B, respectively.

Additionally to the symbols in a language $\mathcal{L}$ we use the following symbols: variable symbols $v, w, v_1, v_2, \ldots$, the Boolean connectives $\wedge, \vee$, and $\neg$, the quantifiers $\exists$ and $\forall$, parentheses (,), and the equality symbol $\doteq$. This list of variables is non-exhaustive, but the context will make the identification of variables clear. To distinguish the formal object language from the metalanguage, we will usually use $\doteq$ as an equality symbol in the formal language, whereas we write the usual equality sign $=$ in the metalanguage. If a language contains the function symbols $+$, $\cdot$, or $<$ we usually write $a + b$, $a \cdot b$, and $a < b$ instead of $+(a, b)$, $\cdot(a, b)$, and $<(a, b)$, respectively, for the sake of a better reading. Let for the rest of this introductory chapter $\mathcal{L}$ be a fixed language.

The set of $\mathcal{L}$-*terms* is the smallest set which contains all variables and all constant symbols, and for each $i \in I$, it contains $f_i(t_1, \ldots, t_{\mu(i)})$ whenever it contains $t_1, \ldots, t_{\mu(i)}$.

We say that ϕ is an *atomic* $\mathcal{L}$-formula if it is either of the form $t_1 \doteq t_2$ for two $\mathcal{L}$-terms t_1 and t_2, or it is of the form $R_j(t_1, \ldots, t_{\lambda(j)})$, where R_j is a relation symbol and $t_1, \ldots, t_{\lambda(j)}$ are $\mathcal{L}$-terms.

The set of $\mathcal{L}$-*formulas* is the smallest set consisting of all atomic $\mathcal{L}$-formulas, and that contains $\neg\phi$, $(\phi \wedge \psi), (\phi \vee \psi), \exists v\, \phi$, and $\forall v\, \phi$ for any variable v, whenever it contains ϕ and ψ. There are two abbreviating notations that we will use: $\phi \to \psi$ stands for $\neg(\phi \vee \psi)$ and $\phi \leftrightarrow \psi$ is short for $(\phi \to \psi) \wedge (\psi \to \phi)$. We will also use the abbreviations $\bigwedge_{i=1}^{n} \phi_i$ and $\bigvee_{i=1}^{n} \phi_i$ for $\phi_1 \wedge \ldots \wedge \phi_n$ and $\phi_1 \vee \ldots \vee \phi_n$, respectively. The two quantifiers can be defined in terms of each other: $\forall v\, \phi$ holds if and only if $\neg\exists v\, \neg\phi$ is fulfilled. Hence, in arguments on the complexity of $\mathcal{L}$-formulas it is unnecessary to consider both.

We often write $\phi(v_1, \ldots, v_n)$ to make explicit the free variables in ϕ. Whenever we write "$\overline{a} \in A$", we mean that we take a tuple $(a_1, \ldots, a_n)$ with components $a_1, \ldots, a_n$ from A. Since in most cases the number n of components does not play an important role and is only meant to suit the corresponding amount of free variables in some $\mathcal{L}$-formula, we avoid naming the number and just write "$\overline{a}$" instead. Another natural abuse of notation is that, given an $\mathcal{L}$-formula $\phi(v_1, \ldots, v_n)$, a tuple $\overline{a} \in A$, and some function $f : A \to B$, instead of "$\phi(f(a_1), \ldots, f(a_n))$" we simply write "$\phi(f(\overline{a}))$". And lastly, if $\overline{a} = (a_1, \ldots, a_n)$, then by $c_{\overline{a}}$ we mean the tuple $(c_{a_1}, \ldots, c_{a_n})$.

If an $\mathcal{L}$-formula has no free variables, we call it an $\mathcal{L}$-*sentence*. A *quantifier-free* $\mathcal{L}$-formula is an $\mathcal{L}$-formula without quantifiers. An $\mathcal{L}$-formula ϕ of the form

$$\bigwedge_{i=1}^{N} \bigvee_{j=1}^{n_i} \phi_{ij} \qquad \text{or} \qquad \bigvee_{i=1}^{N} \bigwedge_{j=1}^{n_i} \phi_{ij},$$

where each ϕ_{ij} is an atomic $\mathcal{L}$-formula or the negation of one, is said to be in *conjunctive normal form* or in *disjunctive normal form*, respectively. Using the distributive law and De Morgan's laws, every quantifier-free $\mathcal{L}$-formula ϕ can be written in both disjunctive normal form and in conjunctive normal form, with the same free variables.

Next we will define what it means for a formula of a formal language to be satisfied or to hold in a certain structure and what it means for a structure to be a model of a particular set of sentences, so that we can, for instance, state that a structure in the language of rings is in fact a ring. For an $\mathcal{L}$-formula $\phi(v_1, \ldots, v_n)$ with free variables from $\overline{v} = (v_1, \ldots, v_n)$ and $\overline{a} = (a_1, \ldots, a_n) \in M^n$ we define recursively $\mathcal{M} \models \phi(\overline{a})$ as follows:

If ϕ is $t_1 \doteq t_2$, then $\mathcal{M} \models \phi(\overline{a})$,	iff $t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a})$;
if ϕ is $R_j(t_1, \ldots t_{\lambda(j)})$, then $\mathcal{M} \models \phi(\overline{a})$,	iff $(t_1^{\mathcal{M}}(\overline{a}), \ldots, t_{\lambda(j)}^{\mathcal{M}}(\overline{a})) \in R_j^{\mathcal{M}}$;
if ϕ is $\neg\psi$, then $\mathcal{M} \models \phi(\overline{a})$,	iff $\mathcal{M} \models \psi(\overline{a})$ does not hold;
if ϕ is $(\psi \wedge \theta)$, then $\mathcal{M} \models \phi(\overline{a})$,	iff $\mathcal{M} \models \psi(\overline{a})$ and $\mathcal{M} \models \theta(\overline{a})$;
if ϕ is $(\psi \vee \theta)$, then $\mathcal{M} \models \phi(\overline{a})$,	iff $\mathcal{M} \models \psi(\overline{a})$ or $\mathcal{M} \models \theta(\overline{a})$;
if ϕ is $\exists w\, \psi(\overline{v}, w)$, then $\mathcal{M} \models \phi(\overline{a})$,	iff there is $b \in M$ such that $\mathcal{M} \models \psi(\overline{a}, b)$;
if ϕ is $\forall w\, \psi(\overline{v}, w)$, then $\mathcal{M} \models \phi(\overline{a})$,	iff $\mathcal{M} \models \psi(\overline{a}, b)$ for all $b \in M$.

An $\mathcal{L}$-*theory* $\mathcal{T}$ is a set of $\mathcal{L}$-sentences, that means a set of $\mathcal{L}$-formulas without any free variables. We say that $\mathcal{M}$ is a *model* of $\mathcal{T}$ and write $\mathcal{M} \models \mathcal{T}$ if $\mathcal{M} \models \phi$ for all $\mathcal{L}$-sentences $\phi \in \mathcal{T}$. Moreover, we write $\mathcal{T} \models \phi$ if for every model $\mathcal{M} \models \mathcal{T}$ it holds $\mathcal{M} \models \phi$. An $\mathcal{L}$-theory that satisfies $\mathcal{T} \models \phi$ or $\mathcal{T} \models \neg\phi$ for each $\mathcal{L}$-sentence ϕ is called *complete*. Occasionally it may be useful to consider the *full theory* $\mathrm{Th}(\mathcal{M})$ of an $\mathcal{L}$-structure $\mathcal{M}$ which consists of all $\mathcal{L}$-sentences ϕ such that $\mathcal{M} \models \phi$. The full theory $\mathrm{Th}(\mathcal{M})$ is in fact a complete $\mathcal{L}$-theory.

Sometimes it is possible to give a set of $\mathcal{L}$-sentences that form axioms for a theory. We will call a set of $\mathcal{L}$-sentences Σ an *axiom system* for an $\mathcal{L}$-theory $\mathcal{T}$ if

$$\{\phi : \ \phi \text{ is an } \mathcal{L}\text{-sentence and } \mathcal{T} \models \phi\} = \{\phi : \ \phi \text{ is an } \mathcal{L}\text{-sentence and } \Sigma \models \phi\}.$$

The $\mathcal{L}$-sentences in Σ are then called *axioms*. If $\mathcal{T}$ already contains each $\mathcal{L}$-sentence ϕ with $\mathcal{T} \models \phi$, we say that $\mathcal{T}$ is *deductively closed*. In this case the $\mathcal{L}$-theory consists exactly of the $\mathcal{L}$-sentences that can be deduced from the axioms and no more. We will later on see a couple of examples for such axiom systems.

Of course, as usual in mathematics, we will also consider maps between $\mathcal{L}$-structures. Here we wish that those maps preserve the interpretation of the symbols in the language $\mathcal{L}$. Hence, we define:

2.1 Definition. Let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathcal{L}$-structures with universes M and N, respectively. An $\mathcal{L}$-*embedding* $\iota : \mathcal{M} \to \mathcal{N}$ is an injective map between the universes $\iota : M \to N$ which preserves the interpretation of all function, relation, and constant symbols of $\mathcal{L}$. To be more precise, this means:

(i) $\iota(f^{\mathcal{M}}(\overline{a})) = f^{\mathcal{N}}(\iota(\overline{a}))$ for all function symbols f and $\overline{a} \in M$.
(ii) $\overline{a} \in R^{\mathcal{M}}$ if and only if $\iota(\overline{a}) \in R^{\mathcal{N}}$ for all relation symbols R and $\overline{a} \in M$.
(iii) $\iota(c^{\mathcal{M}}) = c^{\mathcal{N}}$ for all constant symbols c.

If there exists an $\mathcal{L}$-embedding from $\mathcal{M}$ into $\mathcal{N}$, we say that $\mathcal{M}$ is a *substructure* of $\mathcal{N}$. A bijective $\mathcal{L}$-embedding is called an $\mathcal{L}$-*isomorphism*. Sometimes, however, $\iota(\mathcal{M})$ is identified with $\mathcal{M}$, hence if $\mathcal{M}$ is a substructure of $\mathcal{N}$ we write $\mathcal{M} \subseteq \mathcal{N}$.

The following lemma indicates that $\mathcal{L}$-embeddings preserve quantifier-free formulas that only use parameters from the universe of the substructure. It is therefore known as the Substructure Lemma.

2.2 Lemma (Substructure Lemma)**.** *Let $\mathcal{M}$ be a substructure of $\mathcal{N}$, $\overline{a} \in M$, and let $\phi(\overline{v})$ be a quantifier-free formula. Then, $\mathcal{M} \models \phi(\overline{a})$ if and only if $\mathcal{N} \models \phi(\overline{a})$.*

Proof. For the proof see for example [Mar02, Proposition 1.1.8]. □

There are maps that preserve quantifier-free formulas with parameters from a subset of the domain. They will become very useful later on in Chapter 5.

2.3 Definition. Let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathcal{L}$-structures and A a subset of M, where M is the universe of $\mathcal{M}$. Then the map $\eta : A \to \mathcal{N}$ is called a *partial embedding* if it preserves all quantifier-free formulas. That means, for all quantifier-free $\phi(\overline{v})$ and $\overline{a} \in A$ it holds that

$$\mathcal{M} \models \phi(\overline{a}) \quad \Leftrightarrow \quad \mathcal{N} \models \phi(\eta(\overline{a})).$$

Note that we write a partial embedding $\eta : A \to \mathcal{N}$ technically from a subset into a structure, to point out that the interpretation of the specified formulas is being preserved. However A is only a subset, thus denoted by a Latin letter.

2.4 Definition. We say that a collection $\Sigma(\overline{v})$ of $\mathcal{L}$-formulas in n free variables is *satisfiable* if there exists an $\mathcal{L}$-structure $\mathcal{A}$ with universe A and a tuple $\overline{a} \in A$, such that $\mathcal{A} \models \phi(\overline{a})$ for every $\phi(\overline{v}) \in \Sigma(\overline{v})$. In particular, an $\mathcal{L}$-theory is called *satisfiable* if it has a model.

By his Completeness Theorem (see [Pre86, Theorem 1.5.2]), Kurt Gödel showed that the syntactic notion of provability completely coincides with what we semantically call true. The Completeness Theorem says that a proposition is true in every model of a theory if and only if it is provable from the theory. A very important consequence of the Completeness Theorem is the so called Compactness Theorem. It is the cornerstone of model theory. Until about 50 years ago, all applications of model theory to algebra were corollaries of the Compactness Theorem, cf. [Sac72a]. Throughout this thesis we will use it several times.

2.5 Theorem (Compactness Theorem)**.** *Let $\mathcal{T}$ be an $\mathcal{L}$-theory. Then $\mathcal{T}$ is satisfiable if and only if every finite subset of $\mathcal{T}$ is satisfiable.*

Proof. This follows from Gödel's Completeness Theorem and the fact that any formal proof only requires finitely many assumptions from the theory $\mathcal{T}$. The proof can for example be found in [Mar02, Theorem 2.1.4]. □

2.6 Definition. An $\mathcal{L}$-embedding $\eta : \mathcal{M} \to \mathcal{N}$ is called an *elementary embedding* if

$$\mathcal{M} \models \phi(\overline{a}) \quad \Leftrightarrow \quad \mathcal{N} \models \phi(\eta(\overline{a}))$$

for all $\mathcal{L}$-formulas $\phi(\overline{v})$ and all $\overline{a} \in M$. In this case we say that $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$ and write $\mathcal{M} \preceq \mathcal{N}$.

For a subset $B \subseteq M$, we say that $\eta : B \to \mathcal{N}$ is a *partial elementary* map if

$$\mathcal{M} \models \phi(\overline{b}) \quad \Leftrightarrow \quad \mathcal{N} \models \phi(\eta(\overline{b}))$$

for all $\mathcal{L}$-formulas $\phi(\overline{v})$ and all $\overline{b} \in B$.

Two models $\mathcal{M}, \mathcal{N} \models \mathcal{T}$ of an $\mathcal{L}$-theory $\mathcal{T}$ are called *elementarily equivalent* if

$$\mathcal{M} \models \phi \quad \Leftrightarrow \quad \mathcal{N} \models \phi$$

for every $\mathcal{L}$-sentence ϕ.

Elementary equivalence is strongly related to completeness:

2.7 Proposition. *An $\mathcal{L}$-theory $\mathcal{T}$ is complete if and only if any two models $\mathcal{M}, \mathcal{N} \models \mathcal{T}$ are elementarily equivalent.*

Proof. Let $\mathcal{T}$ be a complete $\mathcal{L}$-theory with $\mathcal{M} \models \mathcal{T}$ and $\mathcal{M} \models \phi$ for some $\mathcal{L}$-sentence ϕ. Assume that $\mathcal{T} \models \neg\phi$. Then $\mathcal{M} \models \neg\phi$, a contradiction. By completeness, $\mathcal{T} \models \phi$ and, hence, $\mathcal{N} \models \phi$ for any other model $\mathcal{N} \models \mathcal{T}$.

Suppose otherwise that any two models of $\mathcal{T}$ are elementarily equivalent. Let ϕ be some $\mathcal{L}$-sentence. If $\mathcal{M} \models \phi$, then for every model $\mathcal{N} \models \mathcal{T}$ we obtain $\mathcal{N} \models \phi$. Hence $\mathcal{T} \models \phi$. If on the other hand $\mathcal{M} \not\models \phi$, then $\mathcal{M} \models \neg\phi$, and therefore, $\mathcal{T} \models \neg\phi$. □

2.8 Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure. By $\mathcal{L}_M$ we denote the language which consists of the symbols in $\mathcal{L}$ and, additionally, a constant symbol c_m for each element $m \in M$. Then $\mathcal{M}$ expands in a natural way to an $\mathcal{L}_M$-structure by interpreting the new symbols in the obvious way $c_m^{\mathcal{M}} = m$. The *atomic diagram* of $\mathcal{M}$ is the set

$$\begin{aligned}\mathrm{Diag}(\mathcal{M}) := \{\phi(c_{\overline{m}}) : \overline{m} \in M,\ \phi(\overline{v}) \text{ is an atomic } \mathcal{L}\text{-formula or} \\ \text{the negation of one, and } \mathcal{M} \models \phi(c_{\overline{m}})\},\end{aligned}$$

where $c_{\overline{m}}$ stands for $(c_{m_1}, \ldots, c_{m_n})$ whenever $\overline{m} = (m_1, \ldots, m_n)$. In a similar way we define the *elementary diagram* of $\mathcal{M}$ to be

$$\mathrm{Diag}_{\mathrm{el}}(\mathcal{M}) := \{\phi(c_{\overline{m}}) :\ \overline{m} \in M,\ \phi(\overline{v}) \text{ is an } \mathcal{L}\text{-formula and } \mathcal{M} \models \phi(c_{\overline{m}})\}.$$

The atomic and the elementary diagram are an effective instrument to prove the existence of $\mathcal{L}$-embeddings. The reason is the next lemma:

2.9 Lemma. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $\mathcal{N}$ an $\mathcal{L}_M$-structure.*

(a) If $\mathcal{N} \models \mathrm{Diag}(\mathcal{M})$, then, viewing $\mathcal{N}$ as an $\mathcal{L}$-structure, there is an $\mathcal{L}$-embedding of $\mathcal{M}$ into $\mathcal{N}$.
(b) If $\mathcal{N} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$, then there is an elementary embedding of $\mathcal{M}$ into $\mathcal{N}$.

Proof. (a) Let j be the interpretation of the constant symbols of $\mathcal{L}_M$ in $\mathcal{N}$, i.e. $j : M \to N$ with $j(m) = c_m^{\mathcal{N}}$. If m_1 and m_2 are two distinct elements in M, then $\neg c_{m_1} \doteq c_{m_2}$ is a formula in $\mathrm{Diag}(\mathcal{M})$, and hence, since $\mathcal{N} \models \mathrm{Diag}(\mathcal{M})$, we obtain $j(m_1) \neq j(m_2)$. Thus, j is an embedding of sets, i.e. injective. It remains to show that j is an $\mathcal{L}$-embedding:

Let f be a function symbol of $\mathcal{L}$, and $f^{\mathcal{M}}(m_1, \ldots, m_n) = m_{n+1}$. Then $f(c_{m_1}, \ldots, c_{m_n}) \doteq c_{m_{n+1}}$ is a formula in $\mathrm{Diag}(\mathcal{M})$ and $f^{\mathcal{N}}(j(m_1), \ldots, j(m_n)) = j(m_{n+1})$.

For a relation symbol R of $\mathcal{L}$ and $\overline{m} \in R^{\mathcal{M}}$ we obtain $R(c_{m_1}, \ldots, c_{m_n}) \in \mathrm{Diag}(\mathcal{M})$ and, thus, $(j(m_1), \ldots, j(m_n)) \in R^{\mathcal{N}}$. Hence, j is an $\mathcal{L}$-embedding.

(b) We will show that if $\mathcal{N} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$, then the map j from above is elementary. Note that $\mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ is a complete theory: either a sentence is in the set or its negation is. Suppose $\mathcal{M} \models \phi(c_{\overline{a}})$ for some $\overline{a} \in M$, i.e. $\phi(c_{\overline{a}}) \in \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$. Since $\mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ is complete, this is equivalent to the fact that $\mathcal{N} \models \phi(j(\overline{a}))$. Thus, j is an elementary $\mathcal{L}$-embedding. □

For the sake of simplicity, we will often write $\phi(\overline{a})$ where ϕ is an $\mathcal{L}$-formula and $\overline{a} \in A$ a tuple, even if $a_1, \ldots, a_n$ are not constant symbols in the language, whenever this does not result in ambiguity. We then mean $\phi(c_{\overline{a}})$ after adding $a_1, \ldots, a_n$ to the constant symbols and interpreting them in the natural way, as in $\mathcal{L}_A$.

In general, the union of models of a certain theory is not even necessarily a well-defined structure. But for elementary extensions we have a very useful property:

2.10 Definition. We say that $(\mathcal{M}_i :\ i \in I)$ is a *chain* of $\mathcal{L}$-structures, if each $\mathcal{M}_i$ is an $\mathcal{L}$-structure and $\mathcal{M}_i \subseteq \mathcal{M}_j$ for every $i < j$. If additionally $\mathcal{M}_i \preceq \mathcal{M}_j$ for every $i < j$, we say that $(\mathcal{M}_i :\ i \in I)$ is an *elementary chain*.

As mentioned before, we will, in particular here, identify a structure with its image under the embedding. This is, however, not a restriction in any sence, but rather a simplification of notation. The union $\mathcal{M} = \bigcup_{i \in I} \mathcal{M}_i$ of a chain of structures is defined as follows: The universe

of $\mathcal{M}$ is $M := \bigcup_{i\in I} M_i$. For a constant c of the language we have $c^{\mathcal{M}_i} = c^{\mathcal{M}_j}$ for all i and j. We set $c^{\mathcal{M}} := c^{\mathcal{M}_i}$. If f is a function symbol of the language, then $f^{\mathcal{M}_i}(\overline{a}) = f^{\mathcal{M}_j}(\overline{a})$ for any $\overline{a} \in M_i \cap M_j$. Since every $\overline{a} \in M$ is already contained in some M_i, $f^{\mathcal{M}} := \bigcup_{i\in I} f^{\mathcal{M}_i}$ is well-defined. For a relation symbol R, we have $\overline{a} \in R^{\mathcal{M}_i}$ if and only if $\overline{a} \in R^{\mathcal{M}_j}$. Thus, we set $R^{\mathcal{M}} := \bigcup_{i\in I} R^{\mathcal{M}_i}$. This implies that each $\mathcal{M}_i$ is a substructure of $\mathcal{M}$.

2.11 Proposition. *Let $(\mathcal{M}_i : i \in I)$ be an elementary chain of $\mathcal{L}$-structures, i.e. $\mathcal{M}_i \preceq \mathcal{M}_j$ for $i < j$. Then its limit*

$$\mathcal{M} := \bigcup_{i\in I} \mathcal{M}_i$$

is an elementary extension of each $\mathcal{M}_i$.

Proof. This proposition is due to Alfred Tarski and Robert Vaught and a proof can be found in [Mar02, Proposition 2.3.11]. □

2.12 Definition. An $\mathcal{L}$-formula of the form $\forall w_1 \forall w_2 \dots \forall w_n\ \phi(\overline{v}, \overline{w})$, where $\phi(\overline{v}, \overline{w})$ is quantifier-free, is called a *universal* $\mathcal{L}$-formula. Similarly, an $\mathcal{L}$-formula of the form $\exists w_1 \exists w_2 \dots \exists w_n\ \phi(\overline{v}, \overline{w})$ with $\phi(\overline{v}, \overline{w})$ quantifier-free is called *existential*. For a theory $\mathcal{T}$ we denote by $\mathcal{T}_\forall$ the set of all the universal $\mathcal{L}$-sentences ϕ such that $\mathcal{T} \models \phi$ and call $\mathcal{T}_\forall$ the *universal theory* of $\mathcal{T}$.

It requires only a little thought to see that universal statements are preserved downwards in inclusion, whereas existential formulas are preserved upwards in inclusion. The next lemma will be very useful in section 6.1.

2.13 Lemma. *For an $\mathcal{L}$-theory $\mathcal{T}$ the following are equivalent:*

(i) $\mathcal{A} \models \mathcal{T}_\forall$.
(ii) There is a model $\mathcal{M} \models \mathcal{T}$ *with* $\mathcal{A} \subseteq \mathcal{M}$.

Proof. Universal statements are preserved downwards in inclusion. Therefore we only need to deal with the implication (i) ⇒ (ii): Let $\mathcal{A} \models \mathcal{T}_\forall$. Consider the theory $\mathcal{T}' := \mathcal{T} \cup \mathrm{Diag}(\mathcal{A})$ in the language $\mathcal{L}_A$. We will show by contradiction that $\mathcal{T}'$ is satisfiable, which implies that there is a model $\mathcal{M} \models \mathcal{T}'$, i.e. $\mathcal{M} \models \mathcal{T}$ and $\mathcal{M} \models \mathrm{Diag}(\mathcal{A})$. With the latter we obtain by Lemma 2.9 an $\mathcal{L}$-embedding of $\mathcal{A}$ into $\mathcal{M}$.

Hence, let us suppose that $\mathcal{T}'$ is not satisfiable. Then, by the Compactness Theorem, already some finite subset $\Delta \subseteq \mathcal{T}'$ is not satisfiable. By forming conjunctions we may assume that the part of Δ coming from $\mathrm{Diag}(\mathcal{A})$ consists only of one formula $\phi(\overline{a})$ for some $\overline{a} \in A$, where $\phi(\overline{a})$ is a conjunction of atomic formulas and the negation of atomic formulas. Thus, we will assume that $\mathcal{T} \cup \{\phi(\overline{a})\}$ is not satisfiable. In particular, $\phi(\overline{a})$ is quantifier-free and, as $\mathrm{Diag}(\mathcal{A}) \models \phi(\overline{a})$, we obtain $\mathcal{A} \models \phi(\overline{a})$.

On the other hand, viewing $\mathcal{T}$ as an $\mathcal{L}_{\overline{a}}$-theory, and because $\mathcal{T} \cup \{\phi(\overline{a})\}$ is not satisfiable, we obtain $\mathcal{T} \models \neg\phi(\overline{a})$. We will show that this implies $\mathcal{T} \models \forall \overline{v}\ \neg\phi(\overline{v})$: Let $\mathcal{C}$ be an $\mathcal{L}$-structure with $\mathcal{C} \models \mathcal{T}$. Let n be the number of components in $\overline{a}$ and $c_1, \dots, c_n \in C$ be any tuple. Let $\mathcal{C}'$ be the $\mathcal{L}_{\overline{a}}$-structure which expands $\mathcal{C}$ by the constant symbols $a_1, \dots, a_n$, that we interpret as $c_1, \dots, c_n$, respectively. Then $\mathcal{C}' \models \mathcal{T}$ and, hence $\mathcal{C}' \models \phi(\overline{c})$. As this follows for any tuple in C, we get $\mathcal{C} \models \forall \overline{v}\ \neg\phi(\overline{v})$ and, thus, $\mathcal{T} \models \forall \overline{v}\ \neg\phi(\overline{v})$ as claimed.

Since $\mathcal{T}_\forall$ consists exactly of the universal formulas which hold in all models of $\mathcal{T}$, we obtain $\mathcal{T}_\forall \models \forall x\ \neg\phi(x)$. Hence, also $\mathcal{A} \models \forall x\ \neg\phi(x)$, which is a contradiction because we also had $\mathcal{A} \models \phi(\overline{a})$.

Therefore, as desired, $\mathcal{T}'$ is indeed satisfiable. □

After this short introduction to mathematical logic and model theory, we can finally give a proper definition of quantifier elimination and hereby start discussing the main purposes of this thesis.

