UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

Some examples of quantifier elimination and o-minimality

Ricardo Shimura

Mestrado em Matemática

Dissertação orientada por:

Professor Doutor Mário Jorge Edmundo

2021

Acknowledgements

I thank my advisor for the patience in guiding this dissertation and incentive in pursuing a PhD.
I thank Clara for the constant support.
I also want to express my gratitude to Milestone Consulting for the granted award in 2020.

Abstract

A structure with a total order that is dense without end-points is o-minimal if every definable set in dimension 1 is a finite union of intervals and points. This notion materialized from observations that many of the proprieties of semialgebraic sets were deduced from very simple axioms, the ones that now define o-minimal structures. Indeed, o-minimality establishes strong regularity results of the definable sets. In this way, o-minimality can be viewed as a candidate to "topologie modérée" mentioned by Grothendieck in his Esquisse d'un programme.

In the context of this dissertation, despite of its intrinsic richness, we study the property of quantifier elimination (abbreviated QE) as a way of proving o-minimality of a given structure.

The goal of this dissertation was to study proofs of o-minimality and QE by studying a concrete example, the real closed ordered fields (abbreviated rcof).

In Chapter 1, we begin by defining basic notions of first-order logic. We present some examples that will be useful later, such as the theory of rcof. We alude to the usefulness of different axiomatizations, such as the universal axiomatization, and simplifications of formulas, such as QE, that make the theories much more easier to understand. We present some criterias for a theory to admit QE. We present a geometrical perspective of the definable sets in general and the special case of o-minimality.

In Chapter 2 we prove that the theory of rcof has QE. As a consequence we prove that every rcof is o-minimal.

In Chapter 3 we study proprieties of o-minimal structures.

In Chapter 4 we study the theory T_{an} of rcof with restricted analytic functions. We state that T_{an} has QE in the language $\mathcal{L}_{an}(^{-1})$ and as a consequence we show that T_{an} admits an universal axiomatization in the language $\mathcal{L}_{an}(^{-1}, (\sqrt[n]{\ })_{n=2,3,\ldots})$.

In Chapter 5 we establish the result that every model of T_{an} can be seen as a substructure of a power series field $\mathbb{R}((t^{\Gamma}))$. We use this fact to deduce key results concerning valuations on these structures and use these to prove that $T_{an}(\exp)$ admits QE and universal axiomatization, both in the language $\mathcal{L}_{an}(\exp, \log)$. In the last section of this chapter we begin by noting that, provided the theory admits QE, o-minimality is equivalent to regularity of the signal (whether it is greater, less or equal to zero) "at infinity" of the definable functions in one variable. This leads us to consider Hardy fields and using properties from these fields we prove that $T_{an}(\exp)$ is o-minimal.

Keywords: o-minimality, quantifier elimination, universal axiomatization, real closed ordered fields, restricted analytic fields

Resumo

Diz-se que uma estrutura com uma ordem total, densa e sem extemidades, é o-minimal se qualquer conjunto definível em dimensão 1 é união finita de intervalos e pontos. Esta noção tem origem na observação de que muitas das propriedades dos conjuntos semialgébricos são deduzidas de axiomas muito simples, essencialmente os axiomas que definem as estruturas o-minimais. De facto, a o-minimalidade permite estabelecer resultados muito fortes quanto à regularidade dos conjuntos definíveis. Deste modo, a o-minimalidade pode ser vista como um candidato à “topologie modérée” mencionada por Grothendieck no seu Esquisse d'un programme.

No contexto desta dissertação, não obstante a sua importância intrínseca, estudamos a propriedade da eliminação de quantificadores como uma das vias para provar a o-minimalidade duma estrutura.

O objectivo desta dissertação consiste em estudar provas de o-minimalidade e eliminação de quantificadores através do estudo dos corpos ordenados reais fechados (abreviado rcof).

Acompanhámos de perto o livro [1] para os capítulos 2 e 3, e o artigo [2] para os capítulos 4 e 5.

No Capítulo 1 começamos por definir noções básicas da lógica de primeira ordem. Apresentamos alguns exemplos de teorias que vão ser úteis posteriormente, como por exemplo a teoria dos rcof.

Quanto a teorias aludimos à vantagem de diferentes axiomatizações através de propriedades da axiomatização universal.

Pode-se associar um noção de complexidade das fórmulas consoante o número de quantificadores que tem. Uma fórmula sem quantificadores é geralmente de fácil tratamento. Se numa estrutura todos os conjuntos definíveis são definidos à custa de fórmulas sem quantificadores dizemos que a estrutura tem eliminação de quantificadores (abreviado QE). Se todas os modelos duma teoria tiverem QE, dizemos que a teoria tem QE. Apresentamos e provamos dois critérios para que uma teoria admita QE que usaremos no último capítulo.

Apelamos para uma perspectiva geométrica dos conjuntos definíveis por fórmulas e notamos um caso importante de regularidade destes conjuntos - a o-minimalidade.

No capítulo 2 provamos que a teoria dos rcof admite QE e como consequência concluímos que todo o rcof é o-minimal. Seja $\mathcal{R} = (R, <, +, -, \cdot, 0, 1)$ um rcof. Os conjuntos definíveis mais elementares em $\mathcal{R}$ são os conjuntos semialgébricos, conjuntos da forma

$$V = \{x \in R^n : f_1(x) = ... = f_k(x) = 0,\ g_1(x) > 0, ..., g_l(x) > 0\},$$

onde $f_1, ..., f_k, g_1, ..., g_l \in R[X],\ X = (X_1, ..., X_n)$. Note-se que estes conjuntos são definidos por fórmulas (equações e inequações) sem quantificadores. É de fácil verificação que estes conjuntos são fechados para a união, intersecção e complementação. Provaremos que são fechados para as projecções, o que implicará de imediato que todos os conjuntos definíveis em $\mathcal{R}$ são precisamente os conjuntos semialgébricos e portanto que $\mathcal{R}$ admite QE. Sai assim que $\mathcal{R}$ é o-minimal pois os conjuntos semialgébricos em dimensão 1 são união finita de pontos e intervalos.

