Lothar Sebastian Krapp

Real Closed Fields and Integer Parts

Sommersemester 2022

Fachbereich Mathematik und Statistik
Universität Konstanz

Last update: 29 July 2022

Dr. Lothar Sebastian Krapp
Universität Konstanz
Fachbereich Mathematik und Statistik
Universitätsstraße 10
78464 Konstanz
E-Mail: sebastian.krapp@uni-konstanz.de

Contents

1. Introduction **1**

2. Model Theory **5**

2.1. Structures 5

2.1.1. $\mathcal{L}$-structures 5

2.1.2. Embeddings and Automorphisms 7

2.2. Terms and Formulas 8

2.2.1. Recursive Construction of Terms 9

2.2.2. Recursive Construction of Formulas 10

2.2.3. Variables and Interpretations 11

2.3. Definable Sets 14

2.3.1. Definability 14

2.3.2. Preservation under Automorphisms 15

2.4. Substructures and Quantifiers 16

2.4.1. Existential and Universal Formulas 16

2.4.2. Preservation Laws 18

2.5. Theories and Axioms 19

2.5.1. Theories 19

2.5.2. Elementary Equivalence 20

2.5.3. Axiom Systems 21

3. Models of Arithmetic **23**

3.1. Peano Arithmetic 23

3.1.1. Axiomatisation 23

3.1.2. Standard and Non-Standard Parts 24

3.1.3. Definable Sets 26

3.1.4. Number Theory 27

3.2. Open Induction 31

3.2.1. Axiomatisation 31

3.2.2. Number Theory 31

4. Real Algebra and Real Closed Fields **33**

4.1. Real Algebra 33

4.1.1. Real Fields 33

4.1.2. Real Closed Fields 35

4.1.3. Sturm Sequences and Uniqueness of Real Closure 38

4.2. Quantifier Elimination . . . 48
4.2.1. Algorithm . . . 48
4.2.2. Implications . . . 58

5. Shepherdson's Theorem **61**
5.1. Rings and Semirings . . . 61
5.1.1. Open Induction for Rings . . . 61
5.1.2. Integer Parts . . . 62
5.2. Statement and Proof . . . 63

6. Hahn Fields **67**
6.1. Generalised Power Series . . . 67
6.1.1. Well-Orderings and Ordinals . . . 67
6.1.2. Definitions . . . 72
6.2. Rayner Fields . . . 73
6.2.1. Field Properties . . . 73
6.2.2. Orderings . . . 77
6.3. Valuation Theory . . . 78
6.3.1. Valuations . . . 78
6.3.2. Natural Valuation . . . 80
6.3.3. Henselian Valuation . . . 82

7. Mourgues–Ressayre Theorem **85**
7.1. Ordered Hahn Fields . . . 85
7.1.1. Residue Field and Value Group . . . 85
7.1.2. Truncation Closed Subfields . . . 88
7.2. Statement and Proof . . . 89
7.2.1. Integer Parts via Pullbacks . . . 89
7.2.2. Construction of Truncation Closed Embedding . . . 90
7.3. Models of Open Induction . . . 100
7.3.1. Irrationality of $\sqrt{2}$ . . . 100
7.3.2. Euclid's Theorem . . . 101

A. Appendix **103**
A.1. Abbreviations within Formulas . . . 103

Bibliography **105**

Index **108**

1. Introduction

Two of the most fundamental algebraic structures are the discretely ordered ring of integers $\mathbb{Z}$ and the ordered field of real numbers $\mathbb{R}$. While questions from, for instance, Elementary Number Theory are set within $\mathbb{Z}$, a wide range of mathematics – from Real Algebraic Geometry to Real Analysis – is conducted over $\mathbb{R}$. In this lecture, we study the interplay of $\mathbb{Z}$ and $\mathbb{R}$ from both a logical and an algebraic perspective.

The logical – or, more precisely, model theoretical – perspective leads to the study of suitable axiom systems formulated in first-order logic. Since this type of logic is not powerful enough to express features like the Completeness Axiom or the Archimedean Property, the axiom systems we work with lead to a wide range of algebraic structures to examine. The underlying language is given by $\mathcal{L}_{\text{or}} = \{+, -, \cdot, 0, 1, <\}$ (the language of ordered rings). All logical statements over this language are only allowed to use standard logical symbols like $\wedge$ and $\neg$ as well as arithmetical expressions only using the operations specified in $\mathcal{L}_{\text{or}}$. Both $\mathbb{Z}$ and $\mathbb{R}$ are naturally equipped with binary operations $+$, $-$, $\cdot$, constants 0 and 1 as well as a strict total ordering $<$. Thus, $\mathcal{L}_{\text{or}}$ is a suitable language to formulate axiom systems describing $\mathbb{Z}$ and $\mathbb{R}$. When we aim to find such axiom systems, we try to translate the most fundamental properties into sentences formulated in the language $\mathcal{L}_{\text{or}}$:

- For the ordered field of real numbers $(\mathbb{R}, +, -, \cdot, 0, 1, <)$, the corresponding axiom system describes $\mathbb{R}$ as an *ordered field* with the property that *any positive number has a square root* and *any polynomial of odd degree has a zero*. For instance, the sentence

  $$\forall x \; x + 0 = x$$

  asserts that 0 is the additive (right-)neutral element of $\mathbb{R}$, and the sentence

  $$\forall x \; (0 < x \to \exists y \; x = y \cdot y)$$

  guarantees the existence of square roots of any non-negative element. An algebraic structure satisfying all the axioms described above is called a **real closed field**. The axiom system for real closed fields has the powerful property that any sentence in the language $\mathcal{L}_{\text{or}}$ can either be proved or disproved from the axioms.

- Describing the discretely ordered ring $(\mathbb{Z}, +, -, \cdot, 0, 1, <)$ axiomatically is more problematic. Certainly the property that $\mathbb{Z}$ is an *ordered ring with* 1 *as least positive element* is fundamental in the description of $\mathbb{Z}$. However, this property alone does not suffice to prove many results from Elementary Number Theory. A key feature of $\mathbb{Z}$ is that statements true for all non-negative integers can be proved by induction. The axiom system describing $\mathbb{Z}$ as an ordered ring with 1 as least positive element and allowing induction is called **Peano Arithmetic**. While Peano Arithmetic is powerful enough to prove most results

from Elementary Number Theory we know, there are sentences the are true for $\mathbb{Z}$ but not deducible from Peano Arithmetic. Unlike for $\mathbb{R}$, there is no possible way to effectively and fully describe $\mathbb{Z}$ by axioms in the language $\mathcal{L}_{\text{or}}$!

The algebraic perspective of this lecture deals with the study of ordered rings and fields satisfying the axiom systems described above. Among all real closed fields, we are mainly interested in those without the Archimedean Property. These non-archimedean fields admit infinitely large and thus also infinitesimally small elements – which will lead to methods from Valuation Theory to keep control over these infinite and infinitesimal sizes. Starting with such a real closed field $(K, +, -, \cdot, 0, 1, <)$, we may consider any subring of $Z \subseteq K$ with 1 as least positive element. We call Z an **integer part** of K if it has the follwoing property:

$$\textit{For any } a \in K \textit{ there exists } b \in Z \textit{ such that } b \leq a < b + 1.$$

In other words, Z is an integer part of K if any element $a \in K$ can be "rounded down" to a unique element $\lfloor a \rfloor = b \in Z$. Naturally, this property describes the order-theoretic interplay between $\mathbb{Z}$ and $\mathbb{R}$ (or any ordered subfield of $\mathbb{R}$ like $\mathbb{Q}$): for any real number r there is a unique integer directly below r.

The main aim of this lecture is to prove two of the main results in the study of integer parts of real closed fields:

1. The Mourgues–Ressayre Theorem (cf. [8]): *Any real closed field admits an integer part.*
2. Shepherdson's Theorem (cf. [9]): *An ordered ring $(Z, +, -, \cdot, 0, 1, <)$ is an integer part of a real closed field if and only if it is a model of open induction.*

At first glance, the Mourgues–Ressayre Theorem may seem unsurprising or even not difficult to prove. However, it turns out that most discretely ordered subrings of ordered fields are not an integer part thereof: in the non-archimedean case the "rounding down" property is difficult to achieve and requires some care in the choice of the desired subring. In fact, there are even ordered fields (that are not real closed) which do not admit any integer part at all. Proving the existence of an integer part for an arbitrary real closed field will require technical methods set in fields of generalised power series.

Shepherdson's Theorem is rather set in the model theoretic part of this lecture. Open induction is an axiom system similar to Peano Arithmetic except that induction is only allowed for logical formulas without quantifiers (i.e. without the use of $\forall$ and $\exists$). (It is therefore a fragment of Peano arithmetic.) Within open induction, many number theoretic results like the irrationality of $\sqrt{2}$ cannot be proven, and there is even a model of open induction in which the set of prime numbers has an upper bound.

Overall, the main theme of this lecture is the interplay between model theory and algebra with particular focus on discretely ordered rings and real closed fields. This interplay is also reflected in the different sections, each of which deals with a specific topic from real algebra or model theory.

General Notations

- We denote by $\mathbb{N} = \{1, 2, \ldots\}$ the set of natural numbers without 0 and by $\omega = \{0, 1, \ldots\}$ the set of natural numbers with 0. (The reason for notation of the latter will become apparent once ordinal numbers have been introduced.)

2. Model Theory

In this section, we follow the overall structure of [4], but also notations and terminology from [7] are used.

2.1. Structures

See [4, Section 1] for further details.

2.1.1. $\mathcal{L}$-structures

Definition 2.1.1. A **language** $\mathcal{L}$ is specified by:

(i) a family of **function symbols** $(f_i)_{i\in I}$,

(ii) a family of **relation symbols** $(R_j)_{j\in J}$,

(iii) a family of **constant symbols** $(c_k)_{k\in K}$,

(iv) for each function and relation symbol, an **arity** $n \in \mathbb{N}$.

The arity specifies the number of arguments that a function or a relation symbol allows. For instance, the function symbol $-$ can be 1-ary (unary, e.g. in the expression $-x$) or 2-ary (binary, e.g. in the expression $x - y$).

Notation 2.1.2. For finite languages, i.e. languages that only consist of finitely many function, relation and constant symbols, one usually simply lists the symbols (in some conventional order). For instance, the most important language in this lecture is the **language of ordered rings** $\mathcal{L}_{\mathrm{or}} = \{+, -, \cdot, 0, 1, <\}$. Here, $+$, $-$ and $\cdot$ are binary function symbols, 0 and 1 are constant symbols and $<$ is a binary relation symbol.

Definition 2.1.3. Let $\mathcal{L}$ be a language. An **$\mathcal{L}$-structure** $\mathcal{M}$ consists of a set $M \neq \emptyset$ called the **domain** of $\mathcal{M}$ together with an **interpretation** for each symbol from $\mathcal{L}$:

(i) for each function symbol f in $\mathcal{L}$ of arity n, a function $f^{\mathcal{M}} \colon M^n \to M$;

(ii) for each relation symbol R in $\mathcal{L}$ of arity n, an n-ary relation $R^{\mathcal{M}}$ on M;

(iii) for each constant symbol c in $\mathcal{L}$, an element $c^{\mathcal{M}} \in M$.

Example 2.1.4. Both

$$\mathbb{Z}_{\mathrm{or}} = (\mathbb{Z}, +^{\mathbb{Z}_{\mathrm{or}}}, -^{\mathbb{Z}_{\mathrm{or}}}, \cdot^{\mathbb{Z}_{\mathrm{or}}}, 0^{\mathbb{Z}_{\mathrm{or}}}, 1^{\mathbb{Z}_{\mathrm{or}}}, <^{\mathbb{Z}_{\mathrm{or}}})$$

and

$$\mathbb{R}_{\mathrm{or}} = (\mathbb{R}, +^{\mathbb{R}_{\mathrm{or}}}, -^{\mathbb{R}_{\mathrm{or}}}, \cdot^{\mathbb{R}_{\mathrm{or}}}, 0^{\mathbb{R}_{\mathrm{or}}}, 1^{\mathbb{R}_{\mathrm{or}}}, <^{\mathbb{R}_{\mathrm{or}}})$$

are $\mathcal{L}_{\mathrm{or}}$-structures with the usual interpretations. For instance, $+^{\mathbb{Z}_{\mathrm{or}}} \colon \mathbb{Z}^2 \to \mathbb{Z}$ describes the standard addition on $\mathbb{Z}$ and $<^{\mathbb{R}_{\mathrm{or}}}$ is the standard strict linear order relation "less than" on $\mathbb{R}$.

Notation 2.1.5. (i) In most cases, the symbols of the language even coincide with standard notations for operations, relations and constants in the given structure. In this case (and also if the interpretations are clear from the context), we omit the superscripts. For instance, we only write

$$\mathbb{Z}_{\mathrm{or}} = (\mathbb{Z}, +, -, \cdot, 0, 1, <)$$

and

$$\mathbb{R}_{\mathrm{or}} = (\mathbb{R}, +, -, \cdot, 0, 1, <).$$

(ii) If $\mathcal{L}_x$ is some langauge and M is some domain over which we have some natural or previously defined interpretation of all symbols in $\mathcal{L}_x$, then M_x denotes the corresponding $\mathcal{L}_x$-structure with domain M. For instance, we write $\mathbb{Q}_{\mathrm{or}}$ for the $\mathcal{L}_{\mathrm{or}}$-structure

$$\mathbb{Q}_{\mathrm{or}} = (\mathbb{Q}, +, -, \cdot, 0, 1, <)$$

with the standard interpretations of all symbols.

(iii) In some cases, we even omit the subscript completely and still mean the corresponding structure. For instance, when we talk about the $\mathcal{L}_{\mathrm{or}}$-structure $\mathbb{Z}$, we actually mean $\mathbb{Z}_{\mathrm{or}}$. It should be clear from the context what structure we actually mean.

Definition 2.1.6. Apart from $\mathcal{L}_{\mathrm{or}}$, the following languages are often used for the study of algebraic structures. (Same symbols have the same arity!)

(i) the **language of linear orderings** $\mathcal{L}_< = \{<\}$;

(ii) the **language of additive monoids** $\mathcal{L}_{\mathrm{admon}} = \{+, 0\}$ and the **language of (multiplicative) monoids** $\mathcal{L}_{\mathrm{mon}} = \{\cdot, 1\}$;

(iii) the **language of (additive) groups** $\mathcal{L}_{\mathrm{g}} = \mathcal{L}_{\mathrm{admon}} \cup \{-\}$ and the **language of multiplicative groups** $\mathcal{L}_{\mathrm{mgp}} = \mathcal{L}_{\mathrm{mon}} \cup \{(\cdot)^{-1}\}$, where $(\cdot)^{-1}$ is a unary function symbol (applied as a superscript);

(iv) the **language of semirings** $\mathcal{L}_{\mathrm{semr}} = \mathcal{L}_{\mathrm{admon}} \cup \mathcal{L}_{\mathrm{mon}}$ and the **language of rings** $\mathcal{L}_{\mathrm{r}} = \mathcal{L}_{\mathrm{semr}} \cup \{-\}$;

(v) the **language of ordered groups** $\mathcal{L}_{\mathrm{og}} = \mathcal{L}_{\mathrm{g}} \cup \mathcal{L}_<$ and the **language of ordered exponential fields** $\mathcal{L}_{\mathrm{exp}} = \mathcal{L}_{\mathrm{or}} \cup \{\exp\}$, where exp is a unary function symbol.

Exercise 2.1.7. Consider the set $B = \{0, 1\}$.

(i) For each language $\mathcal{L}$ in Definition 2.1.6, how many different interpretations on B are there to obtain an $\mathcal{L}$-structure with domain B?

(ii) Find all $\mathcal{L}_<$-structures with domain B that are strict linear orderings.

(iii) Find all $\mathcal{L}_{\mathrm{semr}}$-structures with domain B that are semirings.

(iv) Find all $\mathcal{L}_{\mathrm{r}}$-structures with domain B that are fields.

(v) Is there an $\mathcal{L}_{\mathrm{or}}$-structure with domain B that is an ordered field?

Definition 2.1.8. Let $\mathcal{L}$ and $\mathcal{L}^+$ be languages such that $\mathcal{L} \subseteq \mathcal{L}^+$. Moreover, let $\mathcal{M}^+$ be an $\mathcal{L}^+$-structure with domain M and let $\mathcal{M}$ be the $\mathcal{L}$-structure with domain M and whose interpretations of the symbols in $\mathcal{L}$ coincide with those of $\mathcal{M}^+$. Then we say that $\mathcal{L}^+$ is an **expansion** of $\mathcal{L}$ and $\mathcal{L}$ is a **reduct** of $\mathcal{L}^+$, and likewise that $\mathcal{M}^+$ is an **$\mathcal{L}^+$-expansion** of $\mathcal{M}$ and $\mathcal{M}$ is an **$\mathcal{L}$-reduct** of $\mathcal{M}^+$.

Example 2.1.9. Consider $\omega_{\mathrm{admon}} = (\omega, +, 0)$ and $\omega_{\mathrm{semr}} = (\omega, +, \cdot, 0, 1)$. Then ω_{semr} is an $\mathcal{L}_{\mathrm{semr}}$-expansion of ω_{admon} and ω_{admon} is an $\mathcal{L}_{\mathrm{admon}}$-reduct of ω_{semr}.

2.1.2. Embeddings and Automorphisms

Definition 2.1.10. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathcal{L}$-structures.

(i) A map $\varphi\colon M \to N$ is called an **$\mathcal{L}$-homomorphism** if the following are satisfied:

(1) for any n-ary function symbol f of $\mathcal{L}$ and any $a_1, \ldots, a_n \in M$, we have

$$\varphi(f^{\mathcal{M}}(a_1, \ldots, a_n)) = f^{\mathcal{N}}(\varphi(a_1), \ldots, \varphi(a_n));$$

(2) for any n-ary function symbol R of $\mathcal{L}$ and any $a_1, \ldots, a_n \in M$,

$$R^{\mathcal{M}}(a_1, \ldots, a_n) \text{ if and only if } R^{\mathcal{N}}(\varphi(a_1), \ldots, \varphi(a_n)) \text{ holds;}$$

(3) for any constant symbol c of $\mathcal{L}$, we have

$$\varphi(c^{\mathcal{M}}) = c^{\mathcal{N}}.$$

We write $\varphi\colon \mathcal{M} \to \mathcal{N}$ to express that φ is an $\mathcal{L}$-homomorphism from $\mathcal{M}$ to $\mathcal{N}$.

(ii) Let $\iota\colon \mathcal{M} \to \mathcal{N}$ be injective. Then ι is called an **$\mathcal{L}$-embedding**. We also write $\iota\colon \mathcal{M} \hookrightarrow \mathcal{N}$ expressing that ι is an $\mathcal{L}$-embedding of $\mathcal{M}$ into $\mathcal{N}$.

(iii) Let $\psi\colon \mathcal{M} \to \mathcal{N}$ be bijective. Then it is called an **$\mathcal{L}$-isomorphism** and we write $\psi\colon \mathcal{M} \xrightarrow{\cong} \mathcal{N}$ or simply $\psi\colon \mathcal{M} \cong \mathcal{N}$. An $\mathcal{L}$-isomorphism from $\mathcal{M}$ to $\mathcal{M}$ is called an **$\mathcal{L}$-automorphism**.

Notation 2.1.11. (i) If we write $\mathcal{M} \cong \mathcal{N}$, then we mean that there exists an $\mathcal{L}$-isomorphism from $\mathcal{M}$ to $\mathcal{N}$ and we say that $\mathcal{M}$ and $\mathcal{N}$ are **isomorphic**.

(ii) For the tuple $\underline{a} = (a_1, \ldots, a_n)$ we also write $\varphi(\underline{a})$ rather than $(\varphi(a_1), \ldots, \varphi(a_n))$.

Exercise 2.1.12. Consider the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = (M, +^{\mathcal{M}}, -^{\mathcal{M}}, \cdot^{\mathcal{M}}, 0^{\mathcal{M}}, 1^{\mathcal{M}})$ defined as follows:

- $M := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\} \subseteq \mathbb{R}^{2\times 2}$.
- $+^{\mathcal{M}}$, $-^{\mathcal{M}}$ and $\cdot^{\mathcal{M}}$ are standard addition, subtraction and multiplication of matrices.
- $0^{\mathcal{M}} := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $1^{\mathcal{M}} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Show that $\mathcal{M} \cong \mathbb{C}_{\mathrm{r}}$ by finding a suitable $\mathcal{L}_{\mathrm{r}}$-isomorphism, and deduce that $\mathcal{M}$ is a field. Can $\mathcal{M}$ be expanded to an $\mathcal{L}_{\mathrm{or}}$-structure that is a linearly ordered field?

Exercise 2.1.13. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures and let $\varphi\colon M \to N$. Show that the notion of $\mathcal{L}$-homomorphism coincides with the standard definitions of homomorphisms of algebraic structures for groups, rings and fields. More precisely, show the following:

(i) Let $\mathcal{L} = \mathcal{L}_{\mathrm{mon}}$ and let $\mathcal{M}$ and $\mathcal{N}$ be multiplicative groups. Show that φ is an $\mathcal{L}_{\mathrm{mon}}$-homomorphisms if and only if it is a homomorphism of groups.

(ii) Let $\mathcal{L} = \mathcal{L}_{\mathrm{semr}}$ and let $\mathcal{M}$ and $\mathcal{N}$ be commutative rings with identity. Show that φ is an $\mathcal{L}_{\mathrm{semr}}$-homomorphisms if and only if it is a homomorphism of rings.

(iii) Let $\mathcal{L} = \mathcal{L}_{\mathrm{r}}$ and let $\mathcal{M}$ and $\mathcal{N}$ be fields. Show that φ is an $\mathcal{L}_{\mathrm{r}}$-homomorphisms if and only if it is a homomorphism of fields.

Definition 2.1.14. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathcal{L}$-structures. If $M \subseteq N$ and the identity map id_M is an $\mathcal{L}$-embedding of $\mathcal{M}$ into $\mathcal{N}$, then we write $\mathcal{M} \subseteq \mathcal{N}$ and say that $\mathcal{M}$ is an **$\mathcal{L}$-substructure** of $\mathcal{N}$ and that $\mathcal{N}$ is an **$\mathcal{L}$-extension** of $\mathcal{M}$.

Remark 2.1.15. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures and let $\iota\colon \mathcal{M} \hookrightarrow \mathcal{N}$. Then $\iota(M)$ naturally becomes a domain for an $\mathcal{L}$-substructure $\mathcal{M}'$ of $\mathcal{N}$, where the interpretation of each relation and function symbol in $\mathcal{M}'$ is given by the restriction of the corresponding interpretation in $\mathcal{N}$ to $\iota(M)$. For instance, if f is a unary function symbol of $\mathcal{L}$, then $f^{\mathcal{M}'} := f^{\mathcal{N}}|_{\iota(M)}$.

Example 2.1.16. Obvious chains of substructures are

$$\mathbb{N}_{\mathrm{mon}} \subseteq \omega_{\mathrm{mon}} \subseteq \mathbb{Z}_{\mathrm{mon}} \subseteq \mathbb{Q}_{\mathrm{mon}} \subseteq \mathbb{R}_{\mathrm{mon}} \subseteq \mathbb{C}_{\mathrm{mon}},$$

$$\omega_{\mathrm{semr}} \subseteq \mathbb{Z}_{\mathrm{semr}} \subseteq \mathbb{Q}_{\mathrm{semr}} \subseteq \mathbb{R}_{\mathrm{semr}} \subseteq \mathbb{C}_{\mathrm{semr}},$$

$$\mathbb{Z}_{\mathrm{r}} \subseteq \mathbb{Q}_{\mathrm{r}} \subseteq \mathbb{R}_{\mathrm{r}} \subseteq \mathbb{C}_{\mathrm{r}},$$

and

$$\mathbb{Z}_{\mathrm{or}} \subseteq \mathbb{Q}_{\mathrm{or}} \subseteq \mathbb{R}_{\mathrm{or}}.$$

2.2. Terms and Formulas

See [4, Sections 2 & 3] for further details.

2.2.1. Recursive Construction of Terms

In this and later sections, we will use **recursive definitions** for a set of objects. When we say that such a set is defined recursively by a given number of steps, then we mean that any object within that set needs to be produced by these steps by a finite number of iterations.

Definition 2.2.1. Let $\mathcal{L}$ be a language. The set of **$\mathcal{L}$-terms** is defined recursively as follows:

(i) Each variable is a term.

(ii) Every constant symbol of $\mathcal{L}$ is a term.

(iii) If f is a function symbol of $\mathcal{L}$ of arity n and $t_1, \ldots, t_n$ are $\mathcal{L}$-terms, then $f(t_1, \ldots, t_n)$ is an $\mathcal{L}$-term.

An $\mathcal{L}$-term is called **closed** if it contains no variables.

Example 2.2.2. (i) Typical variables are $x, y, z, x_0, x_1, \ldots$, but theoretically all single letters or even sequences of arbitrary symbols may be allowed as variables.

(ii) The expression $\cdot(\exp(+(0,1)), x)$ is an $\mathcal{L}_{\exp}$-term that is not closed (as it contains the variable x). In order to verify this, one has to recursively build this term: The variable x and the constant symbols 0 and 1 of $\mathcal{L}_{\exp}$ are terms by steps (i) and (ii) (of Definition 2.2.1). Since $+$ is a binary function symbol, also $+(0,1)$ is an $\mathcal{L}_{\exp}$-term by step (iii). Now exp is a unary function symbol, whence $\exp(+(0,1))$ is an $\mathcal{L}_{\exp}$-term. Finally, both $\mathcal{L}_{\exp}$-terms $\exp(+(0,1))$ and x can be used as the arguments of the binary function symbol $\cdot$ to obtain the desired $\mathcal{L}_{\exp}$-term.

Remark 2.2.3. The $\mathcal{L}_{\exp}$-term $\cdot(\exp(+(0,1)), x)$ would usually be written as $\exp(0+1) \cdot x$. The former is called a **prefix notation**, the latter is an **infix notation**. See Section A.1 for this and further abbreviations to ease our notation.

Notation 2.2.4. Let $\mathcal{L}$ be a language and let t be an $\mathcal{L}$-term. We also write $t(x_1, \ldots, x_n)$ (for some $n \in \mathbb{N}$) instead of t to express that the set of variables appearing in t is contained in $\{x_1, \ldots, x_n\}$.

Definition 2.2.5. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $t = t(x_1, \ldots, x_n)$ be an $\mathcal{L}$-term. The **interpretation** $t^{\mathcal{M}} \colon M^n \to M$ of t is defined recursively as follows:

(i) If t is a constant symbol c of $\mathcal{L}$, then $t^{\mathcal{M}} \colon M \to M, a \mapsto c^{\mathcal{M}}$.

(ii) If t is x_i for some $i \in \{1, \ldots, n\}$, then $t^{\mathcal{M}} \colon M^n \to M, (x_1, \ldots, x_n) \mapsto x_i$.

(iii) If t is $f(t_1, \ldots, t_m)$ for some $\mathcal{L}$-terms $t_1, \ldots, t_m$ and an m-ary function symbol f of $\mathcal{L}$, then

$$t^{\mathcal{M}} \colon M^n \to M, (x_1, \ldots, x_n) \mapsto f^{\mathcal{M}}\big(t_1^{\mathcal{M}}(x_1, \ldots, x_n), \ldots, t_m^{\mathcal{M}}(x_1, \ldots, x_n)\big)$$

Remark 2.2.6. (i) If t is a closed $\mathcal{L}$-term, then $t^{\mathcal{M}}$ is often also interpreted as the unique element $a \in M$ in the image of $t^{\mathcal{M}}$. For instance, the closed $\mathcal{L}_{\text{semr}}$-term $0 + 1$ can be interpreted in $\mathbb{Z}$ as the constant 1 rather than the constant function $a \mapsto 1$.

(ii) Note that in Definition 2.2.5, the domain of the function $t^{\mathcal{M}}$ is not well-defined: If the tuple $(x_1, \ldots, x_n)$ contains at least one variable that does not appear in t, then the domain of $t^{\mathcal{M}}$ could also be chosen as M^{n-1}. For instance, the $\mathcal{L}_{\mathrm{r}}$-term t given by $x + y$ gives rise to both the function $t^{\mathbb{R}} \colon \mathbb{R}^2 \to \mathbb{R}, (a, b) \mapsto a + b$ (in case that we regard t as $t(x, y)$) and the function $t^{\mathbb{R}} \colon \mathbb{R}^3 \to \mathbb{R}, (a, b, c) \mapsto a + b$ (in case we regard t as $t(x, y, z)$). The domain of an interpretation of an $\mathcal{L}$-term should always be clear from the context.

Exercise 2.2.7. Find three different $\mathcal{L}_{\mathrm{r}}$-terms t with $t^{\mathbb{Z}} \colon \mathbb{Z} \to \mathbb{Z}, n \mapsto 2n$.

Proposition 2.2.8. *Let $\mathcal{L}$ be a language, let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures and let $\iota \colon \mathcal{M} \hookrightarrow \mathcal{N}$. Moreover, let $t(\underline{x})$ be an $\mathcal{L}$-term with $\underline{x} = (x_1, \ldots, x_n)$ and let $\underline{a} \in M$.*[1] *Then*

$$\iota(t^{\mathcal{M}}(\underline{a})) = t^{\mathcal{N}}(\iota(\underline{a})).$$

Proof. We proceed by induction on the recursive construction of terms.

(i) If t is a constant symbol c of $\mathcal{L}$, then

$$\iota(t^{\mathcal{M}}(\underline{a})) = \iota(c^{\mathcal{M}}) = c^{\mathcal{N}} = t^{\mathcal{N}}(\iota(\underline{a})).$$

(ii) If t is x_i for some $i \in \{1, \ldots, n\}$, then

$$\iota(t^{\mathcal{M}}(\underline{a})) = \iota(a_i) = t^{\mathcal{N}}(\iota(a_1), \ldots, \iota(a_n)) = t^{\mathcal{N}}(\iota(\underline{a})).$$

(iii) If t is $f(t_1, \ldots, t_m)$ for some m-ary function f of $\mathcal{L}$ and some $\mathcal{L}$-terms $t_1, \ldots, t_m$ for which the conclusion already holds, then

$$\begin{aligned}
\iota(t^{\mathcal{M}}(\underline{a})) &= \iota\big(f^{\mathcal{M}}(t_1^{\mathcal{M}}(\underline{a}), \ldots, t_m^{\mathcal{M}}(\underline{a}))\big) \\
&= f^{\mathcal{N}}\big(\iota\big(t_1^{\mathcal{M}}(\underline{a})\big), \ldots, \iota\big(t_m^{\mathcal{M}}(\underline{a})\big)\big) \\
&= f^{\mathcal{N}}\big(t_1^{\mathcal{N}}(\iota(\underline{a})), \ldots, t_m^{\mathcal{N}}(\iota(\underline{a}))\big) \\
&= t^{\mathcal{N}}(\iota(\underline{a})).
\end{aligned}$$

□

2.2.2. Recursive Construction of Formulas

Definition 2.2.9. Let $\mathcal{L}$ be a language. The set of **$\mathcal{L}$-formulas** is defined recursively as follows:

(i) Let R be an n-ary relation symbol of $\mathcal{L}$ and let $t_1, \ldots, t_{n+1}$ be $\mathcal{L}$-terms. Then both $t_1 = t_{n+1}$ and $R(t_1, \ldots, t_n)$ are $\mathcal{L}$-formulas.

(ii) If φ and ψ are $\mathcal{L}$-formulas, then also $\neg\varphi$ and $(\varphi \wedge \psi)$ are $\mathcal{L}$-formulas.

(iii) If φ is an $\mathcal{L}$-formula and x is a variable, then $\exists x\, \varphi$ is an $\mathcal{L}$-formula.

An $\mathcal{L}$-formula is **atomic** if it is produced by only applying step (i). If φ and ψ are $\mathcal{L}$-formulas, then ψ is called a **subformula** of φ if the sequence of symbols of ψ appears as consecutive sequence of symbols within φ.

[1] Here, we would usually have to write $\underline{a} = (a_1, \ldots, a_n) \in M^n$. However, this shorthand notation is unambiguous: the actual length of $\underline{a}$ follows from the context, and the standard convention is that the i-th entry of the tuple $\underline{a}$ is denoted by a_i.

Notation 2.2.10. Let $\mathcal{L}$ be a language.

(i) We usually omit the outermost brackets of an $\mathcal{L}$-formula. Hence, we write $1 = 0 \wedge 1 = 1$ rather than $(1 = 0 \wedge 1 = 1)$ (in the language $\mathcal{L}_{\text{semr}}$).

(ii) For a binary relation symbol R, we also use the infix notation without brackets. For instance, we write $y < 1 + x$ rather than $< (y, 1 + x)$ in the language $\mathcal{L}_{\text{or}}$. Moreover, if t and s are $\mathcal{L}$-terms, then we write $s \mathrel{\not R} t$ for $t \; R \; s$ and $s \not R \; t$ for $\neg \; s \; R \; t$. Hence, $1 + x > y$ stands for $y < 1 + x$ and $y \not< 1 + x$ is short for $\neg \; y < 1 + x$. In this regard, also $=$ is treated as a binary relation symbol.

(iii) Let φ and ψ be $\mathcal{L}$-formulas and let x be a variable. Then we write $\varphi \vee \psi$ for $\neg(\neg\varphi \wedge \neg\psi)$ (*De Morgan's Law*), we write $\varphi \to \psi$ for $\neg\varphi \vee \psi$, we write $\varphi \leftrightarrow \psi$ for $(\varphi \to \psi) \wedge (\psi \to \varphi)$ and we write $\forall x \; \varphi$ for $\neg\exists x \; \neg\varphi$.

(iv) The logical connectors $\vee$ and $\wedge$ are associative. Hence, we omit superfluous brackets. For instance, $\varphi_1 \wedge \varphi_2 \wedge \varphi_3$ stand for $(\varphi_1 \wedge \varphi_2) \wedge \varphi_3$. We also use $\bigwedge$ and $\bigvee$ to denote finite conjunctions and finite disjunctions, e.g.

$$\bigwedge_{i=1}^{n} \varphi_i \text{ expresses } \varphi_1 \wedge \ldots \wedge \varphi_n.$$

(v) For an $\mathcal{L}$-formula φ and variables $x_1, \ldots, x_n$ we also write

$$\exists x_1, \ldots, x_n \; \varphi$$

for

$$\exists x_1 \ldots \exists x_n \; \varphi.$$

A similar shorthand notation is used for $\forall$ instead of $\exists$.

Exercise 2.2.11. Let $\mathcal{L}$ be a language and let φ be an $\mathcal{L}$-formula. Show that φ is atomic if and only if the only subformula of φ is φ itself.

2.2.3. Variables and Interpretations

Definition 2.2.12. Let $\mathcal{L}$ be a language, let φ be an $\mathcal{L}$-formula and let x be a variable. The subformula immediately following an instance of $\exists x$ is called the **scope** of that particular quantifier $\exists$.[2] An instance of x in φ is **bounded** if it occurs within the the scope of some quantifier $\exists$, which is said to **bind** that instance of x. Any instance of x that is not bounded is called **free**. All variables that have free instances in φ are called the **free variables** of φ.

We may always assume that a given variable does not have both free and bounded instances. For example, the $\mathcal{L}_{\text{or}}$-formula

$$\exists x(x < 0 \vee y = 1) \vee x > 0$$

can be replaced by

$$\exists x(x < 0 \vee y = 1) \vee z > 0.$$

[2]We use a similar terminology if an instance of a variable lies within the scope of a universal quantifier $\forall$.

Notation 2.2.13. Let $\mathcal{L}$ be a language and let φ be an $\mathcal{L}$-formula. We also write $\varphi(x_1, \ldots, x_n)$ (for some $n \in \mathbb{N}$) instead of φ to express that the set of free variables of φ is contained in $\{x_1, \ldots, x_n\}$.

Definition 2.2.14. Let $\mathcal{L}$ be a language and let φ be an $\mathcal{L}$-formula. Then φ is called an **$\mathcal{L}$-sentence** if it has no free variables.

Exercise 2.2.15. List all atomic $\mathcal{L}_{\text{admon}}$-sentences.

Exercise 2.2.16. Let $\mathcal{L}$ be a language and let $\varphi(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula. Show that

$$\exists x_1, \ldots, x_n \ \varphi(x_1, \ldots, x_n)$$

is an $\mathcal{L}$-sentence.

Definition 2.2.17. Let $\mathcal{L}$ be a language, let $\varphi(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula, let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $\underline{a} \in M$. We define the notion $\mathcal{M} \models \varphi(\underline{a})$ by recursion on $\mathcal{L}$-formulas:

(i) If φ is of the form $t = s$ for some $\mathcal{L}$-terms t and s, then

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if } t^{\mathcal{M}}(\underline{a}) = s^{\mathcal{M}}(\underline{a}).$$

(ii) If φ is of the form $R(t_1, \ldots, t_m)$ for some m-ary relation symbol R and $\mathcal{L}$-terms $t_1, \ldots, t_m$, then

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if } R^{\mathcal{M}}(t_1^{\mathcal{M}}(\underline{a}), \ldots, t_m^{\mathcal{M}}(\underline{a})) \text{ holds.}$$

(iii) If φ is of the form $\neg\psi$ for some $\mathcal{L}$-formula ψ, then

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if } \mathcal{M} \not\models \psi(\underline{a}),$$

i.e. it is not the case that $\mathcal{M} \models \psi(\underline{a})$.

(iv) If φ is of the form $\psi \wedge \theta$ for some $\mathcal{L}$-formulas ψ and θ, then

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if } \mathcal{M} \models \psi(\underline{a}) \text{ and } \mathcal{M} \models \theta(\underline{a}).$$

(v) If φ is of the form $\exists v \ \psi(\underline{x}, v)$ for some $\mathcal{L}$-formula ψ and some variable v, then

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if } \mathcal{M} \models \psi(\underline{a}, b)$$

for some $b \in M$.

We say that $\mathcal{M}$ **models** or **satisfies**[3] $\varphi(\underline{a})$ or that $\varphi(\underline{a})$ is **true** in $\mathcal{M}$.

In the special case of formulas without free variables, i.e. sentences, we do not have to specify an element $\underline{a} \in M$ to insert into the formula.

[3] A more "colloquial" expression is "$\mathcal{M}$ believes in $\varphi(\underline{a})$".