2.14 Definition. An $\mathcal{L}$-theory $\mathcal{T}$ is said to admit *elimination of quantifiers* if for any $\mathcal{L}$-formula $\phi(\overline{v})$ there is a quantifier-free $\mathcal{L}$-formula $\psi(\overline{v})$ such that the following holds:

$$\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v})).$$

A weaker concept than quantifier elimination is the property of *model completeness*. The following theorem is called Robinson's Test. We call an $\mathcal{L}$-theory $\mathcal{T}$ *model complete* if one of the following equivalent conditions holds:

2.15 Theorem (Robinson's Test)**.** *For an $\mathcal{L}$-theory $\mathcal{T}$ the following are equivalent:*

(i) All $\mathcal{L}$-embeddings of models of $\mathcal{T}$ are elementary.
(ii) Let $\mathcal{M}$,$\mathcal{N} \models \mathcal{T}$ be two models, where $\mathcal{M} \subseteq \mathcal{N}$. For every existential $\mathcal{L}$-formula $\phi(\overline{v})$ and $\overline{a} \in M$ with $\mathcal{N} \models \phi(\overline{a})$ it follows $\mathcal{M} \models \phi(\overline{a})$.
(iii) For every $\mathcal{L}$-formula $\phi(\overline{v})$ there exists a universal $\mathcal{L}$-formula $\psi(\overline{v})$ such that it holds $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$.

Proof. See [Pre98, Lemma 3.3.1 and Theorem 3.3.3]. □

By condition (iii) of Robinson's Test, a theory is obviously model complete whenever it admits quantifier elimination.

A language $\mathcal{L}$ without constant symbols does not produce any quantifier-free $\mathcal{L}$-sentences. Hence, to make sense of the expression "quantifier-free $\mathcal{L}$-sentence", we will always assume that our languages contain at least one constant symbol.

It is important to remark that quantifier elimination is a matter of language. We will see that some theories only admit quantifier elimination after adding some predicates to the language.

Having defined what it means for an $\mathcal{L}$-theory to eliminate quantifiers, we may now end this introductory chapter and start the next one with the first quantifier elimination test.

3 Basic Quantifier Elimination Criteria

3.1 First Approach to Quantifier Elimination

This section is based on [Mar02, Section 3.1]. The proofs, however, will be presented in more detail than in the source. We will prove two lemmas in order to obtain a first quantifier elimination test from the combination of both.

3.1 Lemma. *Let $\mathcal{L}$ be a language that contains at least one constant symbol c, $\mathcal{T}$ an $\mathcal{L}$-theory, and $\phi(\overline{v})$ an $\mathcal{L}$-formula. Then the following are equivalent:*

(i) If $\mathcal{M}$ and $\mathcal{N}$ are models of $\mathcal{T}$, and $\mathcal{A}$ is a common substructure, then for any tuple $\overline{a} \in A$ we have $\mathcal{M} \models \phi(\overline{a})$ if and only if $\mathcal{N} \models \phi(\overline{a})$.

(ii) There is a quantifier-free $\mathcal{L}$-formula $\psi(\overline{v})$ such that $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$.

Proof. (i) $\Rightarrow$ (ii): If $\mathcal{T} \models \forall \overline{v}\ \phi(\overline{v})$, then $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow c \doteq c)$ and we have found the corresponding quantifier-free formula: $c \doteq c$. If, on the other hand, $\mathcal{T} \models \forall \overline{v}\ \neg\phi(\overline{v})$, then we have $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \neg c \doteq c)$ and we are also done. So we may assume that we are in the third case where none of the above is true, i.e., there exists a model $\mathcal{M}_1$ of $\mathcal{T}$ that does not model $\forall \overline{v}\ \phi(\overline{v})$ and there is a model $\mathcal{M}_2$ of $\mathcal{T}$ that does not model $\forall \overline{v}\ \neg\phi(\overline{v})$. This means that $\mathcal{M}_1 \models \exists \overline{v}\ \neg\phi(\overline{v})$ and $\mathcal{M}_2 \models \exists \overline{v}\ \phi(\overline{v})$, and, thus, both $\mathcal{T} \cup \{\neg\phi(\overline{v})\}$ and $\mathcal{T} \cup \{\phi(\overline{v})\}$ are satisfiable.

Define the set $\Gamma(\overline{v}) = \{\psi(\overline{v}) :\ \psi \text{ is quantifier-free and } \mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \rightarrow \psi(\overline{v}))\}$. Let $c_1, \ldots, c_m$ be new constant symbols. We will view $\mathcal{T}$ now as an $\mathcal{L}_{\overline{c}}$-theory where $\mathcal{L}_{\overline{c}}$ is the language $\mathcal{L}$ extended by the constant symbols $c_1, \ldots, c_m$. We will show that $\mathcal{T} \cup \Gamma(\overline{c}) \models \phi(\overline{c})$.

Assume that this is not the case. Then there is a model $\mathcal{M} \models \mathcal{T} \cup \Gamma(\overline{c}) \cup \{\neg\phi(\overline{c})\}$. Let $\mathcal{A}$ be the substructure of $\mathcal{M}$ generated by $\overline{c}$, i.e. the smallest substructure of $\mathcal{M}$ that contains $c_1, \ldots, c_m$.

Let $\Sigma = \mathcal{T} \cup \mathrm{Diag}(\mathcal{A}) \cup \{\phi(\overline{c})\}$. Let us assume that Σ were not satisfiable. So, for any model $\mathcal{B} \models \mathcal{T} \cup \mathrm{Diag}(\mathcal{A})$, one obtains $\mathcal{B} \models \neg\phi(\overline{c})$. Thus $\mathcal{T} \cup \mathrm{Diag}(\mathcal{A}) \models \neg\phi(\overline{c})$. By the Compactness Theorem there are finitely many $\psi_1(\overline{c}), \ldots, \psi_n(\overline{c}) \in \mathrm{Diag}(\mathcal{A})$ which are quantifier-free $\mathcal{L}$-formulas such that

$$\mathcal{T} \cup \{\psi_1(\overline{c}), \ldots, \psi_n(\overline{c})\} \models \neg\phi(\overline{c}).$$

Let $\mathcal{C} \models \mathcal{T}$, and suppose that $\mathcal{C} \models \{\psi_1(\overline{c}), \ldots, \psi_n(\overline{c})\}$, i.e. $\mathcal{C} \models \psi_1(\overline{c}) \wedge \ldots \wedge \psi_n(\overline{c})$. Then, $\mathcal{C} \models \neg\phi(\overline{c})$. Hence

$$\mathcal{T} \models \bigwedge_{i=1}^{n} \psi_i(\overline{c}) \rightarrow \neg\phi(\overline{c}). \tag{3.1}$$

Viewing $\mathcal{T}$ as an $\mathcal{L}$-theory again, this yields

$$\mathcal{T} \models \forall \overline{v} \left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \to \neg \phi(\overline{v}) \right)$$

as in Lemma 2.13: Let $\mathcal{D}$ be an $\mathcal{L}$-structure such that $\mathcal{D} \models \mathcal{T}$. Let $d_1, \ldots, d_m \in D$ be any tuple of the size of $\overline{a}$. Let $\mathcal{D}'$ be the $\mathcal{L}_{\overline{c}}$-structure which expands $\mathcal{D}$ by the constant symbols $c_1, \ldots, c_m$, that we interpret as $d_1, \ldots, d_m$, respectively. Then, $\mathcal{D}' \models \mathcal{T}$ and, by (3.1), we obtain

$$\mathcal{D}' \models \bigwedge_{i=1}^{n} \psi_i(\overline{d}) \to \neg \phi(\overline{d}).$$

Since this does not depend on the choice of the tuple $\overline{d}$, we obtain

$$\mathcal{D} \models \forall \overline{v} \left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \to \neg \phi(\overline{v}) \right) \text{ and thus } \mathcal{T} \models \forall \overline{v} \left(\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \to \neg \phi(\overline{v}) \right),$$

as claimed. Forming the contrapositive we obtain

$$\mathcal{T} \models \forall \overline{v} \left(\phi(\overline{v}) \to \bigvee_{i=1}^{n} \neg \psi_i(\overline{v}) \right).$$

By the definition of Γ, this means

$$\bigvee_{i=1}^{n} \neg \psi_i(\overline{v}) \in \Gamma(\overline{v}).$$

Since $\mathcal{M} \models \Gamma(\overline{c})$ and because $\neg \psi_i(\overline{c})$ is quantifier-free, this also yields

$$\mathcal{A} \models \bigvee_{i=1}^{n} \neg \psi_i(\overline{c})$$

by Lemma 2.2, since $\mathcal{A}$ is the substructure of $\mathcal{M}$ which is generated by $\overline{c}$. This is a contradiction to $\psi_1(\overline{c}), \ldots, \psi_n(\overline{c}) \in \mathrm{Diag}(\mathcal{A})$ and $\mathcal{A} \models \mathrm{Diag}(\mathcal{A})$.

Thus, we may conclude that our assumption "Σ is not satisfiable" was wrong and Σ is indeed satisfiable. Let $\mathcal{N} \models \Sigma$. Then $\mathcal{N} \models \phi(\overline{c})$, and $\mathcal{N} \models \mathrm{Diag}(\mathcal{A})$. By Lemma 2.9, this means that there is an $\mathcal{L}$-embedding from $\mathcal{A}$ into $\mathcal{N}$, i.e. $\mathcal{A}$ is a substructure of $\mathcal{N}$. Recall that $\mathcal{M}$ is a model of $\mathcal{T} \cup \Gamma(\overline{c}) \cup \{\neg \phi(\overline{c})\}$, so $\mathcal{M} \models \neg \phi(\overline{c})$. Since both $\mathcal{M}$ and $\mathcal{N}$ are models of $\mathcal{T}$, we may apply (ii) and conclude that also $\mathcal{N} \models \neg \phi(\overline{c})$. This is a contradiction. Hence, also the assumption that $\mathcal{T} \cup \Gamma(\overline{c}) \not\models \phi(\overline{c})$ was wrong and, thus, we obtain $\mathcal{T} \cup \Gamma(\overline{c}) \models \phi(\overline{c})$.

By the Compactness Theorem, this means that there are finitely many quantifier-free $\mathcal{L}$-formulas $\chi_1(\overline{c}), \ldots, \chi_m(\overline{c}) \in \Gamma(\overline{c})$ such that

$$\mathcal{T} \cup \{\chi_1(\overline{c}), \ldots, \chi_m(\overline{c})\} \models \phi(\overline{c}).$$

Again by the same argumentation as before we may conclude

$$\mathcal{T} \models \forall \overline{v} \left(\bigwedge_{i=1}^{m} \chi_i(\overline{v}) \to \phi(\overline{v}) \right).$$

Since $\chi_1, \ldots, \chi_m \in \Gamma$, this yields

$$\mathcal{T} \models \forall \overline{v} \left(\bigwedge_{i=1}^{m} \chi_i(\overline{v}) \leftrightarrow \phi(\overline{v}) \right),$$

where $\bigwedge_{i=1}^{n} \chi_i(\overline{v})$ is quantifier-free. Thus, we have completed the first—and the more interesting—implication of the proof.

(ii) $\Rightarrow$ (i): Suppose that $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$ for a quantifier-free formula $\psi(\overline{v})$. Let $\mathcal{M}$ and $\mathcal{N}$ be two models of $\mathcal{T}$, $\mathcal{A}$ a common substructure of $\mathcal{M}$ and $\mathcal{N}$, and $\overline{a} \in A$. By Lemma 2.2, quantifier-free formulas are preserved under substructure and extension. Hence, we obtain

$$\begin{aligned}
\mathcal{M} \models \phi(\overline{a}) \quad &\Leftrightarrow \quad \mathcal{M} \models \psi(\overline{a}) && \text{since } \mathcal{M} \models \mathcal{T} \text{ , by assumption of (ii)} \\
&\Leftrightarrow \quad \mathcal{A} \models \psi(\overline{a}) && \text{since } \mathcal{A} \subseteq \mathcal{M} \\
&\Leftrightarrow \quad \mathcal{N} \models \psi(\overline{a}) && \text{since } \mathcal{A} \subseteq \mathcal{N} \\
&\Leftrightarrow \quad \mathcal{N} \models \phi(\overline{a}) && \text{since } \mathcal{N} \models \mathcal{T} \text{ , by assumption of (ii).}
\end{aligned}$$

□

The following lemma states that if one existential quantifier can be eliminated at a time, we already obtain quantifier elimination.

3.2 Lemma. *Let $\mathcal{T}$ be an $\mathcal{L}$-theory. Suppose that for every quantifier-free $\mathcal{L}$-formula $\theta(w, \overline{v})$ there is a quantifier-free formula $\psi(\overline{v})$ such that $\mathcal{T} \models \forall \overline{v}\ ((\exists w\ \theta(w, \overline{v})) \leftrightarrow \psi(\overline{v}))$. Then $\mathcal{T}$ has quantifier elimination.*

Proof. Let $\phi(\overline{v})$ be any $\mathcal{L}$-formula. We want to show that there is some quantifier-free $\mathcal{L}$-formula $\psi(\overline{v})$ such that $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. We will prove this by induction on the complexity of $\phi(\overline{v})$.

If $\phi(\overline{v})$ is quantifier-free, we are already done. So, as induction hypothesis, suppose that for $\phi_1(\overline{v})$ and $\phi_2(\overline{v})$ there already exist quantifier-free $\mathcal{L}$-formulas $\psi_1(\overline{v})$ and $\psi_2(\overline{v})$ such that $\mathcal{T} \models \forall \overline{v}\ (\phi_1(\overline{v}) \leftrightarrow \psi_1(\overline{v}))$ and $\mathcal{T} \models \forall \overline{v}\ (\phi_2(\overline{v}) \leftrightarrow \psi_2(\overline{v}))$. In the case that $\phi(\overline{v}) = \neg\phi_1(\overline{v})$, we have $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow \neg\psi_1(\overline{v}))$. And if $\phi(\overline{v}) = \phi_1(\overline{v}) \wedge \phi_2(\overline{v})$, then $\mathcal{T} \models \forall \overline{v}\ (\phi(\overline{v}) \leftrightarrow (\psi_1(\overline{v}) \wedge \psi_2(\overline{v})))$. In either case, ϕ is equivalent to a quantifier-free formula.

Now suppose $\phi(\overline{v}) = \exists x\ \phi_1(x, \overline{v})$. By induction hypothesis there is a quantifier-free $\mathcal{L}$-formula $\psi_1(x, \overline{v})$ such that $\mathcal{T} \models \forall \overline{v} \forall x\ (\phi_1(x, \overline{v}) \leftrightarrow \psi_1(x, \overline{v}))$. Then we obtain

$$\mathcal{T} \models \forall \overline{v}\ (\exists x\ \phi_1(x, \overline{v}) \leftrightarrow \exists x\ \psi_1(x, \overline{v})) \tag{3.2}$$

as follows: Let $\mathcal{M} \models \mathcal{T}$ and $\overline{a} \in M$. Suppose that $\mathcal{M} \models \phi_1(b, \overline{a})$ for some $b \in M$. Then since $\mathcal{M} \models \forall \overline{v} \forall x\ (\phi_1(x, \overline{v}) \leftrightarrow \psi_1(x, \overline{v}))$, also $\mathcal{M} \models \psi_1(b, \overline{a})$. So, $\mathcal{M} \models \exists x\ \phi_1(x, \overline{a}) \rightarrow \exists x\ \psi_1(x, \overline{a})$. Similarly we obtain the other implication. Hence, $\mathcal{M} \models \exists x\ \phi_1(x, \overline{a}) \leftrightarrow \exists x\ \psi_1(x, \overline{a})$. This shows (3.2) as claimed.

Now by assumption there is $\psi(\overline{v})$ quantifier-free such that

$$\mathcal{T} \models \forall \overline{v}\ (\exists x\ \psi_1(x, \overline{v}) \leftrightarrow \psi(\overline{v})). \tag{3.3}$$

Hence from (3.2) and (3.3) we obtain

$$\mathcal{T} \models \forall \overline{v}\ (\exists x\ \phi_1(x, \overline{v}) \leftrightarrow \psi(\overline{v})),$$

which was to be shown. □

The previous two lemmas set a decent foundation and both of them combined, they yield a simple, yet useful, quantifier elimination test.

3.3 Theorem. *Let $\mathcal{T}$ be an $\mathcal{L}$-theory. The following are equivalent:*

(i) Let $\mathcal{M}, \mathcal{N} \models \mathcal{T}$, $\mathcal{A}$ a common substructure of $\mathcal{M}$ and $\mathcal{N}$, $\phi(w, \overline{v})$ a quantifier-free $\mathcal{L}$-formula, and $\overline{a} \in A$. If $\mathcal{M} \models \exists x\ \phi(x, \overline{a})$, then $\mathcal{N} \models \exists x\ \phi(x, \overline{a})$.

(ii) $\mathcal{T}$ has quantifier elimination.

Proof. (i) $\Rightarrow$ (ii): Considering Lemma 3.2, it suffices to show that for an $\mathcal{L}$-formula $\exists x\ \phi(x, \overline{v})$, where $\phi(x, \overline{v})$ is quantifier-free, there is a quantifier-free $\mathcal{L}$-formula $\psi(\overline{v})$ such that it holds $\mathcal{T} \models \forall \overline{v}\ (\exists x\ \phi(x, \overline{v}) \leftrightarrow \psi(\overline{v}))$. So, suppose that there are two models $\mathcal{M}, \mathcal{N} \models \mathcal{T}$, a common substructure $\mathcal{A}$ of $\mathcal{M}$ and $\mathcal{N}$, and a tuple $\overline{a} \in A$. Suppose further that $\mathcal{M} \models \exists x\ \phi(x, \overline{a})$. Then, by our assumption, it follows that $\mathcal{N} \models \exists x\ \phi(x, \overline{a})$. Since $\mathcal{M}$ and $\mathcal{N}$ are interchangeable, this is an equivalence. Therefore, we may apply Lemma 3.1 and conclude that $\mathcal{T}$ has quantifier elimination.

(ii) $\Rightarrow$ (i): Suppose that $\mathcal{T}$ eliminates quantifiers. Let $\mathcal{M}, \mathcal{N}$, and $\mathcal{A}$ be defined as above. Let $\phi(w, \overline{v})$ be quantifier-free. By quantifier elimination there exists a quantifier-free formula $\psi(\overline{v})$, such that $\mathcal{T} \models \forall \overline{v}\ (\exists x\ \phi(x, \overline{v}) \leftrightarrow \psi(\overline{v}))$. Let $\overline{a} \in A$. We obtain

$$\begin{aligned}
\mathcal{M} \models \exists x\ \phi(x, \overline{a}) \quad &\Leftrightarrow \quad \mathcal{M} \models \psi(\overline{a}) && \text{because } \mathcal{M} \models \mathcal{T} \\
&\Leftrightarrow \quad \mathcal{A} \models \psi(\overline{a}) && \text{by Lemma 2.2} \\
&\Leftrightarrow \quad \mathcal{N} \models \psi(\overline{a}) && \text{again by Lemma 2.2} \\
&\Leftrightarrow \quad \mathcal{N} \models \exists x\ \phi(x, \overline{a}) && \text{because } \mathcal{N} \models \mathcal{T}.
\end{aligned}$$

□

In the following two sections we will apply this test to two well-known examples for theories that allow quantifier elimination.

3.2 Algebraically Closed Fields

We will assume that the reader already knows enough about algebraically closed fields to follow the proof of quantifier elimination for the theory of algebraically closed fields. Nevertheless, we will prove one statement that will be the crucial point at the very end of the proof.

3.4 Lemma. *Every algebraically closed field has infinitely many elements.*

Proof. Assume that there was a finite algebraically closed field $K = \{a_1, a_2, \ldots, a_n\}$ with n elements. Let $f \in K[X]$ be the polynomial

$$f = \prod_{i=1}^{n} (X - a_i),$$

which vanishes on every element of K. Now consider the polynomial $g = f + 1$. One can easily see that g does not have any root in K, which is a contradiction to the fact that K is algebraically closed. □

3.5 Definition. Let $\mathcal{L}$ be the language of rings $\langle +, -, \cdot; 0, 1\rangle$, where "$-$" will throughout the thesis always denote the binary relation of substraction. The theory ACF of algebraically closed fields is axiomatized by the following axioms:

- the field axioms:

  K1: $\neg 0 \doteq 1$
  K2: $\forall x \forall y \forall z\ (x + (y + z) \doteq (x + y) + z)$
  K3: $\forall x\ (x + 0 \doteq x)$
  K4: $\forall x\ (x + (-x) \doteq 0)$
  K5: $\forall x \forall y \forall z\ (x \cdot (y \cdot z) \doteq (x \cdot y) \cdot z)$
  K6: $\forall x\ (x \cdot 1 \doteq x)$
  K7: $\forall x \exists y\ (x \doteq 0 \vee x \cdot y \doteq 1)$
  K8: $\forall x \forall y\ (x \cdot y \doteq y \cdot x)$
  K9: $\forall x \forall y \forall z\ ((x + y) \cdot z \doteq (x \cdot z) + (y \cdot z))$

- every monic polynomial has a zero:

  AKn: $\forall x_0 \forall x_1 \ldots \forall x_n \exists y\ y^{n+1} + x_n y^n + \ldots + x_1 y + x_0 \doteq 0$ for each $n \in \mathbb{N}$.

In axiom **AKn** we used a simplified notation: As it is generally kept in mathematics, we usually relinquish the function symbol $\cdot$ of multiplication, and we write x^n instead of $\underbrace{x \cdot \ldots \cdot x}_{n \text{ times}}$.

We will now show by using Theorem 3.3 that ACF eliminates quantifiers.

3.6 Theorem. *The theory ACF of algebraically closed fields admits quantifier elimination.*

Proof. Let $\mathcal{F}_1, \mathcal{F}_2 \models \text{ACF}$, $\mathcal{A}$ a common substructure of $\mathcal{F}_1$ and $\mathcal{F}_2$. Then $\mathcal{A}$ is a model of the universal theory $\text{ACF}_\forall$. Let us investigate what that means for $\mathcal{A}$: Since in the language $\mathcal{L}$, there is $+$ and $\cdot$, it will be closed under addition and multiplication, and $-$ guarantees the existence of additive inverse elements. Hence, $\mathcal{A}$ is a ring. Since it is a subring of the fields $\mathcal{F}_1$ and $\mathcal{F}_2$, it is even an integral domain. This allows us to form the field of fractions, $\text{Quot}(A)$. Since $\text{Quot}(A)$ is the smallest field which contains $\mathcal{A}$, we obtain $\text{Quot}(A) \subseteq \mathcal{F}_1, \mathcal{F}_2$. Let $\widetilde{\mathcal{F}}$ be the algebraic closure of $\text{Quot}(A)$. Since $\mathcal{F}_1$ and $\mathcal{F}_2$ are two algebraically closed fields, this directly yields that $\widetilde{\mathcal{F}} \subseteq \mathcal{F}_1, \mathcal{F}_2$.

Let $\phi(x, \overline{y})$ be a quantifier-free $\mathcal{L}$-formula and $\overline{a} \in A$. Assume that $\mathcal{F}_1 \models \exists x\ \phi(x, \overline{a})$. We wish to show $\mathcal{F}_2 \models \exists x\ \phi(x, \overline{a})$ in order to apply Theorem 3.3. Without loss of generality, we can assume that

$$\phi(x, \overline{a}) = \bigvee_{i=1}^{N} \underbrace{\left(\bigwedge_{j=1}^{n_i} \phi_{ij}(x, \overline{a}) \right)}_{=:\phi_i(x, \overline{a})},$$

where each $\phi_{ij}(x, \overline{a})$ is of the form $p_{ij}(x) = 0$ or $q_{ij}(x) \neq 0$ for polynomials p_{ij} and q_{ij} in the variable X whose coefficients are themselves polynomials in the constants $\overline{a}$ occurring in ϕ with integer coefficients. Note that thus $p_{ij}(X), q_{ij}(X) \in A[X]$. Further note that the cases $m = 0$ and $n_i = 0$ are not excluded.

Since $\exists x\ \phi(x, \overline{a})$ is logically equivalent to $\exists x\ \phi_1(x, \overline{a}) \vee \ldots \vee \exists x\ \phi_m(x, \overline{a})$ and because of our assumption $\mathcal{F}_1 \models \exists x\ \phi(x, \overline{a})$, we may as well assume that $\mathcal{F}_1 \models \exists x\ \phi_1(x, \overline{a})$. If we show that

$\mathcal{F}_2 \models \exists x\ \phi_1(x, \overline{a})$, then it follows naturally that $\mathcal{F}_1 \models \exists x\ \phi(x, \overline{a})$. We distinguish the following two cases:

Case 1: Suppose that at least one of the $p_{1,j}$ is not the zero polynomial in $A[X]$, say $p_{1,1} \neq 0$. Then there is $b \in F$ such that $\mathcal{F}_1 \models \phi_1(b, \overline{a})$, in particular $p_{1,1}(b) = 0$. But any root of $p_{1,1}$ is already contained in $\widetilde{F}$. Thus, $b \in \widetilde{F}$ and hence, $\widetilde{\mathcal{F}} \models \exists x\ \phi_1(x, \overline{a})$. This yields $\widetilde{\mathcal{F}} \models \exists x\ \phi(x, \overline{a})$, and therefore $\mathcal{F}_2 \models \exists x\ \phi(x, \overline{a})$.

Case 2: If, on the other hand, all terms $p_{1,j}$ are equal to the zero polynomial or if there is no term $p_{1,j}(x) = 0$ in $\phi_1(x, \overline{a})$, then it suffices to find an element $b \in \widetilde{F}$ that differs from all the zeros of the polynomials $q_{1,j}$. One such b does, indeed, exist, since there are only finitely many zeros of the $q_{1,j}$ and, as an algebraically closed field, by Theorem 3.4, $\widetilde{F}$ has infinitely many elements. Therefore we obtain $\widetilde{\mathcal{F}} \models \exists x\ \phi_1(x, \overline{a})$, i.e. $\widetilde{\mathcal{F}} \models \exists x\ \phi(x, \overline{a})$ and, hence, also $\mathcal{F}_2 \models \exists x\ \phi(x, \overline{a})$. □

3.3 Real Closed Fields

Tarski gave an explicit algorithm for eliminating quantifiers in the theory of real closed fields. This is the theory of the field of the reals, which is equipped with a natural order.

In this section we will review some of the necessary results on real closed fields which we will later on use to prove quantifier elimination. We start with some basic notion:

3.7 Definition. An *ordering* on a field K is a total order relation $\leq$ such that for all $a, b, c \in K$ it holds that

$$\begin{aligned} a \leq b &\quad\Rightarrow\quad a + c \leq b + c \qquad \text{and} \\ a \leq b \ \wedge\ c \geq 0 &\quad\Rightarrow\quad ac \leq bc. \end{aligned}$$

An *ordered field* $(K, \leq)$ is a field K, equipped with an ordering $\leq$. If the order is clear, however, we just write K.

3.8 Definition. We say that a field K is *real* if it has an ordering $\leq$. For an ordered field $(K, \leq)$, the subset $P = \{x \in K :\ x \geq 0\}$ is called the *positive cone* of $(K, \leq)$.

Equivalently we could say that a field K is called real, if -1 cannot be written as a sum of squares in K. We are familiar with $\mathbb{Q}$ and $\mathbb{R}$ as real fields with their natural orderings. But also the field of rational functions in one variable over $\mathbb{Q}$ is real. In fact, if R is any ordered field, then $R(t)$, the field of rational functions in one variable over R, also admits an ordering.