No capítulo 3 estudamos algumas das propriedades mais importantes das estruturas o-minimais. Seja $\mathcal{R} = (<, ...)$ uma estrutura o-minimal. Na primeira secção provamos os seguintes teoremas:

TEOREMA (Monotonicity Theorem). Seja $f : I \to R$ uma função definível. Então existem constantes $a_1, ..., a_k$ tais que $I = (a_1, a_2) \cup ... \cup (a_{k-1}, a_k) \cup \{a_1, ..., a_k\}$ e, em cada intervalo (a_i, a_{i+1}), f é constante or estrictamente monótona e contínua.

LEMA (Finiteness Lemma). Seja A um subconjunto definível de R^2 e suponha-se que para cada $x \in R$,

$$A_x = \{y \in R : (x, y) \in A\}$$

é finito (A é finito sobre R). Então existe $n \in \mathbb{N}$ tal que $|A_x| < n$ para todo $x \in R$ (A é uniformemente finito sobre R).

Na segunda secção generalizamos o resultado anterior para qualquer dimensão $n \in \mathbb{N}$:

TEOREMA. Sejam $A, A_1, ..., A_k \subseteq R^n$ e $Y \subseteq R^{n+1}$ conjuntos definíveis. Então

- (Uniform finiteness - UF_n) Se Y é finito sobre R^m então é uniformemente finito sobre R^m;
- (Cell decomposition - CD_n) Existe uma decomposição de R^n e $A_1, ..., A_k$ em células.
- (Piecewise continuity - PC_n) Seja $f : A \to R$ uma função definível. Existe uma decomposição de R^n e A em células tal que para cada célula $C \subseteq A$, $f|_C$ é contínua.

No capítulo 4 passamos a estudar a teoria de rcof com novos símbolos de função. Este tipo de considerações é natural numa tentativa de generalizar resultados e existe muito trabalho feito neste sentido. Seja $\mathbb{R}\{X_1, ..., X_m\}$ o subanel das séries de potências de coeficientes reais que convergem numa vizinhança de I^m, onde $I = [-1, 1]$. Para $f \in \mathbb{R}\{X_1, ..., X_m\}$ seja $\widetilde{f} : \mathbb{R}^m \to \mathbb{R}$ definido por:

$$\widetilde{f}(x) = \begin{cases} f(x), & \text{se } x \in I^m, \\ 0, & \text{se } x \notin I^m. \end{cases}$$

Denominamos este tipo de funções $\widetilde{f}$ por funções analíticas restritas. Neste capítulo estudamos a teoria T_{an} dos reais como corpo ordenado com funções analíticas restritas. Denominamos uma estrutura desta teoria por corpo analítico restrito. Começamos por propor no início do capítulo uma axiomatização para esta teoria e provaremos no fim do capítulo que de facto assim o é. Na primeira secção introduzimos a noção de valoração. Dado um corpo K e um grupo abeliano totalmente ordenado Γ, uma função sobrejectiva $v : K \to \Gamma \cup \{\infty\}$ diz-se uma valoração se

- $v(x) = \infty \leftrightarrow x = 0$;
- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \min(v(x), v(y))$.

Pode-se provar que existe uma valoração num corpo K se e só se existe um domínio de integridade $\mathcal{O} \subseteq K$ com a propriedade

$$\forall x \in K(x \notin \mathcal{O} \to x^{-1} \in \mathcal{O}).$$

Um corpo analítico restrito K admite valoração pela existência do domínio de integridade

$$\text{Fin}(K) := \{x \in K : \text{ existe } q \in \mathbb{Q} \text{ tal que } |x| < q\}.$$

As valorações são aqui consideradas como uma ferramenta de estudo de T_{an}.

Na segunda secção provamos algumas propriedades das valorações e referimos sem prova o resultado de que T_{an} admite QE na linguagem $\mathcal{L}_{an}(^{-1})$. Usando este resultado e as propriedades das valorações provamos que T_{an} admite uma axiomatização universal na linguagem $\mathcal{L}_{an}(^{-1}, (\sqrt[n]{\ })_{n=2,3,...})$.

No capítulo 5 começamos por observar brevemente propriedades das séries de potências. Dado um corpo k e um grupo abeliano totalmente ordenado, uma série de potência é um objecto da forma

$$x = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma,$$

onde $\gamma \in \Gamma$ ("expoentes") e $a_\gamma \in k$ ("coeficientes"), tais que o suporte de x, definido por $\text{supp}(x) := \{\gamma \in \Gamma : a_\gamma \neq 0\}$, é um subconjunto bem ordenado de Γ. O conjunto das séries de potências $k((t^\Gamma))$ admite uma estrutura de corpo definindo as operações

- $x + y = \sum_{\gamma \in \Gamma}(a_\gamma + b_\gamma)t^\gamma$;

- $x \cdot y = \sum_{\gamma\in\Gamma}(\sum_{\gamma_1+\gamma_2=\gamma} a_{\gamma_1} b_{\gamma_2}) t^{\gamma}$.

A função ord : $k((t^{\Gamma}))^{\times} \to \Gamma,\ \mathrm{ord}(x) = \min \mathrm{supp}(x)$ é uma valoração. Estabelecemos na secção 2 o resultado de que todo o modelo de T_{an} se pode ver como uma subestrutura dum corpo de séries de potências $\mathbb{R}((t^{\Gamma}))$. Usamos este facto para deduzir resultados-chave acerca destas estruturas através de valorações e provamos que $T_{an}(\exp)$ admite QE e axiomatização universal na linguagem $\mathcal{L}_{an}(\exp, \log)$. Na última secção começamos por notar que para as teorias que admitem QE, a o-minimalidade é equivalente à regularidade do sinal (positivas, negativas ou iguais a zero) “no infinito” das funções definíveis a uma variável. Isto leva-nos a considerar corpos de Hardy e usando propriedades destes corpos provamos que $T_{an}(\exp)$ é o-minimal.