Definition 2.2.18. Let $\mathcal{L}$ be a language and let $\mathcal{M}$ be an $\mathcal{L}$-structure. We say that $\mathcal{M}$ is a **model** of a sentence φ if $\mathcal{M} \models \varphi$. If Σ is a set of $\mathcal{L}$-sentences, then we say that $\mathcal{M}$ is a **model** of Σ if $\mathcal{M} \models \varphi$ for any $\varphi \in \Sigma$, and we write $\mathcal{M} \models \Sigma$.

Model Theory is the study of the interplay between sets of sentences and corresponding models. Thus, it builds a bridge between logical formulas and algebraic structures in which these are satisfied.

Exercise 2.2.19. Show that $\mathbb{Z}_< \models \forall x \exists y, z\ (y < x \wedge x < z)$. *This sentence says that the linear ordering on $\mathbb{Z}$ has no endpoints.*

Lemma 2.2.20. *Let $\mathcal{L}$ be a language, let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures and let $\iota \colon \mathcal{M} \hookrightarrow \mathcal{N}$. Then for any atomic $\mathcal{L}$-formula $\varphi(\underline{x})$ and any $\underline{a} \in M$ we have*

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if and only if } \mathcal{N} \models \varphi(\iota(\underline{a})).$$

Proof. Let R be an m-ary relation symbol of $\mathcal{L}$ (or the binary relation symbol $=$) and let $t_1, \ldots, t_m$ be $\mathcal{L}$-terms such that $\varphi(\underline{x})$ is given by $R(t_1(\underline{x}), \ldots, t_m(\underline{x}))$. By Proposition 2.2.8, we have

$$\iota\big(t_1^{\mathcal{M}}(\underline{a}), \ldots, t_m^{\mathcal{M}}(\underline{a})\big) = \big(t_1^{\mathcal{N}}(\iota(\underline{a})), \ldots, t_m^{\mathcal{N}}(\iota(\underline{a}))\big)\,.$$

By definition of an $\mathcal{L}$-embedding, we obtain

$$\mathcal{M} \models R(t_1(\underline{a}), \ldots, t_m(\underline{a})) \text{ if and only if } \mathcal{N} \models R(t_1(\iota(\underline{a})), \ldots, t_m(\iota(\underline{a}))),$$

as required. □

Proposition 2.2.21. *Let $\mathcal{L}$ be a language, let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures and let $\psi \colon \mathcal{M} \cong \mathcal{N}$. Then for any $\mathcal{L}$-formula $\varphi(\underline{x})$ and any $\underline{a} \in M$ we have*

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if and only if } \mathcal{N} \models \varphi(\psi(\underline{a})).$$

Proof. We proceed by structural induction on formulas. The statement was proved for atomic $\mathcal{L}$-formulas in Lemma 2.2.20. Let θ and ρ be $\mathcal{L}$-formulas for which the statement already holds.

First suppose that φ is of the form $\neg\theta$. Then

$$\begin{aligned} \mathcal{M} \models \varphi(\underline{a}) &\Leftrightarrow \mathcal{M} \not\models \theta(\underline{a}) \\ &\Leftrightarrow \mathcal{N} \not\models \theta(\psi(\underline{a})) \\ &\Leftrightarrow \mathcal{N} \models \varphi(\psi(\underline{a})). \end{aligned}$$

The case that φ is of the form $\theta \wedge \rho$ can be proved in a similar manner.

Now suppose that φ is given by $\exists v\ \theta(\underline{x}, v)$. Then

$$\begin{aligned} \mathcal{M} \models \varphi(\underline{a}) &\Leftrightarrow \mathcal{M} \models \theta(\underline{a}, c) \text{ for some } c \in M \\ &\Leftrightarrow \mathcal{N} \models \theta(\psi(\underline{a}), \psi(c)) \text{ for some } c \in M. \end{aligned}$$

Now if $\mathcal{N} \models \theta(\psi(\underline{a}), \psi(c))$ for some $c \in M$, then $\mathcal{N} \models \exists v\ \theta(\psi(\underline{a}), v)$. Conversely, if $\mathcal{N} \models \exists v\ \theta(\psi(\underline{a}), v)$, then $\mathcal{N} \models \theta(\psi(\underline{a}), d)$ for some $d \in M$. Setting $c = \psi^{-1}(d)$ yields the required conclusion. □

2.3. Definable Sets

See [4, Section 4] for further details.

2.3.1. Definability

Definition 2.3.1. Let $\mathcal{L}$ be a language and let $\mathcal{M}$ be an $\mathcal{L}$-structure. Moreover, let $n \in \mathbb{N}$ and let $A \subseteq M$. A set $B \subseteq M^n$ is called **A-$\mathcal{L}$-definable** (or **$\mathcal{L}$-definable with parameters from** A or **A-definable** in $\mathcal{M}$) if there exists an $\mathcal{L}$-formula $\varphi(\underline{x}, \underline{y})$ and a tuple $\underline{a} \in A$ such that

$$B = \varphi(\underline{a}, \mathcal{M}) := \{\underline{b} \in M^n \mid \mathcal{M} \models \varphi(\underline{a}, \underline{b})\}.$$

In this case, we say that $\varphi(\underline{a}, \underline{x})$ **defines** B. If there exists $A \subseteq M$ such that $B \subseteq M^n$ is A-$\mathcal{L}$-definable, then we simply say that B is $\mathcal{L}$-definable (with parameters). In the case that we can choose $A = \emptyset$, we also say that B is **$\mathcal{L}$-definable without parameters** or **parameter-free $\mathcal{L}$-definable**.

Definition 2.3.2. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $m, n \in \mathbb{N}$. A function $f\colon C \to D$ with $C \subseteq M^n$ and $D \subseteq M^m$ is called **A-$\mathcal{L}$-definable** if C, D and its graph $\{(\underline{c}, f(\underline{c})) \mid \underline{c} \in M^n\} \subseteq M^{n+m}$ are A-$\mathcal{L}$-definable. Similarly, an n-ary relation R on M is called A-$\mathcal{L}$-definable if its graph $\{\underline{c} \in M^n \mid R(\underline{c}) \text{ holds}\}$ is A-$\mathcal{L}$-definable.

Example 2.3.3. (i) The interval $(-1, 1)$ is $\emptyset$-$\mathcal{L}_{\text{or}}$-definable in $\mathbb{R}_{\text{or}}$ by the formula[4]

$$-1 < x < 1.$$

The same $\mathcal{L}_{\text{or}}$-formula defines the set $\{0\}$ in $\mathbb{Z}_{\text{or}}$.

(ii) The function $\log\colon (0, \infty) \to \mathbb{R}$ is definable in $\mathbb{R}_{\exp}$. Indeed, both $(0, \infty)$ and $\mathbb{R}$ are definable in $\mathbb{R}_{\exp}$. Now log is defined by the $\mathcal{L}_{\exp}$-formula $\varphi(x, y)$ given by

$$(0 < x \wedge \exp(y) = x).$$

One of the central tasks of Model Theory is to characterise all definable sets (and thus also functions and relations) in a given structure. It is often said that a structure is 'tame' if one has some control over the definable sets in it. For instance, one of these tame structures is $\mathbb{R}_{\text{or}}$, in which all $\mathcal{L}_{\text{or}}$-definable subsets of $\mathbb{R}$ are simply finite unions of points and open intervals. This will be a central theorem in a later part of this lecture.

Exercise 2.3.4. Let $\varphi(x, y)$ be the $\mathcal{L}_{\text{semr}}$-formula $x \cdot x = y + y$ and let $\psi(y)$ be the $\mathcal{L}_{\text{semr}}$-formula $\exists x\ x \cdot x = y + y$. Determine the sets that are defined by $\varphi(x, a)$ and by $\psi(y)$ in the $\mathcal{L}_{\text{or}}$-structure $\mathcal{M}$ for the following cases:

(i) $M = \mathbb{R}$ and $a \in \mathbb{R}$.

(ii) $M = \mathbb{Q}$ and $a \in \mathbb{Q}$.

[4] See Section A.1 for the abbreviations we use here.

(iii) $M = \mathbb{Z}$ and $a \in \omega$.

(iv) $M = \omega$ and $a \in \mathbb{N}$.

In some cases, you need to make a case distinction depending on a.

Exercise 2.3.5. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ be an $\mathcal{L}$-structure, let $m, n \in \mathbb{N}$ and let $f\colon C \to D$ with $C \subseteq M^n$ and $D \subseteq M^m$. Suppose that for some $\underline{a} \in M$, the $\mathcal{L}$-formula $\varphi(\underline{a}, \underline{x})$ defines the graph of f. Find an $\mathcal{L}$-formula (with parameters) that defines C and an $\mathcal{L}$-formula (with parameters) that defines D.

Exercise 2.3.6. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ be an $\mathcal{L}$-structure, let $m, n, k \in \mathbb{N}$, let $f\colon C \to D$ and $g\colon D \to E$ with $C \subseteq M^n$, $D \subseteq M^m$ and $E \subseteq M^k$. Suppose that f and g are $\mathcal{L}$-definable. Show that $g \circ f$ is $\mathcal{L}$-definable.

The following lemma shows that there is a connection between logical connectives and set theoretic operations of definable sets.

Lemma 2.3.7. *Let $\mathcal{L}$ be a language, let $\mathcal{M}$ be an $\mathcal{L}$-structure, let $n \in \mathbb{N}$ and let $S, T \subseteq M^n$ be $\mathcal{L}$-definable. Then also $S \cap T$, $S \cup T$ and $M^n \setminus T$ are $\mathcal{L}$-definable. Moreover, the projection (onto the first $n-1$ coordinates)*

$$\pi'_{n-1}(S) := \{\underline{b} \in M^{n-1} \mid (\underline{b}, c) \in S \text{ for some } c \in M\}$$

is $\mathcal{L}$-definable.

Proof. Let φ and ψ be $\mathcal{L}$-formulas and let $\underline{a} \in M$ such that $\varphi(\mathcal{M}, \underline{a}) = S$ and $\psi(\mathcal{M}, \underline{a}) = T$. Then it is easy to verify that

- $S \cap T$ is defined by $\varphi(\underline{x}, \underline{a}) \wedge \psi(\underline{x}, \underline{a})$;
- $S \cup T$ is defined by $\varphi(\underline{x}, \underline{a}) \vee \psi(\underline{x}, \underline{a})$;
- $M^n \setminus T$ is defined by $\neg\psi(\underline{x}, \underline{a})$;
- $\pi'_{n-1}(S)$ is defined by $\exists x_n\ \varphi(\underline{x}, \underline{a})$. □

Remark 2.3.8. There is a version of Lemma 2.3.7 for parameter-free definability as well. In fact, in many definability results, a careful handling of the use of parameters leads to sharper results. To ease the notation, it is, however, sometimes useful to use more parameters than one actually needs. We have done so in the proof of Lemma 2.3.7, where we assumed in the first step that the same parameter tuples are used for the definitions of both sets.

2.3.2. Preservation under Automorphisms

As mentioned before, a prominent question of Model Theory is whether a given set is definable in a given structure. The following result gives a necessary condition for a set to be definable without parameters. This result is often used to show that a given set is not $\emptyset$-$\mathcal{L}$-definable (read: "zero-$\mathcal{L}$-definable").

Proposition 2.3.9. *Let $\mathcal{L}$ be a language, let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $n \in \mathbb{N}$. Then any $\emptyset$-$\mathcal{L}$-definable set $A \subseteq M^n$ is preserved under automorphisms, i.e. for any $\psi\colon \mathcal{M} \cong \mathcal{M}$, we have $\psi(A) = A$, where $\psi(A) = \{\psi(\underline{a}) \mid \underline{a} \in A\}$.*

Proof. We only prove this for the case $n = 1$, as the proof for larger n works similarly. Let $\varphi(x)$ be an $\mathcal{L}$-formula defining A. Then for any $a \in M$ we have $a \in A$ if and only if $\mathcal{M} \models \varphi(a)$. By Proposition 2.2.21, the latter holds if and only if $\mathcal{M} \models \varphi(\psi(a))$. Now $\mathcal{M} \models \varphi(\psi(a))$ if and only if $\psi(a) \in A$. In conclusion, we have shown that for any $a \in M$ we have $a \in A$ if and only if $\psi(a) \in A$. This also implies that for any $a \in M$ we have $a \in A$ if and only if $\psi^{-1}(a) \in A$. Hence, we obtain $\psi(A) \subseteq A$ and $\psi^{-1}(A) \subseteq A$, as required. □

Example 2.3.10. The strict order relation $<$ is not $\emptyset$-$\mathcal{L}_{\mathrm{g}}$-definable in $\mathbb{R}$: Let

$$\psi\colon \mathbb{R} \to \mathbb{R}, x \mapsto -x.$$

It is easy to verify that ψ is an $\mathcal{L}_{\mathrm{g}}$-automorphism on $\mathbb{R}$. Now $0 < 1$ but $\psi(0) \not< \psi(1)$. Hence, the graph of $<$ is not preserved under ψ and thus by Proposition 2.3.9 not $\emptyset$-$\mathcal{L}_{\mathrm{g}}$-definable.

Proposition 2.3.9 says that if a set is definable, then it is preserved under all automorphisms. The following exercise shows that the converse is not true.

Exercise 2.3.11. (i) Let $\psi\colon \mathbb{R}_{\mathrm{or}} \cong \mathbb{R}_{\mathrm{or}}$. Show that $\psi = \mathrm{id}_{\mathbb{R}}$.

(ii) Show that there are only countably many distinct $\emptyset$-$\mathcal{L}_{\mathrm{or}}$-definable subsets of $\mathbb{R}$.

(iii) Deduce that there is a subset $A \subseteq \mathbb{R}$ that is not $\emptyset$-$\mathcal{L}_{\mathrm{or}}$-definable but still preserved by all $\mathcal{L}_{\mathrm{or}}$-automorphisms on $\mathbb{R}$.

2.4. Substructures and Quantifiers

See [4, Section 5] for further details.

2.4.1. Existential and Universal Formulas

Notation 2.4.1. Let $\mathcal{L}$ be a language, let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $n \in \mathbb{N}$.

(i) If R is a binary relation symbol in $\mathcal{L}$, t is an $\mathcal{L}$-term and φ is an $\mathcal{L}$-formula, then

$$\forall(x\ R\ t)\ \varphi$$

stands for

$$\forall x\ (x\ R\ t \to \varphi)$$

and

$$\exists(x\ R\ t)\ \varphi$$

stands for

$$\exists x\ (x\ R\ t \wedge \varphi).$$

Likewise we can deal with abbreviations for binary relations such as $\not R$. For instance, the $\mathcal{L}_{\mathrm{or}}$-formula $\forall(x > 0)\ x > 1$ stands for $\forall x\ (x > 0 \to x > 1)$ and $\exists(x \neq 1)\ x \cdot x = 1$ is short for $\exists x\ (x \neq 1 \wedge x \cdot x = 1)$.

(ii) If $B \subseteq M^n$ is $\mathcal{L}$-definable and $\varphi(\underline{a}, \underline{x})$ defines B, then the string

$$\underline{x} \in B$$

is short for

$$\varphi(\underline{a}, \underline{x})$$

(within $\mathcal{M}$). For instance, the real interval $(-\pi, \pi)$ is defined by $-\pi < x < \pi$ within $\mathbb{R}_{\text{or}}$. The abbreviation $\mathbb{R}_{\text{or}} \models 0 \in (-\pi, \pi)$ is short for $\mathbb{R}_{\text{or}} \models -\pi < 0 < \pi$, and the abbreviation $\mathbb{R}_{\text{or}} \not\models \forall(x \in (-\pi, \pi))\ x < 3$ stands for $\mathbb{R}_{\text{or}} \not\models \forall x\ (-\pi < x < \pi \to x < 3)$.

Quantifiers generally increase the semantic complexity of formulas. In this regard, those formulas that do not contain any quantifiers stand out.

Definition 2.4.2. Let $\mathcal{L}$ be a language. A **quantifier-free** $\mathcal{L}$-formula is an $\mathcal{L}$-formula whose string of symbols does not contain a quantifier $\exists$ (or $\forall$).

Remark 2.4.3. For each formula it is possible to find a logically equivalent formula in **prenex normal form**. This formula φ in prenex normal form begins with a finite number of quantifiers $\exists x$ and $\forall y$ (for distinct variables) at the beginning of φ and end with a quantifier-free formula ψ. More precisely, φ can be chosen as

$$Q_1 x_1 \dots Q_n x_n\ \psi$$

for $Q_1, \dots, Q_n \in \{\exists, \forall\}$. It is easy to prove the claim above by structural induction, and in a basic course on Mathematical Logic one would, indeed, do so. We simply refer to the prenex normal form whenever convenient.

Among the formulas in prenex normal form, two particular classes stand out: those classes that only contain formulas using only one of the two possible quantifiers. This is made precise in the following.

Definition 2.4.4. Let $\mathcal{L}$ be a language. We define recursively the notion of **existential** and of **universal** $\mathcal{L}$-formulas:

(i) Every quantifier-free $\mathcal{L}$-formula is both existential and universal.

(ii) Let x be a variable. If φ is an existential formula, then $\exists x\ \varphi$ is also an existential formula. Likewise, if φ is a universal formula, then $\forall x\ \varphi$ is also a universal formula.

Example 2.4.5. Consider the $\mathcal{L}_<$-sentence

$$\exists x\ (\forall y\ x < y \to \exists z\ x < z).$$

This sentence is not yet in prenex normal form. First, we reformulate the sentence by using logical equivalences (or rather "unwrapping abbreviations"):

$$\exists x\ (\exists y\ x \not< y \vee \exists z\ x < z).$$

Now existential quantifiers over disjunctions can be moved to the front as long as no formerly free variables would become bounded:

$$\exists x \exists y \exists z\ (x \not< y \vee x < z).$$

We have thus transformed the initial $\mathcal{L}_<$-sentence into an existential $\mathcal{L}_<$-sentences in prenex normal form.

2.4.2. Preservation Laws

We now come to one of the main tools that will be used in one direction of the proof of Shepherdson's Theorem: preservation laws of existential and universal formulas. The proof of these laws will be done by structural induction. We thus start with the base case.

Lemma 2.4.6. *Let $\mathcal{L}$ be a language and let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures with $\mathcal{M} \subseteq \mathcal{N}$. Then for any quantifier-free $\mathcal{L}$-formula $\varphi(\underline{x})$ and for any $\underline{a} \in \mathcal{M}$ we have*

$$\mathcal{M} \models \varphi(\underline{a}) \text{ if and only if } \mathcal{N} \models \varphi(\underline{a}).$$

Proof. In detail, one could argue by structural induction using the recursive definition of quantifier-free $\mathcal{L}$-formulas. Since this is left as an exercise, we simply refer to Lemma 2.2.20 for the base case. □

Proposition 2.4.7. *Let $\mathcal{L}$ be a language and let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures with $\mathcal{M} \subseteq \mathcal{N}$. Then for any existential $\mathcal{L}$-formula $\varphi(\underline{x})$ and for any $\underline{a} \in \mathcal{M}$,*

$$\mathcal{M} \models \varphi(\underline{a}) \text{ implies } \mathcal{N} \models \varphi(\underline{a}).$$

Proof. We proceed by structural induction, the base case of which is covered in Lemma 2.4.6. Now let $\psi(\underline{x}, y)$ be an existential formula for which the conclusion already holds. Now let $\underline{a} \in \mathcal{M}$ such that $\mathcal{M} \models \exists y\ \varphi(\underline{a}, y)$. Then for some $c \in M$ we have

$$\mathcal{M} \models \varphi(\underline{a}, c).$$

The inductive hypothesis implies

$$\mathcal{N} \models \varphi(\underline{a}, c),$$

whence $\mathcal{N} \models \exists y\ \varphi(\underline{a}, y)$, as required. □

Proposition 2.4.8. *Let $\mathcal{L}$ be a language and let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures with $\mathcal{M} \subseteq \mathcal{N}$. Then for any universal $\mathcal{L}$-formula $\varphi(\underline{x})$ and for any $\underline{a} \in \mathcal{M}$,*

$$\mathcal{N} \models \varphi(\underline{a}) \text{ implies } \mathcal{M} \models \varphi(\underline{a}).$$

Proof. We simply have to prove the contrapositive of the conclusion in Proposition 2.4.7. Noting that the negation of an existential formula is a universal formula (and *vice versa*), this follows immediately. (The details are left as an exercise.) □

An important category of existential and universal formulas are existential and universal sentences. In these cases, one often says that some substructure 'inherits' something from some superstructure. In Section 2.5, we will see axiom systems that contain many universal sentences, which are thus inherited by substructures. We already give a small motivating exercise here.

Exercise 2.4.9. Let $\mathcal{G}$ be an $\mathcal{L}_{\mathrm{g}}$-structure that is an abelian group. Show that also any $\mathcal{L}_{\mathrm{g}}$-substructure $\mathcal{H} \subseteq \mathcal{G}$ is an abelian group. *The property 'abelian' is thus inherited by H from G.*

2.5. Theories and Axioms

See [4, Section 6] for further details.

2.5.1. Theories

Gödel's Completeness Theorem, which would usually be proved in a lecture on Mathematical Logic, shows that any sentence that is true in any model of a certain set of axioms (i.e. sentences) Σ can be logically derived from those axioms. In Model Theory, we stay on a semantic level, that is, we always treat sentences in connection to suitable structures. However, due to the Completeness Theorem, also on the semantic level we can define what it means that a sentence follows from a set of axioms. This is made precise in the following.

Definition 2.5.1. Let $\mathcal{L}$ be a language and let Σ be a set of $\mathcal{L}$-sentence. Moreover, let φ be an $\mathcal{L}$-sentence and let Θ be a set of $\mathcal{L}$-sentences. Then we write

$$\Sigma \models \varphi$$

if for any $\mathcal{M} \models \Sigma$ we have $\mathcal{M} \models \varphi$. Moreover, we write

$$\Sigma \models \Theta$$

if $\Sigma \models \theta$ for any $\theta \in \Theta$.

The symbol $\models$ is read as "entails" or "implies". One often also writes $\vdash$ instead of $\models$ (the former is a symbol for the syntactic meaning, the latter for the semantic) and reads $\Sigma \models \varphi$ as "φ is a logical consequence of Σ".

Definition 2.5.2. Let $\mathcal{L}$ be a language and let Σ be a set of $\mathcal{L}$-sentences. Then:

(i) The set $\{\varphi \mid \varphi \text{ is an } \mathcal{L}\text{-sentence with } \Sigma \models \varphi\}$ is called the **deductive closure** of Σ.

(ii) Σ is called **deductively closed** if it is equal to its deductive closures.

(iii) Σ is called **satisfiable** if it has a model, i.e. there exists an $\mathcal{L}$-structure $\mathcal{M}$ with $\mathcal{M} \models \Sigma$.

(iv) Σ is an **$\mathcal{L}$-theory** if it is satisfiable and deductively closed.[5]

(v) Σ is called **complete** if for any $\mathcal{L}$-sentence φ we have $\Sigma \models \varphi$ or $\Sigma \models \neg\varphi$.

(vi) For an $\mathcal{L}$-structure $\mathcal{M}$, we call Σ the **(complete) $\mathcal{L}$-theory** of $\mathcal{M}$ if

$$\Sigma = \mathrm{Th}(\mathcal{M}) := \{\varphi \mid \varphi \text{ is an } \mathcal{L}\text{-sentence with } \mathcal{M} \models \varphi\}.$$

Example 2.5.3. (i) Let $\mathcal{L}$ be a language. For any set of $\mathcal{L}$-sentences Σ and any $\sigma \in \Sigma$, we have $\Sigma \models \sigma$. Moreover, if Σ is satisfiable, then $\Sigma \not\models \neg\sigma$.

(ii) Let Σ be a set of $\mathcal{L}_{\mathrm{mon}}$-sentences that is only satisfied by $\mathcal{L}_{\mathrm{mon}}$-structures that are monoids (see Definition E.1.1). Then $\Sigma \models 1 \cdot 1 = 1$.

[5] Some authors call any satisfiable set of $\mathcal{L}$-sentences a theory.

(iii) We have $\exists x\ \exp(x) < 0 \notin \mathrm{Th}(\mathbb{R}_{\exp})$ but $\exp(1+1) = \exp(1) \cdot \exp(1) \in \mathrm{Th}(\mathbb{R}_{\exp})$.

Exercise 2.5.4. Let $\mathcal{L}$ be a language and let $\mathcal{M}$ be an $\mathcal{L}$-structure. Verify that $\mathrm{Th}(\mathcal{M})$ is a complete $\mathcal{L}$-theory.

Over a theory, one sometimes talks about equivalence of formulas. In our context, equivalence to quantifier-free formulas will be of upmost importance.

Definition 2.5.5. Let $\mathcal{L}$ be a language and let T be an $\mathcal{L}$-theory.

(i) Let $\varphi(\underline{x})$ and $\psi(\underline{x})$ be $\mathcal{L}$-formulas. We say that $\varphi(\underline{x})$ and $\psi(\underline{x})$ are **equivalent** over T if

$$T \models \forall \underline{x}\ (\varphi(\underline{x}) \leftrightarrow \psi(\underline{x})).$$

(ii) We say that T admits **quantifier elimination** if any $\mathcal{L}$-formula is equivalent over T to a quantifier-free $\mathcal{L}$-formula.

There are several criteria for theories to admit quantifier elimination (see [7, Section 3.1]), which go beyond the scope of this lecture. Instead, we will present explicitly a quantifier elimination algorithm for the theory $\mathrm{Th}(\mathbb{R}_{\mathrm{or}})$ in Chapter 4.

Exercise 2.5.6. Let $\varphi(\underline{x}, \underline{y})$ be a a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula and let $\underline{b} \in \mathbb{R}$. Show that $\varphi(\underline{x}, \underline{b})$ defines a finite union of open intervals and singletons in $\mathbb{R}_{\mathrm{or}}$.

2.5.2. Elementary Equivalence

We have already established the equivalence relation $\cong$ between $\mathcal{L}$-structures meaning that two $\mathcal{L}$-structures are $\mathcal{L}$-isomorphic. This equivalence relation expresses that two structures are algebraically identical. A weaker notion is elementary equivalence, which establishes the logical equivalence between two structures.

Definition 2.5.7. Let $\mathcal{L}$ be a language and let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures. Then we say that $\mathcal{M}$ and $\mathcal{N}$ are **elementarily equivalent** if $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$. In this case, we write

$$\mathcal{M} \equiv \mathcal{N} \text{ or } M \equiv_{\mathcal{L}} N.$$

Example 2.5.8. We have $\mathbb{R} \not\equiv_{\mathcal{L}_{\mathrm{r}}} \mathbb{Q}$. Indeed, $\exists x\ x \cdot x = 1 + 1$ is an element of $\mathrm{Th}(\mathbb{R}_{\mathrm{r}})$ but not of $\mathrm{Th}(\mathbb{Q}_{\mathrm{r}})$.

Lemma 2.5.9. *Let $\mathcal{L}$ be a language and let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures with $\mathcal{M} \cong \mathcal{N}$. Then $\mathcal{M} \equiv \mathcal{N}$.*

Proof. We only show $\mathrm{Th}(\mathcal{M}) \subseteq \mathrm{Th}(\mathcal{N})$, as the other inclusion follows similary. Let $\psi\colon \mathcal{M} \cong \mathcal{N}$ and let $\varphi \in \mathrm{Th}(\mathcal{M})$. Then $\mathcal{M} \models \varphi$, and by Proposition 2.2.21 we obtain $\mathcal{N} \models \varphi$. Hence, $\varphi \in \mathrm{Th}(\mathcal{N})$, as required. □

Lemma 2.5.9 raises the question whether there are structures that are elementarily equivalent but not isomorphic. This turns out to be a rather difficult exercise at this point. Indeed, for finite structures the two notions of equivalence always coincide (see below). However, for

infinite structures the so-called Löwenheim–Skolem Theorems – which go beyond the scope of this lecture – ensure arbitrarily large models of theories with infinite models. This shows, for instance, that there is an uncountable model $\mathcal{K}$ of the theory $\mathrm{Th}(\mathbb{Q}_{\mathrm{r}})$ implying that $\mathcal{K} \equiv \mathbb{Q}_{\mathrm{r}}$ but $\mathcal{K} \ncong \mathbb{Q}_{\mathrm{r}}$.

Exercise 2.5.10. Let $\mathcal{L}$ be a language and let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures such that M is finite and $\mathcal{M} \equiv \mathcal{N}$. Show that $\mathcal{M} \cong \mathcal{N}$.

2.5.3. Axiom Systems

In Model Theory, we often talk about the axioms for the theory of ..., where ... may be filled by "linear orderings", "rings", "ordered fields" etc. Axioms are basic sentences from which other statments about the particular algebraic structures can be deduced. We make this precise in the following.

Definition 2.5.11. Let $\mathcal{L}$ be a language and let Σ be a set of $\mathcal{L}$-sentences.

(i) Let $\mathcal{C}$ be a class of $\mathcal{L}$-structures. We say that Σ **axiomatises** $\mathcal{C}$ if for any $\mathcal{L}$-structure $\mathcal{M}$ we have $\mathcal{M} \in \mathcal{C}$ if and only if $\mathcal{M} \models \Sigma$. Any $\sigma \in \Sigma$ may then be called an **axiom**[6] for $\mathcal{C}$.

(ii) Let T be an $\mathcal{L}$-theory. We say that Σ **axiomatises** T if T is the deductive closure of Σ. An element of Σ can then be called an **axiom** for T.

In the following, we present axiom systems for some important theories.

Definition 2.5.12. (i) The $\mathcal{L}_<$-theory T_{lo} of **linear orders** is axiomatised by the following set of axioms:

$$\forall x\ x \not< x,$$
$$\forall x, y, z\ ((x < y \wedge y < z) \to x < z),$$
$$\forall x, y\ (x < y \vee x = y \vee y < x).$$

(ii) The $\mathcal{L}_<$-theory T_{dlo} of **dense linear orders without endpoints** is axiomatised by the extension of T_{lo} by the following axioms:

$$\forall x, y\ (x < y \to \exists z\ (x < z \wedge z < y)),$$
$$\forall x \exists y, z\ (y < x \wedge x < z).$$

(iii) The $\mathcal{L}_{\mathrm{g}}$-theory T_{ag} of **abelian groups** is axiomatised by the following set of axioms:

$$\forall x\ 0 + x = x,$$
$$\forall x, y, z\ x + (y + z) = (x + y) + z,$$
$$\forall x\ x - x = 0,$$
$$\forall x, y\ x - y = x + (0 - y),$$

[6] Of course, we always assume Σ to be as small as possible, i.e. not to contain redundant axioms that can be derived from the others. By this definition, we can say that two axiom systems, i.e. sets of sentences, are equivalent if they axiomatise the same class of structures.

$\forall x, y\ x + y = y + x.$

(iv) The $\mathcal{L}_{\mathrm{og}}$-theory T_{oag} of **ordered abelian groups** is axiomatised by the extension of $T_{\mathrm{ag}} \cup T_{\mathrm{lo}}$ by the following axiom:

$\forall x, y, z\ (x < y \to x + z < y + z).$

(v) The $\mathcal{L}_{\mathrm{og}}$-theory T_{doag} of **divisible ordered abelian groups** is axiomatised by the extension of T_{oag} by the following axioms:

$\exists x\ x \neq 0,$

for any $n \in \mathbb{N}$:

$$\forall x \exists y\ \underbrace{y + \ldots + y}_{n \text{ times}} = x.$$

(vi) The $\mathcal{L}_{\mathrm{r}}$-theory T_{cr} of **commutative rings with identity** is axiomaties by the extension of T_{ag} by the following axioms:

$\forall x\ 1 \cdot x = x,$

$\forall x, y, z\ x \cdot (y \cdot z) = (x \cdot y) \cdot z,$

$\forall x, y\ x \cdot y = y \cdot x,$

$\forall x, y, z\ x \cdot (y + z) = (x \cdot y) + (x \cdot z).$

(vii) The $\mathcal{L}_{\mathrm{or}}$-theory T_{or} of **ordered rings** is axiomatised by the extension of $T_{\mathrm{oag}} \cup T_{\mathrm{cr}}$ by the following axioms:

$0 < 1,$

$\forall x, y, z\ ((x < y \wedge 0 < z) \to x \cdot z < y \cdot z).$

(viii) The $\mathcal{L}_{\mathrm{or}}$-theory T_{of} of **ordered fields** is axiomatised by the extension of T_{or} by the following axiom:

$\forall (x \neq 0)\ \exists y\ x \cdot y = 1.$

(ix) The $\mathcal{L}_{\mathrm{or}}$-theory T_{rcf} of **real closed fields** is axiomatised by the extension of T_{of} by the following axioms:

$\forall (x > 0)\ \exists y\ y^2 = x,$

$\forall y_0, \ldots, y_{2n+1} \big(y_{2n+1} \neq 0 \to \exists x\ y_0 + y_1 x + \ldots + y_{2n+1} x^{2n+1} = 0\big)$, for each $n \in \mathbb{N}$.

(x) The $\mathcal{L}_{\mathrm{exp}}$-theory T_{rcef} of **real closed exponential fields** is axiomatised by the extension of T_{rcf} by the following axioms:

$\exp(0) = 1,$

$\forall x \forall y\ (\exp(x + y) = \exp(x) \exp(y)),$

$\forall (y > 0)\ \exists x\ \exp(x) = y,$

$\forall x \forall y\ (x < y \to \exp(x) < \exp(y)).$

In the following chapter, we study the theory of Peano Arithmetic in further detail.

3. Models of Arithmetic

In this chapter, we only present the basics of models of Peano Arithmetic as well as models of Open Induction. Further details can be found in [3].

3.1. Peano Arithmetic

3.1.1. Axiomatisation

Peano Arithmetic was invented in an attempt to axiomatise the semiring of natural numbers, i.e. to describe its defining properties. There is also a version of Peano Arithmetic for the integers, which will be explained in Chapter 5. Here, we concentrate on Peano Arithmetic inspired by the properties of $(\omega, +, \cdot, 0, 1, <)$.

Definition 3.1.1. The **language of Peano Arithmetic** $\mathcal{L}_{\mathrm{PA}}$ is given by $\mathcal{L}_{\mathrm{PA}} := \mathcal{L}_{\mathrm{semr}} \cup \mathcal{L}_{<} = \{+, \cdot, 0, 1, <\}$. The $\mathcal{L}_{\mathrm{PA}}$-theory PA of **Peano Arithmetic** is axiomatised by the following axiom system:

(i) the theory of linear orders T_{lo},

(ii) $\forall x\ 0 \leq x$,

(iii) $0 < 1 \wedge \forall (x > 0)\ 1 \leq x$,

(iv) $\forall x\ 0 + x = x$,

(v) $\forall x, y, z\ x + (y + z) = (x + y) + z$,

(vi) $\forall x, y\ x + y = y + x$,

(vii) $\forall x, y, z\ (x < y \to x + z < y + z)$,

(viii) $\forall x, y\ (x < y \to \exists z\ x + z = y)$,

(ix) $\forall x\ 1 \cdot x = x$,

(x) $\forall x, y, z\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$,

(xi) $\forall x, y\ x \cdot y = y \cdot x$,

(xii) $\forall x, y, z\ x \cdot (y + z) = (x \cdot y) + (x \cdot z)$,

(xiii) $\forall x, y, z\ ((x < y \wedge 0 < z) \to x \cdot z < y \cdot z)$,

(xiv) the induction scheme: for any $\mathcal{L}_{\mathrm{PA}}$-formula $\varphi(x, \underline{y})$,

$$\forall \underline{y}\ ((\varphi(0, \underline{y}) \wedge \forall n\ (\varphi(n, \underline{y}) \to \varphi(n+1, \underline{y}))) \to \forall n\ \varphi(n, \underline{y})).$$

The $\mathcal{L}_{\mathrm{PA}}$-theory axiomatised by (i) to (xiii) is also denoted by PA^-.

The $\mathcal{L}_{\mathrm{PA}}$-theory PA^- axiomatises the class of discretely ordered semirings with 1 as least positive element. There are various theories between PA^- and PA that are usually axiomatised by induction schemes restricted to particular formulas. Such a "fragment" of Peano Arithmetic, called IOpenPA (or Open Induction), is treated in Section 3.2.

Lemma 3.1.2. *Let $\mathcal{M} \models \mathrm{PA}^-$ and let $a, b \in M$ with $a \leq b \leq a+1$. Then $b = a$ or $b = a+1$.*

Proof. Assume, for a contradiction, that $a < b < a+1$. Let $k, \ell \in M$ with

$$a + k = b \text{ and } b + \ell = a + 1.$$

Note that $k, \ell \neq 0$, whence $k, \ell \geq 1$. Hence,

$$a + 1 = b + \ell = a + k + \ell \geq a + k + 1 \geq a + 1 + 1 > a + 1,$$

a contradiction. □

3.1.2. Standard and Non-Standard Parts

The standard model for PA is $\omega_{\mathrm{PA}} = (\omega, +, \cdot, 0, 1, <)$. Surprisingly, it is difficult if not even impossible to construct explicit "non-standard" models of Peano Arithmetic (due to Tennenbaum's Theorem). Non-standard models of Peano Arithmetic contain infinitely large elements, which will be of interest in connection to non-archimedean fields in later parts of this lecture. For now, we make the notions of standard and non-standard parts and models precise.

Lemma 3.1.3. *Let $\mathcal{M} \models \mathrm{PA}^-$. Then for any $n \in M$, we have $n \cdot 0 = 0 \cdot n = 0$.*

Proof. Since 0 is the least element of M, we have $n \cdot 0 \geq 0$. If $n \cdot 0 > 0$, then

$$n \cdot 0 = n \cdot (0 + 0) = n \cdot 0 + n \cdot 0 > n \cdot 0 + 0 = n \cdot 0,$$

a contradiction. □

Proposition 3.1.4. *Let $\mathcal{M} \models \mathrm{PA}^-$ and let*

$$\iota_{\mathcal{M}} \colon \omega \to M$$

be given by $\iota_{\mathcal{M}}(0) = 0^{\mathcal{M}}$ and

$$\iota_{\mathcal{M}}(n) = n_{\mathcal{M}} := \underbrace{1^{\mathcal{M}} +^{\mathcal{M}} \ldots +^{\mathcal{M}} 1^{\mathcal{M}}}_{n \text{ times}}.$$

Then

$$\iota_{\mathcal{M}} \colon \omega_{\mathrm{PA}} \hookrightarrow \mathcal{M}.$$

Proof. By definition of $\iota_{\mathcal{M}}$, we have $\iota_{\mathcal{M}}(0) = 0^{\mathcal{M}}$ and $\iota_{\mathcal{M}}(1) = 1^{\mathcal{M}}$. In order to ease the notation, we omit all further superscript "$\mathcal{M}$".