3.9 Definition. An ordered field R is *real closed* if R is real and does not admit any proper algebraic extension which is real itself and whose ordering extends the ordering on R.

Usually real closed fields are denoted by the letter R. We will stick to this convention. There are many equivalent formulations of a definition for real closed fields:

3.10 Lemma. *Let R be a field. Then the following are equivalent:*

(i) R is real closed.
(ii) There is an ordering on R which cannot be extended to any proper algebraic extension of R.

(iii) *There is an ordering of R whose positive cone is $R^2 = \{a^2 : a \in R\}$, and every polynomial of $R[X]$ of odd degree has a root in R.*

(iv) *R is real, for every $a \in R$, either a or $-a$ is a square in R, and every polynomial of $R[X]$ of odd degree has a root in R.*

Proof. See [KnSc, Section 1.5, Satz 1 and Bemerkung] for a proof. □

3.11 Lemma. *If R is a real closed field, then $R(\sqrt{-1})$ is algebraically closed.*

Proof. A proof, which is due to Carl Friedrich Gauß, can be found in [KnSc, Section 1.5, Theorem 2]. □

Lemma 3.10(iii) immediately yields that the ordered field of real numbers $\mathbb{R}$ is real closed. From Lemma 3.11 we deduce the Intermediate Value Theorem for real closed fields:

3.12 Theorem (Intermediate Value Theorem)**.** *Let R be a real closed field, $f \in R[t]$, $a, b \in R$ with $a < b$. If $f(a) \cdot f(b) < 0$, then the number of zeros in the interval $]a, b[$ is odd. In particular, there exists $x \in]a, b[$ such that $f(x) = 0$.*

Proof. Let $a_1 \leq \ldots \leq a_r$ be the roots of f. By Lemma 3.11, the degree of the field extension $[R(\sqrt{-1}) : R]$ is 2, i.e. the irreducible factors of f are either linear or quadratic polynomials. Hence, f is of the form $f = c \cdot (t - a_1) \cdot \ldots \cdot (t - a_r) \cdot p_1(t) \cdot \ldots \cdot p_s(t)$, where c is a unit in R and $p_1, \ldots, p_s$ are irreducible monic quadratic polynomials. Since the p_k only take positive values, we obtain

$$-1 = \operatorname{sign}\frac{f(a)}{f(b)} = \prod_{i=1}^{r} \operatorname{sign}\frac{a - a_i}{b - a_i}.$$

Thus, the number of a_i with $a < a_i < b$ is odd. □

3.13 Definition. A *real closure* of an ordered field K is a real closed field $R \supseteq K$, such that R is algebraic over K and the order on R extends the order on K.

3.14 Lemma. *Every ordered field K has a real closure. If R and R' are two real closures of K, there is one unique order-preserving K-isomorphism between R and R'. Thus, we speak of* the *real closure of K.*

Proof. We only sketch the proof of the first statement: For an ordered field $(K, \leq)$ one needs to apply Zorn's lemma to the set

$$\mathfrak{L} = \{L \supseteq K : L \text{ is an ordered field, } L \text{ is algebraic over } K, \text{ and extends the order on } K\}$$

and verify that the maximal element of $\mathfrak{L}$ is indeed real closed. The proof of the second part needs some more machinery. The whole proof of the lemma can be found in detail, for example, in [BoCoRo, Theorem 1.3.2]. □

3.15 Lemma. *Let R be a real closed field, $K \subseteq R$ a subfield, and $\widetilde{K}$ the relative algebraic closure of K in R, i.e. $\widetilde{K} = \{x \in R : x \text{ is algebraic over } K\}$. Then $\widetilde{K}$ is real closed.*

Proof. We will verify version (iv) of Lemma 3.10. Since $\widetilde{K}$ is a subfield of R, we can restrict the ordering on R to $\widetilde{K}$. Hence, $\widetilde{K}$ is real. Now let $a \in \widetilde{K}$. We may assume that $a \geq 0$, as otherwise we can consider $-a$ instead. Since R is real closed, the quadratic polynomial $X^2 - a \in \widetilde{K}[X] \subseteq R[X]$ has a root $b \in R$. As b is algebraic over $\widetilde{K}$, it is also algebraic over K, and thus contained in $\widetilde{K}$. A similar argument can be applied to any polynomial in $\widetilde{K}[X]$ of odd degree to show that it has a root in $\widetilde{K}$. □

After giving an axiomatization of the theory of real closed fields, we are ready to prove quantifier elimination.

3.16 Definition. Let $\mathcal{L}$ be the language of ordered rings $\langle +, -, \cdot; <; 0, 1\rangle$. The theory of RCF of real closed fields is axiomatized by the following axiom system:

- the field axioms **K1** to **K9**,
- the order axioms:

  O1: $\forall x\, \neg x < x$
  O2: $\forall x \forall y \forall z\, ((x < y \wedge y < z) \rightarrow x < z)$
  O3: $\forall x \forall y\, (x < y \vee x = y \vee y < x)$
  O4: $\forall x \forall y \forall z\, (x < y \rightarrow x + z < y + z)$
  O5: $\forall x \forall y\, ((0 < x \wedge 0 < y) \rightarrow 0 < x \cdot y)$

- positive elements are squares:

  RK1: $\forall x\, (0 < x \;\rightarrow\; \exists y\, x = y^2)$

- polynomials of odd degree have zeros: For each $n \in \mathbb{N}$ we have:

  RK2*n*: $\forall x_0 \forall x_1 \ldots \forall x_{2n}\, \exists y\, y^{2n+1} + x_{2n} y^{2n} + x_{2n-1} y^{2n-1} + \ldots + x_1 y + x_0 = 0.$

Note that in the language of ordered rings we use $<$ for the order relation while in the definition of ordered fields it is common to use $\leq$. This does not cause any difficulties though, as the two symbols are interdefinable.

Using the criterion of Theorem 3.3 again, we will now show quantifier elimination for real closed fields. The proof is very similar to the one of Theorem 3.6.

3.17 Theorem. *The theory of real closed fields* RCF *admits quantifier elimination.*

Proof. Let $\mathcal{B}_1, \mathcal{B}_2 \models \mathrm{RCF}$ and $\mathcal{A}$ a common substructure of both $\mathcal{B}_1$ and $\mathcal{B}_2$. Let $\phi(x, \overline{y})$ be a quantifier-free $\mathcal{L}$-formula and $\overline{a} \in A$ such that $\mathcal{B}_1 \models \exists x\, \phi(x, \overline{a})$. By Theorem 3.3 we need to show that this implies $\mathcal{B}_2 \models \exists x\, \phi(x, \overline{a})$.

Without loss of generality, $\phi(x, \overline{y})$ only uses the logical operators $\wedge, \vee$, and $\neg$ such that $\neg$ only occurs in front of atomic formulas. Atomic formulas have the form $0 \doteq p(x)$ or $0 < q(x)$, where p and q are polynomials in the variable X whose coefficients are again polynomials in the constants $a_1, \ldots, a_n$ with integer coefficients. Moreover, we can replace $\neg p(x) \doteq 0$ by the expression $(0 < p(x) \;\vee\; 0 < -p(x))$ and $\neg 0 < q(x)$ by $(0 \doteq q(x) \;\vee\; 0 < -q(x))$. Therefore, we can assume that $\phi(x, \overline{a})$ only uses $\wedge$ and $\vee$ as logical connectives. So we have

$$\phi(x, \overline{a}) = \bigvee_{i=1}^{N} \underbrace{\left(\bigwedge_{j=1}^{n_i} \phi_{ij}(x, \overline{a}) \right)}_{=:\phi_i(x, \overline{a})},$$

where $\phi_{ij}(x, \overline{a})$ is of the form $p(x) \doteq 0$ or $0 < q(x)$. The formula $\exists x\, \phi(x, \overline{a})$ is logically equivalent to $\exists x\, \phi_1(x, \overline{a}) \vee \ldots \vee \exists x\, \phi_m(x, \overline{a})$. Because $\mathcal{B}_1 \models \exists x\, \phi(x, \overline{a})$, without loss of generality suppose that $\mathcal{B}_1 \models \exists x\, \phi_1(x, \overline{a})$. We now show that $\mathcal{B}_2 \models \exists x\, \phi_1(x, \overline{a})$, since this implies $\mathcal{B}_2 \models \exists x\, \phi(x, \overline{a})$.

We know that $\phi_1(x, \overline{a})$ is of the form

$$\bigwedge_{k=1}^{s} q_k(x) > 0 \;\wedge\; \bigwedge_{k=s+1}^{n_1} p_k(x) \doteq 0.$$

In ordered fields, it holds that $p_{s+1}(x) = 0, \ldots, p_{n_1}(x) = 0$ if and only if the sum of all squares vanishes, i.e. $\sum_{k=s+1}^{n_1} p_k(x)^2 = 0$. Therefore, $\phi_1(x, \overline{a})$ even has the form

$$\bigwedge_{k=1}^{s} q_k(x) > 0 \ \wedge \ p(x) \doteq 0,$$

where $p(x) := \sum_{k=s+1}^{n_1} p_k(x)^2$. That means

$$\mathcal{B}_1 \models \exists x \left(\bigwedge_{k=1}^{s} q_k(x) > 0 \ \wedge \ p(x) = 0 \right).$$

Since $\mathcal{A}$ is a substructure, it is, again, a subring of a field, hence, an integral domain. Let $\mathrm{Quot}(A)$ be its field of fractions and let $\mathcal{R}_1$ and $\mathcal{R}_2$ be the relative algebraic closures of $\mathrm{Quot}(A)$ in $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively. By Lemma 3.15, $\mathcal{R}_1$ and $\mathcal{R}_2$ are also real closed, i.e. $\mathcal{R}_1 \models \mathrm{RCF}$ and $\mathcal{R}_2 \models \mathrm{RCF}$. By Lemma 3.14, $\mathcal{R}_1$ and $\mathcal{R}_2$ are isomorphic, so we will identify them with each other and just write $\mathcal{R}$ instead. Because $\mathcal{B}_1 \models \exists x \, \phi_1(x, \overline{a})$, there exists $\alpha \in B_1$ such that

$$\mathcal{B}_1 \models \bigwedge_{k=1}^{s} q_k(\alpha) > 0 \ \wedge \ p(\alpha) \doteq 0.$$

We will show that there exists $b \in R$ such that

$$\mathcal{R} \models \bigwedge_{k=1}^{s} q_k(b) > 0 \ \wedge \ p(b) \doteq 0,$$

because in this case it follows $\mathcal{R} \models \exists x \ \phi_1(x, \overline{a})$ and therefore also $\mathcal{B}_2 \models \exists x \ \phi_1(x, \overline{a})$, since $b \in R \subseteq B_2$. We distinguish the following two cases:

Case 1: p is not the zero-polynomial in $R[X]$. Since $\mathcal{R}$ is relatively algebraically closed in $\mathcal{B}_1$, it holds that $\alpha \in R$, so $\alpha \in B_2$ and we are done.

Case 2: p is the zero-polynomial in $R[X]$ or $s = n_1$ which means that there is no condition $p = 0$ in ϕ_1. If the $q_1, \ldots, q_s$ do not have any zeros in R, then they do not change sign and it holds for all $b \in R$ that $q_k(b) > 0$. Otherwise, let $\beta_1 < \ldots < \beta_t$ be the zeros of $q_1, \ldots, q_s$ in R. We have one of the following situations:

(1) $\alpha < \beta_1$,
(2) $\beta_i < \alpha < \beta_{i+1}$ for some $i \in \{1, \ldots, t-1\}$,
(3) $\beta_t < \alpha$.

Note that α is not a zero of any q_k. In situation (1) choose $b = \beta_1 - 1 \in R$. In (2) take $b = \frac{1}{2}(\beta_i + \beta_{i+1}) \in R$. And in the last situation (3), $b = \beta_t + 1 \in R$ will do.

It follows from the Intermediate Value Theorem 3.12 for $\mathcal{B}_1$ that $q_k(b) > 0$ for all $k = 1, \ldots, s$. If not, there would be another zero between b and one β_i in R, not included in $\{\beta_1, \ldots, \beta_t\}$, a contradiction. Hence, b satisfies $\exists x \, \phi_1(x, \overline{a})$ and this yields $\mathcal{B}_2 \models \exists x \, \phi(x, \overline{a})$. □

4 Quantifier Elimination by Algebraically Prime Models

4.1 Algebraically Prime Models and Simple Closedness

For this section we use the terminology that David Marker uses in [Mar02]. The notion of algebraically prime models and simple closedness is not common otherwise in the literature. For the following quantifier elimination test there is nothing really new happening in this section. It will, however, be handy to prove quantifier elimination of Presburger Arithmetic.

4.1 Definition. A theory $\mathcal{T}$ has *algebraically prime models* if for any $\mathcal{A} \models \mathcal{T}_\forall$ there is $\widetilde{\mathcal{A}} \models \mathcal{T}$ and an $\mathcal{L}$-embedding $i : \mathcal{A} \to \widetilde{\mathcal{A}}$ such that for all $\mathcal{N} \models \mathcal{T}$ and $\mathcal{L}$-embeddings $j : \mathcal{A} \to \mathcal{N}$ there is an $\mathcal{L}$-embedding $h : \widetilde{\mathcal{A}} \to \mathcal{N}$ such that $j = h \circ i$.

4.2 Definition. Let $\mathcal{M}, \mathcal{N} \models \mathcal{T}$, where $\mathcal{M} \subseteq \mathcal{N}$. We call $\mathcal{M}$ *simply closed* in $\mathcal{N}$ if for any quantifier-free formula $\phi(\overline{v}, w)$ and any $\overline{a} \in M$, if $\mathcal{N} \models \exists x\ \phi(\overline{a}, x)$ then $\mathcal{M} \models \exists x\ \phi(\overline{a}, x)$.

The following quantifier elimination test can be found in [Mar02, Corollary 3.1.12] and the proof is a modification of the proof of [Mar02, Theorem 3.1.9].

4.3 Theorem. *Suppose that $\mathcal{T}$ is an $\mathcal{L}$-theory such that*

(i) $\mathcal{T}$ has algebraically prime models,
(ii) whenever $\mathcal{M} \subseteq \mathcal{N}$ are models of $\mathcal{T}$, $\mathcal{M}$ is simply closed in $\mathcal{N}$.

Then $\mathcal{T}$ has quantifier elimination.

Proof. We are going to use the quantifier elimination test from Theorem 3.3: Let $\mathcal{T}$ be an $\mathcal{L}$-theory as above. Let $\phi(\overline{v}, x)$ be a quantifier-free formula, $\mathcal{M}, \mathcal{N} \models \mathcal{T}$, $\mathcal{A}$ a common substructure of $\mathcal{M}$ and $\mathcal{N}$, $\overline{a} \in A$, $b \in M$ such that $\mathcal{M} \models \phi(\overline{a}, b)$. We want to show that there is $c \in N$ such that $\mathcal{N} \models \phi(\overline{a}, c)$. For simplicity reasons we suppose without loss of generality that $\mathcal{A}$ is not only a substructure of $\mathcal{M}$ and $\mathcal{N}$ but also properly contained in both such that the substructure embeddings are the identity map.

By Lemma 2.13 we know that $\mathcal{A} \models \mathcal{T}_\forall$. Since $\mathcal{T}$ has algebraically prime models, there is $\widetilde{\mathcal{A}} \models \mathcal{T}$ and an $\mathcal{L}$-embedding $i : \mathcal{A} \to \widetilde{\mathcal{A}}$ such that for all $\mathcal{B} \models \mathcal{T}$ and $\mathcal{L}$-embeddings $j : \mathcal{A} \to \mathcal{B}$ there is an $\mathcal{L}$-embedding $h : \widetilde{\mathcal{A}} \to \mathcal{B}$ such that $j = h \circ i$. In particular, by setting $\mathcal{B} = \mathcal{N}$, we obtain an $\mathcal{L}$-embedding $\beta : \widetilde{\mathcal{A}} \to \mathcal{N}$ such that $\beta \circ i = \mathrm{id}$. Similarly by setting $\mathcal{B} = \mathcal{M}$ we get $\alpha : \widetilde{\mathcal{A}} \to \mathcal{M}$ such that $\alpha \circ i = \mathrm{id}$.

As $\widetilde{\mathcal{A}} \models \mathcal{T}$, $\mathcal{M} \models \mathcal{T}$ and $\widetilde{\mathcal{A}} \subseteq \mathcal{M}$, $\widetilde{\mathcal{A}}$ is simply closed in $\mathcal{M}$. Moreover, we have $i(\overline{a}) \in \widetilde{A}$ and $\alpha(i(\overline{a})) = \overline{a} \in M$. By assumption we have $\mathcal{M} \models \exists x\ \phi(\overline{a}, x)$. Hence, by simple closedness, it

follows $\widetilde{\mathcal{A}} \models \exists x\ \phi(i(\overline{a}), x)$. Now by applying β this yields $\widetilde{\mathcal{A}} \models \exists x\ \phi(\overline{a}, x)$. Thus, we have shown that there exists an element, say $c \in N$, such that $\mathcal{N} \models \phi(\overline{a}, c)$.

So, by Theorem 3.3, $\mathcal{T}$ has quantifier elimination. □

4.2 Presburger Arithmetic

Presburger Arithmetic is formally defined as the theory of the natural numbers with addition. It is due to Mojzesz Presburger and, therefore, named after him Presburger Arithmetic. As it completely omits multiplication, it is much weaker than Peano Arithmetic, which includes both addition and multiplication. It cannot define terms such as prime numbers or divisibility by a variable, for instance. But, unlike Peano Arithmetic, it is a complete and decidable theory. We will come back to this concept in Chapter 7.

Let $\mathcal{L}$ be the language $\langle +, -; <; 0, 1\rangle$. Roughly speaking, Presburger Arithmetic is the theory of the ordered group of integers. It does not have quantifier elimination in the language $\mathcal{L}$. The problem is formulas of the following type

$$\phi(x) = \exists y\ (x \doteq \underbrace{y + \ldots + y}_{n \text{ times}}),$$

which asserts that x is divisible by n. Once having defined properly what Pr, the theory of Presburger Arithmetic, is, we will show that the above formula is not equivalent to a quantifier-free $\mathcal{L}$-formula.

If we add predicates for being divisible by some integer n to the language $\mathcal{L}$, however, quantifier elimination is admitted in the extended language. Thus, let P_n be a unary predicate which we interpret as "the element is divisible by n" and let $\mathcal{L}^* = \mathcal{L} \cup \{P_n :\ n = 2, 3, \ldots\}$ be the extended language. Since we only add predicates for sets that one can already define in $\mathcal{L}$, we do not change the definable sets by extending the language.

There is another axiomatization of Pr than the one that we will give in the following, see for instance [Poi, page 115]. We follow [Mar02, page 82].

4.4 Definition. The $\mathcal{L}^*$-theory Pr for *Presburger Arithmetic* is axiomatized by the following axiom system:

- axioms for Abelian groups,

  AG1: $\forall x\ (0 + x \doteq x + 0 \doteq x)$
  AG2: $\forall x \forall y \forall z\ (x + (y + z) \doteq (x + y) + z)$
  AG3: $\forall x\ (x - x \doteq 0)$
  AG4: $\forall x \forall y\ (x + y \doteq y + x)$

- the order axioms **O1**, **O2**, **O3** and **O4**

- and additionally:

  P1: $0 < 1$
  P2: $\forall x\ (x \leq 0\ \vee\ x \geq 1)$
  P3*n*: $\forall x \left(P_n(x) \leftrightarrow \exists y\ (x \doteq \underbrace{y + \ldots + y}_{n \text{ times}})\right)$ for $n = 2, 3, \ldots$

$$\textbf{P4}\boldsymbol{n}\textbf{:} \quad \forall x \left(\bigvee_{i=0}^{n-1} \left(P_n(x + \underbrace{1 + \ldots + 1}_{i \text{ times}}) \wedge \bigwedge_{j \neq i} \neg P_n(x + \underbrace{1 + \ldots + 1}_{j \text{ times}}) \right) \right) \text{ for } n = 2, 3, \ldots$$

Without adding the predicates P_n to the language, the above formula $\phi(x)$ is not equivalent in the theory to a quantifier-free formula. Let Pr' be the $\mathcal{L}$-theory which is defined by the same axioms as Pr, except for $\mathbf{P3}\boldsymbol{n}$ and $\mathbf{P4}\boldsymbol{n}$, since they require the predicates P_n, which are not in the language $\mathcal{L}$. The following proposition shows that the $\mathcal{L}$-theory Pr' does not admit elimination of quantifiers in $\mathcal{L}$:

4.5 Proposition. *In* Pr'*, the formula* $\exists x\ (y = x + x)$ *is not equivalent to a quantifier-free* $\mathcal{L}$*-formula.*

Proof. Consider the group $\mathcal{G} := \mathbb{Z}[\omega]$, which is generated by the integers and an infinite element ω, and $\mathcal{H} := \mathbb{Z}[\omega/2]$, both equipped with the usual addition. Then $\mathcal{G} \subseteq \mathcal{H}$. Note that in H, there is an element x such that $\omega = x + x$, namely $\omega/2$. In G, however, there is no such element.

Now let us suppose that there is a quantifier-free $\mathcal{L}$-formula $\psi(v)$ such that it holds $\mathrm{Pr} \models \forall y\ (\exists x\ y = x + x \leftrightarrow \psi(y))$. As one can quickly check with the axiomatization of Presburger Arithmetic, $\mathcal{G}$ and $\mathcal{H}$ are both models of Pr. Hence, $\mathcal{H} \models \forall y\ (\exists x\ y = x + x \leftrightarrow \psi(y))$ and $\mathcal{G} \models \forall y\ (\exists x\ y = x + x \leftrightarrow \psi(y))$. Now we are in one of the following two cases:

Case 1: $\mathcal{H} \models \psi(\omega)$. Equivalently one has $\mathcal{H} \models \exists x\ \omega = x + x$. As $\mathcal{G}$ is a substructure of $\mathcal{H}$ and $\psi(\omega)$ is quantifier-free, we also obtain $\mathcal{G} \models \psi(\omega)$, which holds if and only if $\mathcal{G} \models \exists x\ \omega = x + x$. But, as we have noted in the beginning, $\exists x\ \omega = x + x$ holds in $\mathcal{H}$ but not in $\mathcal{G}$. Hence, we are in the second case:

Case 2: $\mathcal{H} \models \neg\psi(\omega)$, i.e. $\mathcal{H} \models \neg\exists x\ \omega = x + x$. Analogously it follows $\mathcal{G} \models \neg\psi(\omega)$, and thus, $\mathcal{G} \models \neg\exists x\ \omega = x + x$. Again, this leads to a contradiction. □

Hence, it makes sense that, in order to admit quantifier elimination, the language needs to be extended by the predicates P_n.

Even though multiplication is not part of the language, we will occasionally write something like $n \cdot x$, where n is an integer. For this we do not need the function of multiplication. It is enough to apply addition a certain (integer, of course) number of times. Hence $n \cdot x$ means nothing else than adding n copies of x together. Also, something like division is not defined in Pr. But one can show that if an element is divisible by some integer, then the division is unique:

4.6 Lemma. *Let* $\mathcal{G} \models \mathrm{Pr}$ *be a model,* $m \in \mathbb{Z}$ *an integer and* $y \in G$ *such that* $\mathcal{G} \models P_m(y)$*. Then there is a unique* $x \in G$ *such that* $\underbrace{x + \ldots + x}_{m \text{ times}} = y$*.*

Proof. Suppose there are two elements x and x' such that $m \cdot x = m \cdot x'$. Then it also holds $2m \cdot x = 2m \cdot x'$. After an easy manipulation we obtain $m \cdot (x - x') = -m \cdot (x - x')$. Since the left hand side is the negative of the right hand side, this yields that $m \cdot (x - x') = 0$. As we work in ordered groups, which are torsion free, it follows that $x = x'$. Hence, dividing by an integer gives a unique solution. □

In Presburger Arithmetic, it is not as easy to see what the universal theory $\mathrm{Pr}_\forall$ looks like. So we will first check how it can be defined. This will be used afterwards in the proof to show

quantifier elimination for Pr. Let us define a theory $\mathcal{T}$ for which we show that it is, indeed, $\mathrm{Pr}_\forall$. Of course, the axioms **AG1**, **AG2**, **AG3**, **AG4**, **O1**, **O2**, **O3**, **O4**, **D1**, **D2**, and **D4*n*** are universal.

4.7 Definition. Define the theory $\mathcal{T}$ by the following axioms:

- the axioms **AG1**, **AG2**, **AG3**, **AG4**, **O1**, **O2**, **O3**, **O4**, **P1**, **P2**, **P4*n***
- together with:

T1: $\forall x \forall y\ ((P_n(x) \wedge P_n(y)) \ \rightarrow \ P_n(x+y))$,
T2: $\forall x \forall y\ ((P_n(x) \wedge P_n(y)) \ \rightarrow \ P_n(x-y))$,
T3: $\forall x \forall y\ \Big((\underbrace{y+\ldots+y}_{n \text{ times}} \doteq x) \rightarrow P_n(x)\Big)$,
T4: for all n dividing m: $\forall x\ (P_m(x) \rightarrow P_n(x))$,
T5: for all $k, n = 2, 3, \ldots$: $\forall x\ \Big(P_n(x) \rightarrow P_{kn}(\underbrace{x+\ldots+x}_{k \text{ times}})\Big)$.

The first two axioms ensure that the P_n are closed under addition and subtraction. Together with axiom **T5** it follows that the P_n are additive subgroups.

For the next 3 lemmas and proofs, we follow [Mar02, Lemma 3.1.9 and Lemma 3.1.20].

4.8 Lemma. *The above defined theory $\mathcal{T}$ axiomatizes the universal theory* $\mathrm{Pr}_\forall$.

Proof. It is easy to see that $\mathcal{T} \subseteq \mathrm{Pr}_\forall$, i.e. that each model of $\mathrm{Pr}_\forall$ is also a model of $\mathcal{T}$. We need to show the other implication. Let $\mathcal{G}$ be a model of $\mathcal{T}$. We will show that there is $\mathcal{H} \supseteq \mathcal{G}$, where $\mathcal{H} \models \mathrm{Pr}$. Then, by Lemma 2.13, the claim follows. Hence, let

$$H := \left\{ \frac{x}{n} :\ x \in G \text{ and } (n = 1 \text{ or } \mathcal{G} \models P_n(x)) \right\},$$

where $\frac{x}{n}$ is the equivalence class of (x, n) under the equivalence relation $\approx$, where $(y_1, m_1) \approx (y_2, m_2)$ if and only if

$$\underbrace{y_1+\ldots+y_1}_{m_2 \text{ times}} = \underbrace{y_2+\ldots+y_2}_{m_1 \text{ times}}.$$

For each n, let

$$P_n^{\mathcal{H}} := nH := \{\underbrace{h+\ldots+h}_{n \text{ times}} :\ h \in H\}.$$

Consider the $\mathcal{L}^*$-structure $\mathcal{H} := \langle H\,; +, -\,; <, P_n^{\mathcal{H}}\,; 0, 1\rangle$. We first show that $\mathcal{H}$ is an ordered Abelian group: Let $x/m, y/n \in H$. If both m and n are equal to 1, we are already done. We only show the case where neither m nor n is equal to 1, of which the other cases are simplifications. Hence, we assume $m, n \neq 1$. Then $\mathcal{G} \models P_m(x)$ and $\mathcal{G} \models P_n(y)$. By axiom **T5** we obtain $\mathcal{G} \models P_{mn}(nx)$ and $\mathcal{G} \models P_{mn}(my)$. In $\mathcal{H}$, rules as in $\mathbb{Q}$ apply. Since P_{mn} is closed under addition and subtraction, $(nx \pm my)/mn \in H$. Thus, also $\mathcal{H}$ is closed under addition and subtraction. Because the P_n are subgroups of $\mathcal{G}$, they are Abelian. Hence, so is $\mathcal{H}$. The existence of a neutral element and of inverse elements as well as associativity and commutativity is inherited from $\mathcal{G}$. Thus, $\mathcal{H}$ is an Abelian group. For two elements x/m and y/n in H we have $\mathcal{H} \models x/m \leq y/n$ if and only if $\mathcal{G} \models nx \leq my$. Hence $\mathcal{H}$ is an ordered Abelian group.