Palavras-chave: o-minimalidade, eliminação de quantificadores, axiomatização universal, corpos reais fechados ordenados, corpos analíticos restritos.

Contents

1 Preliminaries of Model Theory **1**
- 1.1 First-order languages and interpretation . . . 1
- 1.2 Homomorphisms and formulas . . . 5
- 1.3 Theories . . . 6
- 1.4 Definable sets and quantifier elimination . . . 9
- 1.5 Brief digression on types . . . 11

2 QE for the theory of rcof **14**
- 2.1 Roots of polynomials in $R[X]$ . . . 14
- 2.2 Semialgebraic cell decomposition . . . 17

3 O-minimality **22**
- 3.1 Monotonicity Theorem and Uniform Finiteness . . . 23
- 3.2 Cell decomposition . . . 27

4 The theory of restricted analytic fields **32**
- 4.1 Valuations . . . 34
- 4.2 Ordered fields as $\mathcal{L}_{an}$-structures . . . 36

5 The theory of $\mathbb{R}_{an}(\exp)$ **39**
- 5.1 Power series fields . . . 39
- 5.2 Models of T_{an} as power series fields . . . 40
- 5.3 The theory of $\mathbb{R}_{an}$(exp) and quantifier elimination . . . 41
- 5.4 O-minimality and Hardy fields . . . 46

Chapter 1

Preliminaries of Model Theory

In this chapter we lay down some basic notions from model theory.

1.1 First-order languages and interpretation

In this section we define the notion of first-order languages, formulas, structures and truth of formulas by Tarski's definition of truth.

DEFINITION 1.1.1. *A* ***first-order language*** $\mathcal{L}$ *is a list constituted by:*

- *A* ***type*** $\sigma = (I, J, K, \rho, \mu)$*, where* I, J, K *are sets and* $\rho : I \to \mathbb{N}$*,* $\mu : J \to \mathbb{N}$ *are functions.*
- *Logical symbols*
  - *A countable set of variable symbols* $v_1, v_2, \ldots$*;*
  - *The equality symbol* $=$*;*
  - *The connective symbols* $\neg$*,* $\wedge$*,* $\vee$*,* $\Rightarrow$ *and* $\Leftrightarrow$*;*
  - *The existential quantifier symbol* $\exists$ *and universal quantifier symbol* $\forall$*;*
  - *Parentheses* $($*,* $)$ *and commas* $,$.
- *Non-logical symbols*
  - *For each* $i \in I$*, an* $\rho(i)$*-ary relation symbol* R_i*;*
  - *For each* $j \in J$*, an* $\mu(j)$*-ary function symbol* f_j*;*
  - *For each* $k \in K$*, a constant symbol* c_k.

We write $\mathcal{L} = (\{R_i\}_{i \in I}, \{f_j\}_{j \in J}, \{c_k\}_{k \in K})$ *followed by indication of the arities.*

NOTE 1.1.2. We may use different notations for the variable symbols. The correspondence to the index number of the usual variable symbol will be self-evident. For example x, y, z to denote v_1, v_2, v_3, or $x_1, x_2, \ldots$ to denote $v_1, v_2, \ldots$.

NOTE 1.1.3. Let $\mathcal{L} = (\{R_i\}_{i \in I}, \{f_j\}_{j \in J}, \{c_k\}_{k \in K})$ be a first-order language with arities $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. We may use different notations for the non-logical symbols. For example if $\sigma = (\{a\}, \{a\}, \{0, 1\}, \rho(a) = 2, \mu(a) = 1)$ we may write $\mathcal{L} = (\{<\}, \{\sin\}, \{0, 1\})$ instead of , $\mathcal{L} = (\{R_a\}, \{f_a\}, \{c_0, c_1\})$. We may also drop the brackets and write $\mathcal{L} = (<, \sin, 0, 1)$ or drop it partially like $\mathcal{L} = (<, \sin, \{0, 1\})$. Sometimes the discourse is independent of the arities or those are implicit so, in such cases, we will invoke languages without mentioning the arities.

We now establish the syntax of the language, or in other words, the allowed sequences of symbols given by the language.

DEFINITION 1.1.4. *Let* $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ *be a first-order language with arities* $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. *We define the notion of* ***$\mathcal{L}$-term*** *by induction:*

- *If* v *is a variable symbol then* v *is an* $\mathcal{L}$*-term;*
- *If* c_k *is a constant symbol then* c_k *is an* $\mathcal{L}$*-term;*
- *If* f_j *is a function symbol and* $\tau_1, ..., \tau_{\mu(j)}$ *are* $\mathcal{L}$*-terms, then* $f_j(\tau_1, ..., \tau_{\mu(j)})$ *is an* $\mathcal{L}$*-term;*
- *Nothing else is an* $\mathcal{L}$*-term.*

The set of $\mathcal{L}$*-terms is denoted by* $\mathcal{T}$.