Let $m \in \omega$. Then

$$\iota_{\mathcal{M}}(m+0) = \iota_{\mathcal{M}}(m) = \iota_{\mathcal{M}}(m) + 0 = \iota_{\mathcal{M}}(m) + \iota_{\mathcal{M}}(0).$$

Likewise, $\iota_{\mathcal{M}}(0+m) = \iota_{\mathcal{M}}(0) + \iota_{\mathcal{M}}(m)$. Now let $n, m \in \mathbb{N}$. Then by associativity we have

$$\iota_{\mathcal{M}}(m+n) = m_{\mathcal{M}} + n_{\mathcal{M}} = \iota_{\mathcal{M}}(m) + \iota_{\mathcal{M}}(n).$$

We show by induction in ω that also $\cdot$ is preserved: Let $m \in \omega$ be fixed. Then

$$\iota_{\mathcal{M}}(m \cdot 0) = \iota_{\mathcal{M}}(0) = 0 = m_{\mathcal{M}} \cdot 0$$

by Lemma 3.1.3. Now let $n \in \omega$ with $\iota_{\mathcal{M}}(mn) = m_{\mathcal{M}} \cdot n_{\mathcal{M}}$. Then

$$\iota_{\mathcal{M}}(m(n+1)) = \iota_{\mathcal{M}}(mn+m) = (mn)_{\mathcal{M}} + m_{\mathcal{M}} = (m_{\mathcal{M}} \cdot n_{\mathcal{M}}) + m_{\mathcal{M}} = m_{\mathcal{M}} \cdot (n_{\mathcal{M}} + 1_{\mathcal{M}}).$$

We now show that $<$ is preserved: Let $n, m \in \omega$. Suppose that $n < m$ and set $k = m - n$. Then $m = n + k$, whence

$$m_{\mathcal{M}} = n_{\mathcal{M}} + k_{\mathcal{M}}.$$

Since $k_{\mathcal{M}} \neq 0$ i.e. $k_{\mathcal{M}} > 0$, we obtain $n_{\mathcal{M}} < m_{\mathcal{M}}$. Now suppose that $n \not< m$. If $m < n$, then $m_{\mathcal{M}} < n_{\mathcal{M}}$ follows as above, and if $n = m$, then $n_{\mathcal{M}} = m_{\mathcal{M}}$. In either case, $n_{\mathcal{M}} \not< m_{\mathcal{M}}$.

Finally, we have to verify that $\iota_{\mathcal{M}}$ is injective. Let $m, n \in \omega$ with $n \neq m$. Without loss of generality, we have $n < m$ and thus $n_{\mathcal{M}} < m_{\mathcal{M}}$. This yields $n \neq m$, as required. □

The map $\iota_{\mathcal{M}}$ now allows us to define standard and non-standard elements.

Definition 3.1.5. Let $\mathcal{M} \models \mathrm{PA}^-$. Then any element in the **standard part** $\iota_{\mathcal{M}}(\omega)$ of $\mathcal{M}$ is called a **standard element** and any element in the **non-standard part** $M \setminus \iota_{\mathcal{M}}(\omega)$ of $\mathcal{M}$ is called a **non-standard element**. If $\iota_{\mathcal{M}}(\omega) \neq M$, then $\mathcal{M}$ is called a **non-standard model** of PA^-.

Definition 3.1.6. Let $(J, <) \models T_{\mathrm{lo}}$.

(i) For any $a, b \in J$, we denote by $[a, b]_J$ the interval $\{j \in J \mid a \leq j \leq b\}$. Likewise, we use notions like $(a, b)_J$, $[a, b)_J$ etc., as well as $(-\infty, b)_J$ for $\{j \in J \mid j < b\}$, $(a, \infty)_J$ for $\{j \in J \mid a < j\}$ etc.

(ii) Let $(I, <) \subseteq (J, <)$. Then I is called an **initial segment** of J if for any $i \in I$, we have $(-\infty, i]_J \subseteq I$.

(iii) Let $\mathcal{M} \models \mathrm{PA}^-$. A non-empty subset $I \subseteq M$ is called a **cut** of $\mathcal{M}$ if it is an initial segment of M and it is closed under $+1$, i.e. for any $i \in I$ also $i + 1 \in I$. If additionally $I \neq M$, then I is called a **proper cut** of $\mathcal{M}$.

Remark 3.1.7. (i) The map $\iota_{\mathcal{M}}$ in is the only possible embedding of ω_{PA} into $\mathcal{M}$. Indeed, since it needs to map 0 to $0^{\mathcal{M}}$ and 1 to $1^{\mathcal{M}}$, it is uniquely determined.

(ii) Usually, we identify $\iota_{\mathcal{M}}(\omega)$ with ω and thus consider ω as a subset of any domain of a model of PA^-. In particular, ω is a cut of any $\mathcal{M} \models \mathrm{PA}^-$ and a proper cut of any non-standard $\mathcal{M} \models \mathrm{PA}^-$. Moreover, ω is always the smallest cut.

3.1.3. Definable Sets

Definable sets within models of PA are of particular interest. The two results in this section show that definable sets always have minimum and never form a proper cut.

Definition 3.1.8. Let $(I, <) \models T_{\text{lo}}$.

(i) Let $J \subseteq I$ and let $c \in I$. We write $c > J$ to express that $c > j$ for any $j \in J$. Similarly, $c < J$ expresses that $c < j$ for any $j \in J$.

(ii) An element $a \in I$ is called the **least element** of I if for any $b \in I$ we have $b \geq a$.

Proposition 3.1.9 (Least Number Principle)**.** *Let $\mathcal{M} \models \text{PA}$ and let $A \subseteq M$ be non-empty and $\mathcal{L}_{\text{PA}}$-definable in $\mathcal{M}$. Then A contains a least element.*

Proof. Let $\varphi(x, \underline{y})$ be an $\mathcal{L}_{\text{PA}}$-formula and let $\underline{b} \in M$ such that $A = \varphi(\mathcal{M}, \underline{b})$. Moreover, let $C \supseteq A$ be the upward closure of A, i.e.

$$C = \{c \in M \mid n \leq c \text{ for some } n \in A\}.$$

Note that C is defined by $\psi(x, \underline{b})$:

$$\exists (n \in A)\ n \leq x.$$

If $0 \in C$, then it must already be the least element of C. Hence, $0 \geq n$ for some $n \in A$ implying that $0 = n \in A$ is the least element of A.

Now suppose that $0 \in \overline{C} := M \setminus C$. Note that $\overline{C}$ is defined by $\neg\psi(x, \underline{b})$. Assume, for a contradiction, that for any $c \in \overline{C}$ also $c + 1 \in \overline{C}$. Then

$$\mathcal{M} \models \neg\psi(0, \underline{b}) \wedge \forall n\ (\neg\psi(n, \underline{b}) \to \neg\psi(n + 1, \underline{b})).$$

By induction, we obtain

$$\mathcal{M} \models \forall n\ \neg\psi(n, \underline{b}),$$

i.e. $\overline{C} = M$. This shows that $C = \emptyset$ and thus $A = \emptyset$, a contradiction.

Hence, let $c_0 \in \overline{C}$ such that $c_0 + 1 \notin \overline{C}$. Then $c_0 + 1 \in C$ but $c_0 \notin C$. In particular, $c_0 < A$. Since $c_0 + 1 \geq n_0$ for some $n_0 \in A$, we obtain $c_0 < n_0 \leq c_0 + 1$. Lemma 3.1.2 implies $n_0 = c_0 + 1$. Now for any $\ell \in A$ with $\ell < n_0$, we have again by Lemma 3.1.2 that $\ell \leq c_0$, contradicting $c_0 < A$. Hence, n_0 is the least element of A. □

Proposition 3.1.10 (Overspill)**.** *Let $\mathcal{M} \models \text{PA}$ and let $I \subseteq M$ be a proper cut of $\mathcal{M}$. Let $A \subseteq M$ be $\mathcal{L}_{\text{PA}}$-definable in $\mathcal{M}$ with $I \subseteq A$. Then there exists $c \in M$ such that $I \subsetneq [0, c]_M \subseteq A$.*

Proof. Let $C \subseteq M$ be the set defined by:[7]

$$\forall (n \leq x)\ n \in A.$$

Then for any $x \in C$, we have $[0, x]_M \subseteq A$ and thus $C \subseteq A$. Moreover, for any $i \in I$, we have $[0, i]_M \subseteq I \subseteq A$ and thus $I \subseteq C$.

[7] The set C is the first connected component of A.

Assume, for a contradiction, that $I = C$. Since then $\overline{I} = M \setminus I \subseteq M$ is $\mathcal{L}_{\mathrm{PA}}$-definable in $\mathcal{M}$, Proposition 3.1.9 shows that it contains a least element i_0. Since $0, 1 \in I$, we obtain $i_0 > 1$. Let $k \in M$ with $1 + k = i_0$. Then $k \notin \overline{I}$, as $k < i_0$. Hence $k \in I$ but $k + 1 = i_0 \notin I$, contradicting the choice of I as a cut.

Hence, $I \subsetneq C \subseteq A$. Now let $c \in C \setminus I$. Then since I is an initial segment of M, it is also an initial segment of $[0, c]_M$. Hence,

$$I \subsetneq [0, c]_M \subseteq A,$$

as required. □

Exercise 3.1.11. Let $\mathcal{M} \models \mathrm{PA}$ be non-standard. Show that neither the standard part nor the non-standard part of $\mathcal{M}$ are $\mathcal{L}_{\mathrm{PA}}$-definable in $\mathcal{M}$.

3.1.4. Number Theory

In this section, we present several results from Elementary Number Theory for any model of PA, thus verifying that those statements can be deduced from the axioms of Peano Arithmetic. Some of these results are of particular interest, as they will not hold in all models of Open Induction. This will show that their proof indeed needs the full induction scheme.

Proposition 3.1.12 (Euclidean Division)**.** *Let $\mathcal{M} \models \mathrm{PA}$ and let $a, b \in M$ with $a \neq 0$. Then there exist unique $r, s \in M$ with*

$$b = as + r \text{ and } r < a.$$

Proof. We first prove by induction on n that

$$\mathcal{M} \models \forall n \exists r, s \ (n = as + r \wedge r < a).$$

For $n = 0$, simply set $r = s = 0$. Then $n = as + r$ and $r < a$, as $a > 0$.

Now let $n, r, s \in M$ with $n = as + r$ and $r < a$. If $r + 1 < a$, then $n + 1 = as + (r + 1)$ and we are done. Otherwise, $r + 1 = a$. Hence, $n + 1 = as + a = a(s + 1) + 0$ and we are also done, as $0 < a$. This completes the induction.

In order to prove uniqueness, let $r, r', s, s' \in M$ with $b = as + r = as' + r'$ with $r, r' < a$. If $s < s'$, then

$$b = as + r < as + a = a(s + 1) \leq as' \leq as' + r' = b,$$

a contradiction. Thus, $s' \geq s$. Likewise $s' \leq s$, establishing $s = s'$. Now if $r' < r$, then

$$b = as + r = as' + r' = as + r' < as + r,$$

also a contradiction. This shows $r' \geq r$, and also $r' \leq r$ can be verified this way. □

Notation 3.1.13. Within $\mathcal{L}_{\mathrm{PA}}$, we use the following abbreviations, where s, t and u are $\mathcal{L}_{\mathrm{PA}}$-terms:

(i) The integer part of s divided by t

$$\left\lfloor \frac{s}{t} \right\rfloor$$

stands for z with $zt \leq s < (z + 1)t$ if $t \neq 0$ and 0 if $t = 0$.

(ii) The remainder on dividing s by t

$$\left(\frac{s}{t}\right)$$

stands for z with $\exists(w \leq s)\ (tw + z = s \wedge z < t)$ if $t \neq 0$ and 0 if $t = 0$.

(iii) The binary relation "s divides t"

$$s \mid t$$

stands for $\exists(z \leq t)\ (sz = t \wedge s \neq 0)$.

(iv) The 3-ary relation "s is congruent to t modulo u"

$$s \equiv t \mod u$$

stands for $u \neq 0 \wedge \left(\frac{s}{u}\right) = \left(\frac{t}{u}\right)$.

(v) The unary relation "s is prime"

$$\mathrm{pr}(s)$$

stands for $s \geq 2 \wedge \forall x, y\ (s \mid xy \to (s \mid x \vee s \mid y))$.

(vi) The unary relation "s is irreducible"

$$\mathrm{irr}(s)$$

stands for $s \geq 2 \wedge \forall(x \mid s)\ (x = 1 \vee x = s)$.

(vii) The binary relation "s and t are coprime"

$$(s, t) = 1$$

stands for $s \geq 1 \wedge t \geq 1 \wedge \forall x\ ((x \mid s \wedge x \mid t) \to x = 1)$.

(viii) The expression $s - t$ stands for z with $z + t = s$ if $t \leq s$ and 0 if $s < t$.

We also use the notations above outside $\mathcal{L}_{\mathrm{PA}}$-formulas (but within models of PA) with the same meaning.

Proposition 3.1.14 (Bézout's Lemma)**.** *Let $\mathcal{M} \models \mathrm{PA}$. Then for any $n, m \in M$ with $(n, m) = 1$, there exists $a \in M$ with $a < m$ and $an \equiv 1 \mod m$.*

Proof. If $n = 1$ or $m = 1$, then the conclusion is easy to verify. Otherwise, $w = \left(\frac{n}{m}\right)$, we have

$$\mathcal{M} \models w \geq 1 \wedge \exists(a < m)\ an \equiv w \mod m$$

(setting $a = 1$). Hence, the subset of M defined by

$$w \geq 1 \wedge \exists(a < m)\ an \equiv w \mod m$$

(where w is the free variable in this formula) has a least element $w_0 \in M$ by Proposition 3.1.9. Note that $w_0 \leq \left(\frac{n}{m}\right) \leq \min(n, m)$. We show that $w_0 = 1$, proving the desired conclusion. In order to do so, we verify that $w_0 \mid n$ and $w_0 \mid m$. This suffices, as $(n, m) = 1$.

Let $a \in M$ with $a < m_0$ and $an \equiv w_0 \mod m$. Set

$$t = \left\lfloor \frac{an}{m} \right\rfloor$$

and note that $an = tm + w_0$, as $w_0 < m$. Moreover, set

$$s = \left\lfloor \frac{n}{w_0} \right\rfloor \text{ and } r = \left(\frac{n}{w_0} \right).$$

Then $n = sw_0 + r$ and $r < w_0$. This implies

$$r = n - sw_0 = n - s(an - tm) = n + stm - san,$$

and thus

$$r \equiv (1 + um - sa)n \mod m,$$

where

$$u = \left\lfloor \frac{sa + m - 2}{m} \right\rfloor$$

and $1 + um - sa \leq m - 1 < m$. But $r < w_0$, and by choice of w_0 we obtain $r = 0$. Hence, $n = sw_0$ implying $w_0 \mid n$.

Now set

$$c = \left\lfloor \frac{m}{w_0} \right\rfloor \text{ and } d = \left(\frac{m}{w_0} \right).$$

Then $m = cw_0 + d$ with $d < w_0$ and

$$d = m - cw_0 = m - c(an - tm) = (1 + ct)m - can.$$

Setting

$$b = \left\lfloor \frac{ca + m - 1}{m} \right\rfloor,$$

we have $bm - ca \leq m - 1 < m$ and

$$d \equiv (bm - ca)n \mod m.$$

Hence, $d = 0$ and $w_0 \mid m$, as required. □

Corollary 3.1.15. *The formulas* $\mathrm{pr}(x)$ *and* $\mathrm{irr}(x)$ *are equivalent over* PA.

Proof. Let $\mathcal{M} \models \mathrm{PA}$ and let $n \in M$ with $n \geq 2$. First suppose that n is not irreducible. Then let $x \in M$ with $x \mid n$ but neither $x = 1$ nor $x = n$. Let $a \in M$ with $n = ax$ and note that $a \neq 1$ and $a \neq n$. Moreover, $a, x < n$. Hence, $n \mid ax$ but neither $n \mid a$ nor $n \mid x$, showing that n is not prime.

Now suppose that n is irreducible. Let $x, y, m \in M \setminus \{0\}$ with $n \mid xy$ and $nm = xy$. Assume, for a contradiction, that $n \nmid x$ and $n \nmid y$. Then $(n, x) = 1$: Indeed, let $\ell \in M$ with $\ell \mid n$ and $\ell \mid x$. By irreducibility of n, we have $\ell = 1$ or $\ell = n$. But if $\ell = n$, then $n \mid x$, contradicting our assumption. Likewise, $(n, y) = 1$.

Noting that $\left(\frac{1}{n}\right) = 1$, we obtain by Proposition 3.1.14 that there exist $r, s, u, v \in M$ with

$$rx = un + 1 \text{ and } sy = vn + 1.$$

Hence,

$$rsnm = rsxy = uvn^2 + (u+v)n + 1,$$

implying that

$$0 = \left(\frac{rsnm}{n}\right) = \left(\frac{rsxy}{n}\right) = 1,$$

a contradiction. □

The following exercise shows that the square root of 2 is irrational in any model of Peano Arithmetic.[8]

Exercise 3.1.16 (Irrationality of $\sqrt{2}$)**.** Show that PA $\models \neg\exists m\exists(n \neq 0)\ m^2 = 2n^2$.

Exercise 3.1.17 (Prime Divisors)**.** Show that PA $\models \forall(x > 1)\exists p\ (\mathrm{pr}(p) \wedge p \mid x)$.

The final result of this section shows that in any model of Peano Arithmetic, the set of prime numbers is unbounded (and thus, in particular, infinite).

Proposition 3.1.18 (Euclid's Theorem)**.** PA $\models \forall n\exists(m > n)\ \mathrm{pr}(m)$.

Proof. Let $\mathcal{M} \models$ PA. We first show by induction on n that

$$\mathcal{M} \models \forall n\exists(\ell \neq 0)\ (\forall(p \leq n)\ (\mathrm{pr}(p) \to p \mid \ell)). \tag{3.1.1}$$

For $n \in \{0,1,2\}$ set $\ell = 2$: For $n \in \{0,1\}$, it is vacuously true that $\forall(p \leq n)\ (\mathrm{pr}(p) \to p \mid 2)$ is vacuously true. For $n = 2$, the statement holds as 2 is the only prime in $\{0,1,2\}$ and $2 \mid 2$.

Let $n, \ell \in M$ with $n \geq 2$ and $\ell \neq 0$ such that $\forall(p \leq n)\ (\mathrm{pr}(p) \to p \mid \ell)$ holds. If $n+1$ is not prime, then

$$\{p \in M \mid \mathcal{M} \models p \leq n \wedge \mathrm{pr}(p)\} = \{p \in M \mid \mathcal{M} \models p \leq n+1 \wedge \mathrm{pr}(p)\},$$

and we are done. Otherwise, set $\ell' = \ell(n+1)$. Then certainly $n+1 \mid \ell'$. Moreover, for any prime $p \in M$ with $p \leq n$, there exists $k \in M$ with $k \leq \ell$ and $pk = \ell$. Hence, $pk(n+1) = \ell'$. Since $k(n+1) \leq \ell(n+1) = \ell'$, we obtain $p \mid \ell'$, as required. This completes the induction.

Now assume, for a contradiction, that there exists $n \in M$ with

$$\mathcal{M} \models \forall(m > n)\ \neg\,\mathrm{pr}(m). \tag{3.1.2}$$

Since the set $\{n \in M \mid \mathcal{M} \models \forall(m > n)\ \neg\,\mathrm{pr}(m)\} \neq \emptyset$ is $\mathcal{L}_{\mathrm{PA}}$-definable in $\mathcal{M}$, by Proposition 3.1.9 we may take $n \in M$ as the least element with property (3.1.2). In particular, n must be prime, as otherwise we can find a smaller n satisfying (3.1.2). By Proposition 3.1.9 and (3.1.1), we can let $\ell \in M$ be least such that $\ell \neq 0$ and for any prime $p \in M$ with $p \leq n$ we have $p \mid \ell$. In particular, $n \mid \ell$, whence $n \leq \ell$.

We now show that $\ell + 1 > n$ is prime, contradicting our assumption. If $\ell + 1$ were not prime, then by Exercise 3.1.17 we can let $q \in M$ be prime with $q \mid \ell + 1$. By our assumption, $q \leq n$ and thus $q \mid \ell$. Now let $r, s \in M$ with $qr = \ell$ and $qs = \ell + 1$. Then $r < s$ and for $t \in M \setminus \{0\}$ with $r + t = s$ we obtain

$$\ell + 1 = q(r+t) = qr + qt = \ell + qt > \ell + 1,$$

as $q \geq 2$ and $t \geq 1$, a contradiction. □

[8] Here, we use standard abbreviations such as n^2 for $n \cdot n$ and 2 for $1 + 1$.

3.2. Open Induction

We now consider the fragment of PA where the induction scheme only holds for quantifier-free formulas. This is only a very brief introduction and further properties are presented once they are needed in Chapter 5.

3.2.1. Axiomatisation

Definition 3.2.1. The $\mathcal{L}_{\mathrm{PA}}$-theory IOpen of **Open Induction** is axiomatised by the extension of PA^- by the induction scheme restricted to quantifier-free $\mathcal{L}_{\mathrm{PA}}$-formulas:

for any quantifier-free $\mathcal{L}_{\mathrm{PA}}$-formula $\varphi(x, \underline{y})$,

$$\forall \underline{y}\ ((\varphi(0, \underline{y}) \wedge \forall n\ (\varphi(n, \underline{y}) \to \varphi(n+1, \underline{y}))) \to \forall n\ \varphi(n, \underline{y})).$$

The theory IOpen is of particular interest, as restricting the induction scheme to $\mathcal{L}_{\mathrm{PA}}$-formulas of particularly simple form, i.e. to those using no quantifiers at all, is a natural reduction of the full induction scheme in PA. While we lose properties like the Least Number Principle and Overspill for *all* $\mathcal{L}_{\mathrm{PA}}$-definable sets, there are also versions of the results from Subsection 3.1.3 for sets defined within models of IOpen by quantifier-free $\mathcal{L}_{\mathrm{PA}}$-formulas. We will, however, not state these results explicitly.

While we lose the strength of full induction, we gain a better understanding of models of this particular kind of arithmetic. More precisely, the two main theorems of this lecture will give us a way to explicitly construct non-standard models of IOpen, which is not possible in the case of PA.

3.2.2. Number Theory

While we will show that neither the irrationality of 2 nor Euclid's Theorem can be proved within IOpen, we can still obtain some basic arithmetical results from Number Theory. As an example, we present Euclidean Division. Some results directly following from Euclidean Division could then also be deduced within IOpen.

Proposition 3.2.2 (Euclidean Division in IOpen)**.** *Let $\mathcal{M} \models$ IOpen and let $a, b \in M$ with $a \neq 0$. Then there exist unique $r, s \in M$ with*

$$b = as + r \text{ and } r < a.$$

Proof. Once we have established the existence of r and s, their uniqueness can be derived like in the proof of Proposition 3.1.12, as this only requires properties of PA^-.

Assume, for a contradiction, that there are $a, b \in M$ with $a \neq 0$ not satisfying the conclusion. Then $b \geq a$, as otherwise we could set $s = 0$ and $r = b$. Consider the quantifier-free $\mathcal{L}_{\mathrm{PA}}$-formula (with parameters) $\varphi(n, a, b)$ given by

$$b > n \cdot a.$$

Since $b \geq a > 0$, we have $\mathcal{M} \models \varphi(0, a, b)$.

Now let $n \in M$ with $b > na$ and let $r \in M$ with $na + r = b$. Assume that $b \leq (n+1)a$. Then $b = na + r \leq na + a$, whence $r \leq a$. By assumption on a and b, we obtain $r = a$ and thus $b = na + a = (n+1)a + 0$, also contradicting the choice of a and b. We thus obtain $b > (n+1)a$. In conclusion,

$$\mathcal{M} \models \forall n \ (\varphi(n, a, b) \to \varphi(n+1, a, b)).$$

By induction, we obtain that for all $n \in M$ we have $b > na$. However, since $a \neq 0$,

$$b > ba \geq b,$$

a contradiction. □

4. Real Algebra and Real Closed Fields

4.1. Real Algebra

This section follows [7, Appendix B]. We always abbreviate the $\mathcal{L}_{\mathrm{r}}$-structure of a field $(K, +, -, \cdot, 0, 1)$ by K. An $\mathcal{L}_{\mathrm{or}}$-expansion of K is then denoted by $(K, <)$.

4.1.1. Real Fields

Notation 4.1.1. Let K be a field. Then

$$\sum K^2 := \{a_1^2 + \ldots + a_n^2 \mid n \in \mathbb{N}, a_1, \ldots, a_n \in K\}$$

denotes the set of **sums of squares** from K.

Definition 4.1.2. Let K be a field. Then K is called **(formally) real** if $-1 \notin \sum K^2$.

Exercise 4.1.3. Let $(K, <)$ be an ordered field, i.e. $(K, <) \models T_{\mathrm{of}}$. Show that K is real.

Certainly, $\mathbb{R}$ is real and $\mathbb{C}$ is not real. In the following, we show that a field is real if and only if it can be expanded to an ordered field.

Lemma 4.1.4. *Let K be a real field and let $a \in K^\times$. Then $\{a, -a\} \not\subseteq \sum K^2$.*

Proof. We prove the contrapositive. Suppose that $\{a, -a\} \subseteq \sum K^2$. Let $n \in \mathbb{N}$ and $c_1, \ldots, c_n$, $d_1, \ldots, d_n \in K$ such that

$$a = c_1^2 + \ldots + c_n^2 \text{ and } -a = d_1^2 + \ldots + d_n^2.$$

Then

$$-1 = \frac{a}{-a} = \frac{a}{a^2}(-a) = \frac{c_1^2 + \ldots + c_n^2}{a^2}(d_1^2 + \ldots + d_n^2) = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\frac{c_i d_j}{a}\right)^2 \in \sum K^2.$$

Hence, K is not real. □

Recall that for any field K and any $a \in K$, we denote by $\sqrt{a}$ a zero of the polynomial $X^2 - a$ in some algebraic closure of K.

Lemma 4.1.5. *Let K be a real field and let $a \in K$. Then either $K(\sqrt{a})$ or $K(\sqrt{-a})$ is real.*

Proof. By Lemma 4.1.4, not both a and $-a$ can be a sum of squares. Suppose that $-a \in K \setminus \sum K^2$. We show that $K(\sqrt{a})$ is real. (In the case $a \in K \setminus \sum K^2$, one can similarly prove that $K(\sqrt{-a})$ is real.)

If $\sqrt{a} \in K$, then $K(\sqrt{a}) = K$ and we are done. Otherwise, assume, for a contradiction, that $K(\sqrt{a})$ is not real. Then there are $b_i, c_i \in K$ with $i \in \{1, \dots, n\}$ for some $n \in \mathbb{N}$ such that

$$-1 = \sum_{i=1}^{n} (b_i + c_i\sqrt{a})^2 = \sum_{i=1}^{n} (b_i^2 + c_i^2 a) + \sqrt{a} \sum_{i=1}^{n} 2c_i b_i.$$

Since $\{1, \sqrt{a}\}$ is a basis of $K(\sqrt{a})$ over K, we obtain

$$-1 = \sum_{i=1}^{n} (b_i^2 + c_i^2 a).$$

Hence,

$$-a = \frac{1 + \sum_{i=1}^{n} b_i^2}{\sum_{i=1}^{n} c_i^2} = \frac{\left(\sum_{i=1}^{n} b_i^2\right)\left(\sum_{i=1}^{n} c_i^2\right)}{\left(\sum_{i=1}^{n} c_i^2\right)^2} \in \sum K^2,$$

a contradiction. □

Lemma 4.1.6. *Let K be a real field and let $f \in K[X]$ be of odd degree n and irreducible. Then for any α in the algebraic closure of K with $f(\alpha) = 0$, the field $K(\alpha)$ is real.*

Proof. We proceed by induction on n, where the case $n = 1$ is clear. Let $n \in \mathbb{N}$ be odd such that the statement holds for any odd k up to $n - 2$. Assume, for a contradiction, that $K(\alpha)$ is not real. Since

$$K(\alpha) = \{g(\alpha) \mid g \in K[X], \deg(g) \leq n - 1\},$$

for some $m \in \mathbb{N}$, there are $g_1, \dots, g_m \in K[X]$ of degree at most $n - 1$ such that

$$-1 = \sum_{i=1}^{m} g_i^2(\alpha).$$

As K is real, some g_i is non-constant. Recall that

$$\varphi \colon K[X]/\langle f \rangle \xrightarrow{\cong} K(\alpha), h(X) + \langle f \rangle \mapsto h(\alpha).$$

Hence,

$$-1 + \langle f \rangle = \varphi^{-1}\left(\sum_{i=1}^{m} g_i^2(\alpha)\right) = \sum_{i=1}^{m} g_i^2(X) + \langle f \rangle.$$

Thus, there is some $q \in K[X]$ with

$$-1 = \sum_{i=1}^{m} g_i^2(X) + q(X)f(X).$$

Now $\deg\left(\sum_{i=1}^{m} g_i^2(X)\right)$ is even with

$$2 \leq \deg\left(\sum_{i=1}^{m} g_i^2(X)\right) \leq 2n - 2,$$

and $\deg(qf) = \deg(q) + n$. Hence, $\deg(q)$ is odd and at most $n-2$. Let $p \in K[X]$ be an irreducible factor of q of odd degree $k \leq n-2$ and let $r \in K[X]$ with $pr = q$. Then for any zero β of p, we have

$$-1 = \sum_{i=1}^{m} g_i^2(\beta) + p(\beta)r(\beta)f(\beta) = \sum_{i=1}^{m} g_i^2(\beta) \in K(\beta).$$

Thus, $K(\beta)$ is not real, contradicting the inductive hypothesis. □

Definition 4.1.7. Let K be a real field. Then we say that K is **real closed** if no proper algebraic field extension of K is real, i.e. for any algebraic field extension F/K with $K \subsetneq F$ the field F is not real.

Example 4.1.8. (i) Since $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$, it is also the only proper algebraic extension of $\mathbb{R}$. As $\mathbb{C}$ is not real, $\mathbb{R}$ is a real closed field.

(ii) The field $\mathbb{Q}$ is real, as $-1 \notin \sum \mathbb{Q}^2$. However, also the algebraic extension $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$ is real (see Lemma 4.1.5), whence $\mathbb{Q}$ is not real closed.

The following exercise justifies why in Definition 4.1.7 only *algebraic* field extensions are considered.

Exercise 4.1.9. Find a proper field extension of $\mathbb{R}$ that is real.

Definition 4.1.10. Let K be a real closed field. We define the binary relation $<$ on K by letting

$$a < b :\Leftrightarrow K \models \exists (c \neq 0)\ a + c^2 = b.$$

Exercise 4.1.11. Let K be a real closed field.

(i) Show that $(K, <) \models T_{\text{of}}$, i.e. $(K, <)$ is an ordered field.

(ii) Let $\prec$ be a binary relation on K that does not coincide with $<$. Show that $(K, \prec) \not\models T_{\text{of}}$. *(Hence, $<$ is the unique binary relation on K making $(K, <)$ an ordered field.)*

Remark 4.1.12. In Definition 2.5.12 (ix), we introduced the $\mathcal{L}_{\text{or}}$-theory T_{rcf} of real closed fields. By Definition 4.1.7, real closed fields are $\mathcal{L}_{\text{r}}$-structures. However, by Definition 4.1.10, any $\mathcal{L}_{\text{r}}$-structure of a real closed field can be expanded naturally to an $\mathcal{L}_{\text{or}}$-structure. It therefore always depends on the context whether a real closed field is considered as an $\mathcal{L}_{\text{r}}$- or an $\mathcal{L}_{\text{or}}$-structure. In the following subsection, we will also justify this ambiguity by verifying that the described $\mathcal{L}_{\text{or}}$-expansion of a real closed field becomes a model of T_{rcf}.

4.1.2. Real Closed Fields

Definition 4.1.13. Let K be a real field and let R/K be algebraic such that R is real closed. Then R is called a **real closure** of K.

Exercise 4.1.14. (i) Use Zorn's Lemma to show that any real field has a real closure.

(ii) Let K be a real field and let $a \in K$ with $-a \notin \sum K^2$. Show that there is a binary relation $<$ on K such that $(K, <) \models T_{\text{of}}$ and $a > 0$.

Proposition 4.1.15. *Let K be a real field with the following properties:*

(i) For any $a \in K$, either $\sqrt{a} \in K$ or $\sqrt{-a} \in K$.

(ii) Any polynomial $f \in K[X]$ of odd degree has a zero in K.

Further, let $i = \sqrt{-1}$. Then $C = K(i)$ is algebraically closed.

Proof. Let $<$ be a linear ordering on K such that $(K, <)$ is an ordered field. First note that for any $x \in K$ with $x > 0$, we have $\sqrt{x} \in K$: If not, then $\sqrt{-x} \in K$ for some positive $x \in K$. Then $-x \in \sum K^2$, whence $-x \geq 0$, a contradiction.

We now show that any element of C has a square root in C. To this end, let $a, b \in K$ with $(a, b) \neq (0, 0)$. Since $a^2 + b^2 > 0$, we can let $s \in K$ with $s > 0$ such that $s^2 = a^2 + b^2$. Consider

$$r = \frac{a+s}{2} \in K.$$

If $s < -a$, then $a^2 + b^2 < a^2$, a contradiction. Thus, $s \geq -a$ and $r \geq 0$. Hence, $\sqrt{r} \in K$. Setting

$$c = \sqrt{r} \text{ and } d = \tfrac{b}{2c},$$

we obtain

$$\begin{aligned}
(c+di)^2 &= c^2 - d^2 + 2cdi \\
&= r - \tfrac{b^2}{4r} + bi \\
&= \frac{(2r+b)(2r-b)}{4r} + bi \\
&= \frac{(s+a+b)(s+a-b)}{4r} + bi \\
&= \frac{s^2 + 2as + a^2 - b^2}{4r} + bi \\
&= \frac{2a^2 + 2as}{2(a+s)} + bi \\
&= a + bi,
\end{aligned}$$

as required.

To prove that C is algebraically closed, it suffices to verify that it has no proper finite field extension. Let L/C be a finite field extension. We may assume that the extension L/K is a Galois extension, as otherwise we can replace L by its normal hull. Let $G = \mathrm{Gal}(L/K)$ be the Galois group of L over K. Since

$$|G| = [L : K] = [L : C][C : K] = 2[L : C],$$

there are $k, m \in \mathbb{N}$ such that m is odd and $|G| = 2^k m$.

Let H be a 2-Sylow subgroup of G. Then $|H| = 2^k$. Let F be the fixed field of H, i.e. $F = \mathrm{Inv}(H)$. Then

$$[L : F] = |H| = 2^k \text{ and } [F : K] = [G : H] = m.$$

Now for any $\alpha \in F$, the degree of the minimal polynomial $m_{\alpha,K} \in K[X]$ of α over K divides m and must therefore be odd. By property (ii), we obtain that $m_{\alpha,K}$ has a zero in K. Hence, $\deg(m_{\alpha,K}) = 1$ and $\alpha \in K$. This shows that $F = K$ and $m = 1$. We thus obtain

$$[L : C] = \frac{[L : K]}{[C : K]} = \frac{2^k}{2} = 2^{k-1}.$$

We show that $k = 1$, establishing our desired conclusion $L = C$.

Let $G' = \mathrm{Gal}(L/C)$. Assume, for a contradiction, that $k \geq 2$. Then $|G'| = [L : C] = 2^{k-1} \geq 2$. By the Sylow Theorems, G' has a subgroup H' of order $|H'| = 2^{k-2}$. Then

$$[\mathrm{Inv}(H') : C] = [G' : H'] = 2.$$

This shows that the fixed field $\mathrm{Inv}(H')$ of H' is a degree 2 extension of C. This contradicts the fact that any element of C has a square root in C. □

Corollary 4.1.16. *Let K be a real field and let $i = \sqrt{-1}$. Then $C = K(i)$ is algebraically closed if and only if K is real closed.*

Proof. First suppose that K is real closed. Then K is a real field satisfying the properties of Proposition 4.1.15: Lemma 4.1.5 shows that for any $a \in K$, either $K(\sqrt{a})$ or $K(\sqrt{-a})$ is real and thus equal to K, establishing property (i). Now let $f \in K[X]$ be of odd degree. Then f must have an irreducibel factor g of odd degree. Lemma 4.1.6 implies that for any zero α of g, also $K(\alpha)$ is real and thus equal to K, establishing property (ii). Proposition 4.1.15 now yields that C is algebraically closed.

Conversely, suppose that C is algebraically closed. Note that C is the only algebraic extension of K (up to $\mathcal{L}_{\mathrm{r}}$-isomorphism), as $[C : K] = 2$. Since C is not real ($-1 = i^2 \in \sum C^2$), we obtain that K is real closed. □

We now turn to ordered fields.

Remark 4.1.17. Let $(K, <) \models T_{\mathrm{of}}$. Then $(K, <)$ is called a real closed field if $(K, <) \models T_{\mathrm{rcf}}$. Note that if $(K, <)$ is real closed, then K is real closed. Indeed, by Corollary 4.1.16 it suffices to show that $K(i)$ is algebraically closed. In order to do so, simply note that the conditions of Proposition 4.1.15 are directly implied by the axioms of T_{rcf}.

Definition 4.1.18. An ordered field $(K, <)$ has the **intermediate value property** if for any $p \in K[X]$ and any $a, b \in K$ with $a < b$ and $p(a) < 0 < p(b)$ there is some $c \in (a, b)_K$ such that $p(c) = 0$.

Note that the intermediate value property can be expressed by an $\mathcal{L}_{\mathrm{or}}$-axiom scheme.

Notation 4.1.19. Let $(R, <) \models T_{\mathrm{or}}$. For any $a \in R$, we denote by $|a|$ the element a if $a \geq 0$ and the element $-a$ if $a < 0$. A similar abbreviation is used within $\mathcal{L}_{\mathrm{or}}$-formulas.