Let us check the other axioms. Clearly, $\mathcal{H}$ satisfies **P1**. Suppose that there is $x/m \in H$ with $0 < x/m < 1$, thus, $0 < x < m$. Since $x \in G$ and $\mathcal{G}$ fulfills axiom **P2**, $m \neq 1$. This means that

x is some integer from $\{1, 2, \ldots, m-1\}$. But then, because obviously $\mathcal{G} \models P_m(m)$, by axiom **P4*m*** for $\mathcal{G}$ it follows that $\mathcal{G} \models \neg P_m(x)$, which is a contradiction to $x/m \in H$. Hence, axiom **P2** holds. By construction, $P_n^{\mathcal{H}}$ fulfills **P3*n***. It remains to check axiom **P4*n***: Let $x/m \in H$, so $\mathcal{G} \models P_m(x)$. By axiom **P4*mn*** for $x \in G$ there is a unique i with $0 \leq i < mn$ such that $x + i \in P_{mn}^{\mathcal{G}}$. By **T4** it follows $\mathcal{G} \models P_m(x+i)$. Since P_m is a subgroup of $\mathcal{G}$, also $\mathcal{G} \models P_m(i)$. Thus, $i = \ell m$ for some $0 \leq \ell < n$. In H, there is y such that

$$\underbrace{y + \ldots + y}_{mn \text{ times}} = x + \ell m,$$

i.e. $mn \cdot y = x + \ell m$. Dividing by m yields $n \cdot y = x/m + \ell$, which is unique by Lemma 4.6. As i was unique, also ℓ is unique.

Hence, $\mathcal{H}$ fulfills all axioms of Pr, i.e. $\mathcal{H} \models \mathrm{Pr}$. We have now proven that every model of $\mathcal{T}$ can be embedded into a model of Pr. This proves that $\mathcal{T} \models \mathrm{Pr}_\forall$. □

4.9 Theorem. *The theory* Pr *has algebraically prime models.*

Proof. In order to verify the existence of algebraically prime models we need to show that for any $\mathcal{G} \models \mathrm{Pr}_\forall$ there is $\mathcal{H} \models \mathrm{Pr}$ and an $\mathcal{L}^*$-embedding $i : \mathcal{G} \to \mathcal{H}$ such that for all $\mathcal{H}' \models \mathrm{Pr}$ and $\mathcal{L}^*$-embeddings $j : \mathcal{G} \to \mathcal{H}'$ there is an $\mathcal{L}^*$-embedding $h : \mathcal{H} \to \mathcal{H}'$ such that $j = h \circ i$.

Let $\mathcal{G} \models \mathrm{Pr}_\forall$ and $\mathcal{H} \models \mathrm{Pr}$ be defined as in Lemma 4.8. Let $i : \mathcal{G} \to \mathcal{H}$ be the canonical $\mathcal{L}^*$-embedding. Suppose there is another model $\mathcal{H}' \models \mathrm{Pr}$ and an $\mathcal{L}^*$-embedding $j : \mathcal{G} \to \mathcal{H}'$. It remains to show that $\mathcal{H}$ can be embedded over $\mathcal{G}$ into $\mathcal{H}'$.

Let $x/m \in H$ with $\mathcal{G} \models P_m(x)$. Since $\mathcal{G}$ is a substructure of $\mathcal{H}'$ it follows that $\mathcal{H}' \models P_m(x)$. This means, there exists some $y \in H'$ such that

$$\underbrace{y + \ldots + y}_{m \text{ times}} = x,$$

which is unique by Lemma 4.6. Hence, by sending x/m to y we obtain a well-defined map h. To see that it is injective, we check the kernel: If $h(x/m) = 0$, then $m \cdot 0 = x$, i.e. $x = 0$. Thus, $x/m = 0$ and therefore h is injective. The homomorphic properties are easy to check. So, without carrying them out, we may conclude that h is an $\mathcal{L}^*$-embedding of $\mathcal{H}$ into $\mathcal{H}'$ that fixes $\mathcal{G}$. □

4.10 Theorem. *If* $\mathcal{G}, \mathcal{H} \models \mathrm{Pr}$ *are two models with* $\mathcal{G} \subseteq \mathcal{H}$*, then* $\mathcal{G}$ *is simply closed in* $\mathcal{H}$*.*

Proof. Let $\phi(v, \overline{w})$ be a quantifier-free $\mathcal{L}^*$-formula and $\overline{a} \in G$. Suppose that there is $b \in H$ such that $\mathcal{H} \models \phi(b, \overline{a})$. What we need to show is that there exists $c \in G$ such that $\mathcal{G} \models \phi(c, \overline{a})$.

Axiom **P4*n*** states that for fixed n and x, there is $i \in \{0, \ldots, n-1\}$ such that $P_n(x+i)$ and for every $j \in \{0, \ldots, n-1\}$ with $j \neq i$ it holds $\neg P_n(x+j)$. That means that the disjunction in **P4*n*** is actually an exclusive disjunction, i.e. **P4*n*** holds if and only if for all x, exactly one $i \in \{0, \ldots, n-1\}$ fulfills $P_n(x+i)$ and $\neg P_n(x+j)$ for every $j \in \{0, \ldots, n-1\}$ with $j \neq i$. Hence, by axiom **P4*n***, $P_n(x)$ is in Pr equivalent to $\bigwedge_{i=1}^{n-1} \neg P_n(x+i)$. That means $\neg P_n(x)$ is equivalent to $\bigvee_{i=1}^{n-1} P_n(x+i)$. Hence, we may replace all negative occurrences of P_n in $\phi(v, \overline{a})$ by a disjunction of positive occurrences. Let us assume that $\phi(v, \overline{a})$ is already in disjunctive normal

form. Thus, without loss of generality, we obtain

$$\phi(v,\overline{a}) = \bigvee_{i=1}^{N} \Big(\underbrace{\bigwedge_{j=1}^{n_i} \phi_{ij}(v,\overline{a})}_{=:\phi_i(v,\overline{a})} \Big),$$

where the $\phi_{ij}(v,\overline{a})$ are atomic formulas. Since we have $\mathcal{H} \models \exists x\ \phi(x,\overline{a})$, we may assume that $\mathcal{H} \models \exists x\ \phi_1(x,\overline{a})$. All $\mathcal{L}^*$-terms t are of the form $t \doteq mv + g$, where $m \in \mathbb{Z}, g \in G$. Since all models of Pr are discretely ordered, we can replace formulas like $\neg v \doteq 1$ by $v < 1 \ \vee \ 1 < v$. Hence, considering the equivalence $m_1 v + g_1 \doteq m_2 v + g_2 \ \leftrightarrow \ (m_1 - m_2)v \doteq g_2 - g_1$, atomic $\mathcal{L}^*$-formulas are of the forms

$$\begin{aligned} mv &\doteq g, \text{ where } m \in \mathbb{Z}, g \in G, \\ mv &< g, \text{ where } m \in \mathbb{Z}, g \in G, \text{ and} \\ P_k(\ell v + g), &\text{ where } k, \ell \in \mathbb{Z}, g \in G. \end{aligned}$$

In the second formula we may replace $mv < g$ by $v < h$, where h is the least element in G such that $mh \geq g$. Before we explain, why we may make this replacement, we illustrate why such an element h exists: If $\mathcal{G} \models P_m(g)$, then set $h := g/m$. If on the contrary $\mathcal{G} \models \neg P_m(g)$, then by axiom $\mathbf{P4}\boldsymbol{m}$ there is $i \in \{1,\dots,m-1\}$ such that $\mathcal{G} \models P_m(g+i)$. Hence, set $h := (g+i)/m$. Now, to see that we may replace $mv < g$ by $v < h$, assume that $v < h$. Further suppose that, by choice of h, we have $mh \geq g > m(h-1)$. Then $v \leq h-1$, and therefore $g > m(h-1) \geq mv$. Suppose conversely that $v \geq h$. Then, $mv \geq mh \geq g$.

Hence, without loss of generality, we may assume that $\phi_1(v,\overline{a})$ is of the form

$$\bigwedge_{j=1}^{s} P_{k_j}(\ell_j v + h_j) \ \wedge \bigwedge_{j=s+1}^{t} m_j v \doteq g_j \ \wedge \bigwedge_{j=t+1}^{n_1} d_j < v < e_j,$$

where $0 \leq s \leq t \leq n_1$, $k_j, \ell_j, m_j \in \mathbb{Z}$, and $h_j, g_j, d_j, e_j \in G$ for each $1 \leq j \leq n_1$. If there is a part in ϕ_1 of the form $m_j v \doteq g_j$, i.e. if $s < t$ and $m_j \neq 0$ for some j, then $b = g_j/m_j$. Hence, $\mathcal{H} \models P_{m_j}(g_j)$. Since $\mathcal{G} \subseteq \mathcal{H}$, we obtain $\mathcal{G} \models P_{m_j}(g_j)$ and therefore $b \in G$, which means that we are done by setting $c := b$. So, suppose there is no part in ϕ_1 of this form, i.e. that $s = t$. By setting $d := \max\{d_j : \ t+1 \leq j \leq n_1\}$ and $e := \min\{e_j : \ t+1 \leq j \leq n_1\}$ we obtain $d_j \leq d < b < e \leq e_j$ for each $j \in \{t+1,\dots,n_1\}$. Subtracting d yields $0 = d - d < b - d < e - d$. If $e - d$ is finite, i.e. bounded by some natural number, then so is $b - d$. Since $d \in G$ and G is closed under "$+$" and "$-$", it follows $b \in G$. Therefore we will assume that $e - d$ is not finite.

Note that b is a solution to the system of congruences

$$\begin{aligned} \ell_1 v + h_1 &\equiv 0 \bmod k_1 \\ \ell_2 v + h_2 &\equiv 0 \bmod k_2 \\ &\vdots \\ \ell_s v + h_s &\equiv 0 \bmod k_s. \end{aligned}$$

Let $k := \prod_{i=1}^{s} k_i$. Axiom $\mathbf{P4}\boldsymbol{k}$ assures that there exists $z \in \{0,\dots,k-1\}$ such that $\mathcal{G} \models P_k(b-z)$. Then also z is a solution to the system of congruences above. Again by $\mathbf{P4}\boldsymbol{k}$ there is

$q \in \{k, \ldots, 2k-1\}$ such that $\mathcal{G} \models P_k(d+q-z)$. As $e-d$ is infinite, this yields that $d+q<e$ and, thus, $d < d+q < e$. Since $d+q \in G$, by setting $c := d+q$, we have found the desired element: It hold $\mathcal{G} \models P_k(c-z)$. Then c is also a solution to the above system. That means, $\mathcal{G} \models \phi_1(c, \overline{a})$, and thus $\mathcal{G} \models \phi(c, \overline{a})$, as desired. □

4.11 Corollary. *The theory of Presburger Arithmetic admits elimination of quantifiers.*

Proof. By Theorem 4.3, a theory $\mathcal{T}$ eliminates quantifiers if it has algebraically prime models and if for two models $\mathcal{M} \subseteq \mathcal{N}$ of $\mathcal{T}$ then $\mathcal{M}$ is simply closed in $\mathcal{N}$. The two previous theorems show these two conditions. □

5 Quantifier Elimination by Types and Saturation

The next quantifier elimination test is about saturated models. We will develop some theory about types and saturation. These notions were worked out in the 1950s, cf. [Poi, page 63].

5.1 Types and Saturated Models

For this section we follow [Mar02], although we do not presuppose the theory to be complete as it is done in the source. Consider a structure $\mathcal{M}$ with universe M in a language $\mathcal{L}$. Recall from Definition 2.8 that for a subset $A \subseteq M$, $\mathcal{L}_A$ is the language obtained from $\mathcal{L}$ by adding a constant symbol c_a for each $a \in A$ to $\mathcal{L}$. By $\mathrm{Th}_A(\mathcal{M})$ we denote the set of all $\mathcal{L}_A$-sentences which are true in $\mathcal{M}$.

5.1 Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $A \subseteq M$ a subset. For a set p of $\mathcal{L}_A$-formulas in n free variables $v_1, \ldots, v_n$, we call p an *n-type* (over A) if $p \cup \mathrm{Th}_A(\mathcal{M})$ is satisfiable. We say that p is a *complete* n-type if for all $\mathcal{L}_A$-formulas $\phi(\overline{v})$ with free variables taken from $v_1, \ldots, v_n$, either $\phi(\overline{v}) \in p$ or $\neg\phi(\overline{v}) \in p$. By $S_n^{\mathcal{M}}(A)$ we denote the set of all complete n-types.

Zorn's Lemma assures that an incomplete theory can always be extended to a complete theory. Thus, viewing each n-type as a theory in the language $\mathcal{L}_{A \cup \{x_1, \ldots, x_n\}}$, also each n-type can be extended to a complete n-type $p^* \in S_n^{\mathcal{M}}(A)$ with $p^* \supseteq p$. This result is also known as Lindenbaum's Lemma, see [Man, Lemma 3.22].

5.2 Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure, $A \subseteq M$, and p an n-type over A. We say that p is *realized* by $\overline{a} \in M^n$ if $\mathcal{M} \models \phi(\overline{a})$ for each $\phi(\overline{v}) \in p$.

Having defined types we may now continue with saturated models.

5.3 Definition. Let κ be an infinite cardinal. We say that $\mathcal{M} \models \mathcal{T}$ is *κ-saturated* if, for all $A \subseteq M$, if $|A| < \kappa$ and $p \in S_n^{\mathcal{M}}(A)$, then p is realized by some element in $\mathcal{M}$. We call $\mathcal{M}$ simply *saturated* if it is $|M|$-saturated.

Since every type is contained in some complete type, also every incomplete type is realized in κ-saturated models. It turns out that for a model $\mathcal{M}$ to be κ-saturated it is even enough that every 1-type over A is realized in $\mathcal{M}$:

5.4 Lemma. *Let κ be an infinite cardinal. Then the following are equivalent:*

(i) $\mathcal{M}$ *is* κ*-saturated.*
(ii) If $A \subseteq M$ *with* $|A| < \kappa$ *and* p *is a* 1*-type over* A*, then* p *is realized in* $\mathcal{M}$*.*

Proof. (i) $\Rightarrow$ (ii): Being κ-saturated means that every complete n-type over any subset $A \subseteq M$ with cardinality less than κ is realized in $\mathcal{M}$. But every 1-type can be extended to a complete 1-type. Thus, this implication is clear.

(ii) $\Rightarrow$ (i): We prove the other direction by induction on n. Since (ii) states the base case for $n = 1$, we only need to deal with the induction step. Suppose that for a fixed $n \in \mathbb{N}$ and $A \subseteq M$ with $|A| < \kappa$ every complete n-type is realized in $\mathcal{M}$. Let $p \in S^{\mathcal{M}}_{n+1}(A)$. We need to show that p is realized in $\mathcal{M}$.

Let $q \in S^{\mathcal{M}}_n(A)$ be the type $\{\phi(v_1, \ldots, v_n) : \phi \in p\}$. By the induction hypothesis q is realized in $\mathcal{M}$ by some $\overline{a} \in M$. Let r be the type $\{\psi(\overline{a}, w) : \psi(\overline{v}) \in p\}$. Then r is a complete 1-type in $S^{\mathcal{M}}_1(A \cup \{a_1, \ldots, a_n\})$. By (ii), r is realized by some $b \in M$. Hence, the tuple $(\overline{a}, b)$ realizes p. This shows that $\mathcal{M}$ is κ-saturated. □

The traditional examples of saturated structures are the rationals as a dense linear order without endpoints, and the complex numbers as an algebraically closed field of characteristic 0, see [Sac72a, Proposition 16.1 and Proposition 16.2].

Sometimes, it can be hard to determine for a concrete model whether it is κ-saturated or not. However, it is not so hard to prove that there exists an extension that is saturated. We will prove this in three steps. Lemma 5.5 shows that every type can be realized in some elementary extension. Iterating this construction, we show in Lemma 5.6 that there is an elementary extension in which every type is realized. And finally we use this machinery to prove the existence of saturated elementary extensions in Theorem 5.10.

5.5 Lemma. *Let* $\mathcal{M}$ *be an* $\mathcal{L}$*-structure,* $A \subseteq M$ *a subset, and* p *an* n*-type over* A*. There exists an elementary extension* $\mathcal{N} \succeq \mathcal{M}$ *such that* p *is realized in* $\mathcal{N}$*.*

Proof. Let $c_1, \ldots, c_n$ be new constants not contained in $\mathcal{L}_A$. Define

$$\Gamma := \{\phi(\overline{c}, \overline{a}) : \ \phi(\overline{v}, \overline{a}) \in p\} \ \cup \ \mathrm{Diag}_{\mathrm{el}}(\mathcal{M}).$$

Let $\Delta \subseteq \Gamma$ be a finite subset. We ought to show that Δ has a model, i.e. that Δ is satisfiable. Without loss of generality we may assume that p is closed under conjunction. Thus, the part of Δ coming from the first part of Γ is one single sentence $\phi(\overline{c}, \overline{a})$. On the other hand, since $\mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ is a complete theory, we may further assume that also the part of Δ that comes from $\mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ is one single sentence. Thus we obtain that $\Delta = \{\phi(\overline{c}, \overline{a}), \psi(\overline{a}, \overline{b})\}$, where $\overline{a} \in A$, $\overline{b} \in M \setminus A$, $\phi(\overline{v}, \overline{a}) \in p$, and $\psi(\overline{a}, \overline{b}) \in \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$. The latter yields $\mathcal{M} \models \psi(\overline{a}, \overline{b})$. We have $\mathcal{M} \models \exists \overline{v}\ \phi(\overline{v}, \overline{a})$, i.e. there is $\overline{d} \in M$ such that $\mathcal{M} \models \phi(\overline{d}, \overline{a})$.

Let us consider the model $\mathcal{M}_{\overline{c}}$, where we interpret $\overline{c}^{\mathcal{M}_{\overline{c}}} = \overline{d}$. Since $\mathcal{M}_{\overline{c}} \models \phi(\overline{c}, \overline{a})$, we obtain $\mathcal{M}_{\overline{c}} \models \Delta$. Thus, there exists a model $\mathcal{N} \models \Gamma$ in which p is realized. Since $\mathcal{N} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$, there is an elementary $\mathcal{L}$-embedding $\mathcal{M} \preceq \mathcal{N}$, which was to be shown. □

5.6 Lemma. *Let* κ *be some infinite cardinal. For an* $\mathcal{L}$*-structure* $\mathcal{M}$ *there exists an elementary extension* $\mathcal{N} \succeq \mathcal{M}$ *such that for any subset* $A \subseteq M$ *with cardinality less than* κ*, each* 1*-type over* A *is realized in* $\mathcal{N}$*.*

Proof. Let $(p_\alpha : \alpha < \zeta)$ be an enumeration of all 1-types in $S_1^{\mathcal{M}}(A)$ for all subsets $A \subseteq M$ with $|A| < \kappa$ for some sufficiently large ordinal number ζ. We build an elementary chain of models $(\mathcal{M}_\alpha : \alpha < \zeta)$:

Let $\mathcal{M}_0 := \mathcal{M}$. If $\mathcal{M}_\alpha$ is already constructed, then let $\mathcal{M}_{\alpha+1}$ be the elementary extension of $\mathcal{M}_\alpha$ in which p_α is realized. This elementary extension exists by Lemma 5.5. For a limit ordinal λ let $\mathcal{M}_\lambda := \bigcup_{\alpha<\lambda} \mathcal{M}_\alpha$. Proposition 2.11 assures that the union of an elementary chain of models is an elementary extension of each member of the chain. Let

$$\mathcal{N} := \bigcup_{\alpha<\zeta} \mathcal{M}_\alpha.$$

Then every 1-type is realized in $\mathcal{N}$. Again by Proposition 2.11, $\mathcal{M}_\alpha \preceq \mathcal{M}$ for each $\alpha < \zeta$ and, hence, $\mathcal{M} \preceq \mathcal{N}$. □

5.7 Corollary. *In the situation of Lemma 5.6, also each n-type for $n \in \mathbb{N}$ is realized in $\mathcal{N}$.*

Proof. This follows immediately from Lemma 5.4. □

We will now show that for each regular infinite cardinal κ, every structure has an elementary extension that is κ-saturated. A reader that is not familiar with set theory and regular cardinals may as well imagine any infinite successor cardinal instead, since every infinite successor cardinal number is regular, see [Del, Theorem 3.8.6]. For the sake of completeness we give the definition of regularity:

5.8 Definition. Let $(B, <)$ be a totally ordered set. A subset $A \subseteq B$ is called *cofinal* in B if and only if for all $b \in B$ there exists $a \in A$ such that $a > b$. The *cofinality* of B, denoted by $\mathrm{cf}(B)$, is the least cardinal κ such that there exists a subset $C \subseteq B$ which has cardinality κ and is cofinal in B.

5.9 Definition. An infinite cardinal κ is said to be *regular* if $\mathrm{cf}(\kappa) = \kappa$.

5.10 Theorem. *Let κ be a regular infinite cardinal and $\mathcal{M}$ a model of a theory $\mathcal{T}$. There exists a κ-saturated $\mathcal{N} \models \mathcal{T}$ such that $\mathcal{M} \preceq \mathcal{N}$.*

Proof. We build an elementary chain $(\mathcal{N}_\alpha : \alpha < \kappa)$, such that its limit will be the desired κ-saturated elementary extension $\mathcal{N}$: Let $\mathcal{N}_0 := \mathcal{M}$. Assuming that $\mathcal{N}_\alpha$ is already constructed, let $\mathcal{N}_{\alpha+1}$ be the elementary extension of $\mathcal{N}_\alpha$ such that for any subset $A \subseteq M$ with cardinality less than κ, any 1-type over A is realized in $\mathcal{N}_{\alpha+1}$. Such an extension exists by Lemma 5.6. For a limit ordinal λ, we set

$$\mathcal{N}_\lambda := \bigcup_{\alpha<\lambda} \mathcal{N}_\alpha.$$

By Proposition 2.11, $\mathcal{N}_\lambda$ is an elementary extension of every $\mathcal{N}_\alpha$. We finally set

$$\mathcal{N} := \bigcup_{\alpha<\kappa} \mathcal{N}_\alpha.$$

Again, by Proposition 2.11, $\mathcal{N}$ is an elementary extension of each $\mathcal{N}_\alpha$.

It remains to show that $\mathcal{N}$ is κ-saturated. Let $A \subseteq N$ with $|A| < \kappa$, and let p be an n-type over A for some $n \in \mathbb{N}$. Since κ is regular, its cofinality is equal to itself. Now the cardinality of

A is smaller than κ. Hence, A cannot be cofinal in N, which implies that $|A|$ is already contained in some $\mathbb{N}_\alpha$. Since every 1-type is realized in $\mathcal{N}_\alpha$, by Lemma 5.4 also every n-type for any $n \in \mathbb{N}$, in particular p, is realized in $\mathcal{N}_\alpha$. Since $\mathcal{N}_\alpha \preceq \mathcal{N}$, this shows that $\mathcal{N}$ is κ-saturated. □

5.11 Lemma. *Let κ be an infinite cardinal, $\mathcal{M}$ and $\mathcal{N}$ two models of a theory $\mathcal{T}$, where $\mathcal{M}$ is κ-saturated and $|N| \leq \kappa$, and let $A \subseteq N$ be a subset. Then, any partial elementary embedding $f : A \to \mathcal{M}$ extends to an elementary embedding of $\mathcal{N}$ into $\mathcal{M}$.*

Proof. Let $\kappa_0 := |N \setminus A|$ and $(n_\alpha : \alpha < \kappa_0)$ be an enumeration of $N \setminus A$. Define $A_\alpha := A \cup \{n_\beta : \beta < \alpha\}$ for each $\alpha < \kappa_0$. Then, $A_0 = A$. We build a sequence of partial elementary embeddings $f_0 \subsetneq f_1 \subsetneq \ldots \subsetneq f_\alpha \subsetneq \ldots$ for $\alpha < \kappa_0$ with $f_\alpha : A_\alpha \to \mathcal{M}$.

We want the desired map to be

$$\widetilde{f} := \bigcup_{\alpha<\kappa_0} f_\alpha.$$

By transfinite induction we show that for every $\alpha < \kappa_0$, the map f_α is partial elementary. We set $f_0 := f$, which is by assumption partial elementary. If α is a limit ordinal, let $f_\alpha := \bigcup_{\beta<\alpha} f_\beta$. Then, given that all f_β are partial elementary, also f_α is partial elementary, since it is the union of partial elementary functions.

For the successor ordinals let f_α be already constructed and partial elementary. We need to extend this to a map $f_{\alpha+1}$ that is also partial elementary. Since both f_α and $f_{\alpha+1}$ coincide on A_α, it remains to define $f_{\alpha+1}(n_\alpha)$. Define the set

$$\Gamma(v) := \{\phi(v, f_\alpha(a_1), \ldots, f_\alpha(a_m)) : \mathcal{N} \models \phi(n_\alpha, a_1, \ldots, a_m) \text{ where } a_1, \ldots, a_m \in A_\alpha\}.$$

We will show that $\Gamma(v)$ is a 1-type. For this, we need to show that $\Gamma(v) \cup \mathrm{Th}(\mathcal{M})$ is satisfiable. By the Compactness Theorem it suffices to show that every finite subset of $\Gamma(v) \cup \mathrm{Th}(\mathcal{M})$ is satisfiable. Let $\Delta := \{\phi_1(v, f_\alpha(\overline{a_1})), \ldots, \phi_n(v, f_\alpha(\overline{a_n}))\} \subseteq \Gamma(v)$ be an arbitrary finite subset. If we show that there is an element $m \in M$, such that $\mathcal{M} \models \phi_i(m, f_\alpha(\overline{a_i}))$ for each $i = 1, \ldots, n$, i.e. $\mathcal{M} \models \bigvee_{i=1}^n \phi_i(x, f_\alpha(\overline{a_i}))$, we are done. Since $\Gamma(v)$ is closed under conjunction, $\phi(v, f_\alpha(\overline{a})) := \bigvee_{i=1}^n \phi_i(v, f_\alpha(\overline{a_i})) \in \Gamma(v)$. Then, $\mathcal{N} \models \exists v\ \phi(v, \overline{a})$. Since f_α is partial elementary this implies that $\mathcal{M} \models \exists v\ \phi(v, f_\alpha(\overline{a}))$. Since $\mathcal{M} \models \mathrm{Th}(\mathcal{M})$, $\Delta \cup \mathrm{Th}(\mathcal{M})$ is satisfiable. Hence, $\Gamma(v) \cup \mathrm{Th}(\mathcal{M})$ is satisfiable. Thus, we have shown that $\Gamma(v)$ is a 1-type.