DEFINITION 1.1.5. *Let* $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ *be a first-order language with arities* $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. *We say that* ϕ *is an* ***atomic $\mathcal{L}$-formula*** *if* ϕ *is either*

- $\tau_1 = \tau_2$ *where* $\tau_1, \tau_2 \in \mathcal{T}$ *(which should be read as "*τ_1 *equal to* τ_2*"), or*
- $R_i(\tau_1, ..., \tau_{\rho(i)})$ *where* $\tau_1, ..., \tau_{\rho(i)} \in \mathcal{T}$ *and* R_i *is a predicate symbol.*

DEFINITION 1.1.6. *Let* $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ *be a first-order language with arities* $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. *We define the notion of* ***$\mathcal{L}$-formulas*** *by induction:*

- *If* ϕ *is an atomic* $\mathcal{L}$*-formula then* ϕ *is an* $\mathcal{L}$*-formula;*
- *If* ϕ *is an* $\mathcal{L}$*-formula then* $\neg\phi$ *is an* $\mathcal{L}$*-formula (which should be read as "not* ϕ*");*
- *If* ϕ, ψ *are* $\mathcal{L}$*-formulas then* $\phi \vee \psi$, $\phi \wedge \psi$, $\phi \Rightarrow \psi$, $\phi \Leftrightarrow \psi$ *are* $\mathcal{L}$*-formulas (which should be respectively read as "*ϕ *or* ψ*", "*ϕ *and* ψ*", "if* ϕ *then* ψ*", "*ϕ *if and only if* ψ*");*
- *If* ϕ *is an* $\mathcal{L}$*-formula then* $\exists v\phi$ *and* $\forall v\phi$ *are* $\mathcal{L}$*-formulas for all variable symbols* v *(which should be respectively read as "there is* v *such that* ϕ*" and "for all* v *we have* ϕ*");*
- *Nothing else is an* $\mathcal{L}$*-formula.*

The strings of symbols considered in a language are precisely the $\mathcal{L}$-formulas.

Now we turn to the semantics of the language. The semantics adopted in first-order model theory is based on Tarski's definition of truth.

DEFINITION 1.1.7. *Let* $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ *be a first-order language with arities* $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. *An* ***$\mathcal{L}$-structure*** $\mathcal{M}$ *is a list constituted by:*

- *A set* M *called the* ***domain*** *of* $\mathcal{M}$*, and sometimes denoted dom*$(\mathcal{M})$*;*
- *For each* $i \in I$*, a* $\rho(i)$*-ary relation* $R_i^{\mathcal{M}} \subseteq M^{\rho(i)}$*;*
- *For each* $j \in J$*, a* $\mu(i)$*-ary function* $f_j^{\mathcal{M}} : M^{\mu(j)} \to M$*;*
- *For each* $k \in K$*, an element* $c_k \in M$.

NOTATION. Let $\mathcal{L}$ be a first-order language. Sometimes we will use the notation of the non-logical symbols to denote the correspondent relations, functions and constants of an $\mathcal{L}$-structure whenever ambiguity of the discourse can be avoided. For example, let $\mathcal{L} = (<, +, -, \cdot, 0, 1)$ where $<$ is a binary relation, $+$ and $\cdot$ are binary functions, $-$ is an unary function, 0 and 1 are constants. We may invoke an $\mathcal{L}$-structure as $\mathcal{R} = (\mathbb{R}, <, +, -, \cdot, 0, 1)$.

NOTATION. Given a set M we denote

$$M^\omega := \{\overline{a} = (a_1, ..., a_p, ...) : a_i \in M \text{ for all } i \in \mathbb{N}\}$$

Let $f : M^n \to M$ be an n-ary function, $R \subseteq M^n$ an n-ary relation and $\overline{a} \in M^\omega$. We write $f(\overline{a})$ to mean $f(a_1, ..., a_n)$; we write $\overline{a} \in R$ to mean $(a_1, ..., a_n) \in R$.

DEFINITION 1.1.8. *Let $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ be a first-order language with arities $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. Let τ be an $\mathcal{L}$-term. Let $\mathcal{M} = (M, \{R_i^{\mathcal{M}}\}_{i\in I}, \{f_j^{\mathcal{M}}\}_{j\in J}, \{c_k^{\mathcal{M}}\}_{k\in K})$ be an $\mathcal{L}$-structure. The **interpretation** of τ in $\mathcal{M}$ is the function*

$$\tau^{\mathcal{M}} : M^{\omega} \to M$$

defined inductively for all $\overline{a} \in M^{\omega}$ by:

- *If τ is c_k then $\tau^{\mathcal{M}}(\overline{a}) = c_k^{\mathcal{M}}$;*
- *If τ is v_p then $\tau^{\mathcal{M}}(\overline{a}) = a_p$;*
- *If τ is $f_j(\tau_1, ..., \tau_{\mu(j)})$ and $\tau_1^{\mathcal{M}}, ..., \tau_{\mu(j)}^{\mathcal{M}}$ are defined, then $\tau^{\mathcal{M}}(\overline{a}) = f_j^{\mathcal{M}}(\tau_1^{\mathcal{M}}(\overline{a}), ..., \tau_{\mu(j)}^{\mathcal{M}}(\overline{a}))$.*

NOTATION. Let M be a set. Let $\overline{a} \in M^{\omega}$. Let $p \in \mathbb{N}$. We write

$$\overline{a}(p/b) := (a_1, ..., a_{p-1}, b, a_{p+1}, ...)$$

DEFINITION 1.1.9 (Tarski's definition of truth). *Let $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ be a first-order language with arities $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. Let $\mathcal{M} = (M, \{R_i^{\mathcal{M}}\}_{i\in I}, \{f_j^{\mathcal{M}}\}_{j\in J}, \{c_k^{\mathcal{M}}\}_{k\in K})$ be a $\mathcal{L}$-structure. Let ϕ be an $\mathcal{L}$-formula. Let $\overline{a} \in M^{\omega}$. We define $\mathcal{M} \vDash \phi(\overline{a})$ inductively:*