Exercise 4.1.20. Let $(K, <)$ be an ordered field and for some $n \in \mathbb{N}$ and let

$$p(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$$

with $a_n \neq 0$. Show that for

$$B(p) := \sum_{i=0}^{n} \left| \frac{a_i}{a_n} \right| + 1$$

no zero of p in K lies outside the interval $(-B(p), B(p))_K$.

Proposition 4.1.21. *Let $(K, <)$ be an ordered field. Then $(K, <)$ is real closed if and only if it has the intermediate value property.*

Proof. First suppose that $(K, <)$ has the intermediate value property. Let $a \in (0, \infty)_K$ and consider the polynomial $s(X) = X^2 - a$. Then

$$s(0) = 0 - a < 0 < 1 + a + a^2 = s(a + 1).$$

Hence, there exists some $c \in (0, a + 1)_K$ with $c^2 = a$, establishing the first required axiom. Now let $p \in K[X]$ be of odd degree and set

$$p(X) = \sum_{i=0}^{n} a_i X^i$$

with $a_n \neq 0$. Replacing p by $-p$ if necessary, we may assume that $a_n > 0$. Let $B = B(p)$ be as in Exercise 4.1.20. Proceeding as in the proof of Exercise 4.1.20, we obtain $p(-B) < 0 < p(B)$. Hence, p has a zero in $(-B, B)_K$ by the intermediate value property, establishing the second required axiom scheme.

Now suppose that $(K, <)$ is real closed. Let $p \in K[X]$ and let $a, b \in K$ with $a < b$ and $p(a) < 0 < p(b)$. We may assume that p has leading coefficient 1 and is irreducible, as at least one factor of p must change sign within $[a, b]_K$. By Remark 4.1.17, also K is real closed, whence $K(i)$ is algebraically closed by Corollary 4.1.16. As $[K(i) : K] = 2$, the degree of p is either 1 or 2. If $\deg(p) = 1$, then it is linear and thus has a zero in K. Otherwise,

$$p(X) = X^2 + cX + d$$

for some $c, d \in K$ with $c^2 - 4d < 0$. But then

$$p(x) = \left(x + \frac{c}{2}\right)^2 + \left(\sqrt{d - \frac{c^2}{4}}\right)^2 > 0$$

for any $x \in K$, a contradiction. □

4.1.3. Sturm Sequences and Uniqueness of Real Closure

In this section, we show that the real closure of an ordered field is unique (up to $\mathcal{L}_{\text{or}}$-isomorphism). We do so by using Sturm's Algorithm. Besides [7, Appendix B], we also follow [1, Section 2.2.2].

Exercise 4.1.22. Let $(K, <)$ be an ordered field. Show that there exists a real closure R of K such that $(K, <) \subseteq (R, <)$. *The ordered field $(R, <)$ is then called a* ***real closure*** *of $(K, <)$.*

Notation 4.1.23. Let f be a polynomial expression in the variable X, i.e.

$$f = \sum_{i=0}^{n} a_i X^i$$

for some $n \in \omega$ and coefficients a_i.

(i) The **formal derivative** f' of f is given by

$$f' = \sum_{i=1}^{n} i a_i X^{i-1}.$$

(ii) The **leading monomial** $\mathrm{lm}(f)$ is given by

$$\mathrm{lm}(f) = a_n X^n$$

if $a_n \neq 0$.

In Notation 4.1.23, we do not specify the polynomial ring over which f is defined. The reason for this is that we will also use the introduced notations within $\mathcal{L}_{\mathrm{or}}$-formulas, where the coefficients are given by $\mathcal{L}_{\mathrm{or}}$-terms. It should always be clear from the context how the notions are interpreted.

Definition 4.1.24. Let $(K, <)$ be an ordered field. Then for any $a \in K$, we define the **sign** of a to be

$$\mathrm{sign}(a) = \begin{cases} 1 & \text{if } a > 0, \\ -1 & \text{if } a < 0, \\ 0 & \text{if } a = 0. \end{cases}$$

Due to the intermediate value property, we can define what it means that a polynomial (or, more generally, a rational function) changes its sign at a root.

Definition 4.1.25. Let $(R, <)$ be a real closed field, let $f, g \in R[X]$ with $f, g \neq 0$ and let $c \in R$ be a root of f.

(i) We say that the **sign of $\frac{f}{g}$ at the right of c is positive** (respectively **negative**) if there exists $\varepsilon \in (0, \infty)_R$ such that $\frac{f}{g}$ is positive (respectively **negative**) on the interval $(c, c+\varepsilon)_R$. The same notions are defined **at the left of** c, where the interval $(c, c+\varepsilon)_R$ is replaced by $(c-\varepsilon, c)_R$.

(ii) We say that $\frac{f}{g}$ **changes its sign at c from negative to positive** if the sign of $\frac{f}{g}$ at the left of c is negative and at the right of c is positive. Likewise, $\frac{f}{g}$ **changes its sign at c from positive to negative** if the sign of $\frac{f}{g}$ at the left of c and at the right of c are different.

Naturally, Definition 4.1.25 also applies to polynomials by setting $g = 1$.

Remark 4.1.26. Let $(R,<)$ be a real closed field, let $f,g \in R[X]$ with $f,g \neq 0$ and let $c \in R$ be a root of f. Then the sign of $\frac{f}{g}$ at the right of c is either positive or negative. Indeed, if for a given $\delta \in (0,\infty)_R$ the sign of $\frac{f}{g}$ on $(c,c+\delta)_R$ can be both positive and negative, then by the intermediate value property $\frac{f}{g}$ must have a zero in this interval. However, $\frac{f}{g}$ only has finitely many zeros, whence for some sufficiently small $\varepsilon \in (0,\infty)_R$, there is no sign change of $\frac{f}{g}$ in $(c,c+\varepsilon)_R$.

The same argument applies to the sign at the left of c. We denote by $\varepsilon(f/g,c) \in (0,\infty)_K$ an element such that the only sign change of $\frac{f}{g}$ in the interval $(c-\varepsilon(f/g,c),c+\varepsilon(f/g,c))_R$ happens at c

As a preparation for quantifier elimination in the next section, we now establish a result of counting those roots of one polynomial for which the other one is positive. A special case of this result will give us a way of counting the number of roots of a polynomial within a given interval.

Definition 4.1.27. Let $(R,<)$ be a real closed field and let $p,q \in R[X]$ with $p \neq 0$.

(i) Let $x \in R$ be a root of p. We say that $\frac{q}{p}$ **jumps** at x if the following hold:

- The multiplicity μ of x in p is bigger than the multiplicity ν of x in q.[9]
- The difference $\mu - \nu$ is odd.

Moreover, it **jumps from** $-\infty$ **to** ∞ if additionally the sign of $\frac{q}{p}$ at the right of x is positive, and it **jumps from** ∞ **to** $-\infty$ if the sign of $\frac{q}{p}$ at the right of x is negative.

(ii) Let $a,b \in R \cup \{-\infty,\infty\}$. Then the **Cauchy index**

$$\mathrm{CInd}(\tfrac{q}{p};a,b)$$

of $\frac{q}{p}$ on $(a,b)_R$ is the number of jumps of $\frac{q}{p}$ in $(a,b)_R$ from $-\infty$ to ∞ minus the number of jumps of $\frac{q}{p}$ in $(a,b)_R$ from ∞ to $-\infty$. We denote $\mathrm{CInd}(\frac{q}{p};-\infty,\infty)$ simply by $\mathrm{CInd}(\frac{q}{p})$.

Definition 4.1.28. Let $(R,<)$ be a real closed field, let $p,q \in R[X]$ with $p \neq 0$ and let $a,b \in R \cup \{-\infty,\infty\}$ with $a<b$. Then the **Tarski query** of q for p in $(a,b)_R$ is given by

$$\mathrm{TaQ}(q,p;a,b) = \sum_{x \in p^{-1}(0) \cap (a,b)_R} \mathrm{sign}(q(x)).$$

We denote $\mathrm{TaQ}(q,p;-\infty,\infty)$ simply by $\mathrm{TaQ}(q,p)$.

Note that $\mathrm{TaQ}(q,p;a,b)$ counts the number of roots of p in the interval $(a,b)_R$ for which q is positive minus those for which q is negative. We now establish a connection between the Cauchy index and the Tarski query.

Lemma 4.1.29. *Let $(R,<)$ be a real closed field and let $p \in R[X]$ with $p \neq 0$. Then $\frac{p'}{p}$ jumps from $-\infty$ to ∞ at any root $c \in R$ of p.*

[9] We set $\nu = 0$ if x is not a root of q.

Proof. Let $\mu \in \mathbb{N}$ be the multiplicity of c in p. Then there is $q \in R[X]$ with

$$p(X) = q(X)(X-c)^\mu \text{ and } p'(X) = \mu q(X)(X-c)^{\mu-1} + q'(X)(X-c)^\mu.$$

Set

$$s(X) = q(X)(X-c) \text{ and } r(X) = \mu q(X) + q'(X)(X-c)$$

and note that $r(c) = \mu q(c) \neq 0$. Then $\frac{p'}{p} = \frac{r}{s}$.

We now verify that $\frac{r}{s}$ jumps from $-\infty$ to ∞ at c. First note that the multiplicity of c in r is 0 and the multiplicity of c in s is 1. We thus only have to show that the sign of $\frac{r}{s}$ at the right of c is positive. First let $\varepsilon = \varepsilon(r/s, c)$ (see Remark 4.1.26). We have to find $d \in (c, c+\varepsilon)_R$ such that $\frac{r(d)}{s(d)} > 0$. It suffices to find such d with

$$|q'(d)(d-c)| \leq \frac{1}{2}|\mu q(d)|, \tag{4.1.1}$$

as then

$$\operatorname{sign}\left(\frac{r(d)}{s(d)}\right) = \operatorname{sign}\left(\frac{\mu q(d) + q'(d)(d-c)}{q(d)(d-c)}\right) = \operatorname{sign}\left(\frac{\mu q(d)}{q(d)}\right) = 1.$$

First express q' as

$$q'(X) = \sum_{i=0}^{m} a_i X^i$$

and set

$$M = \sum_{i=0}^{m} |a_i|\big(|c|^i + |c+\varepsilon|^i\big).$$

Then q' is bounded from above by M on the interval $(c, c+\varepsilon)_R$. Hence, (4.1.1) reduces to finding $d \in (c, c+\varepsilon)_R$ such that

$$d - c \leq \frac{\mu}{2M}|q(d)|$$

Set $\delta = q(c) \neq 0$. First suppose that $\delta > 0$ and set $t(X) = q(X) - \frac{\delta}{2}$. Then $t(c) > 0$ and by the intermediate value property, there must be some $\rho \in (0, \varepsilon)_R$ such that t is positive on $(c, c+\rho)_R$. Let $d \in (c, c+\rho)_R$ with

$$d \leq c + \frac{\mu\delta}{4M}.$$

Then $q(d) = t(d) + \frac{\delta}{2} > \frac{\delta}{2}$ and

$$d - c \leq \frac{\mu\delta}{4M} = \frac{\mu}{2M} \cdot \frac{\delta}{2} < \frac{\mu}{2M}|q(d)|,$$

as required. For the case $\delta < 0$, one can simply replace q by $-q$ and argue similarly. □

Proposition 4.1.30. *Let $(R, <)$ be a real closed field, let $p, q \in R[X]$ with $p \neq 0$ and let $a, b \in R \cup \{-\infty, \infty\}$ with $a < b$. Then*

$$\operatorname{TaQ}(q, p; a, b) = \operatorname{CInd}(\tfrac{p'q}{p}; a, b).$$

In particular, the number of roots of p in $(a, b)_R$ is $\operatorname{CInd}(\frac{p'}{p}; a, b)$.

Proof. Let $V = p^{-1}(0) \cap (a,b)_R$ and $r = \frac{p'q}{p}$. It suffices to establish the following:

$$\begin{aligned}
\{x \in V \mid q(x) = 0\} &= \{x \in V \mid r \text{ has no jump at } x\},\\
\{x \in V \mid q(x) > 0\} &= \{x \in V \mid r \text{ jumps from } -\infty \text{ to } \infty \text{ at } x\},\\
\{x \in V \mid q(x) < 0\} &= \{x \in V \mid r \text{ jumps from } \infty \text{ to } -\infty \text{ at } x\}.
\end{aligned}$$

Let $c \in V$. First suppose that $q(c) = 0$. Let $\mu \in \mathbb{N}$ be the multiplicity of c in p and let $\nu \in \mathbb{N}$ be the multiplicity of c in q. Then the multiplicity of c in $p'q$ is given by $\nu + \mu - 1 \geq \mu$, whence r has no jump at c.

For the remaining two cases, first recall that by Lemma 4.1.29, $\frac{p'}{p}$ jumps from $-\infty$ to ∞ at c. Hence, r also jumps from $-\infty$ to ∞ at c if $q(c) > 0$ and r jumps from ∞ to $-\infty$ at c if $q(c) < 0$. This establishes all of the set equalities above. □

We now establish a way to determine the Cauchy index by counting the number of sign changes in a particular sequence of polynomials.

Definition 4.1.31. Let $(K, <)$ be an ordered field and let $n \in \mathbb{N}$.

(i) The **number of sign variations** $\operatorname{Var}(\underline{a})$ of the sequence $\underline{a} = (a_0, \ldots, a_n) \in K^\times$ is defined iteratively for any $p \in \{1, \ldots, n\}$:

$$\begin{aligned}
\operatorname{Var}(a_0) &:= 0,\\
\operatorname{Var}(a_0, \ldots, a_p) &:= \begin{cases} \operatorname{Var}(a_0, \ldots, a_{p-1}) & \text{if } \operatorname{sign}(a_{p-1}) = \operatorname{sign}(a_p),\\ \operatorname{Var}(a_0, \ldots, a_{p-1}) + 1 & \text{if } \operatorname{sign}(a_{p-1}) \neq \operatorname{sign}(a_p). \end{cases}
\end{aligned}$$

Moreover, we set $\operatorname{Var}(0, \ldots, 0) = 0$, and for a sequence $\underline{a} = (a_0, \ldots, a_n) \in K$, not all a_i equal to 0, we let $\operatorname{Var}(\underline{a})$ be the number of sign variations of the sequence $\underline{a}$ after removing all 0 entries.

(ii) Let $\underline{f} = (f_0, \ldots, f_n) \in K[X]$ and let $a \in K$. The **number of sign variations** of $\underline{f}$ at a is given by

$$\operatorname{Var}(\underline{f}; a) := \operatorname{Var}(f_0(a), \ldots, f_n(a)).$$

Moreover, we set

$$\begin{aligned}
\operatorname{Var}(\underline{f}; -\infty) &:= \operatorname{Var}(\operatorname{lm}(f_0)(-1), \ldots, \operatorname{lm}(f_n)(-1)) \text{ and}\\
\operatorname{Var}(\underline{f}; \infty) &:= \operatorname{Var}(\operatorname{lm}(f_0)(1), \ldots, \operatorname{lm}(f_n)(1)).
\end{aligned}$$

For any $a, b \in K \cup \{-\infty, \infty\}$, we set

$$\operatorname{Var}(\underline{f}; a, b) := \operatorname{Var}(\underline{f}; a) - \operatorname{Var}(\underline{f}; b).$$

Moreover,

$$\operatorname{Var}(\underline{f}) := \operatorname{Var}(\underline{f}; -\infty, \infty).$$

Example 4.1.32. Consider the ordered field $(\mathbb{R}, <)$.

(i) We have

$$\begin{aligned}&\operatorname{Var}(1,2,-3,0,2,0,3,0,0,0,-4,-2,1,3,0)\\=&\operatorname{Var}(1,2,-3,2,3,-4,-2,1,3)=4.\end{aligned}$$

(ii) Let $f_0(X)=X^2-2, f_1(X)=-X^3+2X, f_2(X)=3X\in\mathbb{R}[X]$. Then

$$\begin{aligned}\operatorname{Var}(f_0,f_1,f_2;0)&=\operatorname{Var}(-2,0,0)=0,\\ \operatorname{Var}(f_0,f_1,f_2;1)&=\operatorname{Var}(-1,1,3)=1,\\ \operatorname{Var}(f_0,f_1,f_2;0,1)&=0-1=-1,\\ \operatorname{Var}(f_0,f_1,f_2;\infty)&=\operatorname{Var}(1,-1,3)=2.\end{aligned}$$

Definition 4.1.33. Let F be a field and let $p,q\in F[X]$ with $q\neq 0$.

(i) The unique polynomial $r\in F[X]$ with

$$p=aq+r \text{ and } \deg(r)<\deg(q)$$

for some $a\in F[X]$ is called the **remainder** (in the Euclidean division of p by q) and denoted by $\operatorname{rem}(p,q)$.

(ii) We define the **signed remainder sequence** of p and q as the sequence of polynomials in $F[X]$ given by

$$\operatorname{SRS}(p,q)=(\operatorname{SRS}_0(p,q),\dots,\operatorname{SRS}_n(p,q))$$

for $n\in\mathbb{N}$ with the property[10]

$$\begin{aligned}\operatorname{SRS}_0(p,q)&=p,\\ \operatorname{SRS}_1(p,q)&=q,\\ \operatorname{SRS}_2(p,q)&=-\operatorname{rem}(\operatorname{SRS}_0(p,q),\operatorname{SRS}_1(p,q)),\\ &\vdots\\ \operatorname{SRS}_n(p,q)&=-\operatorname{rem}(\operatorname{SRS}_{n-2}(p,q),\operatorname{SRS}_{n-1}(p,q))\neq 0,\\ \operatorname{SRS}_{n+1}(p,q)&=-\operatorname{rem}(\operatorname{SRS}_{n-1}(p,q),\operatorname{SRS}_n(p,q))=0.\end{aligned}$$

Moreover, we set $\operatorname{SRS}(p,0)=(p,0)$.

Signed remainder sequences of the form $\operatorname{SRS}(p,p')$ will be used to count the number of roots of p inside a given open interval.

In the following statements and proofs, for given polynomials p and q with $q\neq 0$, we set $r=\operatorname{rem}(p,q)$. Moreover, we denote by $\sigma(x)$ the sign of pq at x. We use the convention that $\operatorname{sign}((pq)(-\infty))=\operatorname{sign}(\operatorname{lm}(pq)(-1))$ and $\operatorname{sign}((pq)(\infty))=\operatorname{sign}(\operatorname{lm}(pq)(1))$.

[10] In other words, $\operatorname{SRS}(p,q)$ is the sequence of remainders in Euclidean division of p by q where in each step the negative is taken.

Lemma 4.1.34. *Let $(R,<)$ be a real closed field, let $p,q \in R[X]$ with $q \neq 0$ and let $a,b \in R \cup \{-\infty,\infty\}$ such that $a<b$ and a,b are not roots of any polynomial in $\mathrm{SRS}(p,q)$. Then the following hold:*

(i)

$$\mathrm{Var}(\mathrm{SRS}(p,q);a,b) = \begin{cases} \mathrm{Var}(\mathrm{SRS}(q,-r);a,b)+\sigma(b) & \text{if } \sigma(a)\sigma(b)=-1, \\ \mathrm{Var}(\mathrm{SRS}(q,-r);a,b) & \text{if } \sigma(a)\sigma(b)=1. \end{cases}$$

(ii)

$$\mathrm{CInd}(\tfrac{q}{p};a,b) = \begin{cases} \mathrm{CInd}(\tfrac{-r}{p};a,b)+\sigma(b) & \text{if } \sigma(a)\sigma(b)=-1, \\ \mathrm{CInd}(\tfrac{-r}{p};a,b) & \text{if } \sigma(a)\sigma(b)=1. \end{cases}$$

Proof. (i) Recall that

$$\begin{aligned} \mathrm{SRS}_0(p,q) &= p, \\ \mathrm{SRS}_1(p,q) &= q, \\ \mathrm{SRS}_2(p,q) &= -r. \end{aligned}$$

Suppose that $\sigma(a)\sigma(b)=-1$. Then $p(a)q(a)$ and $p(b)q(b)$ have opposite signs. If the sign of $p(a)q(a)$ is positive, then $\sigma(b)=-1$ and

$$\mathrm{Var}(\mathrm{SRS}(p,q);a)-\mathrm{Var}(\mathrm{SRS}(p,q);b) = \mathrm{Var}(\mathrm{SRS}(q,-r);a)-(\mathrm{Var}(\mathrm{SRS}(q,-r);b)+1).$$

Otherwise, $\sigma(b)=1$ and

$$\mathrm{Var}(\mathrm{SRS}(p,q);a)-\mathrm{Var}(\mathrm{SRS}(p,q);b) = (\mathrm{Var}(\mathrm{SRS}(q,-r);a)+1)-\mathrm{Var}(\mathrm{SRS}(q,-r);b).$$

Now suppose that $\sigma(a)\sigma(b)=1$. Then $p(a)q(a)$ and $p(b)q(b)$ have the same sign and either

$$\mathrm{Var}(\mathrm{SRS}(p,q);a)-\mathrm{Var}(\mathrm{SRS}(p,q);b) = (\mathrm{Var}(\mathrm{SRS}(q,-r);a)+1)-(\mathrm{Var}(\mathrm{SRS}(q,-r);b)+1)$$

or

$$\mathrm{Var}(\mathrm{SRS}(p,q);a)-\mathrm{Var}(\mathrm{SRS}(p,q);b) = \mathrm{Var}(\mathrm{SRS}(q,-r);a)-(\mathrm{Var}(\mathrm{SRS}(q,-r);b).$$

(ii) Without loss of generality, we may assume that p and q are coprime. Otherwise, we can replace p by $\frac{p}{d}$ and q by $\frac{q}{d}$, where d is the monic greatest common divisor of p and q. Indeed, we have $\mathrm{rem}(\frac{p}{d},\frac{q}{d})=\frac{r}{d}$,

$$\mathrm{CInd}(\tfrac{q}{p};a,b)=\mathrm{CInd}(\tfrac{q/d}{p/d};a,b), \mathrm{CInd}(\tfrac{-r}{p};a,b)=\mathrm{CInd}(\tfrac{-r/d}{p/d};a,b),$$

and the sign of $\frac{pq}{d^2}$ concides with that of pq at any point that is not a root of pq.

We let n_+ be the total number of sign changes from negative to positive of pq on $(a,b)_R$. Likewise, n_- denotes the total number of sign changes from positive to negative of pq on $(a,b)_R$. Then

$$n_+ - n_- = \begin{cases} \sigma(b) & \text{if } \sigma(a)\sigma(b)=-1, \\ 0 & \text{if } \sigma(a)\sigma(b)=1. \end{cases}$$

Let $c \in (a,b)_R$ be a root of p (and thus not a root of q by coprimality). Then pq changes its sign from negative to positive at c if and only if $\frac{q}{p} = \frac{pq}{p^2}$ jumps from $-\infty$ to ∞ at c. Since we obtain a similar correspondence for roots of q, we obtain

$$\mathrm{CInd}(\tfrac{q}{p}; a, b) + \mathrm{CInd}(\tfrac{p}{q}; a, b) = n_+ + n_-.$$

Now for $g \in R[X]$ with $p = gq + r$, we obtain

$$\mathrm{CInd}(\tfrac{-r}{q}; a, b) = -\mathrm{CInd}(\tfrac{r}{q}; a, b) = -\mathrm{CInd}(\tfrac{p-gq}{q}; a, b) = -\mathrm{CInd}(\tfrac{p}{q}; a, b).$$

Hence,

$$\begin{aligned}\mathrm{CInd}(\tfrac{q}{p}; a, b) &= n_+ + n_- - \mathrm{CInd}(\tfrac{p}{q}; a, b)\\ &= \mathrm{CInd}(\tfrac{-r}{q}; a, b) + n_+ + n_-\\ &= \begin{cases}\mathrm{CInd}(\tfrac{-r}{p}; a, b) + \sigma(b) & \text{if } \sigma(a)\sigma(b) = -1,\\ \mathrm{CInd}(\tfrac{-r}{p}; a, b) & \text{if } \sigma(a)\sigma(b) = 1.\end{cases}\end{aligned}$$

□

Proposition 4.1.35. *Let $(R, <)$ be a real closed field, let $p, q \in R[X]$ with $p \neq 0$ and let $a, b \in R \cup \{-\infty, \infty\}$ with $a < b$ such that a, b are not roots of p. Then*

$$\mathrm{Var}(\mathrm{SRS}(p,q); a, b) = \mathrm{CInd}(\tfrac{q}{p}; a, b).$$

Proof. Let $\underline{s} = (s_0, \ldots, s_n) = \mathrm{SRS}(p,q)$ and let $g_j \in R[X]$ with

$$s_{j-1} = g_j s_j - s_{j+1}$$

for any $j \in \{1, \ldots, n\}$. We may assume that a and b are not roots of any polynomial in $\underline{s}$: If they are, we may replace them by a', b', respectively, with $a < a' < b' < b$ such that $(a, a']_R$ and $[b', b)_R$ contain no root of the polynomials in $\underline{s}$. For these a', b' we have

$$\mathrm{CInd}(\tfrac{q}{p}; a, b) = \mathrm{CInd}(\tfrac{q}{p}; a', b').$$

We also show that

$$\mathrm{Var}(\underline{s}; a, b) = \mathrm{Var}(\underline{s}; a', b').$$

Assume, for a contradiction, that for some $j \in \{1, \ldots, n\}$ we have that a is a root of both s_j and s_{j+1}. Then a is also be a root of s_{j-1}. Taking j least with this property, we thus obtain that a is a root of $s_0 = p$, contradicting our assumption on p. Suppose that a is a root of s_j for some $j \in \{1, \ldots, n\}$. Then it is not a root of s_{j-1} and not a root of s_{j+1}. Since

$$s_{j-1}(a) = g_j(a)s_j(a) - s_{j+1}(a) = -s_{j+1}(a),$$

we obtain $s_{j-1}(a)s_{j+1}(a) < 0$. Since

$$\mathrm{sign}(s_{j-1}(a)) = \mathrm{sign}(s_{j-1}(a')), \mathrm{sign}(s_{j+1}(a)) = \mathrm{sign}(s_{j+1}(a')) \text{ and } s_j(a') \neq 0,$$

we obtain

$$1 = \mathrm{Var}(s_{j-1}, s_j, s_{j+1}; a) = \mathrm{Var}(s_{j-1}, s_j, s_{j+1}; a').$$

Hence, switching from a to a' does not change the number of sign variations of $\underline{s}$, i.e.

$$\mathrm{Var}(\underline{s}; a) = \mathrm{Var}(\underline{s}; a').$$

A similar argument shows that $\mathrm{Var}(\underline{s}; b) = \mathrm{Var}(\underline{s}; b')$, establishing our claim.

The proof of $\mathrm{Var}(\underline{s}; a, b) = \mathrm{CInd}(\frac{q}{p}; a, b)$ follows by induction on n. First suppose that $n = 1$. Then $r = \mathrm{rem}(p, q) = 0$ and we obtain

$$\mathrm{Var}(\mathrm{SRS}(q, -r); a, b) = \mathrm{Var}(q, 0; a, b) = 0 \text{ and } \mathrm{CInd}(\tfrac{-r}{q}; a, b) = \mathrm{CInd}(0; a, b) = 0.$$

Now Lemma 4.1.34 implies $\mathrm{Var}(p, q; a, b) = \mathrm{CInd}(\frac{q}{p}; a, b)$.

Now suppose that for some $n \in \mathbb{N}$ with $n \geq 2$, the conclusion holds for all signed remainder sequences with exactly n elements. Note that

$$\mathrm{SRS}(q, -r) = (s_1, \ldots, s_n).$$

Hence,

$$\mathrm{Var}(\mathrm{SRS}(q, -r); a, b) = \mathrm{CInd}(\tfrac{-r}{q}; a, b).$$

The conclusion now follows immediately from Lemma 4.1.34. □

We are now ready to prove the main theorems of this section.

Theorem 4.1.36 (Tarski's Theorem)**.** *Let $(R, <)$ be a real closed field, let $p, q \in R[X]$ with $p \neq 0$ and let $a, b \in R \cup \{-\infty, \infty\}$ with $a < b$ such that a, b are not roots of p. Then*

$$\mathrm{Var}(\mathrm{SRS}(p, p'q); a, b) = \mathrm{TaQ}(q, p; a, b).$$

Proof. Proposition 4.1.35 implies

$$\mathrm{Var}(\mathrm{SRS}(p, p'q); a, b) = \mathrm{CInd}(\tfrac{p'q}{p}; a, b),$$

and Proposition 4.1.30 already shows

$$\mathrm{TaQ}(q, p; a, b) = \mathrm{CInd}(\tfrac{p'q}{p}; a, b).$$

□

Theorem 4.1.37 (Sturm's Theorem)**.** *Let $(R, <)$ be a real closed field, let $p \in R[X]$ with $p \neq 0$ and let $a, b \in R \cup \{-\infty, \infty\}$ with $a < b$ such that a, b are not roots of p. Then the number of distinct roots of p in $(a, b)_R$ is given by*

$$\mathrm{Var}(\mathrm{SRS}(p, p'); a, b).$$

In particular, the number of distinct roots of p in R is

$$\mathrm{Var}(\mathrm{SRS}(p, p')).$$

Proof. It suffices to set $q = 1$ in Theorem 4.1.36. □

Due to Sturm's Theorem, the sequence $\mathrm{SRS}(p, p')$ is also called a **Sturm sequence**. Sturm sequences can thus be used to determine the number of roots of a given polynomial within a certain inverval of a real closed field.

Theorem 4.1.38. *Let $(K, <)$ be an ordered field and let R_1 and R_2 be real closures of K such that*

$$(K, <) \subseteq (R_1, <) \text{ and } (K, <) \subseteq (R_2, <).$$

Then there exists a unique $\mathcal{L}_{\mathrm{or}}$-isomorphism $\varphi\colon (R_1, <) \cong (R_2, <)$ such that $\varphi|_K = \mathrm{id}_K$.

Proof. We first show uniqueness by demonstrating that each element of R_1 can only be mapped to one specific element of R_2. Let $\varphi\colon (R_1, <) \cong (R_2, <)$ such that $\varphi|_K = \mathrm{id}_K$ and let $\alpha \in R_1$. Let $m_\alpha \in K[X]$ be the minimal polynomial of α over K. By Theorem 4.1.37, the number k of distinct roots of m_α in R_1 is identical with the number of distinct roots of m_α in R_2. Indeed, both are equal to $\mathrm{Var}(\mathrm{SRS}(m_\alpha, m'_\alpha))$. Let $\alpha_1, \ldots, \alpha_k \in R_1$ and $\beta_1, \ldots, \beta_k \in R_2$ be those roots of m_α with $\alpha_1 < \ldots < \alpha_k$ and $\beta_1 < \ldots < \beta_k$. Since $\varphi\colon R_1 \cong R_2$, it must map roots of m_α in R_1 to roots of m_α in R_2. To preserve the order, φ must satisfy $\varphi(\alpha_i) = \beta_i$ for any $i \in \{1, \ldots, n\}$. Hence, if $\alpha = \alpha_j$ for some $j \in \{1, \ldots, n\}$, then $\varphi(\alpha) = \beta_j$.

We now verify the existence of an $\mathcal{L}_{\mathrm{or}}$-isomorphism $\varphi\colon (R_1, <) \cong (R_2, <)$ with $\varphi|_K = \mathrm{id}_K$. Let

$$\mathcal{C} = \{\iota\colon (F, <) \hookrightarrow (R_2, <) \mid (K, <) \subseteq (F, <) \subseteq (R_1, <) \text{ and } \iota|_K = \mathrm{id}_K\}.$$

Note that the identity id_K is contained in $\mathcal{C}$. Moreover, the union of any chain in $\mathcal{C}$ (with respect to set inclusion, where we identify each function with its graph) is again contained in $\mathcal{C}$. Hence, by Zorn's Lemma, there exists a maximal $\iota \in \mathcal{C}$ with domain F. To establish existence of the desired φ, we have to show that ι is surjective and $F = R_1$. Assume not. Set $L = \iota(F) \subseteq R_2$. Then ι is an $\mathcal{L}_{\mathrm{or}}$-isomorphism from $(F, <)$ to $(L, <)$. Let $\alpha \in R_1$ and let $\gamma \in R_2$ such that not both $\alpha \in F$ and $\gamma \in L$ (which is possible by our assumption). As described above, there is a unique element $\delta \in R_1$ such that an $\mathcal{L}_{\mathrm{or}}$-isomorphism from $(R_1, <)$ to $(R_2, <)$ fixing K must map δ to γ. Let $\theta \in R_1$ such that

$$F \subsetneq F(\alpha, \delta) \subseteq F(\theta) \subseteq R_1.$$

We show that ι can be extended to an $\mathcal{L}_{\mathrm{or}}$-embedding

$$\iota'\colon (F(\theta), <) \hookrightarrow (R_2, <),$$

contradicting the maximality of ι. Since

$$\iota\colon (F, <) \cong (L, <),$$

we may identify $(F, <)$ and $(L, <)$ with each other and treat ι is the identity function $\iota = \mathrm{id}_F$. (By this identification, $(F, <) \subseteq (R_2, <)$.)

Let $m_\theta \in F[X]$ be the minimal polynomial of θ over F and let $\sigma \in R_2$ be the uniquely determined root of m_θ in R_2 to which any $\mathcal{L}_{\mathrm{or}}$-isomorphism from R_1 to R_2 needs to map θ (as

described above). For some $r \in \mathbb{N}$, let $\psi_1, \dots, \psi_r$ be all possible $\mathcal{L}_{\mathrm{r}}$-isomorphisms from $F(\theta)$ to $F(\sigma)$. Assume, for a contradiction, that none of them is an $\mathcal{L}_{\mathrm{or}}$-isomorphism. Then there are positive $b_1, \dots, b_r \in F(\theta)$ such that all of $\psi_1(b_1), \dots, \psi_r(b_r) \in F(\sigma)$ are negative. Consider

$$M = F(\theta)(\sqrt{b_1}, \dots, \sqrt{b_r}) \subseteq R_1.$$

Let $\xi \in R_1$ be a primitive element such that $M = F(\theta)(\xi)$. As before, there is some $\xi' \in R_2$ such that there exists

$$\psi \colon F(\theta)(\xi) \cong F(\sigma)(\xi')$$

with $\psi(F(\theta)) = F(\sigma)$. Then $\psi|_{F(\theta)}$ must be one of $\psi_1, \dots, \psi_r$, say ψ_1. But then

$$0 > \psi_1(b_1) = \psi\Big((\sqrt{b_1})^2\Big) = \psi(\sqrt{b_1})^2 > 0,$$

a contradiction. Hence, ψ_1 is the desired extension of ι contradicting the maximality of ι in $\mathcal{C}$. □

4.2. Quantifier Elimination

In this section, we prove that the $\mathcal{L}_{\mathrm{or}}$-theory of real closed fields T_{rcf} admits quantifier elimination. While there are several non-constructive proofs for this fact using certain model theoretic criteria for a theory to admit quantifier elimination, we, instead, present an explicit procedure to transform any $\mathcal{L}_{\mathrm{or}}$-formula into an equivalent quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula. We thus establish the following:

Theorem 4.2.1. *The $\mathcal{L}_{\mathrm{or}}$-theory T_{rcf} admits quantifier eliminiation, i.e. for any $\mathcal{L}_{\mathrm{or}}$-formula $\varphi(\underline{x})$, there is a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula $\psi(\underline{x})$ such that*

$$T_{\mathrm{rcf}} \models \forall \underline{x}\ (\varphi(\underline{x}) \leftrightarrow \psi(\underline{x})).$$

Several model theoretic properties will be deduced from Theorem 4.2.1 in Subsection 4.2.2.

4.2.1. Algorithm

In this section, we present several transformation procedures. Generally, each of these procedures describes a way to transform a given $\mathcal{L}_{\mathrm{or}}$-formula φ of a specific shape into an $\mathcal{L}_{\mathrm{or}}$-formula ψ that is equivalent over T_{rcf} to φ. The most important step, in which a single existential quantifier is eliminated, utilises Tarski's Theorem (Theorem 4.1.36).

Recursion on $\mathcal{L}_{\mathrm{or}}$-formulas

Let φ and φ' be $\mathcal{L}_{\mathrm{or}}$-formulas and let ψ and ψ' be quantifier-free $\mathcal{L}_{\mathrm{or}}$-formulas that are equivalent over T_{rcf} to φ and φ', respectively. Then over T_{rcf}

- $\neg\varphi$ is equivalent to $\neg\psi$.
- $\varphi \vee \varphi'$ is equivalent to $\psi \vee \psi'$.

- $\varphi \wedge \varphi'$ is equivalent to $\psi \wedge \psi'$.
- $\varphi \to \varphi'$ is equivalent to $\psi \to \psi'$.
- $\varphi \leftrightarrow \varphi'$ is equivalent to $\psi \leftrightarrow \psi'$.
- $\exists x\ \varphi$ is equivalent to $\exists x\ \psi$ for any variable x.

Only in the last transformation, we still have an $\mathcal{L}_{\mathrm{or}}$-formula with a single existential quantifier. It thus remains to describe a procedure to find for a given $\mathcal{L}_{\mathrm{or}}$-formula of the form $\exists x\ \psi$, where ψ is quantifier-free, an equivalent quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula.

Example 4.2.2. Over T_{rcf}, the $\mathcal{L}_{\mathrm{or}}$-formula $\exists y\ xy = 1$ is equivalent to $x \neq 0$ and the $\mathcal{L}_{\mathrm{or}}$-formula $\forall z\ z^2 \geq 0$ is equivalent to $0 = 0$. Hence,

$$\begin{gathered}\neg\forall z\ z^2 \geq 0 \text{ is equivalent to } \neg\ 0 = 0,\\ \exists y\ xy = 1 \wedge \forall z\ z^2 \geq 0 \text{ is equivalent to } x \neq 0 \wedge 0 = 0, \text{ and}\\ \exists x \exists y\ xy = 1 \text{ is equivalent to } \exists x\ x \neq 0.\end{gathered}$$

In the last case, it remains to transform $\exists x\ x \neq 0$ into an equivalent quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula.