By Lindebaum's Theorem it can be extended to a complete type $\Gamma(v)^* \in S_1^{\mathcal{M}}(A_\alpha)$. Since $\mathcal{M}$ is κ-saturated, $\Gamma(v)^*$ is realized in $\mathcal{M}$ by some $b \in M$. Because $\Gamma(v)$ is fully contained in $\Gamma(v)^*$, also the type $\Gamma(v)$ is realized by b. We set $f_{\alpha+1}(n_\alpha) := b$, i.e. $f_{\alpha+1} = f_\alpha \cup \{(n_\alpha, b)\}$. By construction, $f_{\alpha+1}$ is a partial elementary embedding. Thus, we obtain an elementary map $\widetilde{f} : \mathcal{N} \to \mathcal{M}$ by

$$\widetilde{f} := \bigcup_{\alpha<\kappa} f_\alpha.$$

□

We are now ready to state and proof another quantifier elimination criterion.

5.12 Theorem. *Let $\mathcal{L}$ be a language containing at least one constant symbol and $\mathcal{T}$ an $\mathcal{L}$-theory. Then the following are equivalent:*

(i) $\mathcal{T}$ has quantifier elimination.

(ii) If $\mathcal{M} \models \mathcal{T}$, $A \subseteq M$, $\mathcal{N} \models \mathcal{T}$ is $|M|^+$-saturated, $f : A \to \mathcal{N}$ is a partial embedding, then f extends to an $\mathcal{L}$-embedding $\mathcal{M} \to \mathcal{N}$.

Proof. (i) $\Rightarrow$ (ii): Let ϕ be an $\mathcal{L}$-formula and $\overline{a} \in A$ such that $\mathcal{M} \models \phi(\overline{a})$. By quantifier elimination there is a quantifier-free formula ψ such that $\mathcal{M} \models \psi(\overline{a})$. Since f is a partial embedding and, thus, preserves quantifier-free formulas, we obtain $\mathcal{N} \models \psi(\overline{a})$. Hence, $\mathcal{N} \models \phi(\overline{a})$. This shows that f is partial elementary. By Lemma 5.11, f extends to an $\mathcal{L}$-embedding from $\mathcal{M}$ into $\mathcal{N}$.

(ii) $\Rightarrow$ (i): We will use the previous quantifier elimination criterion from Theorem 3.3. Suppose $\mathcal{M}, \mathcal{N} \models \mathcal{T}$, $\mathcal{A}$ is a common substructure of $\mathcal{M}$ and $\mathcal{N}$, and ϕ is a quantifier-free formula. Further let $b \in M$ and $\overline{a} \in A$ such that $\mathcal{M} \models \phi(b, \overline{a})$. We need to show that there is $c \in N$ such that $\mathcal{N} \models \phi(c, \overline{a})$.

Let $\mathcal{N}' \models \mathcal{T}$ be an elementary extension of $\mathcal{N}$ which is $|M|^+$-saturated. Such an extension exists by Theorem 5.10. Let $f : A \to \mathcal{N}'$ be the identity map on A. By assumption f extends to an $\mathcal{L}$-embedding $f : \mathcal{M} \to \mathcal{N}'$. This yields $\mathcal{N}' \models \phi(f(b), f(\overline{a}))$ and also $\mathcal{N}' \models \phi(f(b), \overline{a})$, since $f(\overline{a}) = \overline{a}$. Therefore, $\mathcal{N}' \models \exists v\, \phi(v, \overline{a})$. Since $\mathcal{N}$ is an elementary substructure of $\mathcal{N}'$, we obtain $\mathcal{N} \models \exists v\, \phi(v, \overline{a})$, as desired. Now the quantifier elimination criterion from Theorem 3.3 yields that $\mathcal{T}$ has quantifier elimination, which was to be shown. □

5.2 Differentially Closed Fields

Since ancient times mathematicians have investigated roots of polynomial equations. A long amount of time later, they began to consider differential equations. It was an important contribution of model theory to algebra to introduce the axiomatic notion of differentially closed fields. They are to differential polynomial equations what algebraically closed fields are to polynomial equations, cf. [Poi, page 71].

According to [Mar96, page 53], the first work on the model theory of differentially closed fields was done by Abraham Robinson, whose work was influenced by earlier work of Abraham Seidenberg.

After giving a brief introduction to differential fields, we will axiomatize the theory of differentially closed fields and use the above criterion from Theorem 5.12 to show that this theory admits quantifier elimination. If not stated differently, we stick very closely to [Mar02, pages 148–151].

5.13 Definition. A *derivation* on a commutative ring R is a map $\delta : R \to R$ such that the Leibniz rule holds:

$$\delta(x + y) = \delta(x) + \delta(y)$$

$$\delta(xy) = x\delta(y) + y\delta(x).$$

We will write $a', a'', \ldots$ instead of $\delta(a), \delta(\delta(a)), \ldots$ and we denote the nth derivative of a by $a^{(n)}$.

The Leibniz rules yield a way to extend the derivation on a ring to its field of fraction: Namely the quotient rule

$$\delta\left(\frac{x}{y}\right) = \frac{y \cdot \delta(x) - x \cdot \delta(y)}{y^2}.$$

5.14 Definition. A *differential field* (K, δ) is a field K equipped with a derivation $\delta : K \to K$. We define the *ring of differential polynomials* over K to be the following polynomial ring in infinitely many variables:

$$K\{X\} = K[X, \delta(X), \delta^2(X), \ldots, \delta^m(X), \ldots].$$

If the corresponding derivation is clear, we will simply write K instead of (K, δ). We can extend δ to a derivation on $K\{X\}$ by setting $\delta(\delta^n(X)) := \delta^{n+1}(X)$. As above, we write $\delta^n(X) = X^{(n)}$.

5.15 Definition. A *differential field isomorphism* $\psi : K \to K'$ between two differential fields (K, δ) and (K', δ') is a field isomorphism that preserves the derivation. That means for every $k \in K$ we have $\psi(\delta(k)) = \delta'(\psi(k))$. Similarly a *differential field embedding* $\psi : K \to K'$ is a field embedding which preserves the derivation.

We will only consider fields of characteristic 0 with one single derivation. One could also investigate the theory DCF_p of differentially closed fields of characteristic $p > 0$. This theory is much less well-behaved [Sac72b]. In [Gra] however, the author shows that the theory m-DCF of differentially closed fields of characteristic 0 which have m many commuting derivations has very similar model theoretic properties to those of DCF: m-DCF admits quantifier elimination [Gra, Theorem 3.1.7] and is complete [Gra, Theorem 3.1.9]. Henceforth, all fields in this section will be of characteristic 0 and equipped with one single derivation.

5.16 Definition. Let (K, δ) be a differential field. For $f \in K\{X\} \setminus K$, the *order* of f is the largest n such that $\delta^n(X)$ occurs in f. If f is a constant, we say that f has order $-\infty$.

In case $f \in K\{X\}$ has order n, we can write

$$f(x) = \sum_{i=0}^{m} g_i \left(X, X', \ldots, X^{(n-1)}\right) \left(X^{(n)}\right)^i,$$

where $g_i \in K[X, X', \ldots, X^{(n-1)}]$. If $g_m \neq 0$, we say that f has *degree* m.

5.17 Definition. If $k \subseteq K$ are differential fields equipped with the same derivation δ, and $a \in K$, we denote by $k\langle a \rangle$ the differential subfield of K generated by a over k.

5.18 Lemma. *Let $k \subseteq K$ be differential fields of characteristic 0 and $f \in k\{X\} \setminus \{0\}$ be of order n. Let $a, b \in K$ with $f(a) = f(b) = 0$ such that $a, \ldots, a^{(n-1)}$ are algebraically independent over k, and $b, \ldots, b^{(n-1)}$ are algebraically independent over k, and $g(a) \neq 0$, $g(b) \neq 0$ for any g of order n of lower degree in $X^{(n)}$. Then, there is a differential field isomorphism between $k\langle a \rangle$ and $k\langle b \rangle$ that fixes k.*

Proof. A brief sketch of this proof can be found in [Mar02, Proposition 4.3.30 i)], here we present more detail.

The elements $a, \ldots, a^{(n-1)}$ and $b, \ldots, b^{(n-1)}$ are algebraically independent over k. This means, by sending $a^{(i)}$ to $b^{(i)}$ for each $i < n$, $k(a, \ldots, a^{(n-1)})$ and $k(b, \ldots, b^{(n-1)})$ are clearly isomorphic over k as fields. Let us call this isomorphism ψ.

Further, $f(a) = f(b) = 0$ and every differential polynomial g of order n and lower degree in $X^{(n)}$ vanishes neither in a nor in b. There is a polynomial $\widetilde{f} \in k[X_0, \ldots, X_n]$ such that $f(a) = \widetilde{f}(a, \ldots, a^{(n)})$. It holds $\widetilde{f}(a, \ldots, a^{(n-1)}, t) \in k(a, \ldots, a^{(n-1)})[t]$ and by dividing it by a constant

from $k(a,\ldots,a^{(n-1)})$, we may assume without loss of generality that it is a monic polynomial. Hence, $\widetilde{f}(a,\ldots,a^{(n-1)},t)$ is the minimal polynomial of $a^{(n)}$ over $k(a,\ldots,a^{(n-1)})$. Similarly, $\widetilde{f}(b,\ldots,b^{(n-1)},t) \in k(b,\ldots,b^{(n-1)})[t]$ is the minimal polynomial of $b^{(n)}$ over $k(b,\ldots,b^{(n-1)})$. By applying the isomorphism ψ to the coefficients of the former minimal polynomial, one obtains the latter. Hence, also $k(a,\ldots,a^{(n)})$ and $k(b,\ldots,b^{(n)})$ are isomorphic as fields. Since this isomorphism extends ψ, we will keep its name.

In order to see that ψ extends to an isomorphism from $k\langle a\rangle = k(a,\ldots,a^{(n)},\ldots)$ into $k\langle b\rangle = k(b,\ldots,b^{(n)},\ldots)$, we will show that $\delta(a^{(n)})$ and $\delta(b^{(n)})$ can be expressed only using terms of lower order:

For all $i < n$ we already have that $\delta(a^{(i)}) = a^{(i+1)}$ and $\delta(b^{(i)}) = b^{(i+1)}$. Let

$$f(x) = \sum_{i=0}^{n}\sum_{j=0}^{m} c_{i,j}(x^{(i)})^j.$$

Differentiating yields

$$\begin{aligned}
\delta(f(a)) &= \delta\left(\sum_{i=0}^{n}\sum_{j=0}^{m} c_{i,j}\left(a^{(i)}\right)^j\right)\\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} \delta\left(c_{i,j}\left(a^{(i)}\right)^j\right)\\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} \left(\delta(c_{i,j})\left(a^{(i)}\right)^j + c_{i,j}j\left(a^{(i)}\right)^{j-1}a^{(i+1)}\right)\\
&= f^{\delta}(a) + \sum_{i=0}^{n}\frac{\partial f}{\partial X^{(i)}}(a)a^{(i+1)},
\end{aligned}$$

where f^{δ} is the polynomial obtained by differentiating the coefficients of f and $\frac{\partial f}{\partial X^{(n)}}$ denotes the nth partial derivative of f with respect to $X^{(n)}$. Since $\frac{\partial f}{\partial X^{(n)}}$ has lower degree in $X^{(n)}$ than f, by assumption, it holds $\frac{\partial f}{\partial X^{(n)}}(a) \neq 0$. Because $f(a) = 0$, and also $\delta(f(a)) = 0$, it follows

$$-f^{\delta}(a) = \sum_{i=0}^{n}\frac{\partial f}{\partial X^{(i)}}(a)\delta(a^{(i)}),$$

which is equivalent to

$$\delta(a^{(n)}) = \frac{-f^{\delta}(a) - \sum_{i=0}^{n-1}\frac{\partial f}{\partial X^{(i)}}(a)\delta(a^{(i)})}{\frac{\partial f}{\partial X^{(n)}}(a)}. \tag{5.1}$$

Similarly we get

$$\delta(b^{(n)}) = \frac{-f^{\delta}(b) - \sum_{i=0}^{n-1}\frac{\partial f}{\partial X^{(i)}}(b)\delta(b^{(i)})}{\frac{\partial f}{\partial X^{(n)}}(b)}. \tag{5.2}$$

Since both (5.1) and (5.2) use only terms of lower order to express $\delta(a^{(n)})$ and $\delta(b^{(n)})$, we have shown that $k(a,\ldots,a^{(n)},\ldots)$ and $k(b,\ldots,b^{(n)},\ldots)$ are isomorphic as fields. Again, this

isomorphism will be called ψ. What remains to be shown is that under ψ, the derivation is preserved. For this we will first show that for each $k \in \mathbb{N}$ it holds $\psi(\delta(a^{(k)})) = \delta(\psi(a^{(k)}))$. Afterwards we will conclude that the equation also holds for every $c \in k\langle a\rangle$.

Let $k \in \{0, \dots, n-1\}$. Since $\psi(a^{(k+1)}) = b^{(k+1)}$, it holds $\psi(\delta(a^{(k)})) = \psi(a^{(k+1)}) = b^{(k+1)} = \delta(b^{(k)}) = \delta(\psi(a^{(k)}))$. The case where $k \geq n$, reduces to the former by considering the equations (5.1) and (5.2).

Now, let $c \in k\langle a\rangle$. Then there is $f, g \in k[X_0, \dots, X_m]$ for some m such that

$$c = \frac{f(a, \dots, a^{(m)})}{g(a, \dots, a^{(m)})}$$

and for the derivation it holds

$$\delta(c) = \frac{\delta(f(a, \dots, a^{(m)}))g(a, \dots, a^{(m)}) - f(a, \dots, a^{(m)})\delta(g(a, \dots, a^{(m)}))}{g(a, \dots, a^{(m)})^2}.$$

Hence, by applying the isomorphism ψ we obtain

$$\begin{aligned}\psi(\delta(c)) &= \frac{\psi\Big(\delta(f(a, \dots, a^{(m)}))g(a, \dots, a^{(m)}) - f(a, \dots, a^{(m)})\delta(g(a, \dots, a^{(m)}))\Big)}{\psi\Big(g(a, \dots, a^{(m)})^2\Big)} \\ &= \frac{\psi\Big(\delta(f(a, \dots, a^{(m)}))\Big)\psi\Big(g(a, \dots, a^{(m)})\Big) - \psi\Big(f(a, \dots, a^{(m)})\Big)\psi\Big(\delta(g(a, \dots, a^{(m)}))\Big)}{\psi\Big(g(a, \dots, a^{(m)})\Big)^2}.\end{aligned}$$

Since ψ has the homomorphic property one can move ψ into the polynomials f and g, such that it is only applied to the elements $a, \dots, a^{(m)}$. But for those elements we already have shown that ψ commutes with the derivation. Thus, we obtain $\psi(\delta(c)) = \delta(\psi(c))$.

Hence, we have shown that the ψ is indeed a differential field isomorphism. □

5.19 Definition. Let $k \subseteq K$ be differential fields. We say that $a \in K$ is *differentially algebraic* over k if $f(a) = 0$ for some nonzero $f \in k\{X\}$. Otherwise a is *differentially transcendental.*

5.20 Lemma. *Let $k \subseteq K$ be differential fields. If $a \in K$ is differentially algebraic over k, then there is a nonzero differential polynomial f such that $f(a) = 0$ and for all $g \in k\{X\} \setminus \{0\}$ of lower order it holds that $g(a) \neq 0$. Moreover, one can choose f such that if there is $b \in K$ with $f(b) = 0$ and $g(b) \neq 0$ for any lower order g, then $k\langle a\rangle$ and $k\langle b\rangle$ are isomorphic over k.*

Proof. See [Mar02, Proposition 4.3.30 ii)]. Let $a \in K$ be differentially algebraic over k. Let n be minimal such that $a, \dots, a^{(n)}$ are algebraically dependent over k, and let $f \in k\{X\}$ be of order n and of minimal degree in $X^{(n)}$ such that $f(a, \dots, a^{(n)}) = 0$. Obviously, $g(a) \neq 0$ for any nonzero $g \in k\{X\}$ of order less than n.

If $f(b) = 0$ and $g(b) \neq 0$ for any lower order polynomial g, then $b, \dots, b^{(n-1)}$ are algebraically independent over k. So $b^{(n)}$ is zero of the irreducible polynomial $f(b, \dots, b^{(n-1)}, Y) \in k(b, \dots, b^{(n-1)})[Y]$. Now, since all the assumptions of Lemma 5.18 are fulfilled, we conclude that $k\langle a\rangle$ and $k\langle b\rangle$ are isomorphic over k. □

5.21 Definition. A differential field K is *differentially closed* if, whenever $f, g \in K\{X\}$, g is nonzero and the order of f is greater than the order of g, there is $a \in K$ such that $f(a) = 0$ and $g(a) \neq 0$.

That means in particular, if f has order zero, i.e. $f \in K[X]$, there is $a \in K$ with $f(a) = 0$. Hence, every differentially closed field is algebraically closed.

There are many examples of differential fields: the field of formal power series $K((X))$ for some field K with its usual derivation, or the field of meromorphic functions on an open connected subset of $\mathbb{C}$. These, and further examples can be found for instance in [Poi, page 71]. However, there is no natural example of a differentially closed field.

In the following we will show that every differential field can be embedded into a differentially closed field. This part will be based on [Mar96, Section 1]. For a long time it was not clear if the differential closure is somehow unique like the algebraic or the real closure. Saharon Shelah has shown that it is indeed unique up to isomorphism, cf. [Sac72a]

5.22 Definition. An ideal $I \trianglelefteq K\{X\}$ is called a *differential ideal* if for every $f \in I$ it also contains its derivative. By $\langle f \rangle$ we denote the differential ideal generated by f. A *prime differential ideal* $I \subseteq K\{X\}$ is a differential ideal which is also a prime ideal, i.e. if $ab \in I$ for some $a, b \in K$, then $a \in I$ or $b \in I$. Moreover, for a differential polynomial $f \in K\{X\}$ we define

$$I(f) := \left\{ h \in k\{X\} : \frac{\partial^m}{\partial^m X^{(n)}} h \in \langle f \rangle \text{ for some } m \in \mathbb{N} \right\}.$$

Even if f is irreducible, $\langle f \rangle$ may not be prime. For example if $f(X) = (X'')2 - 2X'$. Then $\delta(f(X)) = 2X'' \cdot X''' - 2X'' = 2X''(X''' - 1)$ is in $\langle f \rangle$, but neither $2X''$ nor $X''' - 1$ is in $\langle f \rangle$. But, however, the following holds:

5.23 Lemma. *If f is an irreducible differential polynomial, then $I(f)$ is a differential prime ideal.*

Proof. This proof is not trivial and needs some additional theory. We refer to [Poi, Lemma 6.10] or [Mar96, Corollary 1.7]. □

5.24 Theorem. *Every differential field k has an extension K which is differentially closed.*

Proof. [Mar96, Lemma 2.2] Let $f \in k\{X\}$ be of order n and $g \in k\{X\}$ of order less than n. By taking an irreducible factor of f of order n, we may as well assume that f is irreducible. It follows that $g \notin I(f)$, since g has order less than f.

By Lemma 5.23, $I(f)$ is a differential prime ideal. Thus, let F be the fraction field $F := \mathrm{Quot}(k\{X\}/I(f))$. To see that δ is well-defined on F, let $p, q \in k\{X\}$ with $p - q \in I(f)$. Then also $\delta(a) - \delta(b) = \delta(a - b) \in I(f)$, as $\langle f \rangle$ is closed under differentiation. By the quotient rule, δ extends to F.

Hence, let $a \in F$ be the image of X mod $I(f)$. Since $f \in I(f)$, $f(a) = 0$ in F, while $g \notin I(f)$ yields $g(a) \neq 0$.

Iterating this process we can build $K \supseteq k$ a differentially closed field. □

We have now developed the theory of differential fields that is needed for the proof of quantifier elimination of differentially closed fields. We will proceed by giving an axiomatization of DCF. The theory of differential fields is given by the axioms for fields of characteristic 0 together with the Leibniz rule. In order to formalize that a differential field is differentially closed we need additionally a countable infinite family of axioms. It is difficult to write down a general axiom as there are many varying parameters: the orders of the two polynomials and the degree of them in every "variable" $X^{(i)}$. We will not use any axioms, the important point for us is that one is convinced that there exists an axiomatization. But this is not hard to see, since we can easily formalize differential polynomials and the fact that there exists an element in which one differential polynomial vanishes and the other one does not.

5.25 Definition. Let $\mathcal{L}$ be the language $\langle +, -, \cdot, \delta; 0, 1 \rangle$, where δ is a unary function symbol for the derivation. The theory DCF of differentially closed fields is axiomatized as follows:

- the field axioms **K1** to **K9**,
- characteristic 0: For each $n \in \mathbb{N}$ we have:

K0*n*: $\forall x\ (\underbrace{(x + \ldots + x}_{n \text{ times}} \doteq 0) \to x \doteq 0)$

- the Leibniz rule for differentiation:

  D1: $\forall x \forall y\ \delta(x + y) \doteq \delta(x) + \delta(y)$,
  D2: $\forall x \forall y\ \delta(x \cdot y) \doteq x\delta(y) + y\delta(x)$.

- and additionally differential closedness: For any non-constant differential polynomials f and g where the order of g is less than the order of f, there exists an x such that $f(x) = 0$ and $g(x) \neq 0$.

5.26 Theorem. *The theory of differentially closed fields admits quantifier elimination.*

Proof. See [Mar02, Theorem 4.3.32]. Suppose that $\mathcal{K} \models \mathrm{DCF}$ is a differentially closed field, $R \subseteq K$ a subset, $\mathcal{M} \models \mathrm{DCF}$ $|K|^+$-saturated. Let $f : R \to \mathcal{M}$ be a partial embedding. As we will see in Chapter 6, without loss of generality, by Lemma 6.2, we may assume that R is a substructure of $\mathcal{K}$, i.e. the substructure $\mathcal{R} \subseteq \mathcal{K}$ that is generated by R, that means the smallest substructure of $\mathcal{K}$ which contains R. Hence, $\mathcal{R}$ is a differential subring of $\mathcal{K}$ and f is a differential ring embedding, that means a ring embedding which preserves the derivation. In order to apply Theorem 5.12, we must show that f extends to a differential field embedding of $\mathcal{K}$ into $\mathcal{M}$.

Surely, f extends to a differential field embedding of $\mathrm{Quot}(R)$ into $\mathcal{M}$, since there is a unique extension of the derivation from $\mathcal{R}$ to $\mathrm{Quot}(R)$. Therefore, we may assume that $\mathcal{R}$ is already a field. If we show that for every $a \in K \setminus R$, there is a differential field embedding of $R\langle a\rangle$ into $\mathcal{M}$, then by transfinite induction we are done. By identifying R with $f(R)$ we may assume that $\mathcal{R} \subseteq \mathcal{M}$ and that f is the identity on $\mathcal{R}$. Now, a is either differentially algebraic or transcendental over R. We consider both cases:

Case 1: a is differentially algebraic over R. Let $f \in R\{X\} \setminus \{0\}$ be as in Lemma 5.20. Let n be the order of f. Let p be the type $\{f(v) = 0\} \cup \{g(v) \neq 0 : g \text{ is nonzero of order less than } n\}$. If $g_1, \ldots, g_m$ are nonzero differential polynomials of order less than n, then $g_i(a) \neq 0$ for all i, while $f(a) = 0$. Therefore, there exists $s \in M$ such that $f(s) = 0$ and $\prod_{i=1}^m g_i(s) \neq 0$. Thus, p is satisfiable, and since $\mathcal{M}$ is $|K|^+$-saturated, p is realized by some $b \in M$. Since $g(b) \neq 0$ for all nonzero differential polynomials g of order less than n, it follows that $b, b', \ldots, b^{(n-1)}$ are algebraically independent over R. Also $a, a', \ldots, a^{(n-1)}$ are algebraically independent over R, so by Lemma 5.18, $R\langle a\rangle$ and $R\langle b\rangle$ are isomorphic over R. Thus, we can extend the differential field embedding by sending a to b.

Case 2: a is differentially transcendental over R. Let p be the type $\{g(v) \neq 0 : g \in R\{X\} \setminus \{0\}\}$. Let $g_1, \ldots, g_n \in R\{X\} \setminus \{0\}$. Let $N := \max\{\deg(g_i) : i = 1, \ldots, n\} + 1$ and let $f(x) = x^{(N)}$. Since $\mathcal{M}$ is differentially closed, there is $s \in M$ such that $f(s) = s^{(N)} = 0$ and $g_i(s) \neq 0$ for all $i = 1, \ldots, n$. Thus, p is satisfiable and, by $|K|^+$-saturation, realized by some $b \in M$ that is differentially transcendental over R. Since $R\langle a\rangle$ and $R\langle b\rangle$ are over $\mathcal{R}$ isomorphic to the fraction field $\mathrm{Quot}R\{X\}$, we can extend the differential field embedding again by sending a to b. □

6 Quantifier Elimination by Lou van den Dries

Back in the 1980s there did not exist a good documentation of quantifier elimination test. In 1985, Lou van den Dries gave in [vdD] a new quantifier elimination test. So far, there has not been published a systematic proof of this test. The goal of the following section is to serve this purpose.

In the second section of this chapter we will apply this quantifier elimination test to the theory of the field of reals with a predicate for the powers of 2.

Let us start by proving some lemmas that we will use in the following. Throughout this chapter let $\mathcal{L}$ be a language with at least one constant symbol and $\mathcal{T}$ an $\mathcal{L}$-theory.