- *If ϕ is $\tau_1 = \tau_2$ for some $\tau_1, \tau_2 \in \mathcal{T}$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if $\tau_1^{\mathcal{M}}(\overline{a}) = \tau_2^{\mathcal{M}}(\overline{a})$;*
- *If ϕ is $R_i(\tau_1, ..., \tau_{\rho(i)})$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if $(\tau_1^{\mathcal{M}}(\overline{a}), ..., \tau_{\rho(i)}^{\mathcal{M}}(\overline{a})) \in R_i^{\mathcal{M}}$;*
- *If ϕ is $\neg\psi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if we don't have $\mathcal{M} \vDash \psi(\overline{a})$;*
- *If ϕ is $\psi \vee \chi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if $\mathcal{M} \vDash \psi(\overline{a})$ or $\mathcal{M} \vDash \chi(\overline{a})$;*
- *If ϕ is $\psi \wedge \chi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if $\mathcal{M} \vDash \psi(\overline{a})$ and $\mathcal{M} \vDash \chi(\overline{a})$;*
- *If ϕ is $\psi \Rightarrow \chi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if, whenever $\mathcal{M} \vDash \psi(\overline{a})$ then $\mathcal{M} \vDash \chi(\overline{a})$;*
- *If ϕ is $\psi \Leftrightarrow \chi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if, whenever $\mathcal{M} \vDash \psi(\overline{a})$ then $\mathcal{M} \vDash \chi(\overline{a})$, and whenever $\mathcal{M} \vDash \chi(\overline{a})$ then $\mathcal{M} \vDash \psi(\overline{a})$;*
- *If ϕ is $\exists v_p \psi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if there is $b \in M$ such that $\mathcal{M} \vDash \phi(\overline{a}(p/b))$;*
- *If ϕ is $\forall v_p \psi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if for all $b \in M$ we have $\mathcal{M} \vDash \phi(\overline{a}(p/b))$.*

*$\mathcal{M} \vDash \phi(\overline{a})$ should be read as "the formula ϕ is **true** in $\mathcal{M}$ whenever we replace the ordered variables by the values of $\overline{a}$ respectively".*

NOTE 1.1.10. Given an $\mathcal{L}$-formula $\phi(v_1, ..., v_n)$ and an $\mathcal{L}$-structure we will sometimes say that an element $a \in M^n$ satisfies $\phi(v)$ to mean $\mathcal{M} vDash \phi(a)$.

NOTE 1.1.11. Whenever a language $\mathcal{L}$ is implicit or the discourse is independent of it, we will drop the "$\mathcal{L}$" part of designations involving "$\mathcal{L}$" (so, for example, an $\mathcal{L}$-formula will sometimes be called more succintly a "formula").

DEFINITION 1.1.12. *Let $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ be a first-order language with arities $\rho : I \to \mathbb{N}$, $\mu : J \to \mathbb{N}$. We say that a variable v is **free** in a term $\tau \in \mathcal{T}$ if one of the following occurs:*

- *τ is v;*
- *τ is $f_j(\tau_1, ..., \tau_{\mu(j)})$ and v is free in τ_r for some $1 \leq r \leq \mu(j)$.*

*We say that a variable v is **free** in an atomic $\mathcal{L}$-formula ϕ if one of the following occurs:*

- *ϕ is $\tau_1 = \tau_2$ for some $\tau_1, \tau_2 \in \mathcal{T}$ and v is free in τ_1 or τ_2;*
- *ϕ is $R_i(\tau_1, ..., \tau_{\rho(i)})$ and v is free in τ_r for some $1 \leq r \leq \rho(i)$.*

*We say that a variable v_p is **free** in an $\mathcal{L}_\sigma$-formula ϕ if one of the following occurs:*

- *ϕ is an atomic formula and v_p is free in ϕ;*
- *ϕ is $\neg\psi$ and v_p is free in ψ;*
- *ϕ is $\psi \wedge \chi$, $\psi \vee \chi$, $\psi \Rightarrow \chi$ or $\psi \Leftrightarrow \chi$ and v_p is free in ψ or χ;*
- *ϕ is $\exists v_q\psi$ or $\forall v_q\psi$, $p \neq q$ and v_p is free in ψ.*

*Otherwise we say that v_p is **bound** in ϕ. An $\mathcal{L}$-formula with no free variables is called an **$\mathcal{L}$-sentence**.*

PROPERTY 1.1.13. *Let τ be a term. Let $\mathcal{M}$ be a structure. Suppose $v_{q_1}, ..., v_{q_n}$ are the free variables in τ and let $\overline{a}, \overline{b} \in M^\omega$ such that $a_{q_i} = b_{q_i}$ for $i = 1, ..., n$. Then $\tau(\overline{a}) = \tau(\overline{b})$.*

Proof. We prove this by induction on the terms. If τ is a constant symbol then it is obvious. If τ is a variable symbol, then $\tau = v_{q_i}$ for some $i = 1, ..., n$, therefore $\tau(\overline{a}) = a_{q_i} = b_{q_i} = \tau(\overline{b})$. Suppose $\tau = f_j(\tau_1, ..., \tau_{\mu(j)})$ and the property is valide for τ_r, $r = 1, ..., n$. Then,

$$\begin{aligned}\tau^{\mathcal{M}}(\overline{a}) &= f_j^{\mathcal{M}}(\tau_1^{\mathcal{M}}(\overline{a}), ..., \tau_{\mu(j)}^{\mathcal{M}}(\overline{a})) \\ &= f_j^{\mathcal{M}}(\tau_1^{\mathcal{M}}(\overline{b}), ..., \tau_{\mu(j)}^{\mathcal{M}}(\overline{b})) \\ &= \tau^{\mathcal{M}}(\overline{b}).\end{aligned}$$

□

PROPERTY 1.1.14. *Let ϕ be a formula. Let $\mathcal{M}$ be a structure. Suppose $v_{q_1}, ..., v_{q_n}$ are the free variables in ϕ and let $\overline{a}, \overline{b} \in M^\omega$ such that $a_{q_i} = b_{q_i}$ for $i = 1, ..., n$. Then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if $\mathcal{M} \vDash \phi(\overline{b})$.*