Disjunctive Normal Form

Let φ be a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula and let x be a variable. By application of De Morgan's Law on $\neg$, $\vee$ and $\wedge$ as well as the distributivity of $\vee$ and $\wedge$, we can transform φ into an equivalent $\mathcal{L}_{\mathrm{or}}$-formula of the form

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{n} \varphi_{ij}, \tag{4.2.1}$$

where $n \in \mathbb{N}$ and each φ_{ij} is an atomic $\mathcal{L}_{\mathrm{or}}$-formula or the negation of an atomic $\mathcal{L}_{\mathrm{or}}$-formula. The $\mathcal{L}_{\mathrm{or}}$-formula (4.2.1) is called a **disjunctive normal form** of φ. Since the tools needed for this transformation all give us logical equivalences, φ is even equivalent to an $\mathcal{L}_{\mathrm{or}}$-formula of the form (4.2.1) over any $\mathcal{L}_{\mathrm{or}}$-theory, not only over T_{rcf}.

By this procedure, $\exists x\ \varphi$ is equivalent over T_{rcf} to

$$\bigvee_{i=1}^{n} \exists x \bigwedge_{j=1}^{n} \varphi_{ij}.$$

It thus remains to transform each

$$\exists x \bigwedge_{j=1}^{n} \varphi_{ij}$$

into an equivalent quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula ψ_i, as then

$$\bigvee_{i=1}^{n} \exists x \bigwedge_{j=1}^{n} \varphi_{ij} \text{ is equivalent to } \bigvee_{i=1}^{n} \psi_i$$

over T_{rcf}.

Example 4.2.3. Consider the quantifier-free $\mathcal{L}_{\text{or}}$-formula φ given by

$$x \geq 0 \wedge \neg(y < 0 \to y + z = 1).$$

We first transform this into a quantifier-free formula only using $\neg$, $\vee$ and $\wedge$ as logical connectives:

$$(0 < x \vee x = 0) \wedge \neg(\neg\, y < 0 \vee y + z = 1).$$

Using De Morgan's Laws, we transform this formula into

$$(0 < x \vee x = 0) \wedge (y < 0 \wedge \neg\, y + z = 1).$$

Lastly, we apply distributivity of $\vee$ and $\wedge$:

$$(0 < x \wedge (y < 0 \wedge \neg\, y + z = 1)) \vee (x = 0 \wedge (y < 0 \wedge \neg\, y + z = 1)).$$

This formula is already in disjunctive normal form, as it would be found in the literature. However, to obtain the form (4.2.1), we artificially have to add "false sentences" to obtain the following equivalent $\mathcal{L}_{\text{or}}$-formula:[11]

$$\begin{aligned}(0 < x \wedge y < 0 \wedge \neg\, y + z = 1) \vee (x = 0 \wedge y < 0 \wedge \neg\, y + z = 1)\\ \vee (1 = 0 \wedge 1 = 0 \wedge 1 = 0).\end{aligned}$$

The $\mathcal{L}_{\text{or}}$-formula

$$\exists x\ [x \geq 0 \wedge \neg(y < 0 \to y + z = 1)]$$

is thus equivalent to

$$\begin{aligned}\exists x\ (0 < x \wedge y < 0 \wedge \neg\, y + z = 1) \vee \exists x\ (x = 0 \wedge y < 0 \wedge \neg\, y + z = 1)\\ \vee \exists x\ (1 = 0 \wedge 1 = 0 \wedge 1 = 0).\end{aligned}$$

Polynomial Equalities and Inequalities

Let $n \in \mathbb{N}$ and let $\varphi_i = \varphi_i(x, \underline{y})$ be either an atomic $\mathcal{L}_{\text{or}}$-formula or a negation of one for each $i \in \{1, \ldots, n\}$. We transform

$$\bigwedge_{i=1}^{n} \varphi_i$$

into an $\mathcal{L}_{\text{or}}$-formula of the form

$$p(x) = 0 \wedge \bigwedge_{j=1}^{m} q_j(x) > 0$$

for some $m \in \mathbb{N}$ and some $p, q_1, \ldots, q_m \in \mathbb{Q}(\underline{y})[X]$. To make sense of the latter, we need the following convention.

[11] Adding true or false sentences is a general tool that can be used to obtain formulas of a prescribed length or form.

Notation 4.2.4. Let s_1, s_2, t_1, t_2 be $\mathcal{L}_{\text{or}}$-terms. Then the expression

$$\frac{s_1}{s_2} = \frac{t_1}{t_2}$$

stands for

$$s_2 \neq 0 \wedge t_2 \neq 0 \wedge s_1 t_2 = t_1 s_2.$$

Moreover, the expression

$$\frac{s_1}{s_2} < \frac{t_1}{t_2}$$

stands for

$$(s_2 t_2 > 0 \wedge s_1 t_2 < t_1 s_2) \vee (s_2 t_2 < 0 \wedge s_1 t_2 > t_1 s_2).$$

By Notation 4.2.4, for any $\mathcal{L}_{\text{or}}$-terms $t_1(\underline{y})$ and $t_2(\underline{y})$ we can identify $\frac{t_1}{t_2}$ with an element of $\mathbb{Q}(\underline{y})$. Naturally, we identify t_1 with $\frac{t_1}{1}$.

For any $\mathcal{L}_{\text{or}}$-terms t, s, we obtain atomic formulas or negations thereof of the form

- $t = s$,
- $t \neq s$,
- $t < s$,
- $t \geq s$.

These are all possible representations of formulas of the form φ_i from above. Each of these formulas can now be transformed into an equivalent one over T_{rcf}:

- $t = s$ is equivalent to $t - s = 0$.
- $t \neq s$ is equivalent to $(t - s)^2 > 0$.
- $t < s$ is equivalent to $s - t > 0$.
- $t \geq s$ is equivalent to $t - s = 0 \vee t - s > 0$.

If the transformation of $t \geq s$ into $t - s = 0 \vee 0 < t - s$ is applied, one has to perform a transformation into the disjunctive normal form once more, as a further disjuction has been added.

We have described how to transform

$$\bigwedge_{i=1}^{n} \varphi_i$$

into an equivalent $\mathcal{L}_{\text{or}}$-formula of the form

$$\bigwedge_{k=1}^{\ell} p_k(x) = 0 \wedge \bigwedge_{j=1}^{m} q_j(x) > 0$$

for some $\ell, m \in \mathbb{N}$ and some $p_k, q_j \in \mathbb{Q}(\underline{y})[X]$. We now set[12]

$$p = p_1^2 + \ldots + p_\ell^2$$

[12]If $\ell = 1$, then one can also simply set $p = p_1$.

to obtain the desired equivalent $\mathcal{L}_{\mathrm{or}}$-formula

$$p(x) = 0 \wedge \bigwedge_{j=1}^{m} q_j(x) > 0.$$

Hence,

$$\exists x \bigwedge_{i=1}^{n} \varphi_i$$

is equivalent over T_{rcf} to

$$\exists x \left(p(x) = 0 \wedge \bigwedge_{j=1}^{m} q_j(x) > 0 \right)$$

and we only need to eliminate the existential quantifier from the latter.

Example 4.2.5. Consider the $\mathcal{L}_{\mathrm{or}}$-formula

$$y^2 \geq x \wedge z = zx - yx - xy.$$

This is equivalent over T_{rcf} to

$$(-x + y^2 = 0 \vee -x + y^2 > 0) \wedge (z - 2y)x - z = 0.$$

Since we added a disjunction, we transform this formula into the equivalent disjunctive normal form

$$(-x + y^2 = 0 \wedge (z - 2y)x - z = 0) \vee (-x + y^2 > 0 \wedge (z - 2y)x - z = 0).$$

Hence,

$$\exists x \ (y^2 \geq x \wedge z = zx - yx - xy)$$

is equivalent over T_{rcf} to

$$\exists x \ [(-x + y^2)^2 + ((z - 2y)x - z)^2 = 0 \wedge 1 > 0] \vee \exists x \ [(z - 2y)x - z = 0 \wedge -x + y^2 > 0],$$

where we added $1 > 0$ in the first clause to obtain the required form.

Reducing Inequalities

Let $m \in \mathbb{N}$ and let $p, q_1, \ldots, q_m \in \mathbb{Q}(\underline{y})[X]$. Consider the $\mathcal{L}_{\mathrm{or}}$-formula φ given by

$$\exists x \left(p(x) = 0 \wedge \bigwedge_{j=1}^{m} q_j(x) > 0 \right).$$

In the transformation procedure we now describe, we technically increase the number of quantifiers. However, this will be done in a way such that the new quantifiers we introduce are eliminated in the next transformation procedure.

Notation 4.2.6. Let $k \in \omega$. Then the quantifier $\exists_k$ stands for "there exist exactly k many". Hence, for a formula $\psi(x)$, the sentence $\exists_k x \ \varphi(x)$ states that there are exactly k many distinct x making the formula $\varphi(x)$ true. (See also Exercise 3.3 for details on how $\exists_k$ can be formalised.)

Let d' be the degree of p. Then φ is equivalent over T_{rcf} to

$$\bigvee_{k=1}^{d'} \exists_k x \left(p(x) = 0 \wedge \bigwedge_{j=1}^{m} q_j(x) > 0 \right),$$

as p can have at most d' distinct roots. Fix $k \in \{1, \ldots, d\}$. We transform

$$\exists_k x \left(p(x) = 0 \wedge \bigwedge_{j=1}^{m} q_j(x) > 0 \right) \tag{4.2.2}$$

into a disjunctive normal form of equivalent $\mathcal{L}_{\mathrm{or}}$-formulas only using one polynomial inequality. We do so inductively, where for the case $m = 1$ we already have the desired form. Suppose that $m \geq 2$ and consider

$$\exists_k x \ (p(x) = 0 \wedge q_1(x) > 0 \wedge q_2(x) > 0).$$

Note that

(a) $q_1(x)q_2^2(x) > 0$ if and only if $q_1(x) > 0$ and $q_2(x) \neq 0$;

(b) $q_1^2(x)q_2(x) > 0$ if and only if $q_1(x) \neq 0$ and $q_2(x) > 0$;

(c) $q_1^2(x)q_2^2(x) > 0$ if and only if $q_1(x) \neq 0$ and $q_2(x) \neq 0$;

(d) $q_1(x)q_2(x) > 0$ if and only if $q_1(x) > 0 \wedge q_2(x) > 0$ or $q_1(x) < 0 \wedge q_2(x) < 0$.

Let a, b, c, d be the number of distinct roots of p satisfying the respective conditions on q_1 and q_2 above. Then the number of distinct roots x of p with $q_1(x) > 0 \wedge q_2(x) > 0$ is given by

$$\frac{a + b - (c - d)}{2}.$$

This counting argument now gives us that

$$\exists_k x \ (p(x) = 0 \wedge q_1(x) > 0 \wedge q_2(x) > 0)$$

is equivalent over T_{rcf} to

$$\bigvee_{\substack{a,b,c,d \in \{0,\ldots,d'\} \\ a+b-(c-d)=2k}} [\exists_a x \ (p(x) = 0 \wedge q_1(x)q_2^2(x) > 0) \wedge \exists_b x \ (p(x) = 0 \wedge q_1^2(x)q_2(x) > 0)$$
$$\wedge \exists_c x \ (p(x) = 0 \wedge q_1^2(x)q_2^2(x) > 0)$$
$$\wedge \exists_d x \ (p(x) = 0 \wedge q_1(x)q_2(x) > 0)].$$

Hence, the $\mathcal{L}_{\mathrm{or}}$-formula (4.2.2) is equivalent over T_{rcf} to

$$\bigvee_{\substack{a,b,c,d \in \{0,\ldots,d'\} \\ a+b-(c-d)=2k}} [\exists_a x \ (p(x) = 0 \wedge q_1(x)q_2^2(x) > 0 \wedge q_3(x) > 0 \ldots \wedge q_m(x) > 0)$$
$$\wedge \exists_b x \ (p(x) = 0 \wedge q_1^2(x)q_2(x) > 0 \wedge q_3(x) > 0 \ldots \wedge q_m(x) > 0)$$
$$\wedge \exists_c x \ (p(x) = 0 \wedge q_1^2(x)q_2^2(x) > 0 \wedge q_3(x) > 0 \ldots \wedge q_m(x) > 0)$$
$$\wedge \exists_d x \ (p(x) = 0 \wedge q_1(x)q_2(x) > 0 \wedge q_3(x) > 0 \ldots \wedge q_m(x) > 0)].$$

In each clause, the number of inequalities has reduced to $m-1$. We can thus repeat the procedure to obtain an equivalent $\mathcal{L}_{\text{or}}$-formula of the form

$$\bigvee_{i=1}^{M} \bigwedge_{j=1}^{M} \exists_{k_{ij}} x \ (p(x) = 0 \wedge Q_{ij}(x) > 0)$$

for some $M \in \mathbb{N}$, $k_{ij} \in \omega$ and $Q_{ij} \in \mathbb{Q}(\underline{y})[X]$. It remains to eliminate the quantifier $\exists_{k_{ij}}$ in each formula

$$\exists_{k_{ij}} x \ (p(x) = 0 \wedge Q_{ij}(x) > 0).$$

Example 4.2.7. Consider the $\mathcal{L}_{\text{or}}$-formula

$$\exists x \ (x^2 + y = 0 \wedge x - y > 0 \wedge xz > 0).$$

This is equivalent to

$$\exists_1 x \ (x^2 + y = 0 \wedge x - y > 0 \wedge xz > 0) \vee \exists_2 x \ (x^2 + y = 0 \wedge x - y > 0 \wedge xz > 0).$$

We now perform the reduction procedure for multiple inequalities to the second clause

$$\exists_2 x \ (x^2 + y = 0 \wedge x - y > 0 \wedge xz > 0)$$

to obtain

$$\begin{aligned} \bigvee_{\substack{a,b,c,d \in \{0,1,2\} \\ a+b-(c-d)=4}} [&\exists_a x \ (x^2 + y = 0 \wedge (x-y)(xz)^2 > 0) \\ &\wedge \exists_b x \ (x^2 + y = 0 \wedge (x-y)^2 xz > 0) \\ &\wedge \exists_c x \ (x^2 + y = 0 \wedge (x-y)^2 (xz)^2 > 0) \\ &\wedge \exists_d x \ (x^2 + y = 0 \wedge (x-y) xz > 0)]. \end{aligned}$$

Tarski's Theorem

Consider the $\mathcal{L}_{\text{or}}$-formula

$$\exists_k x \ (p(x) = 0 \wedge q(x) > 0)$$

for some $k \in \omega$, and $p, q \in \mathbb{Q}(\underline{y})[x]$. We transform this $\mathcal{L}_{\text{or}}$-formula into an equivalent quantifier-free $\mathcal{L}_{\text{or}}$-formula. Recall that by Theorem 4.1.36, we have

$$\text{Var}(\text{SRS}(p, p'q)) = \text{TaQ}(q, p) = \sum_{x \in p^{-1}(0)} \text{sign}(q(x)).$$

Recall that $\text{TaQ}(q, p)$ is the number of distinct roots of p at which q is positive minus the distinct roots of p at which q is negative. Hence, $\text{TaQ}(q^2, p)$ is the number of distinct roots of p at which q is non-zero. We obtain that p has exactly k distinct roots at which q is positive if and only if

$$\frac{\text{TaQ}(q, p) + \text{TaQ}(q^2, p)}{2} = k.$$

Hence, the $\mathcal{L}_{\mathrm{or}}$-formula

$$\exists_k x\ (p(x) = 0 \wedge q(x) > 0)$$

is equivalent over T_{rcf} to

$$\bigvee_{\ell=0}^{2k} (\mathrm{TaQ}(q,p) = \ell \wedge \mathrm{TaQ}(q^2,p) = 2k - \ell).$$

We now describe how $\mathrm{TaQ}(q,p) = \ell$ can be expressed as a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula for any $\ell \in \{0,\dots,2k\}$. Similarly, $\mathrm{TaQ}(q^2,p) = 2k-\ell$ can be expressed as a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula.

Let $\ell \in \{0,\dots,2k\}$ be fixed. By Tarski's Theorem, $\mathrm{TaQ}(q,p) = \ell$ describes that

$$\mathrm{Var}(\mathrm{SRS}(p,p'q)) = \ell.$$

We thus have to express by an $\mathcal{L}_{\mathrm{or}}$-formula that the signed remainder sequence $\mathrm{SRS}(p,p'q)$ has exactly ℓ many sign variations. Set $s = p'q$. Since $p, s \in \mathbb{Q}(\underline{y})[X]$, the signed remainder sequence of p and s can be computed over $\mathbb{Q}(\underline{y})[X]$. However, since we possible need to divide coefficients within $\mathbb{Q}(\underline{y})$, in each step we need to make sure that no division by 0 is happening. In other words, if the degree of ps is given by d, then there may be up to d different signed remainder sequences to consider.

Example 4.2.8. Consider $p(X) = yX^2 + 1$ and $q(X) = (y+1)X + 1$. Then

$$p'(X)q(X) = 2y(y+1)X^2 + 2yX.$$

Let $\underline{s} = \mathrm{SRS}(p,p'q)$. We make a case distinction on the coefficients of the polynomials by which we divide. For later use, we give the polynomials in the signed remainder sequence superscripts referring to the cases.

(i) Suppose that $y \neq 0$, $y+1 \neq 0$ and $y^2+3y+1 \neq 0$. Then

$$\begin{aligned} s_0^{(1)} &= yX^2 + 1 \\ s_1^{(1)} &= 2y(y+1)X^2 + 2yX \\ s_2^{(1)} &= \frac{y}{y+1}X - 1 \\ s_3^{(1)} &= -\frac{2(y+1)(y^2+3y+1)}{y} \\ s_4^{(1)} &= 0. \end{aligned}$$

(ii) Suppose that $y \neq 0$, $y+1 \neq 0$ and $y^2+3y+1 = 0$. Then

$$\begin{aligned} s_0^{(2)} &= yX^2 + 1 \\ s_1^{(2)} &= 2y(y+1)X^2 + 2yX \\ s_2^{(2)} &= \frac{y}{y+1}X - 1 \\ s_3^{(2)} &= 0. \end{aligned}$$

(iii) Suppose that $y \neq 0$ and $y+1=0$. Then

$$\begin{aligned} s_0^{(3)} &= yX^2+1 \\ s_1^{(3)} &= 2yX \\ s_2^{(3)} &= -1 \\ s_3^{(3)} &= 0. \end{aligned}$$

(iv) Suppose that $y = 0$. Then

$$\begin{aligned} s_0^{(4)} &= 1 \\ s_1^{(4)} &= 0. \end{aligned}$$

In order to express that $\mathrm{SRS}(p, p'q)$ has exactly ℓ many sign variations, we may use a disjunction of the form

$$\bigvee_{j=1}^{m} (\rho_j(\underline{y}) \wedge \mathrm{Var}(\mathrm{SRS}(p,p'q)) = \ell),$$

where $m \in \mathbb{N}$ and each $\rho_j(\underline{y})$ is a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula only depending on the variables $\underline{y}$ that determines which of the coefficients in the signed remainder sequence are non-zero. Of course, $\mathrm{Var}(\mathrm{SRS}(p,p'q)) = \ell$ is not yet an $\mathcal{L}_{\mathrm{or}}$-formula. However, once the conditions on the coefficients of the signed remainder sequence are determined by $\rho_j(\underline{y})$, the signed remainder sequence can be calculated explicitly. It remains to replace $\mathrm{Var}(\mathrm{SRS}(p,p'q)) = \ell$ by all possible sign combinations of the leading monomials evaluated at -1 and all possible sign combinations of the leading monomials evaluated at 1 giving a difference of exactly ℓ sign variations in the former compared to the latter. We illustrate this by continuing Example 4.2.8

Example 4.2.9. Let p and q (and all other notations) be as in Example 4.2.8, i.e. $p(X) = yX^2+1$ and $q(X) = (y+1)X+1$. We illustrate how to express $\mathrm{Var}(\mathrm{SRS}(p,p'q)) = 2$ as an $\mathcal{L}_{\mathrm{or}}$-formula. In each clause, we simply express all combinations asserting that

$$\mathrm{Var}(\mathrm{SRS}(p,p'q);-\infty) - \mathrm{Var}(\mathrm{SRS}(p,p'q);\infty) = 2.$$

$$\begin{aligned} &[y \neq 0 \wedge y+1 \neq 0 \wedge y^2+3y+1 \neq 0 \wedge \varphi_1(\underline{y})] \\ \vee&[y \neq 0 \wedge y+1 \neq 0 \wedge y^2+3y+1 = 0 \wedge \varphi_2(\underline{y})] \\ \vee&[y \neq 0 \wedge y+1 = 0 \wedge \varphi_3(\underline{y})] \\ \vee&[y = 0 \wedge \varphi_4(\underline{y})] \end{aligned}$$

As an example, we only present all possible combination of sign variations that are expressed by $\varphi_1(\underline{y})$. To ease the notation, we let $t_i = \mathrm{lm}(s_i^{(1)})(-1)$ and $r_i = \mathrm{lm}(s_i^{(1)})(1)$ for $i \in \{0,1,2,3\}$. Now $\varphi_1(\underline{y})$ is given by

$$(\mathrm{Var}(t_0,t_1,t_2,t_3) = 3 \wedge \mathrm{Var}(r_0,r_1,r_2,r_3) = 1) \vee (\mathrm{Var}(t_0,t_1,t_2,t_3) = 2 \wedge \mathrm{Var}(r_0,r_1,r_2,r_3) = 0)$$

As a final illustration, we also express $\mathrm{Var}(t_0, t_1, t_2, t_3) = 2$ explicitly as:

$$\begin{aligned}&(t_0 > 0 \wedge t_1 < 0 \wedge t_2 > 0 \wedge t_3 \geq 0) \vee (t_0 < 0 \wedge t_1 > 0 \wedge t_2 < 0 \wedge t_3 \leq 0)\\ \vee&(t_0 > 0 \wedge t_1 < 0 \wedge t_2 \leq 0 \wedge t_3 > 0) \vee (t_0 < 0 \wedge t_1 > 0 \wedge t_2 \geq 0 \wedge t_3 < 0)\\ \vee&(t_0 \geq 0 \wedge t_1 > 0 \wedge t_2 < 0 \wedge t_3 > 0) \vee (t_0 \leq 0 \wedge t_1 < 0 \wedge t_2 > 0 \wedge t_3 < 0)\\ \vee&(t_0 > 0 \wedge t_1 \geq 0 \wedge t_2 < 0 \wedge t_3 > 0) \vee (t_0 < 0 \wedge t_1 \leq 0 \wedge t_2 > 0 \wedge t_3 < 0).\end{aligned}$$

Single Inequality

During the quantifier elimination procedure, it may happen that one obtains formulas of the form

$$\exists x\ (0 = 0 \wedge q(x) > 0).$$

for some $q \in \mathbb{Q}(\underline{y})[X]$. In this case we have $p = 0$, and Tarski's Theorem as well as the general way of counting roots via signed remainder sequences is not applicable. However, here we can perform the following procedure.

We have to transform $\exists x\ q(x) > 0$ into a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula equivalent over T_{rcf}. If $q \in \mathbb{Q}(\underline{y})$ (i.e. $\deg(q) = 0$ or $q = 0$), then this quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula is already given by

$$q(x) > 0.$$

Otherwise, express q as $q = \sum_{i=0}^{\ell} a_i X^i$ with $a_0, \ldots, a_\ell \in \mathbb{Q}(\underline{y})$. We obtain that $\exists x\ q(x) > 0$ is equivalent over T_{rcf} to

$$\bigvee_{i=0}^{\ell}\left(a_i \neq 0 \wedge \left[q\left(\sum_{j=0}^{\ell}\left|\frac{a_j}{a_i}\right| + 1\right) > 0 \vee q\left(-\sum_{j=0}^{\ell}\left|\frac{a_j}{a_i}\right| - 1\right) > 0\right]\right) \vee \exists x\ (q'(x) = 0 \wedge q(x) > 0).$$

The first part of this formula is quantifier-free and simply expresses that evaluating q in some suitable large point, it becomes positive (see Exercise 4.1.20). The reason for the disjunction $\bigvee_{i=0}^{\ell}$ is that all possible leading coefficients have to be considered.

Suppose that q does not become positive outside some interval I containing all roots of q. If q becomes positive in some point $a \in I$, then there must also be a point b with $q'(b) = 0$ and $q(b) > 0$. Indeed, q must have two roots $c, d \in I$ with $c < a < d$ and no further root strictly between c and d. Moreover, q is positive between c and d. Now since $q(c) = 0 = q(d)$ by Rolle's Theorem for real closed fields (see [1, Proposition 2.22]), we obtain that there must also be some b with $c < b < d$ and $q'(b) = 0$.

It remains to note that the quantifier in

$$\exists x\ (q'(x) = 0 \wedge q(x) > 0)$$

can be eliminated by the procedures previously described.

In order to eliminate an existential quantifier from a formula of the form

$$\exists x\ (q_1(x) > 0 \wedge q_2(x) > 0)$$

for some non-constant $q_1, q_2 \in \mathbb{Q}(\underline{y})[X]$, note that this is equivalent over T_{rcf} to

$$\exists x\ (\varphi_1 \wedge q_2(x) > 0) \vee \exists x\ (\varphi_2 \wedge q_1(x) > 0)$$

with φ_k (for $k \in \{1,2\}$) of the form

$$\bigvee_{i=0}^{\ell}\left(a_i \neq 0 \wedge \left[q_k\left(\sum_{j=0}^{\ell}\left|\frac{a_j}{a_i}\right|+1\right)>0 \vee q_k\left(-\sum_{j=0}^{\ell}\left|\frac{a_j}{a_i}\right|-1\right)>0\right]\right) \vee (q_k'(x)=0 \wedge q_k(x)>0),$$

(where the a_j are the coefficients of q_k as above). For further inequalities, simply proceed inductively.

4.2.2. Implications

We now deduce some powerful properties of T_{rcf} from Theorem 4.2.1.

Theorem 4.2.10. *The theory T_{rcf} is complete.*

Proof. Let σ be an $\mathcal{L}_{\mathrm{or}}$-sentence. Then by Theorem 4.2.1, there is a quantifier-free $\mathcal{L}_{\mathrm{or}}$-sentence ρ such that

$$T_{\mathrm{rcf}} \models \sigma \leftrightarrow \rho.$$

However, the quantifier-free $\mathcal{L}_{\mathrm{or}}$-sentence simply consists of a combination of atomic $\mathcal{L}_{\mathrm{or}}$-formulas without free variables. More specifically, as shown in Subsection 4.2.1, ρ is equivalent to

$$\bigvee_{i=1}^{\ell}\left(\bigwedge_{j=1}^{\ell} p_{ij}=0 \wedge \bigwedge_{j=1}^{\ell} q_{ij}>0\right)$$

for some $\ell \in \mathbb{N}$ and $p_{ij}, q_{ij} \in \mathbb{Z}$. Whether $p_{ij}=0$, respectively $q_{ij}>0$, holds is independent of the specific choice of a model of T_{rcf}. Hence, either ρ holds for all real closed fields or $\neg\rho$ holds for all real closed fields. Hence, we obtain

$$T_{\mathrm{rcf}} \models \sigma \text{ or } T_{\mathrm{rcf}} \models \neg\sigma.$$

□

Theorem 4.2.11. *The theory T_{rcf} is decidable, i.e. there exists an algorithm that, for any given $\mathcal{L}_{\mathrm{or}}$-sentence ρ, decides (after a finite processing time) whether ρ is true ($T_{\mathrm{rcf}} \models \rho$) or false ($T_{\mathrm{rcf}} \models \neg\rho$) over T_{rcf}.*

Proof. The decision algorithm was presented in Subsection 4.2.1: For a given $\mathcal{L}_{\mathrm{or}}$-sentence ρ, our quantifier elimination algorithm transforms ρ into a quantifier-free $\mathcal{L}_{\mathrm{or}}$-sentence. As explained before, this is simply a combination of numerical equalities and inequalities. Whether these are true or false can be determined by direct calculation. □

Definition 4.2.12. Let $(M,<) \models T_{\mathrm{lo}}$, let $\mathcal{L}$ be an expansion of $\mathcal{L}_<$ and let $\mathcal{M}$ be an $\mathcal{L}$-expansion of $(M,<)$. Then $\mathcal{M}$ is called **o-minimal** if every $\mathcal{L}$-definable subset of M is a finite union of points and open intervals in M, i.e. for any $\mathcal{L}$-definable set $A \subseteq M$, there exist $n,m \in \omega$, $a_1,\ldots,a_n,b_1,\ldots,b_n \in M \cup \{-\infty,\infty\}$ with $a_i < b_i$ for any $i \in \{1,\ldots,n\}$ and $c_1,\ldots,c_m \in M$ such that

$$A = \bigcup_{i=1}^{n}(a_i,b_i)_M \cup \{c_1,\ldots,c_m\}.$$

Theorem 4.2.13. *Let $(R, <)$ be a real closed field. Then $(R, <)$ is o-minimal.*

Proof. Let $A \subseteq R$ be $\mathcal{L}_{\text{or}}$-definable. Then by Theorem 4.2.1, there exists a quantifier-free $\mathcal{L}_{\text{or}}$-formula $\varphi(x, \underline{y})$ such that

$$A = \varphi((R, <), \underline{b})$$

for some $\underline{b} \in R$. Now $\varphi(x, \underline{b})$ is simply a boolean combination of polynomial equations and inequations with coefficients in $\mathbb{Z}[\underline{b}] \subseteq R$. For any $p(X) \in R[X]$, the solution set of $p(X) = 0$ and $p(X) > 0$ is either empty, a finite set of points or a finite union of open intervals. Since the class of finite unions of points and open intervals is closed under boolean operations, we obtain the required result. □

5. Shepherdson's Theorem

In this section, we prove the first main result of this lecture, which is due to [9]. We always abbreviate $\mathcal{L}_{\mathrm{PA}}$-structures $\mathcal{M}$ simply by $(M,<)$ and $\mathcal{L}_{\mathrm{or}}$-structures $\mathcal{Z}$ simply by $(Z,<)$. The ordering should always be clear from the context.

5.1. Rings and Semirings

5.1.1. Open Induction for Rings

Notation 5.1.1. Recall from Exercise 4.3 the following notations.

(i) Let $(M,<) \models \mathrm{PA}^-$. Then

$$Z_M := M \cup (-M) := M \cup \{-m \mid m \in M \setminus \{0\}\}$$

can be equipped with operations and an order relation such that $(M,<) \subseteq (Z_M,<)$. Moreover, $(Z_M,<)$ is a discretely ordered ring.

(ii) Let $(Z,<) \models T_{\mathrm{dor}}$. Then

$$M_Z := Z^{\geq 0}$$

inherits its operations and its order relation from $(Z,<)$ such that $(M_Z,<) \subseteq (Z,<)$. Moreover, $(M_Z,<)$ is a discretely ordered semiring.

Notation 5.1.1 gives us a way to switch between discretely ordered rings and discretely ordered semirings. In fact, it was shown in Exercise 4.3 that there is a one-to-one correspondence between these two classes of structures by the identification above. Also axiomatisations of arithmetic have counterparts for discretely ordered *rings*. We introduce such a counterpart for open induction.

Definition 5.1.2. The $\mathcal{L}_{\mathrm{or}}$-theory IOpen' of **open induction (for rings)** is axiomatised by the extension of T_{dor} by the induction scheme restricted to quantifier-free $\mathcal{L}_{\mathrm{or}}$-formulas:

for any quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula $\varphi(x,\underline{y})$,

$$\forall \underline{y}\ [(\varphi(0,\underline{y}) \wedge \forall(n \geq 0)\ [\varphi(n,\underline{y}) \to (\varphi(n+1,\underline{y}) \wedge \varphi(-n,\underline{y}))]) \to \forall n\ \varphi(n,\underline{y})].$$

It is now an easy but somewhat tedious exercise that IOpen and IOpen' axiomatise the corresponding classes of rings and semirings, i.e. the following.

Exercise 5.1.3. Let $(M,<) \models \mathrm{PA}^-$ and let $(Z,<) \models T_{\mathrm{dor}}$. Show that:

(i) $(M,<) \models \mathrm{IOpen}$ if and only if $(Z_M,<) \models \mathrm{IOpen}'$.

(ii) $(Z,<) \models \mathrm{IOpen}'$ if and only if $(M_Z,<) \models \mathrm{IOpen}$.

5.1.2. Integer Parts

Definition 5.1.4. Let $(K, <)$ be an ordered field and let $(Z, <) \subseteq (K, <)$. Then Z is called an **integer part** of K if it is a discretely ordered ring such that for any $a \in K$ there exists $z \in Z$ such that

$$z \leq a < z + 1.$$

The element z is then called the[13] **integer part** of a and denoted by $\lfloor a \rfloor$.

Example 5.1.5. Let $(K, <) \subseteq (\mathbb{R}, <)$. Since $(\mathbb{Z}, <)$ is the only integer part of $\mathbb{R}$, it is also the only integer part of $(K, <)$.

As the integer part of an ordered field takes the same role as $\mathbb{Z}$ in $\mathbb{R}$, one is often interested in the elements that can be written as a fraction of two elements in the integer part.

Notation 5.1.6. Let $(Z, <)$ be a discretely ordered ring. We denote by Q_Z the field of fractions

$$\mathrm{ff}(Z) = \left\{ \frac{a}{b} \;\middle|\; a \in Z, b \in Z \setminus \{0\} \right\}$$

of Z.

Remark 5.1.7. If Z is the integer part of some ordered field $(K, <)$, then Q_Z inherits an ordering from K making $(Q_Z, <)$ an ordered field. In fact, also for any discretely ordered ring $(Z, <)$, we can endow Q_Z with an ordering $<$ making it an ordered field with $(Z, <) \subseteq (Q_Z, <)$ by setting

$$\frac{a}{b} > 0$$

if and only if $ab > 0$ for any $a, b \in Z$ with $b \neq 0$.

Exercise 5.1.8. Prove, or disprove by providing a counterexample, the following statement: *For any $(Z, <) \models T_{\mathrm{dor}}$, we have that Z is an integer part of $(Q_Z, <)$.*

Exercise 5.1.9. Let $(K, <)$ be an ordered field and let Z be an integer part of $(K, <)$. Moreover, let $m, n \in \omega$, let $a_1, \ldots, a_n, b_1, \ldots, b_n \in K \cup \{-\infty, \infty\}$ with $a_1 < b_1 < a_2 < b_2 < \ldots < a_n < b_n$ and let $c_1, \ldots, c_m \in K$ with $c_1 < \ldots < c_m$. Suppose that A is given by the disjoint union

$$A = \bigsqcup_{i=1}^{n} (a_i, b_i)_K \sqcup \bigsqcup_{j=1}^{m} \{c_j\}.$$

Show that there are $k \in \omega$ and $s_1, \ldots, s_k, t_1, \ldots, t_k, r \in Z$ with $s_i \leq t_i$ for any $i \in \{1, \ldots, k\}$ such that $A' = A \cap Z$ is of the form

$$A' = \bigsqcup_{i=1}^{k} [s_i, t_i]_Z \sqcup I,$$

where I is one of $\emptyset$, $(-\infty, r]_Z$, $[r, \infty)_Z$ and Z.

[13] Its uniqueness is proved in Exercise 7.3 (a).

5.2. Statement and Proof

Theorem 5.2.1 (Shepherdson)**.** *Let $(Z,<) \models T_{\mathrm{dor}}$. Then the following are equivalent:*

(i) $(Z,<) \models \mathrm{IOpen}'$.

(ii) Z is an integer part of the real closure of $(Q_Z,<)$.

Proof. We denote by $(R,<)$ the real closure of $(Q_Z,<)$. Let us first suppose that $(Z,<) \models \mathrm{IOpen}'$. Let $a \in R$. We need to find $z \in Z$ such that $z \leq a < z+1$. If $a \in Z$, then $z = a$ will do. Suppose that $a \in (0,\infty)_R \setminus Z$. Since R is algebraic over Q_Z, there exists a non-zero polynomial $p \in Q_Z[X]$ such that $p(a) = 0$. Let $k \in \mathbb{N}$ such that a is the k-th positive root of p in R. By clearing fractions, i.e. multiplying with a sufficiently large element from Z, we may assume that all coefficients of p lie in Z, i.e. $p \in Z[X]$. Let $d = \deg(p)$ and let $\varphi(x,\underline{b})$ be the $\mathcal{L}_{\mathrm{or}}$-formula (with parameters $\underline{b} \in Z$) given by

$$\bigvee_{j=k}^{d} \exists_j y \ (0 < y < x \wedge p(y) = 0).$$

Note that $\varphi(x,\underline{b})$ expresses that there are at least k many distinct positive roots of p strictly below x. By Theorem 4.2.1, there exists a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula ψ such that

$$(R,<) \models \forall x \ (\varphi(x,\underline{b}) \leftrightarrow \psi(x,\underline{b})).$$

For any $c \in (-\infty,0]_R$, we have

$$(R,<) \models \neg\varphi(c,\underline{b})$$

and hence

$$(R,<) \models \neg\psi(c,\underline{b}).$$

Since $(Z,<) \subseteq (R,<)$, we obtain by Lemma 2.4.6 that

$$(Z,<) \models \neg\psi(-n,\underline{b}).$$

for any $n \in M_Z$. Hence,

$$(Z,<) \models \neg\psi(0,\underline{b}) \wedge \forall(n \geq 0) \ [\neg\psi(n,\underline{b}) \rightarrow \neg\psi(-n,\underline{b})].$$

Assume, for a contradiction, that

$$(Z,<) \models \forall(n \geq 0) \ [\neg\psi(n,\underline{b}) \rightarrow \neg\psi(n+1,\underline{b})].$$

Since $(Z,<) \models \mathrm{IOpen}'$, we obtain

$$(Z,<) \models \forall n \ \neg\psi(n,\underline{b}).$$

Again, by Lemma 2.4.6, we obtain that for any $n \in M_Z$ we have

$$(R,<) \models \neg\psi(n,\underline{b})$$

and thus

$$(R, <) \models \neg\varphi(n, \underline{b}).$$

We now express $p \in Z[X]$ as

$$p(X) = \sum_{\ell=0}^{d} a_\ell X^\ell.$$

Set

$$B = B(p) = \sum_{\ell=0}^{d} \left| \frac{a_\ell}{a_d} \right| + 1$$

and recall that by Exercise 4.1.20, all positive roots of p in R must lie in $[0, B)_R$. Since $|a_d|B \in M_Z$, we obtain

$$(R, <) \models \neg\varphi(|a_d|B, \underline{b}).$$

Hence, it is not true that there are there are at least k many distinct positive roots of p strictly below $|a_d|B$. This shows that $a \geq |a_d|B$. However, $|a_d|B \geq B$ and thus $a \in R$ is a positive root of p in R outside the interval $[0, B)_R$, a contradiction.