6.1 Extensions of Partial Embeddings

6.1 Lemma. *The union of any increasing chain of models of $\mathcal{T}_\forall$ is also a model of $\mathcal{T}_\forall$.*

Proof. Let $\mathcal{T}$ be a theory. Let I be an ordered indexing set and $(\mathcal{M}_i)_{i\in I}$ an increasing chain of models of $\mathcal{T}_\forall$, i.e. for all $i \in I$, $\mathcal{M}_i \models \mathcal{T}_\forall$ and for all $i < j \in I$, $\mathcal{M}_i \subseteq \mathcal{M}_j$. Let $\forall x_1 \forall x_2 \ldots \forall x_n\ \phi(\overline{x})$, with ϕ quantifier-free, be a universal formula in $\mathcal{T}$. Let $\overline{a}$ be an arbitrary n-tuple in $\bigcup_{i\in I} M_i$. Since it has only finitely many components, there is an M_j which already contains all of them. Since $\mathcal{M}_j \models \mathcal{T}_\forall$, we have $\mathcal{M}_j \models \phi(\overline{a})$. Therefore,

$$\bigcup_{i\in I} \mathcal{M}_i \models \phi(\overline{a}).$$

Since $\overline{a}$ was arbitrary,

$$\bigcup_{i\in I} \mathcal{M}_i \models \forall \overline{x}\ \phi(\overline{a}).$$

Hence,

$$\bigcup_{i\in I} \mathcal{M}_i \models \mathcal{T}_\forall.$$

□

The following will be the key lemma for the proof of the quantifier elimination test.

6.2 Lemma. *Consider two $\mathcal{L}$-structures $\mathcal{B}_1$ and $\mathcal{B}_2$, a subset $X \subseteq B_1$, and a partial embedding $\eta : X \to \mathcal{B}_2$. There is an extension of η to an $\mathcal{L}$-embedding $\eta' : \mathcal{D} \to \mathcal{B}_2$, where $\mathcal{D}$ is the substructure of $\mathcal{B}_1$ generated by X, i.e. the smallest substructure of $\mathcal{B}_1$ that contains X.*

Proof. We will first explain how to construct $\mathcal{D}$, the substructure of $\mathcal{B}_1$ generated by X. Secondly we will show that η can be extended to an $\mathcal{L}$-embedding from $\mathcal{D}$ into $\mathcal{B}_2$. What we need to do is add to X all the elements that arise from applying terms to every tuple $\overline{x} \in X$ and define what happens to them when applying f.

Set $D := \{t^{\mathcal{B}_1}(\overline{x}) : t \text{ is a term and } \overline{x} \in X\}$. Then D is closed under terms. For every constant $c \in \mathcal{L}$, let $c^{\mathcal{D}} := c^{\mathcal{B}_1}$. To see that $c^{\mathcal{D}}$ is an element of D, consider the term $t = c$, then $t^{\mathcal{B}_1} \in D$, thus $c^{\mathcal{D}} \in D$.

Let $g(\overline{v})$ be an r-ary function symbol in $\mathcal{B}_1$. For $\overline{d} \in D$ define $g^{\mathcal{D}}(\overline{d}) := g^{\mathcal{B}_1}(\overline{d})$. Now $\overline{d}$ is not necessarily a tuple in X. However, it was constructed by a term. Thus, let $t_1, \ldots, t_r$ be terms such that $\overline{d} = (d_1, \ldots, d_r) = (t_1^{\mathcal{B}_1}(\overline{x_1}), \ldots, t_r^{\mathcal{B}_1}(\overline{x_r}))$ for some $\overline{x_1}, \ldots, \overline{x_r} \in X$, and let $t(\overline{v_1}, \ldots, \overline{v_r})$ be the term $g(t_1(\overline{v_1}), \ldots, t_r(\overline{v_r}))$. Therefore, $g^{\mathcal{D}}(\overline{d}) = t^{\mathcal{B}_1}(\overline{x_1}, \ldots, \overline{x_r}) \in D$.

For a relation symbol R we define $\mathcal{D} \models R^{\mathcal{D}}(\overline{d})$ if and only if $\mathcal{B}_1 \models R^{\mathcal{B}_1}(\overline{d})$.

Since the $\mathcal{L}$-embedding is the identity map on D into B_1, it is injective. Thus, by construction, $\mathcal{D}$ is a substructure of $\mathcal{B}_1$.

Now let $\eta : X \to \mathcal{B}_2$ be a partial embedding. For any $d \in D$, say $d = t^{\mathcal{D}}(\overline{x})$ for some term t, and some tuple $\overline{x} \in X$, we define $\eta'(t^{\mathcal{D}}(\overline{x})) := t^{\mathcal{B}_2}(\eta(\overline{x}))$. For $d \in D$ the choice of a term t such that $d = t^{\mathcal{D}}(\overline{x})$ might not be unique. In order to see well-definedness, note that $\mathcal{D} \models t_1(\overline{x}) \doteq t_2(\overline{x})$ for $\overline{x} \in X$ immediately yields that $\mathcal{B}_2 \models t_1(\eta(\overline{x})) \doteq t_2(\eta(\overline{x}))$, since η is a partial embedding. Hence, η' is well-defined. We claim that η' is an $\mathcal{L}$-embedding.

For a constant symbol c in $\mathcal{L}$ we have $\eta'(c^{\mathcal{D}}) = \eta'(c^{\mathcal{B}_1}) = c^{\mathcal{B}_2}$. Let f be a function symbol. Then:

$$\begin{aligned}
\eta(f^{\mathcal{D}}(t_1^{\mathcal{D}}(\overline{x_1}), \ldots, t_n^{\mathcal{D}}(\overline{x_n}))) &= \eta((f^{\mathcal{D}}(t_1^{\mathcal{D}}, \ldots, t_n^{\mathcal{D}}))(\overline{x_1}, \ldots, \overline{x_n})) \\
&= f^{\mathcal{B}_2}(t_1^{\mathcal{B}_2}, \ldots, t_n^{\mathcal{B}_2})(\eta(\overline{x_1}), \ldots, \eta(\overline{x_n})) \\
&= f^{\mathcal{B}_2}(t_1^{\mathcal{B}_2}(\eta(\overline{x_1})), \ldots, t_n^{\mathcal{B}_2}(\eta(\overline{x_n}))) \\
&= f^{\mathcal{B}_2}(\eta'(t_1^{\mathcal{D}}(\overline{x_1})), \ldots, \eta'(t_n^{\mathcal{D}}(\overline{x_n}))).
\end{aligned}$$

Let R be a relation symbol in $\mathcal{L}$. Then the following are equivalent:

$$\begin{aligned}
& \mathcal{D} \models R(t_1(\overline{x_1}), \ldots, t_n(\overline{x_n})) \\
\Leftrightarrow\ & \mathcal{B}_1 \models R(t_1(\overline{x_1}), \ldots, t_n(\overline{x_n})) && \text{since } \mathcal{D} \subseteq \mathcal{B}_1 \\
\Leftrightarrow\ & \mathcal{B}_2 \models R(t_1(\overline{x_1}), \ldots, t_n(\overline{x_n})) && \text{since } R(t_1, \ldots, t_n) \text{ is quantifier-free} \\
& && \text{and } \overline{x_1}, \ldots, \overline{x_n} \in X \\
\Leftrightarrow\ & \mathcal{B}_2 \models R(\eta'(t_1(\overline{x_1})), \ldots, \eta'(t_n(\overline{x_n}))) && \text{by definition of } \eta'
\end{aligned}$$

Hence, we have shown that η' is, indeed, an $\mathcal{L}$-embedding. □

We will now come to van den Dries' quantifier elimination test, which he gave in [vdD]:

6.3 Theorem. *Let $\mathcal{T}$ be a theory with at least one constant symbol and suppose that the following conditions hold:*

(1) Each model $\mathcal{M}$ of $\mathcal{T}_\forall$ has a $\mathcal{T}$-closure $\overline{\mathcal{M}}$. This means that for every $\mathcal{M} \models \mathcal{T}_\forall$ there is $\overline{\mathcal{M}} \models \mathcal{T}$ with $\mathcal{M} \subseteq \overline{\mathcal{M}}$, and $\overline{\mathcal{M}}$ can be embedded over $\mathcal{M}$ into each $\mathcal{T}$-extension of $\mathcal{M}$, i.e. into every $\mathcal{N} \models \mathcal{T}$ with $\mathcal{M} \subseteq \mathcal{N}$.

(2) If $\mathcal{M} \subsetneq \mathcal{N}$ are models of $\mathcal{T}$, then there is $b \in N \setminus M$ such that $\mathcal{M}(b)$, the $\mathcal{T}_\forall$-model generated by b over $\mathcal{M}$, can be embedded over $\mathcal{M}$ into an elementary extension of $\mathcal{M}$.

Then $\mathcal{T}$ admits quantifier elimination.

Proof. We will prove this quantifier elimination test by using Theorem 5.12 and by applying the previous lemma several times.

Let $\mathcal{M} \models \mathcal{T}$ be a model, $X \subseteq M$ a subset, $\mathcal{N} \models \mathcal{T}$ an $|M|^+$-saturated model, and $f : X \to \mathcal{N}$ a partial embedding. We need to show that f extends to an $\mathcal{L}$-embedding $f : \mathcal{M} \to \mathcal{N}$. For the sake of simplicity, f will keep its name after each extension.

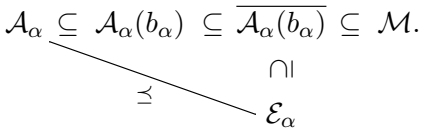
By Lemma 6.2, f extends to an $\mathcal{L}$-embedding $f : \mathcal{A} \to \mathcal{N}$, where $\mathcal{A}$ is the substructure of $\mathcal{M}$ generated by the set X. Thus, $\mathcal{A}$ is a model of the universal theory $\mathcal{T}_\forall$, by Lemma 2.13. We may now apply condition (1). So, $\mathcal{A}$ has a $\mathcal{T}$-closure, i.e. $\mathcal{A} \subseteq \overline{\mathcal{A}} \models \mathcal{T}$ and $\overline{\mathcal{A}}$ can be embedded over $\mathcal{A}$ into $\mathcal{N}$. Thus, f extends to an $\mathcal{L}$-embedding $f' : \overline{\mathcal{A}} \to \mathcal{N}$. Moreover, $\overline{\mathcal{A}}$ is embedded over $\mathcal{A}$ into $\mathcal{M}$.

From this point we start a transfinite iteration. Let $f_0 := f'$ and $\mathcal{A}_0 := \overline{\mathcal{A}}$. We will build a chain of models $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \ldots \subseteq \mathcal{A}_\alpha \subseteq \ldots \subseteq \mathcal{M}$ and, as in Lemma 5.11, a chain of $\mathcal{L}$-embeddings $f_0 \subseteq f_1 \subseteq \ldots \subseteq f_\alpha \subseteq \ldots$, where $f_\alpha : \mathcal{A}_\alpha \to \mathcal{N}$. Let $\kappa = |M \setminus A|$. We want the desired map to be

$$f := \bigcup_{\alpha<\kappa} f_\alpha : \mathcal{M} \to \mathcal{N}.$$

For the successor step suppose that $\mathcal{A}_\alpha$ and $f_\alpha : \mathcal{A}_\alpha \to \mathcal{N}$ are already constructed. Without loss of generality we assume that $\mathcal{A}_\alpha \subsetneq \mathcal{M}$, otherwise set $\mathcal{A}_{\alpha+1} = \mathcal{A}_\alpha$ and $f_{\alpha+1} = f_\alpha$ and we are done.

By condition (2), there is an element $b_\alpha \in M \setminus A_\alpha$ such that $\mathcal{A}_\alpha(b_\alpha)$ can be embedded over $\mathcal{A}_\alpha$ into an elementary extension of $\mathcal{A}_\alpha$, say $\mathcal{E}_\alpha$. Applying condition (1) again, since $\mathcal{A}_\alpha(b_\alpha) \models \mathcal{T}_\forall$, it has a $\mathcal{T}$-closure $\overline{\mathcal{A}_\alpha(b_\alpha)} \models \mathcal{T}$ that can be embedded over $\mathcal{A}_\alpha(b_\alpha)$ into each $\mathcal{T}$-extension of $\mathcal{A}_\alpha(b_\alpha)$, in particular into $\mathcal{E}_\alpha$. Hence, we obtain the following diagram:



We will first construct an $\mathcal{L}$-embedding of $A_\alpha \cup \{b_\alpha\}$ into $\mathcal{N}$, then extend it to an $\mathcal{L}$-embedding from $\mathcal{A}_\alpha(b_\alpha)$ into $\mathcal{N}$, and finally obtain one from $\overline{\mathcal{A}_\alpha(b_\alpha)}$ into $\mathcal{N}$. Let $f_{\alpha+1}\big|_{\mathcal{A}_\alpha} = f_\alpha$. Define the set

$$\Gamma(v) := \{\phi(v, f_\alpha(\overline{a})) : \overline{a} \in A_\alpha, \phi \text{ is a quantifier-free formula, and } \mathcal{M} \models \phi(b_\alpha, \overline{a})\}.$$

In order to show that $\Gamma(v)$ is a type, we need to demonstrate that $\Gamma(v) \cup \mathrm{Th}(\mathcal{N})$ is satisfiable. Let $\Delta \subseteq \Gamma(v)$ be an arbitrary finite subset. We will show that there is $x \in N$ such that $\mathcal{N} \models \phi(x, f_\alpha(\overline{a}))$ for each $\phi(v, f_\alpha(\overline{a})) \in \Delta$. This will imply that $\Gamma(v) \cup \mathrm{Th}(\mathcal{N})$ is satisfiable. Since $\Gamma(v)$ is closed under conjunction, we may assume that $\Delta = \{\phi(v, f_\alpha(\overline{a}))\}$ only consists of one single formula with $\overline{a} \in A_\alpha$. Then $\mathcal{M} \models \phi(b_\alpha, \overline{a})$ and it suffices to show that $\phi(v, f_\alpha(\overline{a}))$ is satisfiable in $\mathcal{N}$. Since ϕ is quantifier-free and $b_\alpha \in \overline{\mathcal{A}_\alpha(b_\alpha)} \subseteq \mathcal{M}$, we have $\overline{\mathcal{A}_\alpha(b_\alpha)} \models \phi(b_\alpha, \overline{a})$, in other words $\overline{\mathcal{A}_\alpha(b_\alpha)} \models \exists v\ \phi(v, \overline{a})$. Then also $\mathcal{E}_\alpha \models \exists v\ \phi(v, \overline{a})$. Since $\mathcal{E}_\alpha$ is an elementary extension of $\mathcal{A}_\alpha$ and $\overline{a} \in A_\alpha$, we obtain $\mathcal{A}_\alpha \models \exists v\ \phi(v, \overline{a})$. By induction hypothesis, we already

have an $\mathcal{L}$-embedding of $\mathcal{A}_\alpha$ into $\mathcal{N}$ and existential formulas are preserved upwards in inclusion. This yields $\mathcal{N} \models \exists v\, \phi(v, f_\alpha(\overline{a}))$.

Thus, we have shown that $\Gamma(v) \cup \mathrm{Th}(\mathcal{N})$ is satisfiable and, hence, that $\Gamma(v)$ is a 1-type which can be extended to a complete type $\Gamma(v)^* \in S_1^{\mathcal{N}}(A_\alpha)$. Since $\mathcal{N}$ is $|M|^+$-saturated, there is some element $c_\alpha \in N$ that realizes $\Gamma(v)^*$ and thus, $\Gamma(v)$. Set $f_{\alpha+1}(b_\alpha) = c_\alpha$.

In order to convince oneself that $f_{\alpha+1}$ is still injective, suppose that $\mathcal{N} \models f_{\alpha+1}(b_\alpha) = f_{\alpha+1}(a)$ for $a \in A_{\alpha+1}$. We will show that this implies already $b_\alpha = a$ in $\mathcal{M}$ which proves injectivity. Let us have a look at the formula $\phi(v, w)$ that denotes the equality $v = w$. This is a quantifier-free formula. Thus, $\phi(v, f_{\alpha+1}(a)) \in \Gamma(v)$, i.e. $\mathcal{M} \models \phi(b_\alpha, a)$. This yields that $\mathcal{M} \models b_\alpha = a$. Hence, we have a partial embedding of $A_\alpha \cup \{b_\alpha\}$ into $\mathcal{N}$.

By Lemma 6.2, it can be extended to an $\mathcal{L}$-embedding from $\mathcal{A}_\alpha(b_\alpha)$ into $\mathcal{N}$, since $\mathcal{A}_\alpha(b_\alpha)$ is the smallest substructure of $\mathcal{M}$ that contains A_α and b_α. By condition (1), $\overline{\mathcal{A}_\alpha(b_\alpha)}$ can be embedded over $\mathcal{A}_\alpha(b_\alpha)$ into $\mathcal{N}$. Hence, we have finished the construction of $f_{\alpha+1}$. Set $\mathcal{A}_{\alpha+1} := \overline{\mathcal{A}_\alpha(b_\alpha)}$. Then $f_{\alpha+1} : \mathcal{A}_{\alpha+1} \to \mathcal{N}$ is an $\mathcal{L}$-embedding of models.

For a limit ordinal α let

$$f'_\alpha := \bigcup_{\lambda<\alpha} f_\lambda : \bigcup_{\lambda<\alpha} \mathcal{A}_\lambda \to \mathcal{N}.$$

Since each f_λ is an $\mathcal{L}$-embedding, also their union f'_α is an $\mathcal{L}$-embedding. Each $\mathcal{A}_\lambda$ is, in particular, a model of $\mathcal{T}_\forall$. By Lemma 6.1 their union is also a model of $\mathcal{T}_\forall$ and by condition (1) this union has a $\mathcal{T}$-closure

$$\overline{\bigcup_{\lambda<\alpha} \mathcal{A}_\lambda} =: \mathcal{A}_\alpha,$$

that can be embedded over $\bigcup_{\lambda<\alpha} \mathcal{A}_\lambda$ into $\mathcal{N}$. Thus, $\mathcal{A}_\alpha \models \mathcal{T}$ and f'_α expands to the $\mathcal{L}$-embedding $f_\alpha : \mathcal{A}_\alpha \to \mathcal{N}$.

This algorithm terminates as soon as $\mathcal{A}_\alpha = \mathcal{M}$. At this point we obtain the desired $\mathcal{L}$-embedding $f := f_\alpha : \mathcal{M} \to \mathcal{N}$.

By Theorem 5.12, $\mathcal{T}$ admits quantifier elimination. □

6.2 The Field of Reals with a Predicate for the Powers of Two

In this chapter we will show that the theory of real closed fields with a certain discrete multiplicative subgroup—in the following denoted by RPT—has quantifier elimination in the language of ordered rings augmented by two new symbols. This section follows [vdD]. We will denote by $\mathcal{L}$ the language $\langle +, -, \cdot; <; 0, 1\rangle$ of ordered rings. For simplicity reasons, we will omit the symbols of $\mathcal{L}$ when talking about a structure.

Let λ be a unary function symbol, A a unary relation symbol and for every $n \in \mathbb{N}$, let P_n be a unary relation symbol. By $\mathcal{L}^*$ we denote the language $\mathcal{L} \cup \{A, \lambda, P_n : n = 1, 2, \ldots\}$.

6.4 Definition. Let RPT, the theory of the field of reals with a predicate for the powers of two, as van den Dries calls it, be the $\mathcal{L}^*$-theory given by the following axioms expressing that:

- R is a real closed ordered field, i.e. axioms **K1** to **K9**, **O1** to **O5**, **RK1**, and **RK2*n***,
- A is a multiplicative subgroup of positive elements of R:

  A1: $\forall x\, (A(x) \to x > 0)$

A2: $\forall x \forall y \, ((A(x) \wedge A(y)) \rightarrow A(x \cdot y))$
A3: $A(1)$
A4: $\forall x \, (A(x) \rightarrow \exists y \, (A(y) \wedge x \cdot y = y \cdot x = 1))$.

- such that:

V1: $A(1+1)$,
V2: $\forall x\ (1 < x < 2 \to \neg A(x))$,
V3*n*: $\forall x\ (P_n(x) \leftrightarrow \exists y\ (A(y) \wedge y^n = x))$, for all $n \in \mathbb{N}$,
V4: $\forall x\ (x \leq 0 \to \lambda(x) = 0)$,
V5: $\forall x\ (x > 0 \to (A(\lambda(x)) \wedge \lambda(x) \leq x < 2\lambda(x)))$.

Axiom **V1** states that $2 \in A$. Since A is a multiplicative group, it contains all powers of 2. By **V1** there is no element in A between 1 and 2. For an element x it holds $P_n(x)$ if and only if x has an nth root which lies in A. The function λ assigns to each positive element y the nearest element in A which is less than or equal to y. If y is not positive, then $\lambda(y) = 0$. Instead of $A(x)$, we will write $x \in A$ in the following as usually.

We will prove the following theorem after we have developed some theory:

6.5 Theorem. *The $\mathcal{L}^*$-theory* RPT *admits elimination of quantifiers.*

First we will go a little into valuation theory. For this part, see [Kuh, pages 9, 15, and 16].

6.6 Definition. We say that two nonzero elements a and b of an ordered field K are of the same *archimedean class* if

$$\frac{1}{n} < \left|\frac{a}{b}\right| < n$$

for some $n \in \mathbb{N}$.

6.7 Definition. Let K be a field and Γ an ordered abelian group. A *valuation* on K is a surjective map $v : K \to \Gamma \cup \{\infty\}$ which satisfies the following properties for all $a, b \in K$:

(i) $v(a) = \infty$ if and only if $a = 0$,
(ii) $v(ab) = v(a) + v(b)$,
(iii) $v(a+b) \geq \min\{v(a), v(b)\}$.

The *value group* of a valuation is the image $v(K^\times)$.

There are some immediate consequences for a valuation $v : K \to \Gamma \cup \{\infty\}$: For every $a \in K$ it holds $v(-a) = v(a)$. For $a \neq 0$ we have $v(a^{-1}) = -v(a)$. Every finite element—that means every element bounded by some natural number—has valuation 0: $v(1) = v(1 \cdot 1) = v(1) + v(1)$, hence, $v(1) = 0$. Now for any finite element r, $1/r$ can be bounded by $1/n$ and n for some $n > r$, thus $v(r) = 0$. Condition (iii) also holds for more than two summands: $v(a_1 + \ldots + a_n) \geq \min\{a_1, \ldots, a_n\}$ for all $n \in \mathbb{N}$ and $a_i \in K$. And finally the inequality in (iii) is an equality $v(a+b) = \min\{v(a), v(b)\}$ if $v(a) \neq v(b)$.

It is not hard to see that the property of being in the same archimedean class forms an equivalence relation. Let Γ be the set of archimedean classes of nonzero element in a field K. We denote by $[a]$ the equivalence class of a. By setting $[a] < [b]$ if and only if $n|b| < |a|$ for every $n \in \mathbb{N}$, we can define an order on Γ. One can easily check that the order is well-defined. We also define an addition on Γ by setting $[a] + [b] := [ab]$. Equipped with this operation and order, Γ becomes an ordered Abelian group with neutral element [1]. We also obtain the following:

6.8 Proposition. *The map $v : K \to \Gamma \cup \{\infty\}$ given by $a \mapsto [a]$ for $a \in K^\times$ and $0 \mapsto \infty$, is a valuation. It reverses order on positive elements, i.e. $0 < a \leq b$ implies that $v(a) \geq v(b)$.*

Proof. We will check the conditions that makes a map into a valuation. It is certainly by definition surjective and (i) is fulfilled. Also (ii) holds by definition.

In order to verify (iii), let $a, b \in K$. If $a = 0$, then $v(a) = \infty$ and $v(a+b) = v(b)$. Similarly for $b = 0$. So let $a, b \neq 0$. First assume that $[a] < [b]$, and that both a and b are positive, as otherwise one can simply consider their negatives. Together these assumptions yield that $nb < a$ for all $n \in \mathbb{N}$, in particular $b < a$. Then it holds $a < a + b \leq n(a + b) = na + nb < na + a = (n + 1)a$. Dividing by a yields

$$\frac{1}{n+1} < 1 < \frac{a+b}{a} < n + 1.$$

Hence, $[a + b] = [a]$.

Now let $[a] = [b]$ and assume that $a \geq b > 0$. Further, assume that $[a+b] < [a]$. Then it follows for all $n \in \mathbb{N}$ that $na < a + b$, in particular, $2a < a + b$. But this yields $a < b$, a contradiction. Hence, $[a + b] \geq [a] = [b]$. This shows condition (iii).

What remains to be shown is that the valuation reverses order on positive elements. Let $a, b \in K$ with $a, b > 0$. Suppose that $a < b$. This implies by definition of the order immediately that $[a] \geq [b]$. Hence $0 < a \leq b$ implies that $v(a) \geq v(b)$. □

From now on, let v denote the above examined valuation, which assigns to each element its archimedean class. We will call this valuation in the following the *natural* valuation.

The natural valuation on K can be extended to the real closure $\overline{K}$:

6.9 Lemma. *Suppose that K is an ordered field. The natural valuation $v : K \to \Gamma \cup \{\infty\}$ can be extended to the natural valuation $\overline{v}$ on the real closure $\overline{K}$ of K. It satisfies $\overline{v} : \overline{K} \to \overline{\Gamma} \cup \{\infty\}$, where $\overline{\Gamma}$ is the divisible hull of Γ, and for all $x \in \overline{K}$, it holds*

$$\overline{v}(x) = \frac{1}{n} \cdot v(y)$$

for some $y \in K$, $y > 0$ and $n > 0$.

Proof. It is easy to see that v can be extended to $\overline{K}$, since $\overline{v}\big|_K = v$. Let $x \in \overline{K} \setminus K$. Let $f(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$ be the minimal polynomial of x over K with $a_n = 1$, $a_0 \neq 0$, and $a_i \in K$ for every $i \in \{0, \ldots, n\}$. Then $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$. Applying the valuation, we obtain

$$v(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x) = v(-a_0).$$

Without loss of generality we assume that for every $i \in \{0, \ldots, n\}$ it holds $a_i \neq 0$, as otherwise we consider only the indices of the nonzero monomials. Suppose that there is $i > j$ such that $v(a_i x^i) = v(a_j x^j)$. This means that $v(a_j) - v(a_i) = v(x^i) - v(x^j)$ and therefore $v(x^{i-j}) = v(a_j/a_i)$. It follows that

$$v(x) = \frac{1}{i-j} \cdot v\left(\frac{a_j}{a_i}\right).$$

If a_j/a_i is negative, by replacing it with a_i/a_j instead, we obtain the claimed form.

If, however, the valuations of the monomials are pairwise different, i.e. if for all $i \neq j$ we have $v(a_i x^i) \neq v(a_j x^j)$, we obtain

$$\begin{aligned} v(a_0) &= v(-a_0) \\ &= \min_{i=1,\dots,n} \{v(a_i x^i)\} \\ &= \min_{i=1,\dots,n} \{v(a_i) + v(x^i)\} \\ &= \min_{i=1,\dots,n} \{v(a_i) + i \cdot v(x)\} \end{aligned}$$

Let $i_0 \in \{0, \dots, n\}$ such that $v(a_{i_0} x^{i_0}) = \min_{i=1,\dots,n}\{v(a_i x^i)\}$. Then $v(a_0) = v(a_{i_0}) + i_0 \cdot v(x)$ and therefore

$$v(x) = \frac{1}{i_0} \cdot v\left(\frac{a_0}{a_{i_0}}\right).$$

As above, if a_0/a_{i_0} is not positive we may replace it by its negative. This proves the claim. □

6.10 Lemma. *Let $\mathcal{K} = (K, A, (P_n), \lambda)$ be a model of the universal theory $\mathrm{RPT}_\forall$, and v the natural valuation on K. Then the following holds:*

(a) Each archimedean class of K is represented by an element in A. Thus, $v(A) = \Gamma$.
(b) $v\big|_A$ has kernel $2^{\mathbb{Z}}$.
(c) There is an isomorphism $A/2^{\mathbb{Z}} \cong \Gamma$.