Proof. We prove this by induction on formulas. If ϕ is $\tau_1 = \tau_2$ for some $\tau_1, \tau_2 \in \mathcal{T}$ or $R_i(\tau_1, ..., \tau_{\rho(i)})$ then it is obvious by Property 1.1.13. If ϕ is $\neg\psi$ then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if we don't have $\mathcal{M} \vDash \psi(\overline{a})$. By inductive hypothesis, $\mathcal{M} \vDash \psi(\overline{a})$ if and only if $\mathcal{M} \vDash \psi(\overline{b})$. Thus $\mathcal{M} \vDash \phi(\overline{a})$ if and only if $\mathcal{M} \vDash \phi(\overline{b})$. If ϕ is $\exists v_p\psi$, where $p \neq q_r$ for all $r = 1, ..., n$, then $\mathcal{M} \vDash \phi(\overline{a})$ if and only if there is $d \in M$ such that $\mathcal{M} \vDash \psi(\overline{a}(p/d))$. We have $\overline{a}(p/d)_q = \overline{b}(p/d)_q$ for every $q = q_1, ..., q_n$ so, by inductive hypothesis, $\mathcal{M} \vDash \psi(\overline{a}(p/d))$ if and only if $\mathcal{M} \vDash \psi(\overline{b}(p/d))$. Thus $\mathcal{M} \vDash \phi(\overline{a})$ if and only if $\mathcal{M} \vDash \phi(\overline{b})$. The other cases are similar. □

NOTATION. A term τ and a formula ϕ with free variables $v_1, ..., v_n$ will sometimes be denoted $\tau(v_{q_1}, ..., v_{q_n})$ and $\phi(v_{q_1}, ..., v_{q_n})$.

We will see in some sense that the number of quantifiers in a formula and whether both the existential and universal quantifiers or just one of them occurs gives an account of the complexity of the formula.

DEFINITION 1.1.15. *We say that a formula ϕ is **quantifier-free** if the logical symbols $\forall$, $\exists$ don't occur in ϕ.*

DEFINITION 1.1.16. *We say that a sentence ϕ is an **universal $\mathcal{L}$-sentence** if*

$$\phi = \forall v_1 ... \forall v_n \psi(v_1, ..., v_n),$$

where $\psi(v_1, ..., v_n)$ is a quantifier-free formula.

DEFINITION 1.1.17. *We say that an $\mathcal{L}$-formula ϕ is an **existential $\mathcal{L}$-formula** if*

$$\phi = \exists v_{q_1} ... \exists v_{q_n} \psi$$

where ψ is a quantifier-free formula.

1.2 Homomorphisms and formulas

In this section we define homomorphisms between $\mathcal{L}$-structures and its relations to formulas.

DEFINITION 1.2.1. *Let* $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$ *with arities* $\rho : I \to \mathbb{N}$ *and* $\mu : J \to \mathbb{N}$. *Let* $\mathcal{M}$ *and* $\mathcal{N}$ *be* $\mathcal{L}$*-structures. We say that* $\pi : \mathcal{M} \to \mathcal{N}$ *is an* ***$\mathcal{L}$-homomorphism*** *if:*

- $\pi : M \to N$ *is a function;*
- *for each* $i \in I$ *and every* $(a_1, ..., a_{\rho(i)}) \in M^{\rho(i)}$*, if* $(a_1, ..., a_{\rho(i)}) \in R_i^{\mathcal{M}}$ *then* $(\pi(a_1), ..., \pi(a_{\rho(i)})) \in R_i^{\mathcal{N}}$*;*
- *for each* $j \in J$ *and every* $(a_1, ..., a_{\mu(i)}) \in M^{\mu(i)}$*,* $\pi(f_j^{\mathcal{M}}(a_1, ..., a_{\mu(j)})) = f_j^{\mathcal{N}}(\pi(a_1), ..., \pi(a_{\mu(j)}))$*;*
- *for each* $k \in K$*,* $\pi(c_k^{\mathcal{M}}) = c_k^{\mathcal{N}}$*.*

We say that $\pi : \mathcal{M} \to \mathcal{N}$ *is an* ***$\mathcal{L}$-embedding*** *if:*

- π *is an* $\mathcal{L}$*-homomorphism;*
- π *is injective;*
- *for each* $i \in I$ *and every* $(a_1, ..., a_{\rho(i)}) \in M^{\rho(i)}$*, if* $(\pi(a_1), ..., \pi(a_{\rho(i)})) \in R_i^{\mathcal{N}}$ *then* $(a_1, ..., a_{\rho(i)}) \in R_i^{\mathcal{M}}$*.*

We say that $\pi : \mathcal{M} \to \mathcal{N}$ *is an* ***$\mathcal{L}$-isomorphism*** *if:*

- π *is an* $\mathcal{L}$*-embedding;*
- π *is surjective.*

DEFINITION 1.2.2. *Let* $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$*. Let* $\mathcal{M}$ *and* $\mathcal{N}$ *be* $\mathcal{L}$*-structures. If* $\pi : M \to N$ *is an* $\mathcal{L}$*-embedding and* $M \subseteq N$*, we say that* $\mathcal{M}$ *is a* ***substructure*** *of* $\mathcal{N}$ *or, equivalently, that* $\mathcal{N}$ *is an* ***extension*** *of* $\mathcal{M}$*. In this case, we write* $\mathcal{M} \subseteq \mathcal{N}$*.*

Homomorphisms commute with interpretations of terms:

PROPERTY 1.2.3. *Let* $\mathcal{M}$ *and* $\mathcal{N}$ *be* $\mathcal{L}$*-structures and* $\pi : \mathcal{M} \to \mathcal{N}$ *an homomorphism. Let* $\tau(v_{q_1}, ..., v_{q_n})$ *be a term. Then*

$$\pi(\tau^{\mathcal{M}}(a_{q_1}, ..., a_{q_n}) = \tau^{\mathcal{N}}(\pi(a_{q_1}), ..., \pi(a_{q_n})).$$

Proof. By induction on the terms. $\square$

Homomorphisms preserve truth of atomic formulas:

PROPERTY 1.2.4. *Let* $\pi : \mathcal{M} \to \mathcal{N}$ *be an homomorphism. Then*

$$\mathcal{M} \vDash \phi(a_1, ..., a_n) \Rightarrow \mathcal{N} \vDash \phi(\pi(a_1), ..., \pi(a_n))$$

for every atomic formula $\phi(v_1, ..., v_n)$ *and* $a_1, ..., a_n \in M$*.*

Proof. By induction on the atomic formulas. $\square$

DEFINITION 1.2.5. *We say that an homomorphism* $\pi : \mathcal{M} \to \mathcal{N}$ *satisfies the* ***transfer principle*** *for a formula* ϕ *if for all* $a \in M^{\omega}$

$$\mathcal{M} \vDash \phi(a_1, ..., a_n) \Leftrightarrow \mathcal{N} \vDash \phi(\pi(a_1), ..., \pi(a_n)).$$

Embeddings satisfy the transfer principle for all quantifier-free formulas:

PROPERTY 1.2.6. *Let* $\pi : \mathcal{M} \to \mathcal{N}$ *be an embedding. Then*

$$\mathcal{M} \vDash \phi(a_1, ..., a_n) \Leftrightarrow \mathcal{N} \vDash \phi(\pi(a_1), ..., \pi(a_n))$$

for every quantifier-free formula $\phi(v_1, ..., v_n)$ *and* $a_1, ..., a_n \in M$*.*

Proof. By induction on the quantifier-free formulas. □

EXAMPLE 1.2.7. Let $\mathcal{L} = (<, +)$. Let $\mathcal{M} = (\mathbb{Z}, <, +)$ and $\mathcal{N} = (\mathbb{Q}, <, +)$. The map $\pi : \mathcal{M} \to \mathcal{N}$ defined by $\pi(m) = m$ is an embedding. Let $\phi(x, y) = (x < y \Rightarrow \exists z(x < z < y))$. We have $\mathcal{N} \vDash \phi(1, 2)$ but $\mathcal{M} \nvDash \phi(1, 2)$.

Embeddings preserve truth of existential formulas.

PROPERTY 1.2.8. *Let $\pi : \mathcal{M} \to \mathcal{N}$ be an embedding. Then*

$$\mathcal{M} \vDash \phi(a_1, ..., a_n) \Rightarrow \mathcal{N} \vDash \phi(\pi(a_1), ..., \pi(a_n))$$

for every existential formula $\phi(v_1, ..., v_n)$ and $a_1, ..., a_n \in M$.

We now consider embeddings that satisfy the transfer principle for all formulas.

DEFINITION 1.2.9. *Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures. We say that $\pi : \mathcal{M} \to \mathcal{N}$ is an **elementary $\mathcal{L}$-embbedding** if*

- *π is an $\mathcal{L}$-embedding;*
- *for every formula $\phi(v_1, ..., v_n)$ and all $a_1, ..., a_n \in M$,*

$$\mathcal{M} \vDash \phi(a_1, ..., a_n) \Leftrightarrow \mathcal{N} \vDash \phi(\pi(a_1), ..., \pi(a_n)).$$

*If in addition $\mathcal{M} \subseteq \mathcal{N}$, then we say that $\mathcal{M}$ is an **elementary substructure** of $\mathcal{N}$ or that $\mathcal{N}$ is an **elementary extension** of $\mathcal{M}$. We write $\mathcal{M} \preceq \mathcal{N}$.*

The next definition is useful when we want to construct embeddings and elementary embeddings.

DEFINITION 1.2.10. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure. We denote by $\mathcal{L}_M$ the language extension of $\mathcal{L}$ obtained by adding constant symbols m for each $m \in M$. The **atomic diagram** of $\mathcal{M}$ is Diag$(\mathcal{M}) = \{\phi(\overline{a}) : \mathcal{M} \vDash \phi(\overline{a})$, $\overline{a} \in M^\omega$, ϕ is an atomic $\mathcal{L}$-formula or the negation of an atomic $\mathcal{L}$-formula$\}$. The **elementary diagram** of $\mathcal{M}$ is Diag$_{el}(\mathcal{M}) = \{\phi(\overline{a}) : \mathcal{M} \vDash \phi(\overline{a})$, $\overline{a} \in M^\omega$, ϕ is an $\mathcal{L}$-formula$\}$.*

LEMMA 1.2.11. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure. Let $\mathcal{N}$ be an $\mathcal{L}_M$-structure. Then, viewing $\mathcal{N}$ as an $\mathcal{L}$-structure*

1) If $\mathcal{N} \vDash$ Diag$(\mathcal{M})$ then $\mathcal{M} \subseteq \mathcal{N}$.

2) If $\mathcal{N} \vDash$ Diag$_{el}(\mathcal{M})$ then $\mathcal{M} \preceq \mathcal{N}$.

Proof. Lemma 2.3.3 of [3]. □

1.3 Theories

In this section we set a basic apparatus to study mathematical theories in general. We will also present some examples that will be useful later.

DEFINITION 1.3.1. *Given a language $\mathcal{L}$, an **$\mathcal{L}$-theory** is any set of $\mathcal{L}$-sentences.*

*Let $\mathcal{M}$ be an $\mathcal{L}$-structure and T an $\mathcal{L}$-theory. We say that $\mathcal{M}$ **models** T, or equivalently that $\mathcal{M}$ is a model of T, if $\mathcal{M} \vDash \phi$ for every $\phi \in T$. We write $\mathcal{M} \vDash T$. We say that an $\mathcal{L}$-sentence ϕ is a **logical consequence** of an $\mathcal{L}$-theory T, and write $T \vDash \phi$, if every model of T is a model of ϕ. We say that an $\mathcal{L}$-theory T is **satisfiable** if T has a model. We say that a class of $\mathcal{L}$-structures is an **elementary class** if there is an $\mathcal{L}$-theory T such that $\mathcal{K} = \{\mathcal{M} : \mathcal{M} \vDash T\}$. In this case we call the sentences in T the **axioms** for the class $\mathcal{K}$. The set of $\mathcal{L}$-sentences ϕ such that $\mathcal{M} \vDash \phi$ is called the **theory** of $\mathcal{M}$, denoted $Th(\mathcal{M})$. We say that an $\mathcal{L}$-theory T' is an **axiomatization** of T if for every $\mathcal{L}$-structure $\mathcal{M}$, $\mathcal{M} \vDash T$ if and only if $\mathcal{M} \vDash T'$. We say that a theory is **complete** if for every sentence ϕ, either $\phi \in T$ or $\neg\phi \in T$.*

Now follows some examples of elementary classes.