Hence, there is some $z \in M_Z$ such that

$$(Z, <) \models \neg\psi(z, \underline{b}) \wedge \psi(z + 1, \underline{b}).$$

By Lemma 2.4.6, we obtain

$$(R, <) \models \neg\psi(z, \underline{b}) \wedge \psi(z + 1, \underline{b})$$

and thus

$$(R, <) \models \neg\varphi(z, \underline{b}) \wedge \varphi(z + 1, \underline{b}).$$

Hence, there are there are at most $k - 1$ many distinct roots of p in $(0, z)_R$ and at least k many distinct roots of p in $(0, z + 1)_R$. This shows that the k-th positive root of p in R must lie in the interval $[z, z + 1)_R$, i.e. $z \leq a < z + 1$, as required. For the case $x \in (-\infty, 0)_R \setminus Z$, it remains to note that $\lfloor x \rfloor = -\lfloor -x \rfloor - 1$.

Conversely, suppose that Z is an integer part of $(R, <)$. Since $(Z, <) \models T_{\mathrm{dor}}$, we only have to verify the induction scheme for quantifier-free $\mathcal{L}_{\mathrm{or}}$-formulas. Let $\varphi(x, \underline{y})$ be a quantifier-free $\mathcal{L}_{\mathrm{or}}$-formula and let $\underline{b} \in Z$. Suppose that

$$(Z, <) \models \varphi(0, \underline{b}) \wedge \forall(n \geq 0)\ [\varphi(n, \underline{b}) \to (\varphi(n + 1, \underline{y}) \wedge \varphi(-n, \underline{b}))]. \tag{5.2.1}$$

We have to show that for any $n \in Z$ we have

$$(Z, <) \models \varphi(n, \underline{b}).$$

Assume, for a contradiction, that there exists $n \in Z$ with $(Z, <) \models \neg\varphi(n, \underline{b})$. We may assume that $n \geq 0$, as otherwise we can replace it by $-n$, since

$$(Z, <) \models \forall(n \leq 0)\ [\neg\varphi(n, \underline{b}) \to \neg\varphi(-n, \underline{b})].$$

Lemma 2.4.6 yields that also

$$(R, <) \models \neg\varphi(n, \underline{b}).$$

Let

$$A = \neg\varphi((R,<),\underline{b}) \cap [0,\infty)_R.$$

Since $n \in A$, we have that A is non-empty. By Theorem 4.2.13, the $\mathcal{L}_{\mathrm{or}}$-definable set A is a non-empty finite union of open intervals and singeltons in R. Consider $B = A \cap Z$. By Exercise 5.1.9, there are $k \in \omega$ and $c_1, \ldots, c_k, d_1, \ldots, d_k, s \in M_Z$ with $c_i \leq d_i$ for any $i \in \{1, \ldots, k\}$ such that B is of the form

$$B = \bigsqcup_{i=1}^{k} [c_i, d_i]_Z \sqcup I,$$

where I is either $\emptyset$ or $[s,\infty)_Z$. Set $c = \min\{c_1, \ldots, c_k\}$ if $k \geq 1$ and $c = s$ if $k = 0$. Then c is the least element of B. Since $(Z,<) \models \varphi(0,\underline{b})$, we have $0 \notin B$. Hence, $c \geq 1$. But then $c - 1 \notin B$ and $c \in B$. This shows that

$$(Z,<) \models \varphi(c-1,\underline{b}) \wedge \neg\varphi(c,\underline{b}),$$

contradicting (5.2.1). □

By Exercise 5.1.3, we immediately obtain the following characterisation of models of open induction.

Corollary 5.2.2. *Let $(M,<) \models \mathrm{PA}^-$. Then the following are equivalent:*

(i) $(M,<) \models \mathrm{IOpen}$.

(ii) Z_M *is an integer part of the real closure of* $(Q_{Z_M},<)$.

Exercise 5.2.3. Let $(Z,<) \models T_{\mathrm{dor}}$. Show that the following are equivalent:

(i) $(Z,<) \models \mathrm{IOpen}'$.

(ii) Z is an integer part of some real closed field $(R,<)$.

6. Hahn Fields

In this chapter, we introduce the class of Hahn fields, which will be used in the proof of our second main result: the Mourgues–Ressayre Theorem.

6.1. Generalised Power Series

6.1.1. Well-Orderings and Ordinals

In this brief excursion, we cover the basics of well-orderings. Since this is only a brief introduction, several basic results on well-orderings and ordinal numbers are left as exercises.

Definition 6.1.1. Let $(I, <) \models T_{\text{lo}}$. A subset $J \subseteq I$ is **well-ordered** if every non-empty subset of J contains a least element. We call $(I, <)$ a **well-ordering** (or also simply well-ordered) if I is well-ordered.

For later use, we introduce the following notation.

Notation 6.1.2. Let $(I, <) \models T_{\text{lo}}$. We denote by $\text{wo}(I)$ the family of all well-ordered subsets of I.

Exercise 6.1.3. Let Let $(I, <) \models T_{\text{lo}}$ and let $J \subseteq I$. Show that J is well-ordered if and only if it contains no infinite strictly decreasing sequence, i.e. for any sequence $(a_i)_{i\in\omega}$ in J it is not possible that $a_0 > a_1 > a_2 > \ldots$.

Exercise 6.1.4. Let $(I, <)$ be a well-ordering and let $f\colon (I, <) \to (I, <)$.

(i) Show that for any $i \in I$ we have $f(i) \geq i$.

(ii) Suppose that $f\colon (I, <) \cong (I, <)$. Show that $f = \text{id}_I$.

(iii) Let $(J, <)$ be an $\mathcal{L}_<$-structure with $(I, <) \cong (J, <)$. Show that there is a unique $\mathcal{L}_<$-isomorphism from I to J.

Remark 6.1.5. Recall that J is an initial segment of some linearly ordered set I if for any $j \in J$, we have $(-\infty, j]_I \subseteq J$. We say that J is a proper initial segment of I if additionally $J \neq I$.

Proposition 6.1.6. *Let $(I, <)$ be a well-ordering and let J be a proper initial segment of I. Then for some $a \in I$, we have*

$$J = I^{<a} := \{i \in I \mid i < a\}.$$

Proof. Since $J \subsetneq I$, we can set $a = \min(I \setminus J)$. Now let $i \in I$. If $i < a$, then $i \notin I \setminus J$, whence $i \in J$. Conversely, if $i \geq a$, then $(-\infty, i]_I$ is not contained in J, as $a \in (-\infty, i]_I$. Hence, $i \notin J$. □

Proposition 6.1.7. *Let $(I,<)$ and $(J,<)$ be well-orderings. Then exactly one of the following holds:*

(i) $(I,<) \cong (J,<)$.

(ii) $(I,<) \cong (J^{<j},<)$ *for some* $j \in J$.

(iii) $(I^{<i},<) \cong (J,<)$ *for some* $i \in I$.

Proof. Assume, for a contradiction, that the three cases were not exclusive. Then there exists a well-ordering $(X,<)$ and some $f\colon (X,<) \cong (X^{<x},<)$ for some $x \in X$, i.e. $(X,<)$ is isomorphic to a proper initial segment of itself. Now $f(x) < x$, and by iterative application of f we obtain

$$x > f(x) > f(f(x)) > \dots,$$

contradicting Exercise 6.1.3.

First suppose that for any $a \in I$, there is some $f_a\colon (I^{<a},<) \cong (J^{<a'},<)$ for some $a' \in J$. By Exercise 6.1.4, each f_a is unique. Hence,

$$f_a|_{(-\infty,b]_I} = f_b$$

for any $a, b \in I$ with $b < a$. Taking

$$f = \bigcup_{a \in I} f_a$$

(considering functions as the corresponding sets of their graphs), we obtain that f is an embedding of $(I,<)$ into $(J,<)$ whose image

$$\bigcup_{a \in I} J^{<a'}$$

is an initial segment of J. Hence, we obtain $(I,<) \cong (J,<)$ or $(I,<) \cong (J^{<j},<)$ for some $j \in J$.

Now suppose that there is some $i \in I$ such that $(I^{<i},<)$ is not $\mathcal{L}_<$-isomorphic to $(J^{<b},<)$ for any $b \in J$. We may take i to be least with that property. However, then for any $c \in I^{<i}$, there is some $g_c\colon (I^{<c},<) \cong (J^{<i'},<)$ for some $i' \in J$. As shown above, this implies that $(I^{<i},<)$ is $\mathcal{L}_<$-isomorphic to some initial segment of J. By assumption, we obtain $(I^{<i},<) \cong (J,<)$. □

Taking $\cong$ as equivalence relation, Proposition 6.1.7 gives rise to a linear ordering on the class of equivalence classes as follows.

Definition 6.1.8. Let $(I,<)$ and $(J,<)$ be well-orderings. We denote by $[I]$ its equivalence class under $\cong$ (i.e. $\mathcal{L}_<$-isomorphisms). Moreover, we write

$$[I] < [J]$$

if $(I,<) \cong (J^{<j},<)$ for some $j \in J$.

Exercise 6.1.9. Show that $<$ from Definition 6.1.8 defines a strict linear ordering on the class of equivalence classes of well-orderings, i.e. for any well-orderings $(I,<)$, $(J,<)$, $(L,<)$, verify the following:

(i) $[I] \not< [I]$;

(ii) if $[I] < [J]$ and $[J] < [L]$, then $[I] < [L]$;

(iii) $[I] < [J]$ or $[I] = [J]$ or $[J] < [I]$.

We now establish a canonical representative for each equivalence class of well-orderings. These representatives will be called ordinal numbers. For these particular well-orderings, the binary relation $<$ coincides with the element relation $\in$.

Example 6.1.10. Set $0 = \emptyset$ and define iteratively for any $n \in \omega$:

$$n + 1 := n \cup \{n\}.$$

Then for any $n \in \omega$, the $\mathcal{L}_<$-structure $(n, \in)$ is a well-ordering.[14] For instance:

$$\begin{aligned}
0 &= \emptyset, \\
1 &= 0 \cup \{0\} = \{0\} = \{\emptyset\}, \\
2 &= 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \\
3 &= 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\
&\vdots \\
n + 1 &= n \cup \{n\} = \{0, \ldots, n\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots\}.
\end{aligned}$$

The set of all well-orderings obtained in this way is called ω, which is also the reason for the notation we use for the natural numbers with 0.

Definition 6.1.11. A well-ordering $(x, <)$ is called an **ordinal (number)** if for any $a \in x$ we have

$$x^{<a} = a.$$

The class of all ordinal numbers is denoted by **On**.

Exercise 6.1.12. Let $(x, <)$ be an ordinal number. Show that the binary relation $<$ on x coincides with the binary relation $\in$ on x.
We will thus always set $<$ to be $\in$ in the context of ordinals.

Example 6.1.13. All well-orderings in Example 6.1.10 are ordinal numbers. For instance, consider 3. Then $2 \in 3$ and

$$3^{<2} = \{0, 1\} = 2.$$

An example of an infinite ordinal larger than ω is $\omega + 1 = \omega \cup \{\omega\}$. In fact, the class of ordinals have no upper bound and for each cardinality there is a least ordinal of the cardinality. For instance, ω is the least ordinal of cardinality $\aleph_0$.

[14] In the special case $(0, \in)$ we technically have no well-ordering since the domain is the empty set. However, allowing this domain, all properties of a well-ordering are vacuously true.

Remark 6.1.14. Several results on ordinals require the fact that for any set A there is no infinite chain $A \ni a_0 \ni a_1 \ni \ldots$. This is usually one of the axioms of set theory (more precisely, of Zermelo–Fraenkel set theory) and we may thus use this fact without any further justification.

Exercise 6.1.15. Let $\alpha, \beta \in \mathbf{On}$. Show that $\alpha \in \beta$ if and only if $\alpha \subsetneq \beta$.

Exercise 6.1.16. Let $A \subseteq \mathbf{On}$ be a set of ordinal numbers. Show that

$$\bigcap_{\alpha \in A} \alpha \in \mathbf{On} \text{ and } \bigcup_{\alpha \in A} \alpha \in \mathbf{On}.$$

Exercise 6.1.17. Show that $(\mathbf{On}, <)$ (where $<$ is given by $\in$) is a well-ordering, i.e. for any $\alpha, \beta, \gamma \in \mathbf{On}$, verify the following:

(i) $\alpha \not< \alpha$;

(ii) if $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$;

(iii) $\alpha < \beta$ or $\alpha = \beta$ or $\beta < \alpha$;

and show that every non-empty subset of $\mathbf{On}$ has a least element.

Definition 6.1.18. Let $\alpha \in \mathbf{On}$ with $0 < \alpha$. Then α is called a **successor ordinal** if

$$\alpha = \beta + 1 := \beta \cup \{\beta\}$$

for some $\beta \in \mathbf{On}$. Otherwise, it is called a **limit ordinal**.

Exercise 6.1.19. Show that the only limit ordinal in $\omega + 1$ is ω.

We now establish that the previously established class of equivalence classes of well-orderings is $\mathcal{L}_<$-isomorphic to $\mathbf{On}$. More precisely, any equivalence class has a unique representative in $\mathbf{On}$ and the ordering $<$ on equivalence classes coincides with $\in$ on $\mathbf{On}$ via this representation.

Proposition 6.1.20. *Let $(I, <)$ and $(J, <)$ be well-orderings. Then there are unique $\alpha, \beta \in \mathbf{On}$ with*

$$(\alpha, <) \in [I] \text{ and } (\beta, <) \in [J].$$

Moreover, $[I] < [J]$ if and only if $\alpha < \beta$.

Proof. We first prove the existence of α (and likewise the existence of β can be proved). By Proposition 6.1.7, there are three cases to consider.

Case 1: For some $\gamma \in \mathbf{On}$, we have $(I, <) \cong (\gamma, <)$. Then we only have to set $\alpha = \gamma$.

Case 2: For some $\gamma \in \mathbf{On}$ and some $\alpha \in \gamma$, we have $(I, <) \cong (\gamma^{<\alpha}, <)$. Then we simply have to note that $\gamma^{<\alpha} = \alpha$.

Case 3: For any $\gamma \in \mathbf{On}$ there is some $i(\gamma) \in I$ such that $(I^{<i(\gamma)}, <) \cong (\gamma, <)$. First note that for any $\gamma, \gamma' \in \mathbf{On}$ with $\gamma < \gamma'$, we have $i(\gamma) < i(\gamma')$, as otherwise we would obtain a contradiction to Exercise 6.1.4. Hence, $i^{-1}(I) = \mathbf{On}$ is a set (rather than a proper class). This implies that

$$\alpha = \bigcup_{\alpha \in \mathbf{On}} \alpha \in \mathbf{On}.$$

But then $\mathbf{On} \leq \alpha \in \mathbf{On}$, a contradiction.

For uniqueness, let $\alpha, \alpha' \in [I] \cap \mathbf{On}$. If $\alpha < \alpha'$ or $\alpha' < \alpha$, then $(I, <)$ is isomorphic to a proper initial segment of itself, which was shown not to be possible in Proposition 6.1.7. Hence, $\alpha = \alpha'$.

Now suppose that $[I] < [J]$. Then $(I, <)$ is isomorphic to a proper initial segment of $(J, <)$ and thus α is a proper initial segment of β. Hence, also $\alpha < \beta$. The converse follows likewise by using the properties of linear orderings. □

Proposition 6.1.20 gives rise to the following.

Definition 6.1.21. Let $(I, <)$ be a well-ordering. Then the **order type** $\mathrm{ot}(I, <)$ (or simply $\mathrm{ot}(I)$) of $(I, <)$ is the unique ordinal $\alpha \in \mathbf{On}$ with $\alpha \in [I]$.

Lastly, we identify the subclass of cardinal numbers amongst all ordinal numbers.

Remark 6.1.22. Let A be a set. Then the **cardinality** $|A|$ of A is the $\mathcal{L}_=$-equivalence class of (A) (see Exercise 3.3). More precisely, two sets A and B have the same cardinality if there exists a bijection from A to B. We write $|A| \leq |B|$ ("the cardinality of A is at most the cardinality of "B") if there exists an injective map from A to B. The Principle of Cardinal Comparability, which is equivalent to the Axiom of Choice, asserts that for any two sets either $|A| \leq |B|$ or $|B| \leq |A|$ and, if both hold, then $|A| = |B|$.

Theorem 6.1.23 (Well-ordering Theorem)**.** *Let A be a set. Then there exists a linear ordering $<$ on A such that $(A, <)$ is a well-ordering.*

Proof. Let $\mathcal{C}$ be the set of all well-orderings on subsets of A. Formally, for any set $B \subseteq A$, we have that $\mathcal{C}$ contains all subsets of B^2 representing the graph of a binary relation on B that is a well-ordering. Note that $\mathcal{C}$ is non-empty, as any finite subset of A can be well-ordered. We define an ordering $<_C$ on $\mathcal{C}$ by setting $R <_C R'$ if $R \subseteq R'$ and the domain B of R is a proper initial segment of (B', R'), where B' is the domain of R'.

Now let $(R_i)_{i \in I}$ be a chain in C, i.e. $(I, <)$ is a linear ordering and $R_i \in C$ for any $i \in I$ such that $R_i <_C R_{i'}$ for any $i, i' \in I$ with $i < i'$. Set

$$R = \bigcup_{i \in I} R_i.$$

Then the domain of R is

$$R = \bigcup_{i \in I} B_i,$$

where B_i is the domain of R_i for each $i \in I$. One can easily verify that R is a linear ordering on B. Let $A \subseteq B$ be non-empty. Let $j \in I$ with $A \cap B_j \neq \emptyset$ and set $a = \min(A \cap B_j)$ (with respect to the ordering R_j). We show that a is the minimal element of A: If not, then there is some $i \in I$ such that $A \cap B_i$ contains an element b smaller than a. However, if B_i is a proper initial segment of B_j (i.e. $i < j$), then $b \in B_j$, and if B_j is a proper initial segment of B_i (i.e. $j < i$), then also $b \in B_j$, both being contradictions. Hence, (B, R) is a well-ordering and thus contained in $\mathcal{C}$.

By Zorn's Lemma, there exists a maximal element $(B, R) \in \mathcal{C}$. If $B \neq A$, then let $a \in A \setminus B$. We extend R to R_a by setting $b \, R_a \, a$ for any $b \in B$. Then B is an initial segment of $(B \cup \{a\}, R_a)$ and R_a extends R. Hence, $(B \cup \{a\}, R_a) \in \mathcal{C}$, contradicting the maximality of (B, R). We thus obtain that $(A, R) \in \mathcal{C}$ for some well-ordering R on A. □

Remark 6.1.24. Let A be a set. By Theorem 6.1.23 and Proposition 6.1.20, there is some well-ordering R on A and some ordinal $\alpha \in \mathbf{On}$ such that $(A, R) \cong (\alpha, <)$. In particular, A and α have the same cardinality. We associate to each set A the smallest ordinal of the same cardinality. Hence, for each equivalence class of sets representing a cardinality, there is an associated ordinal number, which is then called the corresponding cardinal number.

For instance, the sets $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ all have cardinality $\aleph_0$. The smallest ordinal of cardinality $\aleph_0$ is ω. We thus identify ω with $\aleph_0$.

Since the class of cardinal numbers forms a subclass of **On**, any set can be indexed by a unique ordinal number, i.e. for any set A, there exists (a least) $\alpha \in \mathbf{On}$ (its cardinality) such that A can be expressed as

$$A = \{x_\iota \mid \iota < \alpha\}.$$

We conclude this excursion by presenting a powerful tool that can be applied to any set by the discussion above.

Proposition 6.1.25 (Transfinite Induction)**.** *Let $P(x)$ be a property that is formulated for any $x \in \mathbf{On}$ such that for any $\alpha \in \mathbf{On}$*

$$\textit{if } P(\iota) \textit{ holds for any } \iota < \alpha, \textit{ then also } P(\alpha) \textit{ holds.}$$

Then $P(\alpha)$ holds for any $\alpha \in \mathbf{On}$.

Proof. Assume that there is some $\beta \in \mathbf{On}$ such that $P(\beta)$ does not hold. Since **On** is well-ordered, we may take β least with that property. Then for any $\iota \in \beta$, we have that $P(\iota)$ holds. However, by assumption, this already implies that $P(\beta)$ holds. □

6.1.2. Definitions

Throughout the rest of this section, we denote $\mathcal{L}_{\mathrm{r}}$-structures of fields $(k, +, -, \cdot, 0, 1)$ simply by k and $\mathcal{L}_{\mathrm{og}}$-structures of ordered abelian groups $(G, +, -, 0, <)$ simply by G.

Definition 6.1.26. Let k be a field and let G be an ordered abelian group. For any $s \colon G \to k$, we set the **support** $\operatorname{supp}(s)$ to be

$$\operatorname{supp}(s) = \{g \in G \mid s(g) \neq 0\}.$$

Moreover, we let

$$k(\!(G)\!) = \{s \colon k \to G \mid \operatorname{supp}(s) \in \operatorname{wo}(G)\}.$$

An element $s \in k(\!(G)\!)$ is called a **(generalised) power series** or **Hahn series** (over k and G). We denote it by

$$s = \sum_{g \in G} s_g t^g,$$

where $s_g = s(g)$ for any $g \in G$ and t^g may represent the indicator function mapping g to 1 and everything else to 0.

Notation 6.1.27. Let k be a field and let G be an ordered abelian group. For any $s \in k(\!(G)\!)$, we denote by $\mathrm{ot}(s)$ the order type of the support of s, i.e. $\mathrm{ot}(s) := \mathrm{ot}(\mathrm{supp}(s)) \in \mathbf{On}$. We may thus also express s as

$$s = \sum_{\alpha<\gamma} s_\alpha t^{g_\alpha},$$

where $\gamma = \mathrm{ot}(s)$, for some enumeration $\{g_\alpha \mid \alpha < \gamma\}$ of $\mathrm{supp}(s)$. We call this notation of s the **order type notation**.

Example 6.1.28. For any field k, any polynomial $p \in k[t]$ can be considered as an element in $k(\!(\mathbb{Z})\!)$. For instance, the polynomial

$$p(t) = t^3 + 2t - 3$$

can be written as power series

$$\sum_{z\in\mathbb{Z}} p_z t^z$$

with $p_z = 0$ for any $z \in \mathbb{Z} \setminus \{0, 1, 3\}$ and $p_3 = 1$, $p_1 = 2$ and $p_0 = -3$.

In order type notation, we obtain

$$p = \sum_{\alpha<3} p_\alpha t^{z_\alpha}$$

with $(z_0, p_0) = (0, -3)$, $(z_1, p_1) = (1, 2)$ and $(z_2, p_2) = (3, 1)$.

Definition 6.1.29. Let k be a field and let G be an ordered abelian group. Moreover, let $s, r \in k(\!(G)\!)$. Then we define the following operations:

(i)
$$r + s = \sum_{g\in G} (r_g + s_g) t^g.$$

(ii)
$$r \cdot s = \sum_{g\in G} \left(\sum_{h\in G} r_h s_{g-h} \right) t^g.$$

In the next section, we will verify that $+$ and $\cdot$ as defined above make $k(\!(G)\!)$ a field.

6.2. Rayner Fields

6.2.1. Field Properties

In this section, we follow the main arguments of [5].

Definition 6.2.1. Let k be a field, let G be an ordered abelian group and let $\mathcal{F} \subseteq \mathrm{wo}(G)$. Then we call

$$k(\!(\mathcal{F})\!) = \{s \in k(\!(G)\!) \mid \mathrm{supp}(s) \in \mathcal{F}\}$$

the k**-hull** of $\mathcal{F}$. If $\mathcal{F} = \mathrm{wo}(A)$ for some $A \subseteq G$, we also simply write

$$k(\!(A)\!)$$

for the k-hull of $\mathcal{F}$.

Definition 6.2.2. Let G be an ordered abelian group and let $\mathcal{F} \subseteq \mathrm{wo}(G)$ satisfy the following:

(i) $\mathcal{F} \neq \emptyset$.

(ii) For any $A, B \in \mathcal{F}$, also $A \cup B \in \mathcal{F}$.

(iii) For any $A \in \mathcal{F}$ and any $B \subseteq A$, also $B \in \mathcal{F}$.

(iv) $\bigcup_{A \in \mathcal{F}} A$ generates (as a group) all of G.

(v) For any $g \in G$ and any $A \in \mathcal{F}$ also $A + g := \{a + g \mid a \in A\} \in \mathcal{F}$.

(vi) For any $A \in \mathcal{F}$ with $A \subseteq G^{\geq 0}$, we have

$$\sum A := \left\{ \sum_{i=1}^{n} a_i \;\middle|\; n \in \omega, a_1, \ldots, a_i \in A \right\} \in \mathcal{F}.$$

Then for any field k, we call $k(\!(\mathcal{F})\!)$ a **Rayner field**.

In the following, we verify that any Rayner field is indeed a field.

Lemma 6.2.3. *Let $k(\!(\mathcal{F})\!)$ be a Rayner field. Then it is closed under $+$ as well as $\cdot$ and $(k(\!(\mathcal{F})\!), +, -, \cdot, 0, 1)$ forms ring.*

Proof. Let $a, b \in k(\!(\mathcal{F})\!)$ and let $A, B \in \mathcal{F}$ with $\mathrm{supp}(a) = A$ and $\mathrm{supp}(b) = B$. Then

$$a + b = \sum_{g \in A \cup B} a_g t^g + \sum_{g \in A \cup B} b_g t^g = \sum_{g \in A \cup B} (a_g + b_g) t^g.$$

Hence, $\mathrm{supp}(a + b) \subseteq A \cup B$. By the properties of $\mathcal{F}$, we obtain $\mathrm{supp}(a + b) \in \mathcal{F}$ and thus $a + b \in k(\!(\mathcal{F})\!)$.

Now $k(\!(G)\!)$ is an ordered abelian group (under pointwise addition), whence commutativity and associativity also hold in its substructure $k(\!(\mathcal{F})\!)$. Note further that the additive identity 0 is contained in $k(\!(\mathcal{F})\!)$, as its support $\emptyset$ is contained as a subset in any set in $\mathcal{F}$. Finally, since $\mathrm{supp}(-a) = \mathrm{supp}(a)$, also $-a \in k(\!(\mathcal{F})\!)$. This establishes that $(k(\!(\mathcal{F})\!), +, -, 0)$ is an additive abelian group.

Now consider multiplication. We have

$$ab = \sum_{g \in G} \left(\sum_{\substack{i \in A, j \in B \\ i+j=g}} a_i b_j \right) t^g.$$

Hence, $\mathrm{supp}(ab) \subseteq A + B = \{a + b \mid a \in A, b \in B\}$. It remains to verify $A + B \in \mathcal{F}$. First note that $D = (A \cup B) - c \in \mathcal{F}$, where $c = \min(A \cup B)$. Now $D \subseteq G^{\geq 0}$. Hence, $\sum D \in \mathcal{F}$. It remains to note that

$$(A + B) - 2c = \{(a - c) + (b - c) \mid a \in A, b \in B\} \subseteq \sum D.$$

Hence, also $(A + B) - 2c \in \mathcal{F}$ and thus also $A + B = ((A + B) - 2c) + 2c \in \mathcal{F}$.

Now let $r, s, u \in k(\!(\mathcal{F})\!)$. Then

$$\begin{aligned}
1 \cdot r &= \sum_{g\in G}\left(\sum_{h\in G} 1_h r_{g-h}\right) t^g = \sum_{g\in G}(1\cdot r_g)\, t^g = r,\\
rs &= \sum_{g\in G}\left(\sum_{h\in G} r_h s_{g-h}\right) t^g = \sum_{g\in G}\left(\sum_{h'\in G} s_{h'} r_{g-h'}\right) t^g = sr,\\
r(su) &= \sum_{g\in G}\left(\sum_{h\in G} r_h (su)_{g-h}\right) t^g = \sum_{g\in G}\left(\sum_{h\in G} r_h \sum_{i\in G} s_i u_{g-h-i}\right) t^g\\
&= \left(\sum_{g\in G}\sum_{h\in G}\sum_{i\in G} r_h s_i u_{g-h-i}\right) t^g = \sum_{g'\in G}\left(\sum_{j\in G}\sum_{h\in G} r_h s_{j-h} u_{g'-h}\right) t^{g'}\\
&= \sum_{g'\in G}\left(\sum_{j\in G}(rs)_h u_{g'-j}\right) t^{g'} = (rs)u,\\
r(s+u) &= \sum_{g\in G}\left(\sum_{h\in G} r_h (s_{g-h}+u_{g-h})\right) t^g = \sum_{g\in G}\left(\sum_{h\in G} r_h (s_{g-h})\right) t^g + \sum_{g\in G}\left(\sum_{h\in G} r_h (u_{g-h})\right) t^g\\
&= rs + ru.
\end{aligned}$$

This verifies the remaining ring axioms. □

In order to show that a Rayner field $k(\!(\mathcal{F})\!)$ is also closed under taking inverses for non-zero elements, we will use an instance of Neumann's Lemma, the proof of which is part of Real Algebraic Geometry II[15].

Lemma 6.2.4 (Neumann's Lemma)**.** *Let k be a field and let G be an ordered abelian group. Moreover, let $\varepsilon \in k\left(\!\left(G^{>0}\right)\!\right)$. Then*

$$\sigma = \sum_{n\in\omega} \varepsilon^n \in k(\!(G)\!)\,.$$

More precisely, for any $g \in G$, there are only finitely many $n \in \omega$ such that $(\varepsilon^n)_g \neq 0$, whence $(\sigma)_g$ is given by

$$\sum_{n\in\omega} (\varepsilon^n)_g,$$

and $\operatorname{supp}(\sigma) \in \operatorname{wo}(G)$.

Proposition 6.2.5. *Let $k(\!(\mathcal{F})\!)$ be a Rayner field. Then $\left(k(\!(\mathcal{F})\!), +, -, \cdot, 0, 1\right)$, indeed, forms a field.*

Proof. By Lemma 6.2.3, we only have to show that for any $a \in k(\!(\mathcal{F})\!) \setminus \{0\}$ there is some $b \in k(\!(\mathcal{F})\!)$ with $ab = 1$. Let $g_0 = \min(\operatorname{supp}(a))$. Set

$$a' = a_{g_0}^{-1} t^{-g_0} a = 1 + \sum_{g\in G^{>g_0}} a_{g_0}^{-1} a_g t^{g-g_0}.$$

[15] See, for instance, `http://www.math.uni-konstanz.de/~kuhlmann/Lehre/SS19-ReelleAlgGeo2/Scripts/RAG_II-Gesamtskript.pdf`, Lecture 11, Lemma 1.6.

Set

$$\varepsilon = -\sum_{g \in G^{>g_0}} a_{g_0}^{-1} a_g t^{g-g_0} \in k\left(\left(G^{>0}\right)\right).$$

Then $a' = 1 - \varepsilon$. By Lemma 6.2.4, we obtain

$$\sum_{n \in \omega} \varepsilon^n \in k(\!(G)\!).$$

Let $E = \operatorname{supp}(\varepsilon) \subseteq G^{>0}$. Since for any $n \in \mathbb{N}$, we have

$$\operatorname{supp}(\varepsilon^n) \subseteq \underbrace{E + \ldots + E}_{n \text{ times}} \subseteq \sum E,$$

we also obtain

$$\operatorname{supp}\left(\sum_{n \in \omega} \varepsilon^n\right) \subseteq \sum E \in \mathcal{F}.$$

Hence,

$$\sum_{n \in \omega} \varepsilon^n \in k(\!(\mathcal{F})\!).$$

Now note that

$$(1 - \varepsilon) \sum_{n \in \omega} \varepsilon^n = \sum_{n \in \omega} \varepsilon^n - \sum_{n \in \omega} \varepsilon^{n+1} = 1.$$

(This can, for instance, directly be verified by evaluating in g for any $g \in G$.) We can thus write

$$\sum_{n \in \omega} \varepsilon^n = \frac{1}{1 - \varepsilon} = \frac{1}{a'}.$$

It remains to note that

$$a^{-1} = \frac{a_{g_0}^{-1} t^{-g_0}}{a'}.$$

□

Exercise 6.2.6. Let k be a field and let G be an ordered abelian group. Show that $k(\!(G)\!)$ is a Rayner field.

By Proposition 6.2.5 and Exercise 6.2.6, we immediately obtain the following:

Corollary 6.2.7. *Let k be a field and let G be an ordered abelian group. Then*

$$\left(k(\!(G)\!), +, -, \cdot, 0, 1\right)$$

is a field.

Exercise 6.2.8. Let k be a field and let G be an ordered abelian group.

(i) Define $k[G] \subseteq k(\!(G)\!)$ by

$$k[G] = \{s \in k(\!(G)\!) \mid \operatorname{supp}(s) \text{ is finite}\}.$$

Show that $k[G]$ is an integral domain.

(ii) Define $k(G) \subseteq k((G))$ by

$$k(G) = \mathrm{ff}(k[G]).$$

Show that $k(G)$ is the smallest subfield of $k((G))$ containing all monomials, i.e. the set

$$\left\{ at^h \;\middle|\; a \in k, h \in G \right\} \subseteq k((G)).$$

Definition 6.2.9. Let k be a field and let G be an ordered abelian group. A **Hahn field** (over k and G) is a field K with

$$k(G) \subseteq K \subseteq k((G)).$$

We call $k(G)$ the **minimal Hahn field** and $k((G))$ the **maximal Hahn field** (over k and G).

Exercise 6.2.10. Show that every Rayner field is a Hahn field, i.e. show that for any field k, any ordered abelian group G, and any $\mathcal{F} \subseteq \mathrm{wo}(G)$, if $k((\mathcal{F}))$ is a Rayner field, then

$$k(G) \subseteq k((\mathcal{F})) \subseteq k((G)).$$

Not every Hahn field is a Rayner field. Indeed, even the minimal Hahn field $k(G)$ is not (necessarily) a Rayner field as the following example shows.

Example 6.2.11. Consider the minimal Hahn field over $\mathbb{Q}$ and $\mathbb{Z}$, i.e. $K = \mathbb{Q}(\mathbb{Z})$. Assume, for a contradiction, that K is a Rayner field and let $\mathcal{F} \subseteq \mathrm{wo}(G)$ such that $K = \mathbb{Q}((\mathcal{F}))$.

Now

$$s = \frac{1}{1-t} = \sum_{i=0}^{\infty} t^i \in K.$$

The support of this element is given by $\mathrm{supp}(s) = \omega$. Hence, $\omega \in \mathcal{F}$. By the properties of a Rayner field, also for any $B \subseteq \omega$, any element of $k((G))$ whose support equals B is contained in K. However, the power set of ω is uncountable, whence there are uncountably many choices of such B. Hence, K contains uncountably many elements.

It remains to note that $\mathbb{Q}(\mathbb{Z})$ is countable as the field of fractions of the countable ring $\mathbb{Q}[Z]$, giving us the required contradiction.

6.2.2. Orderings

If k is a real field, then any ordering of k induces an ordering of $k((G))$ (for any ordered abelian group G). In this section, we define this ordering on $k((G))$ stemming from an ordering of k. Note that the restriction of an ordering on a field K can be restricted to an ordering on any subfield of K. Hence, by establishing an ordering on $k((G))$, we obtain an ordering on any Hahn field over k and G and, in particular, for any Rayner field.

Definition 6.2.12. Let $(k, <)$ be an ordered field and let G be an ordered abelian group. We define a linear ordering $<$ on $k((G))$ by setting[16]

$$0 < s :\Leftrightarrow (s \neq 0 \wedge s(\min(\mathrm{supp}(s))) > 0).$$

[16]By the Bonus Exercise on Exercise Sheet 5, we then define $s < r$ if and only if $0 < r - s$.

Exercise 6.2.13. Let $(k, <)$ be an ordered field and let G be an ordered abelian group. Verify that $(k(\!(G)\!), <)$ is, indeed, an ordered field.

Example 6.2.14. Recall that by the Bonus Exercise on Exercise Sheet 7, an ordered field is archimedean if and only if $\mathbb{Z}$ is its unique integer part.

Let $(k, <)$ be an ordered field and let G be a non-trivial ordered abelian group (i.e. $G \neq \{0\}$). Then any Hahn field K over k and G is non-archimedean. Indeed, let $g \in G^{<0}$. Then $t^g \in K$. Assume, for a contradiction, that for some $z \in \mathbb{Z}$ we have

$$z \leq t^g < z + 1.$$

Then $-1 \leq t^g - (z+1) < 0$. However, for $s = 1t^g - (z+1)t^0$, we have $\operatorname{supp}(s) = \{g, 0\}$ if $z + 1 \neq 0$ and $\operatorname{supp}(s) = \{g\}$ if $z + 1 = 0$. In either case,

$$s(\min(\operatorname{supp}(s))) = s(g) = 1 > 0,$$

whence $s > 0$, a contradiction.

Example 6.2.14 shows that Hahn fields over non-trivial ordered abelian groups are always non-archimedean. Due to Kaplansky's Embedding Theorem, whose proof goes beyond the scope of this lecture, any ordered field is isomorphic to an ordered Hahn field. Hence, ordered Hahn fields are prototypes for non-archimedean fields. In the next section, we will show how for a general ordered field $(K, <)$ we can find the ordered coefficient field $(k, <)$ and the ordered abelian group G in order that $(K, <)$ is isomorphic to a Hahn field over k and G in the sense of Kaplansky's Embedding Theorem.

6.3. Valuation Theory

This section mainly follows [6, Chapters 0 and 1].

6.3.1. Valuations

Definition 6.3.1. Let G be an ordered abelian group and let K be a field. Let ∞ be a symbol satisfying $\infty > g$ and

$$\infty = \infty + \infty = \infty + g = g + \infty$$

for any $g \in G$. A surjective map

$$v\colon K \to G \cup \{\infty\}$$

is called a **valuation** on K if for any $a, b \in K$, the following hold:

(i) $v(a) = \infty$ implies $a = 0$,

(ii) $v(ab) = v(a) + v(b)$,

(iii) $v(a + b) \geq \min\{v(a), v(b)\}$.