Proof. (a) For $x > 0$ we have $\lambda(x) \leq x < 2\lambda(x)$ and $\lambda(x) \neq 0$, i.e. $1/2 < 1 \leq x/\lambda(x) < 2$ by **V5**, that means that x and $\lambda(x)$ are part of the same archimedean class. So each archimedean class is represented by an element of A, since $\mathrm{im}(\lambda) \subseteq A$.

(b) $\subseteq$: Let $x \in A$ with $v(x) = 0$. As $[x] = [1]$, there is $n \in \mathbb{N}$ such that $1/n < x < n$. Let $k \in \mathbb{Z}$ be minimal such that $x < 2^{k+1} \leq n$. Then $2^k \leq x < 2^{k+1}$. This yields $1 \leq x/2^k < 2$. By axiom **V2** it follows that $x/2^k = 1$, and thus, $x = 2^k$.

$\supseteq$: Since $v(1) = 0$ and $1/3 < 1/2 < 3$, the numbers 1 and 2 are in the same archimedean class, i.e. $v(2) = 0$. Then also $v(2^k) = 0$ for all $k \in \mathbb{Z}$. And since $2^{\mathbb{Z}} \subseteq A$, we are done.

(c) By (a), every archimedean class has one representative from A. Hence, $v\big|_A$ is is surjective. Then the claim follows from (b) and the first isomorphism theorem. □

From part (c) of Lemma 6.10 it follows that two elements in A which are in the same archimedean class only differ by a power of 2. This means that for $a, b \in A$ with $[a] = [b]$ there exists $n \in \mathbb{Z}$ such that $a \cdot 2^n = b$.

Consider a model $(K, A, (P_n), \lambda)$ of the universal theory $\mathrm{RPT}_\forall$. Depending on the structure of K we may draw different conclusions: If K is a field, it follows that A is a group. This shows Lemma 6.11. If, however, K is even real closed, then $(K, A, (P_n), \lambda)$ is even a model of RPT. We will prove this in Lemma 6.12.

6.11 Lemma. *Let $\mathcal{K} = (K, A, (P_n), \lambda) \models \mathrm{RPT}_\forall$, where K is a field. Then A and P_n are groups with $P_n \subseteq A$.*

Proof. Since $\mathcal{K}$ is a model of the universal theory, by Lemma 2.13, there is a model $\mathcal{R} = (R, B, (Q_n), \mu) \models \mathrm{RPT}$ with $\mathcal{K} \subseteq \mathcal{R}$. Let us fix an arbitrary natural number $n \in \mathbb{N}$. By

definition, B is a group. Clearly, Q_n is closed under multiplication and, if x has an nth root y in B, then also $1/x$ has an nth root in B, namely $1/y$. Hence, also Q_n is a group. Because $\mathcal{K}$ is a substructure of $\mathcal{R}$, it holds $A = B \cap K$. Now B is a group and K is a field, hence, their intersection is also a group. Similarly, it follows that $P_n = Q_n \cap K$ is a group. □

6.12 Lemma. *Let* $\mathcal{K} = (K, A, (P_n), \lambda) \models \mathrm{RPT}_\forall$*, where* K *is a real closed field. Then* $\mathcal{K} \models \mathrm{RPT}$.

Proof. Since $\mathcal{K} \models \mathrm{RPT}_\forall$, there is a model $\mathcal{R} = (R, B, (Q_n), \mu) \models \Sigma^*$ such that $\mathcal{K} \subseteq \mathcal{R}$.

Obviously, axioms **K1**–**K9**, **O1**–**O5**, **RK1**, and **RK2*n*** are satisfied in $\mathcal{K}$, since K is real closed. By Lemma 6.11, A is an ordered Abelian group, hence also axioms **A1**–**A4** hold. Now, **V1**, **V2**, **V4**, and **V5** are universal, hence, preserved downwards in inclusion. They hold in $\mathcal{R}$, therefore they also hold in $\mathcal{K}$. It remains to show **V3*n***. If x has an nth root in A, it is certainly contained in P_n. So, let on the contrary $x \in P_n$. Then $x \in Q_n$, which implies that there is $y \in B$ with $y^n = x$. Since K is real closed, y already lies in K. But $K \cap B = A$. Hence, $y \in A$. This establishes axiom **V3*n*** and finishes the proof. □

6.13 Lemma. *Let* $\mathcal{K} = (K, A, (P_n), \lambda) \models \mathrm{RPT}_\forall$*. For each* $x \in A$ *exactly one of* $x, 2x, \ldots, 2^{n-1}x$ *belongs to* P_n*.*

Proof. By Lemma 2.13, there is $\mathcal{R} = (R, B, (Q_n), \mu) \models \mathrm{RPT}$ with $\mathcal{K} \subseteq \mathcal{R}$. Since R is real closed, the value group of the natural valuation $\overline{v}$ on R is divisible and, therefore, by Lemma 6.10 (c), also $B/2^{\mathbb{Z}}$.

This means: For all $n \in \mathbb{N}$ and for all $x \in B$ there exists $b \in B$ such that $b^n 2^{\mathbb{Z}} = x2^{\mathbb{Z}}$. In other words: $\forall n \in \mathbb{N}\, \forall x \in B\, \exists b \in B\, \exists \ell \in \mathbb{Z}:$

$$b^n = x2^\ell.$$

What remains to be shown is that ℓ can be chosen to be $\ell \in \{0, \ldots, n-1\}$ and is unique: By division with remainder we obtain $\ell = rn + k$ where $k \in \{0, \ldots, n-1\}$ is unique, so $b^n = x \cdot 2^k \cdot (2^r)^n$. Set $\widetilde{b} = b \cdot 2^{-r}$. This yields $\widetilde{b}^n = (b \cdot 2^{-r})^n = x \cdot 2^k$.

Formalizing what we have just shown, this gives us the analogue of axiom **P4*n*** from Presburger Arithmetic:

$$\mathcal{R} \models \forall x \left(B(x) \to \bigvee_{i=0}^{n-1} \left(Q_n(2^i x) \wedge \bigwedge_{j \neq i} \neg Q_n(2^j x) \right) \right) \text{ for all } n \in \mathbb{N}.$$

But this is a universal $\mathcal{L}^*$-formula, hence, preserved downwards in inclusion. Thus, it also holds

$$\mathcal{K} \models \forall x \left(A(x) \to \bigvee_{i=0}^{n-1} \left(P_n(2^i x) \wedge \bigwedge_{j \neq i} \neg P_n(2^j x) \right) \right) \text{ for all } n \in \mathbb{N}.$$

This proves the claim. □

The reader may have noticed some analogues to Presburger Arithmetic. In fact, the theory RPT somehow extends Pr:

6.14 Proposition. *Let* $\mathcal{K} = (K, A, (P_n), \lambda)$ *be a model of* RPT*. Then* $\mathcal{A} = (A, \cdot, \div, <, 1, 2, (P_n))$ *is a model of Presburger Arithmetic.*

Proof. A is certainly an ordered Abelian group. Hence, axioms **AG1**–**AG4** and **O1**–**O4** are satisfied. In the proof of Lemma 6.13, we have shown axiom $\mathbf{P4}\boldsymbol{n}$. As $1 < 2$, axiom **P1** holds. Axiom **V2** immediately implies **P2** and $\mathbf{V3}\boldsymbol{n}$ immediately implies $\mathbf{P3}\boldsymbol{n}$. □

With this preliminary work we are now ready to prove 6.5:

Proof of 6.5. We will use Theorem 6.3 to show that the $\mathcal{L}^*$-theory RPT admits quantifier elimination. For the proof of the first condition let $\mathcal{D} = (D, A, (P_n), \lambda)$ be a model of $\mathrm{RPT}_\forall$. Then, by Lemma 2.13, there is $\mathcal{R} = (R, B, (Q_n), \mu) \models \mathrm{RPT}$ with $\mathcal{D} \subseteq \mathcal{R}$. Note that in the language of ordered rings every substructure is an integral domain. Hence, let K be the fraction field of D. Then K is certainly an ordered field and we have $K \subseteq R$.

We will verify condition (1) in two steps. At first we will show that $\mathcal{R}$ induces an $\mathcal{L}^*$-structure on K and that this $\mathcal{L}^*$-structure is actually independent of the specific choice of $\mathcal{R}$, i.e. is the only one that makes K into a $\Sigma^*_\forall$-model and extends the $\mathcal{L}^*$-structure on $\mathcal{D}$. Secondly, we will show that $\mathcal{R}$ also induces an $\mathcal{L}^*$-structure on the real closure $\overline{K}$ of K and that this is the only one which makes $\overline{K}$ into a model of RPT and extends the $\mathcal{L}^*$-structure on $\mathcal{D}$. We will then see that $\overline{K}$ with the induced structure is a RPT-closure of $\mathcal{D}$.

Step 1: It suffices to show the following:

(a) $B \cap K = \{a/b : \ a, b \in A\}$,
(b) $Q_n \cap K = \{a/b : \ a, b \in P_n\}$, and
(c) for $0 < a, b \in D$, where a/b is positive in K, $\mu(a/b)$ only depends on λ.

We will start by showing (c): So, let $0 < a, b \in D$, such that $a/b > 0$ in K. It holds that $0 < \lambda(a) \leq a < 2 \cdot \lambda(a)$, as well as $0 < \lambda(b) \leq b < 2 \cdot \lambda(b)$, so $\lambda(a)/2\lambda(b) < a/b$, and with similar arguments we get

$$\frac{1}{2} \cdot \frac{\lambda(a)}{\lambda(b)} < \frac{a}{b} < 2 \cdot \frac{\lambda(a)}{\lambda(b)}.$$

Note that μ restricted to D is just λ. Since B is a multiplicative group, it holds that $\lambda(a)/\lambda(b) \in B$, as well as $\lambda(a)/2\lambda(b) \in B$ and $2\lambda(a)/\lambda(b) \in B$.

Now we are in one of the two situations: Either we have $a/b < \lambda(a)/\lambda(b)$ or $a/b \geq \lambda(a)/\lambda(b)$. In the case that

$$\frac{1}{2} \cdot \frac{\lambda(a)}{\lambda(b)} < \frac{a}{b} < \frac{\lambda(a)}{\lambda(b)},$$

it follows that

$$\mu\left(\frac{a}{b}\right) = \frac{1}{2} \cdot \frac{\lambda(a)}{\lambda(b)},$$

as μ assigns to a/b the nearest element of B which is less than or equal to a/b. On the other hand if

$$\frac{\lambda(a)}{\lambda(b)} \leq \frac{a}{b} < 2 \cdot \frac{\lambda(a)}{\lambda(b)},$$

then we obtain

$$\mu\left(\frac{a}{b}\right) = \frac{\lambda(a)}{\lambda(b)}.$$

This shows (c). Now it is easy to see (a): $\supseteq$: If $a, b \in A$, then $a/b = \lambda(a)/\lambda(b) = \mu(a/b)$. Hence, $a/b \in B \cap K$. $\subseteq$: For the other inclusion let $x \in B \cap K$. Then $x = a/b$ for some $a, b \in D$. It

holds $a/b = \mu(a/b) = \lambda(a)/\lambda(b)$. Thus, we obtain

$$B \cap K = \left\{ \frac{a}{b} : a, b \in A \right\}.$$

It remains to show (b): $\supseteq$: Let $a, b \in P_n$. Since $P_n \subseteq Q_n$, it follows that $a, b \in Q_n$. By Lemma 6.11, Q_n is a group. Hence, $a/b \in Q_n$. As a and b are in D, clearly $a/b \in K$. Thus, $a/b \in Q_n \cap K$.

$\subseteq$: Let $a, b \in D$ with $a/b \in Q_n \cap K$. Then $a/b \in B \cap K$, which implies by (a) that there exist x and y in A such that $a/b = x/y$. As $x, y \in A$, by Lemma 6.13, there are unique $\ell, k \in \{0, \ldots, n-1\}$ such that $2^\ell x, 2^k y \in P_n$. Hence,

$$\frac{2^\ell x}{2^k y} = 2^{\ell - k} \cdot \frac{x}{y} = 2^{\ell - k} \cdot \frac{a}{b} \in Q_n.$$

But it already holds that $a/b \in Q_n$. By uniqueness of ℓ and k, it follows $\ell - k = 0 \bmod n$. As $\ell, k \in \{0, \ldots n-1\}$, we obtain $\ell = k$. Thus,

$$\frac{a}{b} = \frac{2^k x}{2^k y},$$

where $2^k x, 2^k y \in P_n$. This proves (b).

Step 2: We will now move on to the real closure $\overline{K}$ of K. Analogously we will show that $\mathcal{R}$ induces an $\mathcal{L}^*$-structure on $\overline{K}$ and that this $\mathcal{L}^*$-structure is independent of the specific choice of $\mathcal{R}$, i.e. that it is the only one that makes $\overline{K}$ into a $\Sigma^*_\forall$-model and extends the $\mathcal{L}^*$-structure on $\mathcal{D}$. In order to do so, we consider the extension $\overline{v} : \overline{K} \to \overline{\Gamma} \cup \{\infty\}$, as in Lemma 6.9. We will show that in the representation

$$\overline{v}(x) = \frac{1}{n} \cdot v(y),$$

y can even be chosen such that $y \in Q_n$:

Since y and $\mu(y)$ are in the same archimedean class and therefore have the same valuation, we can replace y by $\mu(y)$ and, thus, assume without loss of generality that $y \in B$. By Lemma 6.13, then exactly one of $y, 2y, \ldots, 2^{n-1}y$ belongs to Q_n. And since this element is also in the same archimedean class as y itself, it has the same valuation and we may even suppose that $y \in Q_n$. Therefore, it has an nth root in B, say $y^{\frac{1}{n}}$, which has the same archimedean class as the element x, that we started with. Now let us fix an arbitrary $x \in \overline{K}$ with $x > 0$. We are going to show the following:

$$2^k \cdot y^{\frac{1}{n}} \leq x < 2^{k+1} \cdot y^{\frac{1}{n}} \quad \text{for some } k \in \mathbb{Z}. \tag{6.1}$$

Since there is $m \in \mathbb{N}$ such that $1/m < x/y^{\frac{1}{n}} < m$, we can take $\ell \in \mathbb{N}$ such that $2^\ell > m$ and obtain

$$2^{-\ell} y^{\frac{1}{n}} < x < 2^\ell y^{\frac{1}{n}}.$$

Now choose $k \in \mathbb{N}$ such that $k \leq \ell$, and such that $x < 2^{k+1} y^{\frac{1}{n}}$ and $x \geq 2^k y^{\frac{1}{n}}$. Thus,

$$2^k y^{\frac{1}{n}} \leq x < 2^{k+1} y^{\frac{1}{n}}$$

and $2^k y^{\frac{1}{n}} \in B \cap \overline{K}$. Hence, $\mu(x) = 2^k y^{\frac{1}{n}}$. This proves (6.1) and shows that $\overline{K}$ is closed under μ.

It remains to show that $B \cap \overline{K}$ and $Q_n \cap \overline{K}$ are independent of $\mathcal{R}$. In order to do so, we will first show that

$$B \cap \overline{K} = \bigcup_{n=1}^{\infty} \{y^{\frac{1}{n}} : y \in Q_n \cap K\}.$$

$\subseteq$: Let $x \in B \cap \overline{K}$. Then, as shown before, there exist $\widetilde{y} \in Q_n$ and $k \in \mathbb{Z}$, such that $\mu(x) = x = 2^k \widetilde{y}^{\frac{1}{n}}$. Thus, $x = \left(2^{kn}\widetilde{y}\right)^{\frac{1}{n}}$ and by setting $y := 2^{kn}\widetilde{y}$ we obtain that $x = y^{\frac{1}{n}}$, where $y \in B \cap \overline{K}$.

$\supseteq$: For the other inclusion let $n \geq 1$ and $y \in Q_n \cap K$. Then it has an nth root in B, which implies that $y^{\frac{1}{n}} \in B$. Since $\overline{K}$ is real closed, this root also lies in $\overline{K}$. We have already shown that $Q_n \cap K$ is independent of $\mathcal{R}$, i.e. also $B \cap \overline{K}$ is independent of $\mathcal{R}$.

Let us consider $Q_n \cap \overline{K}$. An element x taken from this set is positive, lies in $\overline{K}$, and has an nth root in B. Since $\overline{K}$ is real closed, every positive element has an nth root for every n. So, for this element x to be in $Q_n \cap \overline{K}$, means that its uniquely determined nth root is in B. Hence, we obtain $Q_n \cap \overline{K} = \{x^n : x \in B \cap \overline{K}\}$. As $B \cap \overline{K}$ is independent of $\mathcal{R}$, also $Q_n \cap \overline{K}$ is independent of $\mathcal{R}$.

Thus, we have seen that the induced $\mathcal{L}^*$-structure on $\overline{K}$ by $\mathcal{R}$ is the only one which makes $\overline{K}$ into a model of $\mathrm{RPT}_\forall$ and extends the $\mathcal{L}^*$-structure on $\mathcal{D}$. We denote this $\mathcal{L}^*$-structure by $\overline{\mathcal{K}}$. By Lemma 6.12, $\overline{\mathcal{K}}$ is already a model of RPT. This is the desired RPT-closure of $\mathcal{D}$: Since D is an integral domain, the smallest real closed field that contains D is the real closure of its field of fractions. The induced structure on $\overline{K}$ by an arbitrary supermodel $\mathcal{R}$ is unique. Hence, two different supermodels $\mathcal{R}$ and $\mathcal{R}'$ induce the same structure on $\overline{K}$. This means that $\overline{\mathcal{K}}$ can be embedded over $\mathcal{D}$ into any model $\mathcal{N} \models \mathrm{RPT}$ with $\mathcal{D} \subseteq \mathcal{N}$. Thus, we have completed the proof of the first condition of Theorem 6.3.

Next, we come to the verification of condition (2). Let $\mathcal{K} \subsetneq \mathcal{R}$ be two models of RPT, where $\mathcal{K} = (K, A, (P_n), \lambda)$ and $\mathcal{R} = (R, B, (Q_n), \mu)$. Then either they have the same amount of archimedean classes or R has more archimedean classes than K. We will first consider the case in which they have the same number of archimedean classes: Since each archimedean class is respresented by an element of A, or B, respectively, it follows that A and B coincide: Let $a \in A$. Then there is $b \in B$ with $[a] = [b]$. By Lemma 6.10 (c) there is $\ell \in \mathbb{Z}$ such that $2^\ell a = b$, so $b \in A$. The other implication follows similarly. Hence, $A = B$. Further, μ takes its values in K.

Let $\kappa := |R|$. By Theorem 5.10, there exists a κ-saturated elementary extension of $\mathcal{K}$, say $\widetilde{\mathcal{K}} = (\widetilde{K}, \widetilde{A}, (\widetilde{P_n}), \widetilde{\lambda}))$. Note that K, R, and $\widetilde{K}$ are real closed fields with $K \subseteq R$ and $K \preceq \widetilde{K}$. Denote these embeddings by h and f, respectively. By identifying K with its image under h in R, we may assume that $h = \mathrm{id}$. Since the theory of real closed fields RCF admits quantifier elimination, it is model complete. Hence, h is an elementary embedding. Let $\phi(\overline{v})$ be a formula in the language of ordered rings and $\overline{k} \in K$. We have

$$\widetilde{K} \models \phi(f(\overline{k})) \Leftrightarrow K \models \phi(\overline{k}) \Leftrightarrow R \models \phi(\overline{k}).$$

Thus, f is a partial elementary embedding from $K \subseteq R$ to $\widetilde{K}$. Since $\widetilde{K}, R \models \mathrm{RCF}$, $|R| \leq \kappa$, and $K \preceq \widetilde{K}$, the prerequisites of Lemma 5.11 are fulfilled and the partial elementary embedding from K into $\widetilde{K}$ can be extended to an elementary embedding of ordered fields from R into $\widetilde{K}$.

We will now show that the $\mathcal{L}^*$-structure on R given by $\mathcal{R}$ is the only one that makes R into a model of RPT and extends the $\mathcal{L}^*$-structure of $\mathcal{K}$. Because then the $\mathcal{L}^*$-structure on R induced by $\widetilde{\mathcal{K}}$ coincides with the $\mathcal{L}^*$-structure given by $\mathcal{R}$. Hence, it follows that also $\mathcal{R}$ can be embedded over $\mathcal{K}$ into $\widetilde{\mathcal{K}}$ as models of RPT.

So, suppose there is $\mathcal{R}' = (R, B', (Q'_n), \mu')$, another model of RPT which extends $\mathcal{K}$. Then again, $B' = A = B$. The set Q'_n consists exactly of all the elements in R which have an nth root in $B' = B$, thus, $Q'_n = Q_n$. Since R has the same archimedean classes as K, and $K \subseteq R$, K is dense in R. They both extend λ, therefore, also μ and μ' coincide. So the structure of $\mathcal{R}$ is indeed uniquely determined.

We have shown that $\mathcal{R}$ can be embedded over $\mathcal{K}$ into $\widetilde{\mathcal{K}}$. Hence, for any $b \in R \setminus K$, $\mathcal{K}(b)$ can be embedded over $\mathcal{K}$ into $\widetilde{\mathcal{K}}$, an elementary extension of $\mathcal{K}$.

We come to the second case: If on the other hand R has more archimedean classes than K, then clearly $A \subsetneq B$. So let $b \in B \setminus A$. For each natural number $n \in \mathbb{N}$ we take

$$i_n \in \{0, \ldots, n-1\} \quad \text{such that} \quad b = 2^{i_n} \cdot q_n \text{ for some } q_n \in Q_n.$$

By Lemma 6.13, we can choose i_n this way.

Let us consider the field extension $K(b)$ with the order induced by R. First, we will show that there is a structure on $K(b)$ induced by $\mathcal{R}$. It suffices to show that $K(b)$ is closed under μ, as then an $\mathcal{L}^*$-structure on $K(b)$ is given by

$$\mathcal{K}_b = (K(b), B \cap K(b), (Q_n \cap K(b)), \mu\big|_{K(b)}).$$

For this we need the following identity:

The value group of $K(b)$ is

$$v(K(b)^\times) = v(K^\times) \oplus v(\langle b \rangle) = v(K^\times) \oplus \mathbb{Z} \cdot v(b), \tag{6.2}$$

where $\langle b \rangle$ is the multiplicative group generated by b and the sums are direct. This identity can be found, for instance, in [Kuh, Lemma 6.3]. Hence, for every positive element $x \in K(b)$ there exist $y \in K^\times$ and $\ell \in \mathbb{Z}$ such that $v(x) = v(y) + \ell \cdot v(b) = v(yb^\ell)$, where ℓ is unique. By Lemma 6.10 we can replace y by an element a' of A. It follows that $v(x) - v(a'b^\ell) = v(x \cdot a'^{-1}b^{-\ell}) = 0$, which implies that there is $k \in \mathbb{Z}$ such that $2^k \leq x \cdot a'^{-1}b^{-\ell} < 2^{k+1}$. This yields

$$2^k a'b^\ell \leq x < 2^{k+1}a'b^\ell,$$

which means that every positive element x of $K(b)$ lies between two elements ab^ℓ and $2ab^\ell$ where $a = 2^k a' \in A$ and $\ell \in \mathbb{Z}$. These two elements ab^ℓ and $2ab^\ell$ certainly lie in B and in $K(b)$. Hence, $\mu(x) = ab^\ell \in K(b)$, which implies that $K(b)$ is closed under μ.

Thus, $\mathcal{K} \subseteq \mathcal{K}_b \subseteq \mathcal{R}$ and, therefore, $\mathcal{K}_b \models \mathrm{RPT}_\forall$.

Note that for each n, since $b = 2^{i_n} \cdot q_n$ with $q_n \in Q_n$, we have $q_n = 2^{-i_n} \cdot b \in K(b)$. Thus, $b = 2^{i_n} \cdot q_n$, where $q_n \in Q_n \cap K(b)$.

Next, let $\mathcal{K}'_b = (K(b), A(b), (P_n(b)), \lambda_b)$ be another structure on $K(b)$ satisfying for each $n \in \mathbb{N}$ that $b = 2^{i_n} \cdot s_n$ with $s_n \in P_n(b)$. We will show that $\mathcal{K}'_b = \mathcal{K}_b$, i.e. the following:

(a) $B \cap K(b) = A(b)$,
(b) $Q_n \cap K(b) = P_n(b)$, and
(c) $\mu\big|_{K(b)} = \lambda_b$.

First note that in Q_n, there is t_n such that $b = 2^{i_n} \cdot t_n$. But also there is $s_n \in P_n(b)$ such that $b = 2^{i_n} \cdot s_n$. This, however, implies that $t_n = s_n$. Hence, we obtain $b = 2^{i_n} \cdot q_n$ for some $q_n \in Q_n \cap P_n(b)$.

Now, in order to show (a), we first claim that

$$B \cap K(b) = \{ab^\ell : a \in A \text{ and } \ell \in \mathbb{Z}\}. \tag{6.3}$$

$\supseteq$: Let $x = ab^\ell$ for some $a \in A$ and $\ell \in \mathbb{Z}$. Since $A \subseteq B$, it follows immediately that $x \in B \cap K(b)$.

$\subseteq$: Now, let $x \in B \cap K(b)$. Again by (6.2), for every positive element $x \in K(b)$ there are $a \in A$ and $\ell \in \mathbb{Z}$ such that $v(x) = v(a) + \ell \cdot v(b) = v(ab^\ell)$, where ℓ is unique. This means that x and ab^ℓ are both in B and part of the same archimedean class. Hence, they only differ in a power of 2, i.e. $x = a' \cdot b^\ell$, where $a' = 2^k a \in A$ for some $k \in \mathbb{Z}$. This proves equation (6.3) above.

Next, we will show that

$$\{ab^\ell : a \in A \text{ and } \ell \in \mathbb{Z}\} = A(b), \tag{6.4}$$

as this will imply (a).

$\subseteq$: Consider $P_1(b)$. It holds that $b = 2^{i_1} \cdot q_1$ for some $q_1 \in P_1(b) \cap Q_1$. But $Q_1 = B$ and $b \in B$. Therefore, $i_1 = 0$. Hence, $b \in P_1(b) \subseteq A(b)$. So any element of the form ab^ℓ, where $a \in A$ and $\ell \in \mathbb{Z}$, is contained in $A(b)$.

$\supseteq$: By Lemma 6.10, each archimedean class of $K(b)$ has a representative from $A(b)$. Hence, the identity (6.2) also yields, by the same arguments as before, that for every $x \in A(b)$ there is $a \in A$ and $\ell \in \mathbb{Z}$ such that $x = ab^\ell$. This proves equation (6.4) and, thus, implies (a).