We call G the **value group** of K under v and denote it by vK. The pair (K, v) is called a **valued field**. The ring

$$\mathcal{O}_v = \{a \in K \mid v(a) \geq 0\}$$

is called the **valuation ring** of v and the maximal ideal

$$\mathcal{I}_v = \{a \in K \mid v(a) > 0\}$$

of $\mathcal{O}_v$ is called the **valuation ideal** of v. The **residue field** of (K, v) is given by $\mathcal{O}_v/\mathcal{I}_v$ and denoted by $\overline{K}$. For any $a \in \mathcal{O}_v$, we denote $a + \mathcal{I}_v$ by $\overline{a}$ and call it the **residue** of a. Moreover, for any $p \in \mathcal{O}_v[X]$ with $p = \sum_{i=0}^{n} a_i X^i$ we denote by $\overline{p}$ the polynomial $\sum_{i=0}^{n} \overline{a_i} X^i \in \overline{K}[X]$.

Exercise 6.3.2. Let (K, v) be a valued field. Verify that $\mathcal{O}_v$ is a subring of K and that $\mathcal{I}_v$ is a maximal ideal of $\mathcal{O}_v$. Moreover, show that $\mathcal{I}_v$ is the *unique* maximal ideal of $\mathcal{O}_v$.

Remark 6.3.3. Let (K, v) be a valued field. Note that the projection map

$$\mathcal{O}_v \to \overline{K}, a \mapsto \overline{a}$$

defines an $\mathcal{L}_{\mathrm{r}}$-homomorphism. Hence, in particular, for any $p \in \mathcal{O}_v[X]$ and any $a \in \mathcal{O}_v$, we have

$$\overline{p(a)} = \overline{p}(\overline{a}).$$

The most important valuation in the context of Hahn fields is given in the following example.

Example 6.3.4. Let k be a field and let G be an ordered abelian group. We define the following map $v_{\min}$ on $K = k((G))$:

$$v_{\min} \colon K \to G \cup \{\infty\}, s \mapsto \begin{cases} \min(\mathrm{supp}(s)) & \text{if } s \neq 0, \\ \infty & \text{if } s = 0. \end{cases}$$

We verify that $(K, v_{\min})$ is a valued field with $vK = G$ and $\overline{K} \cong k$. To ease the notation, we write v for $v_{\min}$.

First note that v is surjective, as for any $g \in G$ we have $v(t^g) = g$. By definition of v, we have $v(s) = \infty$ if and only if $s = 0$ for any $s \in K$. Now let $a, b \in K$. If $a = 0$ or $b = 0$, then it is easy to verify that $v(ab) = v(a) + v(b)$ and $v(a + b) \geq \min\{v(a), v(b)\}$. Hence, suppose that $a \neq 0$ and $b \neq 0$. We express a and b as

$$a = \sum_{g \in G^{\geq i}} a_g t^g \text{ and } b = \sum_{g \in G^{\geq j}} b_g t^g$$

with $i = v(a)$ and $j = v(b)$. Note that $a_i, b_j \neq 0$. Then

$$ab = a_i b_j t^{i+j} + \sum_{g \in G^{>i+j}} (ab)_g t^g.$$

Hence, $v(ab) = i + j = v(a) + v(b)$.

To verify that $v(a + b) \geq \min\{v(a), v(b)\}$, we may assume that $i \leq j$, i.e. $\min\{v(a), v(b)\} = v(a)$. Then

$$a + b = a_i t^i + b_j t^j + \sum_{g \in G^{>i}} a_g t^g + \sum_{g \in G^{>j}} b_g t^g.$$

If $i < j$ or $a_i + b_j \neq 0$, then we obtain $v(a+b) = i = v(a)$. Otherwise, we have

$$a + b = \sum_{g \in G^{>i}} a_g t^g + \sum_{g \in G^{>j}} b_g t^g$$

and obtain $v(a+b) > \min\{i, j\} = j = v(a)$.

We have thus established that (K, v) is a valued field with value group $vK = G$. Its valuation ring $\mathcal{O}_v$ is given by $k\big(\big(G^{\geq 0}\big)\big)$ and its valuation ideal $\mathcal{I}_v$ by $k\big(\big(G^{>0}\big)\big)$. Set

$$\varphi \colon \overline{K} \to k$$

with $\varphi(\overline{a}) = a_0$ for any $a \in \mathcal{O}_v$. We show that φ is an $\mathcal{L}_{\mathrm{r}}$-isomorphism, establishing that k is (isomorphic to) the residue field of (K, v). First note that φ is well-defined: For any $a, b \in \mathcal{O}_v$ with $\overline{a} = \overline{b}$ we have $a - b \in \mathcal{I}_v$. Hence, $(a-b)_0 = 0$, showing that

$$\varphi(a) = a_0 = b_0 = \varphi(b).$$

Clearly $\varphi(\overline{0}) = 0$ and $\varphi(\overline{1}) = 1$. Now let $a, b \in \mathcal{O}_v$. Then,

$$\varphi(a+b) = (a+b)_0 = a_0 + b_0 = \varphi(a) + \varphi(b),$$

and since $v(a), v(b) \geq 0$, we obtain

$$\varphi(ab) = (ab)_0 = a_0 b_0 = \varphi(a)\varphi(b).$$

Exercise 6.3.5. Let (K, v) be a valued field and let $F \subseteq K$ be a subfield. Show that $w = v|_F$ defines a valuation on F whose value group is a subgroup of vK and whose residue field $\overline{F}$ is a subfield of $\overline{K}$.

If k is a field and G is an ordered abelian group, then $v_{\min}$ on $k(\!(G)\!)$ can be restricted to $k(G)$. We then also write $(k(G), v_{\min})$, where the valuation on $k(G)$ is actually given by $v_{\min}|_{k(G)}$.

Exercise 6.3.6. Let k be a field and let G be an ordered abelian group. Show that for any Hahn field K over k and G we have that $(K, v_{\min})$ has value group G and residue field (isomorphic to) k.

6.3.2. Natural Valuation

Later, we will only be interested in ordered Hahn fields with archimedean residue field. Here, the concept of the natural valuation will become useful.

Definition 6.3.7. Let $(K, <)$ be an ordered field. Denote by $\mathcal{O}_{v_{\mathrm{nat}}}$ the convex hull of $\mathbb{Z}$ in K, i.e. the set

$$\{a \in K \mid c \leq a \leq d \text{ for some } c, d \in \mathbb{Z}\}.$$

We define an equivalence relation $\sim$ on K by setting

$$a \sim b :\Leftrightarrow \left(\frac{a}{b} \in \mathcal{O}_{v_{\mathrm{nat}}} \wedge \frac{b}{a} \in \mathcal{O}_{v_{\mathrm{nat}}}\right)$$

for any $a, b \in K^\times$, as well as $0 \sim 0$ and $0 \not\sim a$ for any $a \in K^\times$. Let $G = \{[a] \mid a \in K^\times\}$, where $[a]$ denotes the equivalence class of a under $\sim$, and define

$$[a] + [b] := [ab]$$

and

$$[a] < [b] :\Leftrightarrow \left(\left(b \neq 0 \wedge \frac{a}{b} \notin \mathcal{O}_{v_{\mathrm{nat}}}\right) \vee (b = 0 \wedge a \neq 0)\right)$$

for any $a, b \in K$. We set $\infty = [0]$ and

$$v_{\mathrm{nat}} \colon K \to G \cup \{\infty\}, a \mapsto [a].$$

Then v_{nat} is called the **natural valuation** on K.

Exercise 6.3.8. Let $(K, <)$ be an ordered field. Show that (K, v_{nat}) is a valued field.

The natural valuation on an ordered field is a coarse measure for the size of the elements with respect to the ordering $<$. If an element of K has a positive valuation, then it is infinitesimal. If it has a negative valuation, then it is infinitely large (positive or negative). This can directly be applied to ordered Hahn fields.

Exercise 6.3.9. Let $(k, <)$ be an archimedean ordered field and let G be an ordered abelian group. Denote by v_{nat} the natural valuation on $(K, <) = (k(\!(G)\!), <)$.

(i) Show that $\mathcal{O}_{v_{\mathrm{min}}} = \mathcal{O}_{v_{\mathrm{nat}}}$.

(ii) Show that

$$\varphi \colon G \to v_{\mathrm{nat}}K, g \mapsto v_{\mathrm{nat}}(t^g)$$

defines an $\mathcal{L}_{\mathrm{og}}$-isomorphism.

(iii) Show that for any $a \in k(\!(G)\!)^\times$ we have

$$v_{\mathrm{nat}}(a) = \varphi(v_{\mathrm{min}}(a)).$$

Remark 6.3.10. Exercise 6.3.9 shows that for an archimedean ordered field $(k, <)$ and an ordered abelian group G, the valuations v_{min} and v_{nat} are equivalent in the sense that they have the same valuation ring and the value groups are isomorphic, where the isomorphism preserves the valuation. Hence, we identify the valuations v_{min} and v_{nat} with each other and, in the following sections and chapters, only denote them by v.

Given a non-archimedean ordered field $(K, <)$, the natural valuation v always gives us a method to naturally associate an archimedean ordered field $(\overline{K}, <)$ to it.

Definition 6.3.11. Let $(K, <)$ be an ordered field. We define an order relation $<$ on $\overline{K}$ as follows:

$$\overline{a} < \overline{b} :\Leftrightarrow (\overline{a} \neq \overline{b} \wedge a < b)$$

for any $a, b \in \mathcal{O}_v$.

Exercise 6.3.12. Let $(K, <)$ be an ordered field. Show that $(\overline{K}, <)$ is an archimedean ordered field.

Remark 6.3.13. Let $(k, <)$ be an archimedean ordered field and let G be an ordered abelian group. As shown in Example 6.3.4, the residue field of $k((G))$ coincides with k (up to the presented isomorphism). We thus identify $\overline{k((G))}$ with k. Now for any $a, b \in \mathcal{O}_v = k\big(\big(G^{\geq 0}\big)\big)$ we have $\overline{a} < \overline{b}$ if and only if $\overline{a} \neq \overline{b}$ and $a < b$, where the ordering here is meant to be the one from Definition 6.3.11. Considering $\overline{a} = a_0, \overline{b} = b_0 \in k$ (via the described identification of the residue field with k), we also obtain $a_0 \neq b_0$ and $a_0 < b_0$, where the ordering here is meant to be the one from $(k, <)$. Hence, the ordering given in Definition 6.3.11 on k coincides with the original ordering on k.

6.3.3. Henselian Valuation

In this last section on the basics of valuation theory, we consider a special class of valuations satisfying the condition that simple roots can be "lifted".

Definition 6.3.14. Let (K, v) be a valued field. Then (K, v) is called **henselian valued** and v is called **henselian** if for any $p \in \mathcal{O}_v[X]$ and any $b \in \mathcal{O}_v$ with $\overline{p}(\overline{b}) = 0$ and $\overline{p}'(\overline{b}) \neq 0$ there is some $c \in \mathcal{O}_v$ with $p(c) = 0$ and $\overline{c} = \overline{b}$.

Generally, one can show that the valuation $v_{\min}$ on any maximal Hahn field is henselian. Since we will mainly be interested in the natural valuation on real closed fields, this proof goes beyond the scope of this lecture. However, we show that the natural valuation is always henselian in any real closed field.

Proposition 6.3.15. *Let $(K, <)$ be a real closed field. Then also $(\overline{K}, <)$ is real closed.*

Proof. We verify that $\overline{K}$ has the intermediate value property. In order to do so, let $p \in \mathcal{O}_v[X]$ and let $a, b \in \mathcal{O}_v$ with $\overline{a} < \overline{b}$ and $\overline{p}(\overline{a})\overline{p}(\overline{b}) < 0$. Then

$$\overline{p(a)p(b)} < 0,$$

whence $p(a)p(b) < 0$. This shows that p has a root $c \in (a, b)_K$. Hence,

$$0 = \overline{p(c)} = \overline{p}(\overline{c}),$$

showing that $\overline{c} \in (\overline{a}, \overline{b})_{\overline{K}}$ is a root of $\overline{p}$. □

Proposition 6.3.16. *Let $(K, <)$ be a real closed field. Then (K, v) is henselian.*

Proof. Let $p \in \mathcal{O}_v[X]$ and let $b \in \mathcal{O}_v$ with $\overline{p}(\overline{b}) = 0$ and $\overline{p}'(\overline{b}) \neq 0$. We need to find $c \in \mathcal{O}_v$ with $p(c) = 0$ and $\overline{c} = \overline{b}$. We may assume that $(K, <)$ is non-archimedean, as otherwise $c = b$ will do.

First note that $\overline{p}$ changes its sign in $\overline{b}$, as $\overline{b}$ is a simple zero of $\overline{p}$ (as $\overline{K}$ is real closed by Proposition 6.3.15). Let $I \subseteq \overline{K}$ be a closed interval such that $\overline{b} \in I$ and $\overline{p}$ has no further roots and thus sign change within I. Moreover, let I be of the form $I = [\overline{s}, \overline{t}]_{\overline{K}}$ for some $s, t \in \mathcal{O}_v$ with $\overline{s} < \overline{b} < \overline{t}$. Then

$$\overline{p(s)p(t)} = \overline{p}(\overline{s})\overline{p}(\overline{t}) < 0.$$

Hence, $p(s)p(t) < 0$. This shows that p must change its sign within the interval $J = [s,t]_K \subseteq K$. Since K is real closed, it must have a root $c \in J$.

Assume, for a contradiction, that $\overline{c} \neq \overline{b}$. We may assume that $c < b$, as we can argue similarly for the case that $b < c$. Then $\overline{c} < \overline{b}$. However,

$$s \leq c \leq t$$

implies that

$$\overline{s} \leq \overline{c} < \overline{b} \leq \overline{t}.$$

Since $p(c) = 0$, we have $\overline{p}(\overline{c}) = \overline{p(c)} = 0$. This contradicts the assumption that $\overline{p}$ has no roots in I except $\overline{b}$. □

7. Mourgues–Ressayre Theorem

7.1. Ordered Hahn Fields

7.1.1. Residue Field and Value Group

We immediately obtain from Proposition 6.3.15 the following.

Corollary 7.1.1. *Let $(k,<)$ be an archimedean ordered field and let G be an ordered abelian group. Suppose that $(k((G)),<)$ is real closed. Then also $(k,<)$ is real closed.*

For any Hahn field K over a field k and an ordered abelian group G, the residue field k of K is naturally embedded, as $k \subseteq k(G) \subseteq K$. We show that this also holds for any real closed field.

Lemma 7.1.2. *Let K be a real closed field and let F be a subfield of K. Then the relative algebraic closure L of F in K is also real closed. Hence, F is real closed if and only if it is relatively algebraically closed in K.*

Proof. We prove that L is real closed by verifying the intermediate value property. Let $p \in L[X]$ and let $a, b \in L$ with $p(a) < 0 < p(b)$. Then there is some $c \in K$ with $c \in (a,b)_K$ and $p(c) = 0$. Hence, c is algebraic over L and thus over F. This implies that $c \in L$, as required. □

Proposition 7.1.3. *Let K be a real closed field. Then there exists an $\mathcal{L}_{\mathrm{or}}$-embedding*

$$\iota\colon (\overline{K},<) \hookrightarrow (K,<).$$

Moreover, $\overline{\iota(a)} = a$ for any $a \in \overline{K}$.

Proof. Let $\mathcal{C}$ be the set of archimedean subfields of K, partially ordered by $\subseteq$. Note that $\mathbb{Q} \in \mathcal{C}$. Moreover, one can easily verify that the union of any increasing chain in $\mathcal{C}$ is again contained in $\mathcal{C}$. Hence, by Zorn's Lemma, $\mathcal{C}$ contains a maximal element F. Note that $F \subseteq \mathcal{O}_v$, as otherwise F would contain an infinitely large element and thus not be archimedean.

We now show that F is real closed. Let L be the relative algebraic closure of F in K. Then for any $a \in L$ there are $n \in \omega$ and $q_0, \ldots, q_n \in F$ with $q_n \neq 0$ such that

$$0 = q_0 a^0 + \ldots + q_n a^n.$$

If we had $v(a) < 0$, then

$$\infty = v(q_0 a^0 + \ldots + q_n a^n) = nv(a) < 0.$$

Hence, L contains no infinitely large element and is thus archimedean. By maximality of F, we obtain $L = F$ and thus F is real closed by Lemma 7.1.2.

Let $\pi\colon \mathcal{O}_v \to \overline{K}, a \mapsto \overline{a}$ and let $\pi' = \pi|_F$. We show that π' is an $\mathcal{L}_{\mathrm{or}}$-isomorphism, yielding that $\iota = (\pi')^{-1}$ is an $\mathcal{L}_{\mathrm{or}}$-embedding of $\overline{K}$ into K. Since π' is the restriction of an $\mathcal{L}_{\mathrm{r}}$-homomorphism, it is itself an $\mathcal{L}_{\mathrm{r}}$-homomorphism. To show that π' is preserves $<$ (and is thus injective), let $a, b \in F$ with $a < b$. Then $\overline{a} \leq \overline{b}$ and $v(b-a) = 0$, as $F \subseteq \mathcal{O}_v$. Hence, $\overline{a} \neq \overline{b}$ and we obtain $\pi'(a) < \pi'(b)$.

We now prove that π' is surjective.[17] Let $c \in \mathcal{O}_v$. We show that $\overline{c} \in \pi'(F)$. We can assume that $c \notin F$ since otherwise it already holds that $\overline{c} = \pi'(c) \in \pi'(F)$. Then $F(c)/F$ is a proper field extension. By maximality of F, the field $F(c)$ is non-archimedean and therefore contains a (non-zero) element of $\mathcal{I}_v$, i.e. there are $p, q \in F[X]$ such that $p(c), q(c) \neq 0$ and

$$0 < v\left(\frac{p(c)}{q(c)}\right) = v(p(c)) - v(q(c)).$$

Then

$$v(q(c)) < v(p(c))\,.$$

Let $n \in \omega$ and let $a_0, \ldots, a_n \in F$ such that $q(X) = \sum_{j=0}^{n} a_j X^j$ and $a_n \neq 0$. Since $c \in \mathcal{O}_v$, we have $v(c) \geq 0$ and therefore

$$v(q(c)) = v\left(\sum_{j=0}^{n}(a_j c^j)\right) \geq \min\{v(a_j c^j) \mid 0 \leq j \leq n\} = \min\{v(a_j) + jv(c) \mid 0 \leq j \leq n\} \geq 0\,.$$

This shows that $0 < v(p(c))$ and therefore $p(c) \in \mathcal{I}_v$. Applying the residue map yields $0 = \overline{p(c)} = \overline{p}(\overline{c})$. Note that the coefficients of p lie in F and therefore no non-zero coefficient in p vanishes by applying the residue map, i.e. $\overline{p} \neq 0$. We obtain that $\overline{c}$ is algebraic over $\overline{F} = \pi'(F)$. Since F is real closed, $\overline{F}$ is real closed by Lemma 7.1.2 and therefore $\overline{F}$ is relatively algebraically closed in $\overline{K}$. Hence $\overline{c} \in \overline{F} = \pi'(F)$, which completes the proof.

We have thus established that

$$\iota\colon (\overline{K}, <) \cong (F, <).$$

Finally, for any $b \in \mathcal{O}_v$, we have

$$\overline{\iota(\overline{b})} = \pi'(\iota(\overline{b})) = \overline{b},$$

showing the further requirement on ι. □

Remark 7.1.4. Note that the embedding ι constructed in Proposition 7.1.3 maps $\overline{K}$ into $\mathcal{O}_v$. Moreover, we have $\iota(\overline{K}^\times) \subseteq \mathcal{O}_v^\times = \mathcal{O}_v \setminus \mathcal{I}_v$.

We now also consider the value group under the natural valuation of a real closed field.

Definition 7.1.5. Let G be an ordered abelian group. We say that G is **divisible** if for any $g \in G$ and any $n \in \mathbb{Z} \setminus \{0\}$ there exists $h \in G$ with $g = nh$. We then also denote h by $\frac{g}{n}$.

Proposition 7.1.6. *Let K be a real closed field. Then $G = vK$ is divisible.*

[17] I thank Daniel Happ for providing this more direct argument.

Proof. Let $g \in G$ and let $n \in \mathbb{N}$. Moreover, fix $a \in K$ with $v(a) = g$. We may assume that $a > 0$, as otherwise we can replace it by $-a$.

Consider the polynomial $p(X) = X^n - a \in K[X]$. Then by the intermediate value property, p has a root $c \in K$, as

$$p(0) = -a < 0 < (1+a)^n - a = p(a).$$

Now for $h = v(c)$ we obtain

$$g = v(a) = v(c^n) = nv(c) = nh,$$

as required. □

We immediately obtain from Proposition 7.1.6 the following.

Corollary 7.1.7. *Let $(k, <)$ be an archimedean ordered field and let G be an ordered abelian group. Suppose that $(k((G)), <)$ is real closed. Then G is divisible.*

The following two exercises establish the embeddability of the value group of a real closed field, analogous to Proposition 7.1.3.

Exercise 7.1.8. (i) Let G be a divisible ordered abelian group. Show that G is a $\mathbb{Q}$-vector space with usual addition and scalar multiplication

$$\frac{m}{n} g = \frac{mg}{n}$$

for any $m, n \in \mathbb{Z}$ with $n \neq 0$ and any $g \in G$.

(ii) Let K be a real closed field. Show that $(K^{>0}, \boxplus, \boxdot)$ is a $\mathbb{Q}$-vector space where the addition operation on $K^{>0}$ is given by $a \boxplus b = ab$ for any $a, b \in K^{>0}$ (i.e. the standard multiplication) and the scalar multiplication is given by

$$\frac{m}{n} \boxdot a = \sqrt[n]{a^m}$$

for any $m \in \mathbb{Z}$, $n \in \mathbb{N}$ and $a \in K^{>0}$. Here, for any $b \in K^{>0}$, we denote by $\sqrt[n]{b}$ the unique positive element c of K with $c^n = b$.

Exercise 7.1.9. Let K be a real closed field and let $G = vK$. Consider both G and $K^{>0}$ as $\mathbb{Q}$-vector spaces as in Exercise 7.1.8.

(i) Let $\mathcal{B}$ be a basis of G. For any $g \in G$, fix an element $a_g \in K^{>0}$ with $v(a_g) = g$. Show that $\{a_g \mid g \in \mathcal{B}\} \subseteq K^{>0}$ is $\mathbb{Q}$-linearly independent.

(ii) Deduce that there exists an embedding

$$\varphi \colon (G, +, 0) \hookrightarrow (K^{>0}, \cdot, 1)$$

with $v(\varphi(g)) = g$ for any $g \in G$ and $\varphi(g) > \varphi(h)$ for any $g, h \in G$ with $g < h$.

Combining Proposition 7.1.3 and Exercise 7.1.9, we obtain the embeddability of the minimal Hahn field over the residue field and the value group of a real closed field as the next exercise shows.

Exercise 7.1.10. Let K be a real closed field. Set $k = \overline{K}$ and $G = vK$. Show that there exists an $\mathcal{L}_{\text{or}}$-embedding of $(k(G), <)$ into $(K, <)$.
(Hint: First find an $\mathcal{L}_{\text{or}}$-embedding of $(k[G], <)$ into $(K, <)$.)

Recalling Corollary 7.1.1 and Corollary 7.1.7, if the maximal ordered Hahn field $(k((G)), <)$ (where $(k, <)$ is archimedean) is real closed, then k is real closed and G is divisible. The converse also holds, but its proof needs more sophisticated tools for valued fields. We thus refer to Real Algebraic Geometry II[18] for its proof and simply state the result here for later application.

Theorem 7.1.11. *Let $(k, <)$ be an archimedean real closed ordered field and let G be a divisible ordered abelian group. Then $(k((G)), <)$ is real closed.*

Example 7.1.12. By Theorem 7.1.11, any Hahn field of the form $k((\mathbb{Q}))$ is real closed, whenever k is a real closed field. In particular, $\mathbb{R}((\mathbb{Q}))$ is a real closed Hahn field. In fact, even its subfield of Puiseux series $\mathbb{R}\langle\langle t\rangle\rangle$ (see Exercise 10.3) is real closed. (The proof for this result works similar to the proof of Theorem 7.1.11.)

7.1.2. Truncation Closed Subfields

Definition 7.1.13. Let k be a field and let G be an ordered abelian group. A subring R of the maximal Hahn field $k((G))$ is called **truncation closed** if for any $s = \sum_{g \in G} s_g t^g \in R$ and any $h \in G$, the **truncation** (at h)

$$s^{<h} := \sum_{g<h} s_g t^g := \sum_{g \in G^{<h}} s_g t^g \in k((G))$$

of s to the initial segment $G^{<h}$ of G also belongs to R. A truncation r of s is called a **strict truncation** of s if $r \neq s$.

Remark 7.1.14. Let k be a field and let G be an ordered abelian group. Then $s \in k((G))$ only has strict truncations if and only if $\operatorname{supp}(s)$ is cofinal in G, i.e. for any $g \in G$ there is some $h \in \operatorname{supp}(s)$ with $g \leq h$. Indeed, if $\operatorname{supp}(s)$ is not cofinal in G, then for any $h \in G$ with $\operatorname{supp}(s) < h$ we have

$$s^{<h} = s.$$

Conversely, if s has a truncation $s^{<h} = s$ for some $h \in \operatorname{supp}(s)$, then necessarily $\operatorname{supp}(s) < h$.

Notation 7.1.15. Let k be a field and let G be an ordered abelian group. Recall that for $s \in k((G))$ we established the order type notation

$$s = \sum_{\alpha<\gamma} s_\alpha t^{g_\alpha},$$

where $\gamma = \operatorname{ot}(s)$. In this notation, the truncation of s to the initial segment $G^{<g_\beta}$ of G for some $\beta < \gamma$ is denoted by

$$s^{<\beta} = \sum_{\alpha<\beta} s_\alpha t^{g_\alpha}.$$

[18] See, for instance, `http://www.math.uni-konstanz.de/~kuhlmann/Lehre/SS19-ReelleAlgGeo2/Scripts/RAG_II-Gesamtskript.pdf`, Lecture 15, Theorem 4.2.

Example 7.1.16. Let k be a field and let G be an ordered abelian group.

(i) The coefficient field k is truncation closed in $k(\!(G)\!)$. Indeed, the truncation of any $s \in k$ is either s itself or 0.

(ii) The group ring $k[G]$ is truncation closed. Indeed, let $n \in \mathbb{N}$, let $g_1, \ldots, g_n \in G$ with $g_1 < \ldots < g_n$ and let $a_1, \ldots, a_n \in k$. Then any truncation of

$$s = a_1 t^{g_1} + \ldots + a_n t^{g_n}$$

is of the form

$$a_1 t^{g_1} + \ldots + a_m t^{g_m} \in k[G]$$

for some $m \leq n$ (possibly $m = 0$).

(iii) Any Rayner field is truncation closed: Let $\mathcal{F} \subseteq \mathrm{wo}(G)$ such that $k(\!(\mathcal{F})\!)$ is a Rayner field. Let $A \in \mathcal{F}$. Then for any $s = \sum_{g \in A} s_g t^g \in k(\!(\mathcal{F})\!)$ and any $h \in G$, the truncation of s at h is given by

$$s^{<h} = \sum_{g \in A^{<h}} s_g t^g \in k(\!(G)\!).$$

Since $A^{<h} \subseteq A$, we obtain $A^{<h} \in \mathcal{F}$ and thus $s^{<h} \in \mathcal{F}$.

Notation 7.1.17. We use several other notations to obtain "restrictions" of an element $s \in k(\!(G)\!)$ to an interval in G similar to the one in Definition 7.1.13. For instance, for any $s \in k(\!(G)\!)$ and $h, h' \in G$ we write $s^{>h}$ for

$$\sum_{g \in G^{>h}} s_g t^g \in k(\!(G)\!)\,,$$

and $s^{h<\cdot<h'}$ for

$$\sum_{g \in G^{>h} \cap G^{<h'}} s_g t^g \in k(\!(G)\!)\,,$$

7.2. Statement and Proof

This section mainly follows the original arguments in [8] specialised to our setting.

7.2.1. Integer Parts via Pullbacks

We now come to the second main result of this lecture. First, we state the core result to prove the Theorem of Mourgues–Ressayre.

Theorem 7.2.1. *Let $(K, <)$ be a real closed field and set $k = \overline{K}$ as well as $G = vK$. Then there exists an $\mathcal{L}_{\mathrm{or}}$-embedding*

$$\iota \colon (K, <) \hookrightarrow (k(\!(G)\!)\,, <)$$

such that $\iota(K)$ is a truncation closed Hahn subfield of $k(\!(G)\!)$, i.e. $k(G) \subseteq \iota(K)$ and $\iota(K)$ is truncation closed in $k(\!(G)\!)$.

The map ι in Theorem 7.2.1 will be constructed step by step in Subsection 7.2.2. For now, we show how from this truncation closed embedding one obtains an integer part via a pullback.

Theorem 7.2.2 (Mourgues–Ressayre)**.** *Let $(K,<)$ be a real closed field. Then $(K,<)$ admits an integer part.*

Proof. Set $k = \overline{K}$ as well as $G = vK$. By Theorem 7.2.1, there exists

$$\iota\colon (K,<) \hookrightarrow (k((G)),<)$$

such that $F = \iota(K)$ is a truncation closed subfield of $k((G))$ with $k(G) \subseteq F$. Recall that by Exercise 12.3 (a)[19], there exists in integer part Z of F. Consider the pullback

$$Z' = \iota^{-1}(Z).$$

It is easy to check that the property of Z being a discretely ordered subring of $k((G))$ is preserved by ι^{-1}, i.e. Z' is a discretely ordered subring of K.

Let $a \in K$ and let $b = \iota(a) \in F$. Then there is $z \in Z \subseteq F$ such that

$$z \leq b < z + 1.$$

Applying ι^{-1}, we obtain

$$\iota^{-1}(z) \leq a < \iota^{-1}(z) + 1.$$

Since $\iota^{-1}(z) \in Z'$, we obtain that Z' is an integer part of K. □

7.2.2. Construction of Truncation Closed Embedding

Throught this section, we fix a real closed field $(K,<)$, its real closed archimedean residue field $k = \overline{K}$ and its value group $G = vK$. We thus consider the ordered fields $(K,<)$ and $(k((G)),<)$ and construct an $\mathcal{L}_{\mathrm{or}}$-embedding from the former into the latter. In this procedure, we iteratively extend a truncation closed embedding of a subfield of K into $k((G))$. To ease the notation, once a subfield F of K is embedded into $k((G))$ by a map ι, we simply identify F with $\iota(F)$ and treat F as a common subfield of K and $k((G))$. Moreover, all following extensions of the embedding are chosen to be the identity on F. We explain this once in detail after Step 1 of the procedure.

Step 1

By Example 7.1.16 (i), k is a truncation closed subfield of $k((G))$. Now Proposition 7.1.3 provides an $\mathcal{L}_{\mathrm{or}}$-embedding

$$\varphi\colon (k,<) \to (K,<).$$

Hence, its inverse is an $\mathcal{L}_{\mathrm{or}}$-embedding of the subfield $F = \varphi(k)$ of K into $k((G))$. We may therefore identify k with F and treat k as a common subfield of K and $k((G))$. All following embeddings will be the identity on k (or, formally, they will extend φ^{-1}).

[19] In this exercise, the following is shown: Let $(k,<)$ be an archimedean ordered field and let G be an ordered abelian group. Consider a truncation closed Hahn field K over k and G and its subring $Z = \{s \in K \mid \mathrm{supp}(s) \subseteq G^{\leq 0} \text{ and } s_0 \in \mathbb{Z}\}$. Then Z is an integer part of K.

Step 2

We now show that $k(G)$ is truncation closed in $k(\!(G)\!)$. Hence by Exercise 7.1.10, $k(G)$ will become a mutual subfield of K and $k(\!(G)\!)$ that is truncation closed in $k(\!(G)\!)$. The corresponding embedding is the identity on the common subfield k of K and $k(\!(G)\!)$ (see Exercise 12.2).

Lemma 7.2.3. *Let $a, b \in k(\!(G)\!)$ and let $d \in G$ such that $(ab)^{<\delta}$ is a strict truncation of ab. Then there are $n \in \omega$, $\alpha_0, \ldots, \alpha_n \in \operatorname{supp}(a)$ with $\alpha_0 < \ldots < \alpha_n$ and $\beta_0, \ldots, \beta_n \in \operatorname{supp}(b)$ with $\beta_0 > \ldots > \beta_n$ such that for any $i \in \{0, \ldots, n\}$ we have $\alpha_i + \beta_i \geq \delta$ and*

$$(ab)^{<\delta} = ba^{<\alpha_0} + b^{<\beta_0}\left(a^{<\alpha_1} - a^{<\alpha_0}\right) + \ldots + b^{<\beta_n}\left(a - a^{<\alpha_n}\right). \tag{7.2.1}$$

Proof. Since $(ab)^{<\delta}$ is a strict truncation of ab, we have that $\delta \not> \operatorname{supp}(ab) \subseteq \operatorname{supp}(a) + \operatorname{supp}(b)$. Hence, there are $\alpha \in \operatorname{supp}(a) =: A$ and $\beta \in \operatorname{supp}(b) =: B$ such that $\alpha + \beta \geq \delta$. Since A and B are well-ordered, we can take $\alpha_0 \in A$ be the least element for which there is some $\beta \in B$ with $\alpha_0 + \beta \geq \delta$, and since B is well-ordered, we can take $\beta_0 \in B$ to be least with $\alpha_0 + \beta_0 \geq \delta$.

First suppose that for any $\alpha \in A$ and any $\beta \in B$ with $\alpha > \alpha_0$ and $\beta < \beta_0$ we have $\alpha + \beta < \delta$. Then

$$(ab)^{<\delta} = ba^{<\alpha_0} + b^{<\beta_0}a^{\geq\alpha_0} = ba^{<\alpha_0} + b^{<\beta_0}\left(a - a^{<\alpha_0}\right),$$

and we are done.

Now suppose that there is some least $\alpha_1 \in A$ with $\alpha_1 > \alpha_0$ such that for some $\beta_1 \in B$ (which is least with the following properties) with $\beta_1 < \beta_0$ we have $\alpha_1 + \beta_1 \geq \delta$. Suppose further that for any $\alpha \in A$ and any $\beta \in B$ with $\alpha > \alpha_1$ and $\beta < \beta_1$ we have $\alpha + \beta < \delta$. Then Then

$$\begin{aligned}(ab)^{<\delta} &= ba^{<\alpha_0} + b^{<\beta_0}a^{\alpha_0 \leq \cdot < \alpha_1} + b^{<\beta_1}a^{\geq\alpha_1} \\ &= ba^{<\alpha_0} + b^{<\beta_0}\left(a^{<\alpha_1} - a^{<\alpha_0}\right) + b^{<\beta_1}\left(a - a^{<\alpha_1}\right),\end{aligned}$$

and we are done again.

This process can be continued iteratively. Since it results in a strictly decreasing sequence in the well-ordered set B, it terminates after finitely many steps, as required. □

Lemma 7.2.4. *Let L be a subfield of $k(\!(G)\!)$ and let $a, b \in L$ with $a \neq 0$ such that any truncation of a and b are also contained in L. Then the following hold:*

(i) Any truncation of $a + b$ and of $a - b$ belongs to L.

(ii) Any truncation of ab belongs to L.

(iii) Any truncation of a^{-1} belongs to L.

Proof. (i) For any $h \in G$, we have

$$(a \pm b)^{<h} = a^{<h} \pm b^{<h} \in L.$$

(ii) This immediately follows from Lemma 7.2.3, as (7.2.1) expresses any strict truncation of ab as a sum and product of truncations of a and truncations of b.

(iii) Let $A = \operatorname{supp}(a)$, let $c = a^{-1}$ and let $C = \operatorname{supp}(c)$. Note that $\min A = -\min C$. Hence, $0 = \min(A + C)$. Assume, for a contradiction, that there is some least $\zeta \in C$ such that $c' = c^{<\zeta} \notin L$. In particular, any strict truncation of c' belongs to L.

Let $\delta \in A + C$ be least with the property $C^{<\zeta} + \min A < \delta$. Note that δ exists, as $A + C$ is well-ordered and $\min A + \zeta \in A + C$ satisfies $C^{<\zeta} + \min A < \min A + \zeta$. In particular, $\delta \leq \min A + \zeta$. As $\delta > 0$, we have $1 = 1^{<\delta} = (ac)^{<\delta}$.

We show the following:

$$(ac)^{<\delta} = c'a^{<\alpha_1} + c^{<\beta_1}\left(a^{<\alpha_2} - a^{<\alpha_1}\right) + \ldots + c^{<\beta_n}\left(a - a^{<\alpha_n}\right), \tag{7.2.2}$$

where the α_i and β_i are as in (7.2.1) *with c in place of b.*

By application of Lemma 7.2.3, there are $n \in \omega$, $\alpha_0, \ldots, \alpha_n \in A$ with $\alpha_0 < \ldots < \alpha_n$ and $\beta_0, \ldots, \beta_n \in C$ with $\beta_0 > \ldots > \beta_n$ such that for any $i \in \{0, \ldots, n\}$ we have $\alpha_i + \beta_i \geq \delta$ and

$$(ac)^{<\delta} = ca^{<\alpha_0} + c^{<\beta_0}\left(a^{<\alpha_1} - a^{<\alpha_0}\right) + \ldots + c^{<\beta_n}\left(a - a^{<\alpha_n}\right).$$

Now $\min A$ is the least element of A such that there is some $\beta \in C$ with $\min A + \beta \geq \delta$. Moreover, ζ is the least element of C with $\min A + \zeta \geq \delta$. Hence, as in the proof of Lemma 7.2.3, we obtain $\alpha_0 = \min A$ and $\beta_0 = \zeta$.

In order to establish (7.2.2), we have to show that

$$ca^{<\alpha_0} + c^{<\beta_0}\left(a^{<\alpha_1} - a^{<\alpha_0}\right) = c^{<\zeta}a^{<\alpha_1}.$$

Indeed, since $a^{<\alpha_0} = a^{<\min A} = 0$, we obtain

$$ca^{<\alpha_0} + c^{<\beta_0}\left(a^{<\alpha_1} - a^{<\alpha_0}\right) = c^{<\beta_0}a^{<\alpha_1} = c^{<\zeta}a^{<\alpha_1}.$$

We have thus established that

$$1 = (ac)^{<\delta} = c'a^{<\alpha_1} + c^{<\beta_1}\left(a^{<\alpha_2} - a^{<\alpha_1}\right) + \ldots + c^{<\beta_n}\left(a - a^{<\alpha_n}\right).$$

Now

$$c^{<\zeta} = c' = \frac{1 - \left(c^{<\beta_1}(a^{<\alpha_2} - a^{<\alpha_1}) + \ldots + c^{<\beta_n}(a - a^{<\alpha_n})\right)}{a^{<\alpha_1}}$$

with $a^{<\alpha_1} \neq 0$, as $\alpha_1 > \min A$. Since $\zeta = \beta_0 > \ldots > \beta_n$, the right-hand side of that equation only uses strict truncations of c'. By assumption, we obtain $c' \in L$, giving us the required contradiction.

□

Lemma 7.2.5. *Let L be a truncation closed subfield of $k((G))$ and let $y \in k((G))$ such that any strict truncation of y belongs to L. Then also $L(y)$ is a truncation closed subfield of $k((G))$.*

Proof. This follows directly from Lemma 7.2.4: We have that $L(y)$ is a subfield of $k((G))$ that contains any truncation of y and any truncation of a for any $a \in L$. Hence, $L(y)$ also contains any truncation of $y \pm a$, ya, $\frac{a}{y}$ and $\frac{y}{a}$ (the later if respectively y and a are non-zero). Since any element in $L(y)$ can be obtained by a finite number of these operations (addition, subtraction, multiplication, fractions) using elements from L and y, we obtain that any truncation of any element of $L(y)$ is also contained in $L(y)$, as required. □

Using the lemmas established above, we can now show that $k(G)$ is truncation closed. In order to do so, let $\kappa = |G|$ and fix an enumeration of G, i.e. $\{g_\alpha \mid \alpha < \kappa\} = G$. Now k is a truncation closed subfield of $k(\!(G)\!)$. The only strict truncation of t^{g_0} equals 0 and is therefore contained in k. Hence, by Lemma 7.2.5, also $k(t^{g_0})$ is truncation closed.

Now let $\delta \leq \kappa$ such that $L = k(t^{g_\alpha} \mid \alpha < \delta)$ is truncation closed. As above, the only strict truncation of t^{g_δ} is 0 and thus also $L(t^{g_\delta}) = k(t^{g_\alpha} \mid \alpha \leq \delta)$ is truncation closed.

By transfinite induction, we obtain that $k(t^{g_\alpha} \mid \alpha < \kappa) = k(G)$ is truncation closed.

Step 3

So far, we have established that $k(G)$ is a common subfield of K and $k(\!(G)\!)$. Let R be the real closure of $k(G)$. Since both K and $k(\!(G)\!)$ are real closed, R is also a common subfield of K and $k(\!(G)\!)$ (see Theorem 4.1.38). We now establish that also R is truncation closed in $k(\!(G)\!)$.

Definition 7.2.6. Let $L \subseteq k(\!(G)\!)$ be a Hahn field and let $y \in k(\!(G)\!)$ be algebraic over L with $v(y) = 0$. We say that y satisfies **condition (H)** over L if there is some $p \in k\big(\big(G^{\geq 0}\big)\big)[X] \cap L[X]$ such that $p(y) = 0$ and $\overline{p}'(\overline{y}) \neq 0$.

Lemma 7.2.7. *Let $L \subseteq k(\!(G)\!)$ be a Hahn field and denote by L' the real closure of L in $k(\!(G)\!)$. Moreover, let $y \in L'$ with $v(y) = 0$. Then there are $d \in \mathbb{N}$ and $y_1, \ldots, y_d \in L'$ such that $y = y_1 + \ldots + y_d$ and for any $i \in \{1, \ldots, d\}$ condition (H) is satisfied by $x_i = \frac{y_i}{t^{v(y_i)}}$ over $L_i = L(y_1, \ldots, y_{i-1})$.*

Proof. First note that for each $i \in \{1, \ldots, d\}$ we have that x_i is algebraic over L and thus over L_i, and $v(x_i) = 0$. Now let $q \in L[X]$ be the minimal polynomial of y over L. Set

$$q(X) = \sum_{i=0}^{\ell} q_i X^i$$

and let $g = \min\{v(q_0), \ldots, v(q_\ell)\}$. Note that since $q_\ell = 1$, we have $g \leq 0$. Let

$$p(X) = \frac{q(X)}{t^g} \in k\big(\big(G^{\geq 0}\big)\big)[X] \cap L[X].$$

Then $p(y) = 0$ and $\overline{p} \neq 0$. Moreover, y is a simple root of p. If $\overline{p}'(\overline{y}) \neq 0$, then we are done by setting $d = 1$ and $y_1 = y$.

Otherwise, let $m \in \mathbb{N}$ be the multiplicity of $\overline{y}$ in $\overline{p}$. Then the $(m-1)$-th formal derivative $r = p^{(m-1)}$ of p has the property $\overline{r}(\overline{y}) = 0$ and $\overline{r}'(\overline{y}) \neq 0$. Since (L', v) is henselian, there is some $y_1 \in L' \cap k\big(\big(G^{\geq 0}\big)\big)$ such that $\overline{y_1} = \overline{y}$ and $r(y_1) = 0$. Hence, y_1 satisfies condition (H) over L, and so does $x_1 = y_1$.

Let $z_1 = y - y_1$. Note that $r(y) = p^{(m-1)}(y) \neq 0$, as y is a simple root of p, and thus $y \neq y_1$. Hence, $\delta = v(z_1) \in G^{>0}$. Let $z_1' = \frac{z_1}{t^\delta}$. Then $v(z_1') = 0$ and z_1' is a root of

$$s(X) = p(t^\delta X + y_1) \in k\big(\big(G^{\geq 0}\big)\big)[X] \cap L(y_1)[X].$$

Setting $a = t^\delta X$ and $b = y_1$ and denoting the j-th formal derivative of p by $p^{(j)}$, we obtain

$$\begin{aligned} s(X) &= p(a+b) \\ &= \sum_{j=0}^{\ell} \frac{a^j p^{(j)}(b)}{j!} \\ &= \sum_{j=0}^{\ell} \frac{t^{j\delta} X^j p^{(j)}(y_1)}{j!}. \end{aligned}$$

Let $s_j = \frac{t^{j\delta} p^{(j)}(y_1)}{j!}$ for any $j \in \{0, \ldots, \ell\}$. Set $h = \min\{v(s_0), \ldots, v(s_\ell)\}$ and

$$u(X) = \sum_{j=0}^{\ell} u_j X^j = \frac{s(X)}{t^h} \in k\big(\big(G^{\geq 0}\big)\big)[X] \cap L(y_1)[X].$$

As $\overline{p}^{(m)}(\overline{y}) \neq 0$, we have

$$v\Big(p^{(m)}(y_1)\Big) = 0$$

and thus

$$v(s_m) = m\delta + v\Big(p^{(m)}(y_1)\Big) = m\delta.$$

Hence, $h \leq m\delta$. Since $r(y_1) = p^{(m-1)}(y_1) = 0$, we have $s_{m-1} = u_{m-1} = 0$. For $j > m$, we have

$$v(s_j) = j\delta + v\Big(p^{(j)}(y_1)\Big) \geq j\delta > m\delta.$$

As a result, we obtain

$$\overline{u}(X) = \overline{u_0} + \overline{u_1} X + \ldots + \overline{u_{m-2}} X^{m-2} + \overline{u_m} X^m.$$

Hence, $\overline{u}$ does not have a non-zero root of multiplicity m. Now $u(z_1') = s(z_1') = 0$, whence $\overline{u}(\overline{z_1'}) = 0$. Thus, $\overline{z_1'}$ must have a multiplicity strictly less than m in $\overline{u}$.

If the multiplicity of $\overline{z_1'}$ in $\overline{u}$ equals 1, then $\overline{u}'(\overline{z_1'}) \neq 0$. Hence, z_1' satisfies condition (H) over $L(y_1)$. We can then set $d = 2$, $y_2 = z_1$ (as then $y = y_1 + z_1 = y_1 + y_2$) and $x_2 = z_1'$ to complete the proof.

Otherwise, it remains to express z_1' as

$$z_1' = y_2' + \ldots + y_d'$$

with $y_i' = \frac{y_i}{t^\delta}$, where the y_i' have the property that $\frac{y_i'}{t^{v(y_i')}}$ satisfies condition (H) over

$$L(y_1)(y_2', \ldots, y_{i-1}').$$

Indeed, then

$$y = y_1 + z_1 = y_1 + t^\delta z_1' = y_1 + y_2 + \ldots + y_d,$$

and for any i we have $L(y_i) = L(y_i')$ and $x_i = \frac{y_i}{t^{v(y_i)}} = \frac{y_i'}{t^{v(y_i')}}$. In order to obtain those y_i', we may iteratively repeat the argument above, starting with $L(y_1)$ instead of L as well as z_1' instead of y and the minimal polynomial of z_1' (dividing u) instead of q instead of q. Since the multiplicity of the root of the residue polynomial decreases in each iteration, this procedure terminates in less than m steps. □

Lemma 7.2.8. *Let $L \subseteq k(\!(G)\!)$ be a truncation closed Hahn field and denote by L' the real closure of L in $k(\!(G)\!)$. Moreover, let $y \in L' \setminus L$ satisfy condition (H) over L. Then*

$$I = \{v(y-z) \mid z \in L\}$$

is an initial segment of G closed under addition.

Proof. We first show that I is an initial segment of G. Let $y = \sum_{i<\alpha} y_i t^{g_i}$ in order type notation. Since $v(y) = 0$, we have $g_0 = 0$. Thus, for any $g \in G^{\leq 0}$,

$$I \ni v(y + y_0 t^g) = g,$$

as $-y_0 t^g \in L$. This shows that $G^{\leq 0} \subseteq I$. Now let $h, h' \in G$ with $h' < h$ and $h \in I$. Let $z \in L$ with $v(y-z) = h$. Then also $z' = z + t^{h'} \in L$ and

$$I \ni v(y - z') = v((y-z) - t^{h'}) = h',$$

as required.

The proof that G is closed under addition is postponed to the end, if time permits. □

Lemma 7.2.9. *Let L be a truncation closed Hahn subfield of $k(\!(G)\!)$ and denote by L' the real closure of L in $k(\!(G)\!)$. Moreover, let $y \in L'$ satisfy condition (H) over L, and let $p(X) = \sum_{i=0}^n p_i X^i \in k\big(\big(G^{\geq 0}\big)\big)[X] \cap L[X]$ with $p(y) = 0$ and $\overline{p}'(\overline{y}) \neq 0$. Let y' be a truncation of y and let G_0 be the smallest convex subgroup of G containing* $\operatorname{supp}(y')$*. For any $s \in k(\!(G)\!)$, denote by $s^{<G_0}$ the largest truncation of s whose support is contained in G_0.*[20] *Then the following hold:*

(i) Let

$$p^{<G_0}(X) = \sum_{i=0}^n p_i^{<G_0} X^i.$$

If $y' = y^{<G_0}$, then $p^{<G_0}$ is a non-zero polynomial in $L[X]$ and $p^{<G_0}(y') = 0$. Hence, $y' \in L'$.

(ii) If $y' \neq y^{<G_0}$, then y' lies in the field extension of L generated by all strict truncations of y'.

Proof. (i) First note that $p^{<G_0}$ is contained in $L[X]$ as L is truncation closed. At least one coefficient of p has valuation 0 and thus $p^{<G_0}$ is non-zero. Let $r = \sum_{i=0}^n r_i X^i \in L[X]$ with

$$p = p^{<G_0} + r.$$

By the choice of the coefficients of $p^{<G_0}$, we have $v(r_i) > G_0$ for any $i \in \{0, \dots, n\}$. Hence,

$$v(r(y)) \geq \min\{v(r_0), \dots, v(r_n)\} > G_0.$$

[20] In other words, let A be the largest initial segment of $\operatorname{supp}(s)$ contained in G_0 and let $s^{<G_0}$ be the truncation of s whose support equals A. If such A does not exist, then $s^{<G_0} = 0$.

Moreover,

$$p^{<G_0}(y) = p^{<G_0}(y' + (y - y')) = p^{<G_0}(y') + \underbrace{\sum_{j=1}^{n} \frac{(y - y')^j (p^{<G_0})^{(j)}(y')}{j!}}_{=:T}.$$

Since $v(y - y') > G_0$ and $v\big((p^{<G_0})^{(j)}(y')\big) \geq 0$ for any $j \in \{1, \ldots, n\}$, we obtain that $v(T) > G_0$. As a result,

$$0 = p(y) = p^{<G_0}(y) + r(y) = p^{<G_0}(y') + T + r(y).$$

Since G_0 is a group containing the support of all coefficients of $p^{<G_0}$ as well as the support of $y' = y^{<G_0}$, we obtain that also $\operatorname{supp}(p^{<G_0}(y')) \subseteq G_0$. Since $v(T + r(y)) > G_0$, we obtain

$$v(p^{<G_0}(y')) = v(-p^{<G_0}(y')) = v(T + r(y)) > G_0,$$

leaving $p^{<G_0}(y') = 0$ as the only possibility.

(ii) In this case, y' is a strict truncation of $y^{<G_0}$. Let F be the field extension of L generated by all strict truncations of y'. Set $\beta = v(y^{<G_0} - y') \in G_0$. Since L is truncation closed, we obtain by Lemma 7.2.5 that F is the union of a chain of truncation closed fields and thus also truncation closed. If $y \in F$, then also $y' \in F$.

Suppose that $y \notin F$. Since the real closure of F contains L' and y satisfies condition (H) over F, we obtain by Lemma 7.2.8 that

$$I = \{v(y - z) \mid z \in F\}$$

is an initial segment of G closed under addition.

For any $\alpha \in \operatorname{supp}(y')$, we have

$$\alpha = v\big(y - (y')^{<\alpha}\big) \in I,$$

as $(y')^{<\alpha} \in F$. Hence, $\operatorname{supp}(y') \subseteq I$. Since I is closed under addition, we obtain $G_0 \subseteq I$. Hence, $\beta \in I$. Let $z \in F$ with $v(y - z) = \beta$. Then

$$v(y' - z) \geq \min\{v(y' - y), v(y - z)\} = \beta.$$

But $\operatorname{supp}(y') < \beta$, implying that y' is a truncation of z. Since $z \in F$ and F is truncation closed, we obtain $y' \in F$, as required.

□

The following proposition now establishes that R is truncation closed in $k((G))$, as required.

Proposition 7.2.10. *Let $L \subseteq k((G))$ be a truncation closed Hahn subfield. Then also the real closure L' of L in $k((G))$ is truncation closed.*

Proof. Let $z \in L'$. We may assume that $v(z) = 0$, as otherwise we may replace z by $\frac{z}{t^{v(z)}}$. By Lemma 7.2.7 there are $d \in \mathbb{N}$ and $y_1, \ldots, y_d \in L'$ such that $z = y_1 + \ldots + y_d$ and for any $i \in \{1, \ldots, d\}$ condition (H) is satisfied by $x_i = \frac{y_i}{t^{v(y_i)}}$ over $L_i = L(y_1, \ldots, y_{i-1})$.

Let $i \in \{1, \ldots, d\}$. Assume that there is a smallest $h \in \operatorname{supp}(x_i)$ such that $x_i' = x_i^{<h}$ is not contained in L'. By Lemma 7.2.9, either x_i' lies in the real closure L' of L_i or x_i' lies in the field extension of L_i generated by all strict truncations of x_i'. Since all strict truncations of x_i' are contained in L', we obtain in either case $x_i' \in L'$, a contradiction. Hence, all truncations of x_i and thus also all truncations of y_i lie in L'.

We have thus shown that all truncations of $y_1, \ldots, y_d$ lie in L'. Since $z = y_1 + \ldots + y_d$, also all truncations of z lie in L', as required. □

Step 4

We have already established that the real closure R of $k(G)$ is a common subfield of K and $k((G))$. This serves as the base case for the transfinite induction we perform in this step. This will also complete the construction of the truncation closed embedding of K into $k((G))$.

Lemma 7.2.11. *Let L be a common real closed subfield of K and $k((G))$ with $k(G) \subseteq L$. Suppose that L is truncation closed in $k((G))$. Let $y \in K \setminus L$ and denote by L' the real closure of $L(y)$ in K. Then there is an embedding $f\colon (L', <) \hookrightarrow (k((G)), <)$ such that $f|_L = \mathrm{id}_L$, for any $a \in L'$ we have $v(a) = v(f(a))$ and $f(L')$ is truncation closed in $k((G))$.*

Proof. We first show that if the embedding f with $f|_L = \mathrm{id}_L$ has been found, then for any $a \in L'$ we have $v(a) = v(f(a))$. Let $a \in L'$. If $a \in L$, then $v(f(a)) = v(\mathrm{id}_L(a)) = v(a)$. Otherwise, assume, for a contradiction, that $v(a) < v(f(a))$. (The case $v(a) > v(f(a))$ leads to a similar contradiction.) We may assume that $a > 0$, as otherwise we can replace it by $-a$. Let $g \in G$ with $v(a) < g < v(f(a))$. We can choose such g, as G is divisible and thus densely ordered. Now $a > t^g$. Since L is a Hahn field, we have $t^g \in L$ and thus, by applying f, we obtain $f(a) > t^g$. However, this shows that $v(f(a)) \leq g$, a contradiction.

Let $a = \sum_{i<\alpha} a_i t^{h_i} \in L$ (in order type notation). We will say that a is a development at order α of y if for any $i < \alpha$ we have

$$v(y - a) > h_i.$$

We first show inductively that for any $n \in \omega$ the element y has a development $a^{(n)} = \sum_{i<n} y_i t^{g_i}$ at order n. Set $g_0 = v(y) \in G$ and $y_0 = \overline{yt^{-g_0}} \in k$. Then

$$v\Big(y - a^{(1)}\Big) = v(y - y_0 t^{g_0}) > g_0,$$

as

$$0 < v(yt^{-g_0} - y_0) = v(y - y_0 t^{g_0}) - g_0.$$

Now suppose that for some $n \in \omega$, we already have that $a^{(n)}$ is a development at order n of y. Let $y' = y - a^{(n)}$. Set $g_n = v(y') \in G$ and $y_n = \overline{yt^{-g_n}} \in k$. As above, we obtain for any $i < n+1$ that

$$v\Big(y - a^{(n+1)}\Big) = v(y' - y_n t^{g_n}) > g_n \geq g_i,$$

completing the induction.

Let $S \subseteq L$ denote the set of all developments of y. Arguing as in the induction above, one can show that if S contains a development at order α of y, then it also contains a development at order $\alpha + 1$ of y. We show that S is linearly ordered by the relation "strict truncation of". Let $a = \sum_{i<\alpha} a_i t^{h_i} \in L$ and $b = \sum_{i<\beta} b_i t^{j_i} \in L$ be developments at order α, respectively β, of y. Suppose that $\alpha < \beta$. We verify that a is a truncation of b. First note that for any $i < \alpha$ we have

$$v(a-b) = v((a-y)-(b-y)) \geq \min\{v(a-y), v(b-y)\} \geq \min\{h_i, j_i\}.$$

Assume, for a contradiction, that there is some least $i < \alpha$ such that $a_i t^{h_i} \neq b_i t^{j_i}$. If $i+1 < \alpha$, then

$$v(a-b) \geq \min\{h_{i+1}, j_{i+1}\} > \min\{h_i, j_i\} = v(a-b),$$

a contradiction. If $i + 1 = \alpha$, then

$$a = \sum_{\ell<i} b_\ell t^{j_\ell} + a_i t^{h_i}$$

and

$$b - a = -a_i t^{h_i} + \sum_{i\leq\ell<\beta} b_\ell t^{j_\ell}.$$

Hence,

$$j_{i+1} < v(y-b) = v((y-a)+(a-b)) = \min\{\underbrace{v(y-a)}_{>h_i}, \underbrace{v(a-b)}_{=\min\{h_i,j_i\}}\} = \min\{h_i, j_i\} \leq j_i,$$

if $i + 1 < \beta$, also a contradiction. Otherwise, $\alpha = \beta$ and

$$b - a = -a_i t^{h_i} + b_i t^{j_i} \neq 0.$$

If $j_i < h_i$, then as above $v(y-b) = j_i$, and if $h_i < j_i$ likewise $v(y-a) = h_i$, both being contradictions to the choice of a and b. Hence, $j_i = h_i$ and

$$b - a = (b_i - a_i)t^{j_i}.$$

Then

$$j_i < v(y-a) = v((y-b) + (b_i - a_i)t^{j_i}) = j_i,$$

as $v(y-b) > j_i$, giving us the final contradiction.

Now let $f(y) \in k(\!(G)\!)$ be the element with smallest support such that all strict truncations of $f(y)$ lie in S. This choice is possible, as the union of all supports of elements in S is well-ordered and we may simply set $f(y)(g) = s(g)$ for any $s \in S$ and any $g \in G$. As observed above, the set of order types of supports of elements in S is closed under taking successors. Hence, S does not have a maximum and $f(y)$ does not lie in S. If $f(y)$ were an element of L, then it would be a development of y. However, since this is not the case, we obtain $f(y) \notin L$. In particular, both y and $f(y)$ are transcendental over L. We now show that $(L(y), <)$ and $(L(f(y)), <)$ are $\mathcal{L}_{\mathrm{or}}$-isomorphic. It suffices to show that for any $z \in L$ we have $z < y$ if and only if $z < f(y)$.

Note that $v(y - f(y)) > g_0 = v(y)$. Thus, $v(f(y)) = v(y)$. Moreover, we have $f(y) > 0$ if and only if $y_0 > 0$, and the latter holds if and only if $y > 0$. Let $z \in L$. If z and $f(y)$ have opposite

signs, then it is easy to show that $z < y$ if and only if $z < f(y)$, as $f(y) > 0$ if and only if $y > 0$. Likewise, if $v(z) \neq v(f(y)) = v(y)$, then we also obtain $z < y$ if and only if $z < f(y)$. Hence, suppose that $v(z) = v(f(y))$.

We show that if $z < y$, then $z < f(y)$. (To show that from $y < z$ it follows that $f(y) < z$ one can argue similarly.) Let $a \in k^{>0}$ and $\alpha \in G$ with

$$y - z = at^\alpha + y'$$

with $v(y') > \alpha = v(y - z)$. Let

$$z' = z^{\leq \alpha} + at^\alpha.$$

Since L is a truncation closed Hahn field, we have $z' \in L$. Moreover, z' is the development of y at order α. Indeed,

$$v(y - z') = v\big(y - z^{\leq\alpha} - at^\alpha\big) = v\big(-z^{\leq\alpha} + z + y'\big) = v\big(-z^{>\alpha} + y'\big) > \alpha \geq h$$

for any $h \in \operatorname{supp}(z')$. We have

$$z < z^{\leq\alpha} + \frac{a}{2}t^\alpha < z' + s$$

for any $s \in L$ with $v(s) > \alpha$. Since $z' \in S$, we obtain, in particular, that z is strictly smaller than any element in S of which z' is a truncation. This implies that $z < f(z)$, as required.

Since $(L(y), <)$ and $(L(f(y)), <)$ are $\mathcal{L}_{\mathrm{or}}$-isomorphic via an isomorphism extending f, we may extend f also to an $\mathcal{L}_{\mathrm{or}}$-isomorphism of $(L', <)$ to $(H, <) \subseteq (k(\!(G)\!), <)$, where H is the real closure of $L(f(y))$ in $k(\!(G)\!)$. Since L is truncation closed and contains al strict truncations of $f(y)$, we obtain by Lemma 7.2.5 that also $L(f(y))$ is truncation closed. By application of Proposition 7.2.10, we also obtain that H is truncation closed. Hence, f is an $\mathcal{L}_{\mathrm{or}}$-embedding of L' into $k(\!(G)\!)$ whose image $H = f(L')$ is truncation closed, as required. □

Let $\kappa = |K|$ and fix an enumeration $\{y_\alpha \mid \alpha < \kappa\}$ of K. First let $\alpha_0 \in \kappa$ be least such that $y_{\alpha_0} \notin R$. By Lemma 7.2.11, there is a truncation closed embedding f_{α_0} over R from the real closure of $R(y_{\alpha_0})$ in K into $k(\!(G)\!)$ that preserves the valuation. We may thus identify $R_{\alpha_0} = R(y_{\alpha_0})$ with its image in $k(\!(G)\!)$ under f_{α_0} and regard R_{α_0} as a common subfield of K and $k(\!(G)\!)$ truncation closed in the latter. Moreover, we set $R_\alpha = R_{\alpha_0}$ for any $\alpha < \alpha_0$.

Now let $\alpha < \kappa$ such that a chain of common subfields of K and $k(\!(G)\!)$ truncation closed in the latter $\{R_\beta \mid \beta < \alpha\}$ has already been established such that $y_\beta \in R_\beta$ for any $\beta < \alpha$. Set

$$R'_\alpha = \bigcup_{\beta<\alpha} R_\alpha.$$

If $y_\alpha \in R'_\alpha$, then simply set $R_\alpha = R'_\alpha$. Otherwise, let R_α be the real closure of $R'_\alpha(y_\alpha)$ in K and proceed as above, noting that R'_α is a truncation closed subfield of $k(\!(G)\!)$.

By transfinite induction, we obtain a common truncation closed subfield R_κ of K and $k(\!(G)\!)$ such that

$$K = \{y_\alpha \mid \alpha < \kappa\} \subseteq R_\kappa.$$

Hence, K can be regarded (via the isomorphisms constructed above) a truncation closed subfield of $k(\!(G)\!)$.

7.3. Models of Open Induction

By Shepherdson's Theorem and the construction of the truncation closed embedding for the Mourgues–Ressayre Theorem, if there is some real closed archimedean ordered field $(k, <)$, some ordered abelian group G and some real closed truncation closed Hahn field $K \subseteq k((G))$ such that an $\mathcal{L}_{\text{or}}$-structure $(Z, <)$ is $\mathcal{L}_{\text{or}}$-isomorphic to

$$\left\{a \in K \mid \operatorname{supp}(a) \subseteq G^{\leq 0} \text{ and } a_0 \in \mathbb{Z}\right\} = \left(k\left(\left(G^{<0}\right)\right) \cap K\right) + \mathbb{Z},$$

then $(Z, <)$ is a model of IOpen'. However, not all integer parts of K must be of the form above. Hence, there may be models of Open Induction which are not obtained by pullbacks of integer parts of truncation closed real closed Hahn fields.

In this section, we re-visit two number theoretic results provable in PA. We will establish that they are not provable in the weaker fragment of arithmetic IOpen.

7.3.1. Irrationality of $\sqrt{2}$

Let $K = \mathbb{R}((\mathbb{Q}))$. Then K is real closed and thus

$$Z = \mathbb{R}\left(\left(\mathbb{Q}^{<0}\right)\right) + \mathbb{Z}$$

is a model of IOpen'. Consider $M_Z = Z^{\geq 0} \models \mathrm{IOpen}$. Set

$$m = \sqrt{2}t^{-1} \in M_Z \text{ and } n = t^{-1} \in M_Z.$$

Then

$$m^2 = 2t^{-2} = 2n^2.$$

We have thus established the following.

Proposition 7.3.1. $\mathrm{IOpen} \not\models \neg\exists m \exists (n \neq 0)\ m^2 = 2n^2$.

We use the observations above to present a real closed field with two integer parts that are not elementarily equivalent and thus, in particular, not isomorphic.

Example 7.3.2. Let $(M, <) \models \mathrm{PA}$ be non-standard. Let R be the real closure of Q_{Z_M} (i.e. the field of fractions of $Z_M = M \cup (-M)$). Then Z_M is an integer part of R. Note that R is non-archimedean. Moreover, its residue field $k = \overline{R}$ is real closed and its value group $G = vR$ is divisible.

Fix a truncation closed embedding $k(G) \subseteq R \subseteq k((G))$. Since k is real closed, we have $\sqrt{2} \in k$. Now as above, we can let $g \in G^{<0}$ be arbitrary and set

$$m = \sqrt{2}t^{-g} \text{ and } n = t^{-g}.$$

Then

$$m^2 = 2n^2.$$

Hence, for the integer part $Z' = k\left(\left(G^{<0}\right)\right) + \mathbb{Z}$ of R we have that $M_{Z'} \not\models \mathrm{PA}$, as PA proves that $\sqrt{2}$ is irrational. In particular, M and $M_{Z'}$ are not isomorphic als $\mathcal{L}_{\text{PA}}$-structures and thus Z_M and Z' are not isomorphic as $\mathcal{L}_{\text{or}}$-structures.

This shows that R is a real closed field with two non-isomorphic integer parts.

7.3.2. Euclid's Theorem

Recall that Euclid's Theorem over PA states that the set of prime numbers is unbounded (see Proposition 3.1.18). In the proof of Corollary 3.1.15 it was shown that any prime is irreducible: the argument used there works also within IOpen instead of PA. We show that IOpen does not suffice to prove Euclid's Theorem.

Proposition 7.3.3. IOpen $\not\models \forall n \exists (m > n)\ \mathrm{pr}(m)$.

In order to do so, we find a model M_Z of IOpen satisfying

$$\exists n \forall (m > n)\ \neg \mathrm{irr}(m).$$

In particular, we then obtain

$$\exists n \forall (m > n)\ \neg \mathrm{pr}(m).$$

Recall from Example 7.1.12 that the field of Puiseux series $K = \mathbb{R}\langle\langle t \rangle\rangle$ is real closed. Since K is a Rayner field, it is, in particular, a truncation closed Hahn subfield of $\mathbb{R}(\!(\mathbb{Q})\!)$. We thus obtain that

$$Z = \left(\mathbb{R}\left(\left(\mathbb{Q}^{<0}\right)\right) \cap K\right) + \mathbb{Z}$$

is an integer part of K. Hence by Shepherdson's Theorem, $M_Z = Z^{\geq 0} \models$ IOpen. We show that the irreducible elements of M_Z are exactly the standard prime numbers in $\mathbb{N} \subseteq M_Z$. Then

$$M_Z \models \forall (m > t^{-1})\ \neg \mathrm{irr}(m),$$

as required.

Let

$$a = \sum_{i=0}^{m} a_i t^{-\frac{i}{n}} \in M_Z,$$

where $n \in \mathbb{N}$ and $a_0 \in \mathbb{Z}$. If $a = 0$, then it is not irreducible. If $a_0 = 0$ and $a \neq 0$, then

$$a = t^{-\frac{1}{2n}} \cdot \sum_{i=1}^{m} a_i t^{-\frac{2i-1}{2n}},$$

where both factors lie in $M_Z \setminus \{1, 0\}$. Thus, a is not irreducible.

Suppose that $a \neq 0$ and $a_0 \neq 0$. If $m = 0$, then $a \in \mathbb{N}$. Since the product of two non-constant elements in M_Z (i.e. elements in $M_Z \setminus \omega$) is also non-constant, we have that a is irreducible in M_Z if and only if it is irreducible in $\mathbb{N}$. Now suppose that $m \geq 1$. Set

$$s = t^{-\frac{1}{3n}}.$$

Then

$$a = \sum_{i=0}^{m} a_i \left(t^{-\frac{1}{3n}}\right)^{3i} = \sum_{i=0}^{m} a_i s^{3i} \in \mathbb{R}[s].$$

Hence, a is a polynomial in $\mathbb{R}[s]$ of degree at least 3 and therefore reducible. We may factorise it as

$$a = a_m \prod_{i=1}^{u} (s + b_i) \prod_{j=1}^{w} (s^2 + c_j s + d_j)$$

with all $b_i, c_j, d_j \in \mathbb{R}$. Since $a_0 \in \mathbb{N}$, we obtain

$$a_m \prod_{i=1}^{u} b_i \prod_{j=1}^{w} d_j \in \mathbb{N}.$$

Hence,

$$\begin{aligned} a &= a_m \prod_{i=1}^{u} \left[\left(\frac{s}{b_i} + 1 \right) b_i \right] \prod_{j=1}^{w} \left[\left(\frac{s^2}{d_j} + \frac{c_j s}{d_j} s + 1 \right) d_j \right] \\ &= a_0 \prod_{i=1}^{u} \left(\frac{s}{b_i} + 1 \right) \prod_{j=1}^{w} \left(\frac{s^2}{d_j} + \frac{c_j s}{d_j} + 1 \right) \\ &= a_0 \prod_{i=1}^{u} \left(\frac{t^{-\frac{1}{3n}}}{b_i} + 1 \right) \prod_{j=1}^{w} \left(\frac{t^{-\frac{2}{3n}}}{d_j} + \frac{c_j t^{-\frac{1}{3n}}}{d_j} + 1 \right), \end{aligned}$$

where the last expression is a product of elements of Z and thus also lies in Z. By adjusting the signs, we obtain a non-trivial factorisation of a into elements of M_Z. Hence, a is not irreducible, as required.

A. Appendix

A.1. Abbreviations within Formulas

Let $\mathcal{L}$ be a language.

- If f is a binary function symbol of $\mathcal{L}$ and t_1 as well as t_2 are $\mathcal{L}$-terms, then the infix notation

  $$(t_1\ f\ t_2)$$

  stands for the prefix notation of the term $f(t_1, t_2)$. In many cases, brackets of infix notations are omitted. This happens, for example, if another function symbol g is applied (e.g. $\exp(0+1)$ rather than $\exp((0+1))$ in the language $\mathcal{L}_{\exp}$), if the brackets are the outermost brackets of the term (e.g. $1+1 < (1+0)\cdot 1$ rather than $(1+1) < ((1+0)\cdot 1)$ in the language $\mathcal{L}_{\mathrm{or}}$), if the usual interpretation of the binary relation is associative (e.g. $1+0+1+1$ rather than $((1+0)+(1+1))$ in the language $\mathcal{L}_{\mathrm{semr}}$) or if the usual interpretation of the binary relation has a natural order of brackets (e.g. $1+1\cdot 0$ rather than $(1+(1\cdot 0))$).

- For binary relations symbols R and S and $\mathcal{L}$-terms t_1, t_2, t_3, we write

  $$t_1\ R\ t_2\ S\ t_3$$

  for

  $$t_1\ R\ t_2 \wedge t_2\ S\ t_3.$$

  Similar abbreviations are used for longer chains of relations.

- If $-$ is a binary relation symbol of $\mathcal{L}$ and 0 is a constant symbol of $\mathcal{L}$, then for any $\mathcal{L}$-term t, we denote by $-t$ the $\mathcal{L}$-term $0 - t$.

Bibliography

[1] S. Basu, R. Pollack and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, Algorithms Comput. Math. 10, 2nd edn (Springer, Berlin, 2006), doi:10.1007/3-540-33099-2.

[2] A. J. Engler and A. Prestel, *Valued Fields*, Springer Monogr. Math. (Springer, Berlin, 2005), doi:10.1007/3-540-30035-X.

[3] R. Kaye, *Models of Peano Arithmetic*, Oxford Logic Guides 15 (Oxford Sci. Publ., Oxford Univ. Press, New York, 1991).

[4] J. Kirby, *An Invitation to Model Theory* (Cambridge Univ. Press, Cambridge, 2019), doi:10.1017/9781316683002.

[5] L. S. Krapp, M. Serra and S. Kuhlmann, 'On Rayner structures', *Comm. Algebra* 50 (2022) 940–948, doi:10.1080/00927872.2021.1976789.

[6] S. Kuhlmann, *Ordered Exponential Fields*, Fields Inst. Monogr. 12 (Amer. Math. Soc., Providence, RI, 2000), doi:10.1090/fim/012.

[7] D. Marker, *Model Theory: An Introduction*, Grad. Texts in Math. 217 (Springer, New York, 2002), doi:10.1007/b98860.

[8] M. H. Mourgues and J. P. Ressayre, 'Every real closed field has an integer part', *J. Symb. Log.* 58 (1993) 641–647, doi:10.2307/2275224.

[9] J. C. Shepherdson, 'A Non-standard Model for a Free Variable Fragment of Number Theory', *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* 12 (1964) 79–86.

Index

IOpen, 24
$\mathcal{I}_v$, 79
$\overline{K}$, 79
$\mathcal{O}_v$, 79
PA, 23

arity, 5
atomic, 10
automorphism, 7
axiom, 21
axiomatisation, 21

bounded variable, 11
Bézout's Lemma, 28

cardinal number, 71
Cauchy index, 40
closed term, 9
complete theory, 19
condition (H), 93
constant symbol, 5
cut, 25

deductive closure, 19
definable, 14
disjunctive normal form, 49
divisible group, 86
domain, 5

elementary equivalence, 20
embedding, 7
equivalent formulas, 20
Euclid's Theorem, 30
Euclidean Division, 31
Euclidean Divison, 27
existential formula, 17
expansion, 7
extension, 8

formal derivative, 39
formally real field, 33
formula, 10
free variable, 11
function symbol, 5

generalised power series, 72

Hahn field, 77
Hahn series, 72
henselian, 82
homomorphism, 7
hull, 73

induction
    scheme, 24
infix notation, 9
initial segment, 25
integer part, 2, 62
intepretation, 5
intermediate value property, 37
interpretation, 9
isomorphism, 7

jump, 40

language, 5
language of ordered rings, 5
leading monomial, 39
least element, 26
Least Number Principle, 26
limit ordinal, 70
linear order, 21
linear ordering, 6

model, 12, 13

Model Theory, 13
model theory, 5
Mourgues–Ressayre, Theorem of, 90

natural valuation, 81
Neumann's Lemma, 75
non-standard, 25

o-minimal, 58
Open Induction, 31
open induction, 61
order type, 71, 73
ordered exponential field, 6
ordered group, 6
ordinal number, 69
Overspill, 26

Peano Arithmetic, 1, 23
power series, 72
prefix notation, 9
prenex normal form, 17

quantifier elimination, 20
quantifier-free, 17

Rayner field, 74
real algebra, 33
real closed, 35
real closed field, 1, 33
real closure, 38
real closures, 35
real field, 33
recursive definition, 9
reduct, 7
relation symbol, 5
remainder, 43
residue
    field, 79

satisfiable, 19
scope, 11
semiring, 6
sentence, 12
Shepherdson's Theorem, 63
sign, 39
sign variation, 42
signed remainder sequence, 43
standard part, 25
structure, 5
Sturm sequence, 47
Sturm's Theorem, 46
subformula, 10
substructure, 8
successor ordinal, 70
sums of squares, 33
support, 72

Tarski query, 40
Tarski's Theorem, 46
term, 9
theory, 19
    of dense linear orders without endpoints, 21
Transfinite Induction, 72
truncation, 88
truncation closed, 88

universal formula, 17

valuation
    ideal, 79
    on a field, 78
    ring, 79
value
    group, 79
valued
    field, 79

well-ordered, 67
Well-ordering Theorem, 71