Next, we will show (b): $\subseteq$: Let $x \in Q_n \cap K(b)$. Then $x \in B \cap K(b)$ and, therefore, by (a), there exists $a \in A$ and $\ell \in \mathbb{Z}$ such that $x = ab^\ell$. By assumption there is $q_n \in P_n(b) \cap Q_n$ such that $b = 2^{i_n} \cdot q_n$. This yields that $x = ab^\ell = a \cdot 2^{i_n \ell} q_n^\ell$. As Q_n is a group, we obtain $xq_n^{-\ell} = a \cdot 2^{i_n \ell} \in Q_n$, because $x, q_n \in Q_n$. But $a \in K$. It follows that $xq_n^{-\ell} \in Q_n \cap K = P_n$. Hence, $xq_n^{-\ell} \in P_n$. As $K(b)$ is a field, by Lemma 6.11, also $P_n(b)$ is a group. Thus, since $P_n \subseteq P_n(b)$, we obtain $x = xq_n^{-\ell} q_n^\ell \in P_n(b)$, which was to be shown.

$\supseteq$: On the contrary, let $x \in P_n(b)$. Certainly, $x \in K(b)$. What we need to show is that $x \in Q_n$. By Lemma 6.11, it holds $P_n(b) \subseteq A(b)$. Hence, there is $a \in A$ and $\ell \in \mathbb{Z}$ such that $x = ab^\ell$. Moreover, there is $q_n \in P_n(b) \cap Q_n$ such that $b = 2^{i_n} \cdot q_n$. Hence, $xq_n^{-\ell} = ab^\ell q_n^{-\ell} = a \cdot 2^{i_n \ell}$. As $xq_n^{-\ell} \in P_n(b)$ and $a \in K$, we obtain $a \cdot 2^{i_n \ell} \in P_n(b) \cap K$. But $P_n(b) \cap K = P_n \subseteq Q_n$. Thus, $a \cdot 2^{i_n \ell} \in Q_n$. This yields $x = ab^\ell = a \cdot 2^{i_n \ell} q_n^\ell \in Q_n$. This finishes the proof of (b).

It remains to show (c): We have already shown that for every positive element x of $K(b)$ there is $a \in A$ and $\ell \in \mathbb{Z}$, such that x lies between ab^ℓ and $2ab^\ell$. By part (a), $ab^\ell, 2ab^\ell \in B \cap K(b)$ and also $ab^\ell, 2ab^\ell \in A(b)$ Hence, $\mu\big|_{K(b)}$ and λ_b coincide. This shows (c).

Hence, we have shown that $\mathcal{K}'_b = \mathcal{K}_b$. We will from now on simply write

$$\mathcal{K}_b = (K(b), A(b), (P_n(b)), \lambda_b).$$

Now, let $\overline{\mathcal{K}_b} = (\overline{K(b)}, \overline{A(b)}, (\overline{P_n(b)}), \overline{\lambda_b})$ be the RPT-closure of $\mathcal{K}_b$. We showed in condition (1) that this exist and that $\overline{K(b)}$ is the real closure of $K(b)$.

Let $\kappa := |\overline{A(b)}|$ and let $\widetilde{\mathcal{K}} = (\widetilde{K}, \widetilde{A}, (\widetilde{P_n}), \widetilde{\lambda})$ be a κ-saturated elementary extension of $\mathcal{K}$. Let us call this elementary embedding ψ. Since $\mathcal{K}$, $\widetilde{\mathcal{K}}$, and $\overline{\mathcal{K}_b}$ are models of RPT, by Lemma 6.14, the structures $\mathcal{A} = (A, \cdot, \div, <, 1, 2, (P_n))$, $\widetilde{\mathcal{A}} = (\widetilde{A}, \cdot, \div, <, 1, 2, (\widetilde{P_n}))$, and $\overline{\mathcal{A}_b} = (\overline{A(b)}, \cdot, \div, <, 1, 2, (\overline{P_n(b)}))$ are models of Pr. Moreover, $\widetilde{\mathcal{A}}$ is as well a κ-saturated elementary extension of $\mathcal{A}$ with elementary embedding $\phi = \psi\big|_A$. Since $\mathcal{A} \preceq \widetilde{\mathcal{A}}$, $\mathcal{A} \subseteq \overline{\mathcal{A}_b}$ and the theory of Presburger

Arithmetic eliminates quantifiers, we are in the same situation as earlier with RCF and can, thus, apply Lemma 5.11. We obtain that $\phi : \mathcal{A} \to \widetilde{\mathcal{A}}$ extends to an elementary embedding $\phi' : \overline{\mathcal{A}_b} \to \widetilde{\mathcal{A}}$.

We will now extend ψ to an embedding ψ' from $\mathcal{K}_b$ into $\widetilde{\mathcal{K}}$. In order to do so, we only need to determine the image of b under ψ'. Since each archimedean class from $K(b)$ is already represented in $A(b)$ and ϕ' preserves the order on $\overline{A(b)}$ and, hence, on $A(b)$, we can define $\psi'(b) = \phi'(b)$. Now ψ' embeds $K(b)$ into $\widetilde{K}$ as ordered fields. We will from now on write ψ' as the identity map.

Now, since $K(b) \subseteq \widetilde{K}$ and $\widetilde{\mathcal{K}} \models \mathrm{RPT}$, by earlier observations $\widetilde{\mathcal{K}}$ induces an $\mathcal{L}^*$-structure on $K(b)$. Moreover, since $b \cdot 2^{-i_n} \in P_n(b) \subseteq \overline{P_n(b)}$,

$$b \cdot 2^{-i_n} = \psi'(b \cdot 2^{-i_n}) = \phi'(b \cdot 2^{-i_n}) \in \widetilde{P_n}.$$

So, $b = 2^{i_n} \cdot p_n$ for some $p_n \in \widetilde{P_n}$. Hence, the $\mathcal{L}^*$-structure which $\widetilde{\mathcal{K}}$ induces on $K(b)$ is $\mathcal{K}_b$. Thus, $\mathcal{K}_b \subseteq \widetilde{\mathcal{K}}$ and this embedding preserves $\mathcal{K}$.

In order to finally establish condition (2), we need to show that $\mathcal{K}(b)$, the smallest substructure of $\mathcal{R}$ which contains both K and b, can be embedded over $\mathcal{K}$ into $\widetilde{\mathcal{K}}$. But since $\mathcal{K}_b$ is a substructure of $\mathcal{R}$ whose underlying universe contains both K and b, also $\mathcal{K}(b) \subseteq \mathcal{K}_b$. As $\mathcal{K}(b)$ is embedded in $\mathcal{K}_b$ over $\mathcal{K}$, it is also embedded in $\widetilde{\mathcal{K}}$ over $\mathcal{K}$.

This finishes our proof. □

Of course, one can replace the number 2 by any positive real number, since it does not play any special role in the results. More precisely, let c be a new constant symbol, and let c-RPT be theory RPT except that "2" is everywhere replaced by "c" and the axiom $c > 1$ is added. We then get the following result:

6.15 Corollary. *c-RPT admits elimination of quantifiers.*

In the proof, we have seen that one is rather free in the choice of b. In [vdD], van den Dries points out that this is the main difference of his quantifier elimination test to the usual tests.

7 Applications

Quantifier elimination is a very powerful property, as it helps in the question of completeness and decidability as well as in the study of definable sets. It also has some geometric interpretations and, hence, many applications in algebraic geometry (see for example [BoCoRo]). The well-known *Tarski–Seidenberg Theorem* or *Hilbert's 17th Problem* follow from quantifier elimination in real closed fields, whereas *Hilbert's Nullstellensatz* follows from quantifier elimination of algebraically closed fields, just to name a few geometric results. In differential algebra, there exists an analogue of Hilbert's Nullstellensatz, which follows from quantifier elimination in differentially closed fields.

This chapter pursues the goal of giving a few examples from different realms of what quantifier elimination can lead to. We will first see one geometric consequence of quantifier elimination, namely the Differential Nullstellensatz. Afterwards we will set our focus on completeness and decidability. We will conclude this last chapter and hereby this thesis with a section on applications of quantifier elimination to the better understanding of definable sets.

7.1 One Geometric Consequence

There are many geometric interpretations of quantifier elimination of different theories. Without denying the importance of such, we will only give one here. While Hilbert's Nullstellensatz for algebraically closed fields is a fundamental theorem in algebraic geometry, there is an analogue in differential algebra, namely the Differential Nullstellensatz. Since the Differential Nullstellensatz is not as well-known, we decided to give a proof of this theorem instead. We will deduce it from quantifier elimination in differentially closed fields.

7.1 Theorem (Differential Nullstellensatz)**.** *Let k be a differential field of characteristic 0 and let Σ be a finite system of differential polynomial equations and inequations over k in several unknowns such that Σ has a solution in some extension $\ell \supseteq k$. Then Σ has a solution in any differentially closed field $K \supseteq k$.*

Proof. See for example [Mar96, Corollary 2.6] or [Poi, Theorem 6.17]. Let L be a differentially closed field containing ℓ and let K be an arbitrary differentially closed field containing k. Their existence is ensured by Theorem 5.24. Since $\ell \subseteq L$, there is also in L a solution to Σ. We will show that K contains a solution to Σ.

The differential field k is a common substructure of L and K. Applying Theorem 3.3, by quantifier elimination, $L \models \exists \bar{v}\ \Sigma(\bar{v})$ implies $K \models \exists \bar{v}\ \Sigma(\bar{v})$. Hence, every differentially closed extension of k contains a solution to Σ. □

7.2 Completeness and Decidability

Lemma 2.7 shows that in a complete theory all of its models satisfy the same $\mathcal{L}$-sentences. This is a very powerful property. In this section we will prove completeness and decidability for all of the treated theories. In the case of decidability we will not give proofs in much detail.

The following theorem gives a sufficient condition for completeness.

7.2 Theorem. *Let $\mathcal{T}$ be a model complete $\mathcal{L}$-theory. If there is $\mathcal{M}_0 \models \mathcal{T}$ which embeds into every model of $\mathcal{T}$, then $\mathcal{T}$ is complete.*

Proof. Suppose that there is $\mathcal{M}_0 \models \mathcal{T}$ such that $\mathcal{M}_0$ embeds into every model of $\mathcal{T}$. Consider two models $\mathcal{M}, \mathcal{N} \models \mathcal{T}$. Then there is an $\mathcal{L}$-embedding from $\mathcal{M}_0$ into $\mathcal{M}$ and one from $\mathcal{M}_0$ into $\mathcal{M}$. Since $\mathcal{T}$ is model complete, the $\mathcal{L}$-embeddings are elementary. Hence, for every $\mathcal{L}$-sentence ϕ we have

$$\mathcal{M} \models \phi \quad \Leftrightarrow \quad \mathcal{M}_0 \models \phi \quad \Leftrightarrow \quad \mathcal{N} \models \phi.$$

Thus, $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent and, by Lemma 2.7, $\mathcal{T}$ is complete. □

We will now apply this theorem to our previous theories and show that all of them are complete.

7.3 Corollary. *(i) The theory* ACF *of algebraically closed fields of characteristic* 0 *in the language of rings is complete.*
(ii) The theory RCF *of real closed fields in the language of ordered rings is complete.*
(iii) The theory Pr *of Presburger Arithmetic in the language $\langle +, -; <, P_2, P_3, \ldots; 0, 1\rangle$ is complete.*
(iv) The theory DCF *of differentially closed fields of characteristic* 0 *in the language $\langle +, -, \cdot, \delta; 0, 1\rangle$ is complete.*
(v) The theory RPT *in the language $\mathcal{L}^* = \langle +, -, \cdot, \lambda; <, A, P_1, P_2, P_3, \ldots; 0, 1\rangle$ is complete.*

Proof. (i) ACF is the theory of algebraically closed fields of characteristic 0. The field of the rationals $\mathbb{Q}$ is contained in every infinite field. Thus, the algebraic closure of $\mathbb{Q}$ can be embedded into every model of ACF. Quantifier elimination implies model completeness. Hence, ACF is complete.

(ii) Every real closed field has characteristic 0. Thus, $\mathbb{Q}$ is also contained in every real closed field. Hence, the real closure of $\mathbb{Q}$ can be embedded into every model of RCF. By quantifier elimination, RCF is complete.

(iii) Every model of Pr contains the ring of integers $\mathbb{Z}$. Since Pr allows elimination of quantifiers and is therefore model complete, Pr is complete.

(iv) DCF is the theory of differentially closed fields of characteristic 0. The field of rationals $\mathbb{Q}$ together with the natural derivation $\delta(c) = 0$ for all $c \in \mathbb{Q}$ is contained in every model of DCF. Hence, again by quantifier elimination, DCF is complete.

(v) Let $\mathbb{Q}^{\mathrm{rc}}$ be the real closure of $\mathbb{Q}$. As $\mathbb{Q}^{\mathrm{rc}}$ is contained in every real closed field, and $2^{\mathbb{Z}}$ is contained in every multiplicative subgroup of positive elements of $\mathbb{Q}^{\mathrm{rc}}$ that contains 2, $(\mathbb{Q}^{\mathrm{rc}}, 2^{\mathbb{Z}})$ can be embedded into every model of RPT. Hence, also RPT is complete. □

Next we come to the concept of decidability. Whenever we use the term "algorithm", the reader who is familiar with theoretical computer science may imagine a register machine or a

Turing machine. They are abstract models of computation which are used to simulate the logic of algorithms. For this part we refer to [Mar02, page 42] or, for a more detailled approach, see [EbFlTh, Sections 10.2 and 10.6].

7.4 Definition. A set S is called *recursive* if there is an algorithm that decides after a finite number of steps whether a given object is an element of the set or not. An $\mathcal{L}$-theory $\mathcal{T}$ is called *decidable* if there is an algorithm that, when given an $\mathcal{L}$-sentence ϕ as input, decides whether $\mathcal{T} \models \phi$.

7.5 Proposition. *Every $\mathcal{L}$-theory $\mathcal{T}$ which is recursively axiomatizable and complete is decidable.*

Proof. See for example [EbFlTh, Satz 10.6.5]. Since many authors use different definitions, we will roughly explain how the proof works: One first shows that $\mathcal{T}$ is recursively enumerable. This means, we show that there is an algorithm which lists exactly the $\mathcal{L}$-sentences ϕ in $\mathcal{T}$. Let Σ be the recursive axiom system of $\mathcal{T}$. Let us first have a list of all $\mathcal{L}$-sentences. Since Σ is recursive, the algorithm can then decide whether or not the antecedent of each $\mathcal{L}$-sentence ϕ is in Σ or is a conjunction of elements of Σ. If this is the case, then the algorithm shall put the consequent of ϕ on the list.

Now, we have a list of all $\mathcal{L}$-sentences in $\mathcal{T}$. Then for a given $\mathcal{L}$-sentence ϕ the algorithm can go systematically through the list and check whether it finds ϕ or $\neg\phi$. □

This proposition yields the following strong results:

7.6 Corollary. *All of the theories from Corollary 7.3 that we have treated in this thesis are decidable.*

It was Tarski who first showed completeness and decidability for the field of real numbers. His proof gave an explicit algorithm for eliminating quantifiers. This proof can be found in [Tar, Section 2]. He makes use of Theorem 3.2 and gives an algorithm to eliminate one existential quantifier at a time. In fact, in his paper, he shows even more: Tarksi gave a decision method, i.e. an algorithm that decides for a given sentences in a finite number of steps if it is contained in a certain class of sentences or not.

So far, all our proofs of quantifier elimination have been non-constructive. Tarksi, however, provided for the theory of real closed fields an algorithm to explicitly find an equivalent quantifier-free formula. Also, Presburger's proof of quantifier elimination for Presburger Arithmetic was constructive. In fact, in all of our cases one can give an explicit effective procedure. The following lemma tells us that for decidable theories there is an algorithm to eliminate quantifers.

7.7 Theorem. *Consider a decidable $\mathcal{L}$-theory $\mathcal{T}$ which allows elimination of quantifiers. Then there is an algorithm which, when given an $\mathcal{L}$-formula $\phi(\overline{v})$ as input, will output a quantifier-free $\mathcal{L}$-formula $\psi(\overline{v})$ such that $\mathcal{T} \models \forall\overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$.*

Proof. See [Mar02, Proposition 3.1.22]. Given $\phi(\overline{v})$ as an input, the algorithm searches for a quantifier-free formula $\psi(\overline{v})$ such that $\mathcal{T} \models \forall\overline{v}\ (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. Since $\mathcal{T}$ is decidable this is an effective search. Because $\mathcal{T}$ has quantifier-elimination, we will eventually find $\psi(\overline{v})$. □

Even though there exist algorithms for effective quantifier elimination, the complexities of these algorithms are in general very high.

In [vdD], van den Dries asks the question whether similar results as completeness and decidability could be obtained for the structure $(\mathbb{R}, 2^{\mathbb{Z}}, 3^{\mathbb{Z}})$. Philipp Hieronymi answered this question in [Hie] negatively: If another predicate for a multiplicative discrete set is added to RPT, then this theory defines the integers. By Gödels Incompleteness Theorem, this means that the theory cannot be complete nor decidable.

7.3 Definable Sets

In model theory we often try to understand which sets one can achieve by only using symbols from the language. Such sets are called *definable*.

7.8 Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $B \subseteq M$. A set $S \subseteq M^n$ is called *B-definable* if there is an $\mathcal{L}$-formula $\phi(v_1, \ldots, v_n, \overline{w})$ and $\overline{b} \in B$ such that

$$S = \{\overline{a} \in M^n : \mathcal{M} \models \phi(\overline{a}, \overline{b})\}.$$

If $B = \emptyset$, we say that S is *0-definable*. A function $f : M^n \to M$ is called *B-definable* if its graph $\{(\overline{x}, y) : f(\overline{x}) = y\} \subseteq M^{n+1}$ is a B-definable set.

We will give a few consequences of quantifier elimination to the understanding of definable sets. The first one is a well-known result about real closed fields. We will start with the definition of o-minimality:

7.9 Definition. Let $\mathcal{T}$ be a theory in a language $\mathcal{L}$ containing $<$, such that the linear order axioms **O1**, **O2**, and **O3** hold in each model of $\mathcal{T}$. Then $\mathcal{T}$ is called *o-minimal*, if for each $\mathcal{M} \models \mathcal{T}$, every definable subset of M is a finite union of points and intervals with endpoints in $M \cup \{\pm\infty\}$.

O-minimality was introduced by Anand Pillay and Charles Steinhorn in 1984, based on van den Dries' ideas. Its aim was to generalize some model-theoretic properties of the field of the real numbers, cf. [Hod, page 82].

7.10 Theorem. *The theory* RCF *is an o-minimal theory.*

Proof. See [Mar02, Corollary 3.3.23]. Let $R \models \mathrm{RCF}$. By quantifier elimination, every definable subset of R is a finite Boolean combination of sets of the form $\{x \in R : p(x) = 0\}$ and $\{x \in R : q(x) > 0\}$. Solution sets of the first type are finite or, in case of the zero-polynomial, they contain all $]-\infty, +\infty[$. Sets of the second form are finite unions of intervals. Hence, we conclude that any definable set is a finite union of points and intervals, also allowing $\pm\infty$ as endpoints. □

One implication of quantifier elimination of RPT that gives us control over the definable sets, is the following theorem, which van den Dries gave in [vdD]:

7.11 Theorem. *Each subset of $\mathbb{R}$ which is $\mathbb{R}$-definable in $\mathcal{L}^*$ is the union of an open set and a countable set.*

Proof. See [vdD, §1. Corollary]. The proof is by induction on complexity of terms. □

One further consequence of quantifier elimination is based on the universal axiomatizability of RPT in an extended language. This axiomatization is obtained as follows:

If we have a brief look at the axioms of RPT, one sees that there are two obstacles: Firstly this is the axiom **A4**, namely the existence of multiplicatively inverse elements. And secondly, axioms $\mathbf{V3}\boldsymbol{n}$ contain existential quantifiers. We can, however, add 0-definable functions to the language.

Let $\mathcal{L}^{**}$ be the language $\mathcal{L}^{*}$ expanded by the new function symbols f and g_n for each $n \in \mathbb{N}$. For the function symbol f we define two new axioms:

U1: $\forall x \forall y\ (f(x) = y \leftrightarrow x \cdot y = 1)$
A4': $\forall x\ A(f(x))$.

Additionally, for the function symbols g_n we define two new classes of axioms

U2*n*: $\forall x \forall y\ ((x \leq 0 \to g_n(x) = 0) \wedge (x > 0 \to (g_n(x) = y \leftrightarrow x^n = y))$
V3*n*': $\forall x\ (P_n(x) \leftrightarrow A(g_n(x)))$.

Now RPT$'$ is obtained from the axioms of RPT except for **A4** and **V3*n*** plus the above defined axioms, i.e.

$$\mathrm{RPT}' = \mathrm{RPT} \setminus \{\textbf{A4},\ \textbf{V3}\boldsymbol{n}, \text{ for all } n \in \mathbb{N}\} \cup \{\textbf{U1},\ \textbf{A4'},\ \textbf{U2}\boldsymbol{n},\ \textbf{V3}\boldsymbol{n}\textbf{'}, \text{ for all } n \in \mathbb{N}\}.$$

The $\mathcal{L}^{**}$-theory RPT$'$ is axiomatized only by universal $\mathcal{L}^{**}$-sentences and, hence, has universal axiomatization. Since the functions f and g_n are definable in the original language $\mathcal{L}^{*}$, we do not obtain any more definable sets after augmenting the language by these function symbols. Also note that we do not change the property of having quantifier elimination: Any $\mathcal{L}^{**}$-formula in which f or g_n occurs is equivalent to an $\mathcal{L}^{*}$-formula and, hence, to a quantifier-free formula.

The consequence of the above observations is the following result due to Chris Miller's doctoral student Michael Tychonievich:

7.12 Proposition. *Let $A \subseteq \mathbb{R}^n$ be an $\mathbb{R}$-definable set in $(\mathbb{R}, 2^{\mathbb{Z}})$. Then there exists $k \in \mathbb{N}$ and an $(n+k)$-ary set B that is $\mathbb{R}$-definable such that the following holds: $x \in A$ if and only if there exists $y \in (2^{\mathbb{Z}})^k$ such that $(x, y) \in B$.*

This result can be found in [Tyc, Corollary 4.1.7]. However, we would like to mention that during the research for this thesis we discovered a gap in his proof. In correspondence with Miller, the result is still true and it follows from the fact that RPT$'$ has universal axiomatization.

Filling the gap is not subject of this work but might be of interest for future investigation.

Bibliography

[BoCoRo] J. Bochnak, M. Coste and M. Roy, *Real Algebraic Geometry* (Springer, Berlin & Heidelberg, 1998).

[Del] K. Delvin, *The Joy of Sets: Fundamentals of Contemporary Set Theory*, Undergrad. Texts Math., 2nd edn (Springer, New York, 1993).

[DoMoTa] J. E. Doner, A. Mostowski and A. Tarski, 'The elementary theory of well-ordering—a metamathematical study', *Logic Colloquium* 77, vol. 96 (eds A. Macintyre, L. Pacholski and J. Paris; North-Holland Publishing Company, 1978) 1–54.

[vdD] L. van den Dries, 'The field of reals with a predicate for the powers of two', *Manuscripta Math.* 54 (Springer, Berlin, 1986) 187–196.

[EbFlTh] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Einführung in die mathematische Logik*, 5th edn (Springer, Berlin & Heidelberg, 2007).

[Hie] P. Hieronymi, 'Defining the Set of Integers in Expansions of the Real Field by a Closed Discrete Set', *Proc. Amer. Math. Soc.* 138, no. 6 (Providence, RI., 2010) 2163–2168.

[Hod] W. Hodge, *Model Theory*, Encyclopedia of Mathematics and its Applications (Cambridge University Press, 1993).

[Kha] M. Khani, 'The first order theory of a dense pair and a discrete group', PhD Thesis, University of Manchester, 2013.

[KnSc] M. Knebusch and C. Scheiderer, *Einführung in die reele Algebra* (Vieweg, Braunschweig & Wiesbaden, 1989).

[Kuh] S. Kuhlmann, *Ordered Exponential Fields*, The Fields Institute for Research in Mathematical Sciences 12 (Amer. Math. Soc., Providence, RI., 2000).

[Man] M. Manzano, *Model Theory*, Oxford Logic Guides (trans. R. J. G. B. de Queiroz; Clarendon Press, New York, 1999).

[Mar96] D. Marker, 'Chapter 2: Model Theory of Differential Fields', *Model Theory of Fields*, Lect. Notes Log. 5 (eds D. Marker, M. Messmer and A. Pillay; Springer, Berlin, 1996) 38–113.

[Mar00] D. Marker, 'Model Theory of Differential Fields', *Model Theory, Algebra, and Geometry*, Math. Sci. Res. Inst. Publ. 39, (Cambridge Univ. Press, Cambridge, 2000) 53–63.

[Mar02] D. Marker, *Model Theory: An Introduction*, Grad. Texts in Math. 217 (Springer, New York, 2002).

[FaFaSm] A. McFarland, J. McFarland and J. T. Smith (eds), Alfred Tarski, *Early Word in Poland—Geometry and Teaching* (Birkhäuser, New York, 2014).

[Gra] T. McGrail, 'The Model Theory of Differential Fields with Finitely Many Com-

muting Derivations', *J. Symb. Log.* 65, no. 2 (2000) 885–913.

[Mil] C. Miller, 'Tameness in Expansions of the real field', *Logic Colloquium '01*, Lect. Notes Log. 20 (Urbana, IL, 2005) 281–316.

[Poi] B. Poizat, *A Course in Model Theory*, An Introduction to Contemporary Mathematical Logic, Universitext (eds S. Axler, F.W. Gehring, K.A. Ribet; Springer, New York, 2000).

[Pre86] A. Prestel, *Einführung in die mathematische Logik und Modelltheorie*, Aufbaukurs Mathematik, vol. 60 (Vieweg-Studium, Braunschweig & Wiesbaden, 1986).

[Pre98] A. Prestel, *Model Theory for the Real Algebraic Geometer*, Dottorato di ricerca in matematica (Istituti editoriali e poligrafici internazionale, Pisa, 1998).

[Sac72a] G. E. Sacks, 'The differential closure of a differential field', *Bull. Amer. Math. Soc.* 78 (1972) 629–634.

[Sac72b] G. E. Sacks, *Saturated Model Theory*, Mathematics lecture note series (Benjamin, Reading, 1972).

[Tar] A. Tarski, 'A Decision Method for a Elementary Algebra and Geometry', *Project Rand* (Rand Corporation, 1948).

[Tyc] M. Tychonievich, 'Tameness Results for Expansions of the Real Field by Groups', Dissertation, Ohio State University, 2013.

[UoI] University of Illinois, 'Lou van den Dries', `https://cas.illinois.edu/person/lou-van-den-dries` (2017).

Declaration of Independent Work

I herby affirm that I have independently written the attached Master's thesis on the topic

"Quantifier Elimination Tests and Examples"

and have not used any other aids or sources other than those I have indicated.

For parts that use the wording or meaning coming from other works, I have identified them in each case by reference to source or the secondary literature.

Furthermore, I hereby affirm that the above mentioned work has not been published or otherwise submitted as a thesis for a Master examination.

Konstanz, 20 June 2017