EXAMPLE 1.3.2. Let $\mathcal{L} = (<)$, where $<$ is a binary relation symbol. We will denote the formula $x < y \vee x = x$ by $x \leq y$. The theory of **ordered sets** is axiomatized by

- $\forall x(x \leq x)$;
- $\forall x \forall y(x \leq y \wedge y \leq x)$;
- $\forall x \forall y \forall z(x \leq y \wedge y \leq z \rightarrow x \leq z)$.

The theory of **linearly ordered sets** is axiomatized by the axioms for ordered sets and

$$\forall x \forall y(x \leq y \vee y \leq x).$$

The theory of **dense ordered sets without extremities** is axiomatized by the axioms for ordered sets and

- $\forall x \forall y(x < y \rightarrow \exists z(x < z \wedge z < y))$ (density);
- $\forall x \exists y \exists z(z < x \wedge x < y)$ ("without end points").

EXAMPLE 1.3.3. Let $\mathcal{L} = (\cdot, e)$, where $\cdot$ is a binary function symbol and e is a constant symbol. The theory of groups is axiomatized by

- $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$;
- $\forall x(x \cdot e = e \cdot x = x)$;
- $\forall x \exists y(x \cdot y = e)$.

For the theory of **abelian groups** we replace the symbol $\cdot$ by $+$ and e by 0. This theory is axiomatized by the groups axioms (as $(+, 0)$-sentences) and

- $\forall x \forall y(x + y = y + x)$.

The theory of **ordered abelian groups** is axiomatized by the abelian groups axioms, the linearly ordered sets axioms and

- $\forall x \forall y \forall z(x < y \rightarrow x + z < y + z)$ (compatibility with the order).

The theory of **ordered divisible abelian groups** is axiomatized by the axioms for ordered abelian groups and

- $\forall x \exists y(x = ny)$, for each natural n (divisibility),

where ny means $y + ... + y$ with y occurring n times.

Now follows an example of logical consequence.

EXAMPLE 1.3.4. Let $\mathcal{L} = (<, +, 0)$. Let T be the $\mathcal{L}$-theory of ordered abelian groups. Then $T \vDash \forall x(x \neq 0 \Rightarrow x + x \neq 0)$

Proof. Let $\mathcal{M} \vDash T$. Let $0 \neq x \in M$. Thus $x < 0$ or $0 < x$. If $x < 0$ then $x + x < x < 0$ and if $x > 0$ then $x + x > x > 0$. $\square$

In general, to show that $T \vDash \phi$, we give an informal mathematical proof as above that $\mathcal{M} \vDash \phi$ whenever $\mathcal{M} \vDash T$ using sentences from T. Lemma 1.3.6 tells us that there is always a finite subset of T that "works" for all models of T. To show that $T \nvDash \phi$, we usually construct a counterexample.

The following theorem is the cornerstone of model theory.

THEOREM 1.3.5 (Compactness Theorem). *Let T be a theory. Then T is satisfiable if and only if every finite subset of T is satisfiable.*

Proof. Consult pp.34-39 of [3]. $\square$

The next lemma is an easy consequence of the Compactness Theorem and says that whenever a sentence ϕ is a logical consequence of a theory T, there is a finite subset of sentences $\Delta \subseteq T$ such that every model of Δ is also a model of ϕ. Thus it is always possible "to argue" using only a finite set of sentences that ϕ is a logical consequence of T.

LEMMA 1.3.6. *Let T be an $\mathcal{L}$-theory and ϕ an $\mathcal{L}$-sentence. If $T \vDash \phi$ then there is a finite subset $\Delta \subseteq T$ such that $\Delta \vDash \phi$.*

Proof. Suppose not. Let $\Delta \subseteq T$ be finite. Then $\Delta \cup \{\neg\phi\}$ is satisfiable. Since Δ is arbitrary, this implies that every finite subset of $T \cup \{\neg\phi\}$ is satisfiable, so, by 1.3.5, $T \cup \{\neg\phi\}$ is satisfiable, contradicting $T \vDash \phi$. □

The axioms we choose for a theory may allow an easier study of the theory.

DEFINITION 1.3.7. *We say that a theory T has an universal axiomatization if it admits an axiomatization with exclusively universal sentences.*

THEOREM 1.3.8. *A theory T has an universal axiomatization if and only if whenever $\mathcal{N} \vDash T$ and $\mathcal{M} \subseteq \mathcal{N}$ then $\mathcal{M} \vDash T$.*

Proof. Consult Theorem 2.3.9 of [3]. □

We present further three elementary classes that will be important for our exposition.

EXAMPLE 1.3.9. Let $\mathcal{L} = (+, -, \cdot, 1, 0)$. The theory of **fields** is axiomatized by the abelian groups axioms as $(+, 0)$-sentences, by the groups axioms as $(\cdot, 1)$-sentences and

- $\forall x(0 \cdot x = 0)$;
- $\forall x\forall y\forall z(x \cdot (y + z)) = (xy + xz)$;
- $\forall x\forall y\forall z((x + y) \cdot z) = (xz + yz)$;
- $\forall x\forall y(x \cdot y = y \cdot x)$;
- $\forall x(x = 0 \vee \exists y(x \cdot y = 1)$.

Let $\mathcal{L} = (+, -, \cdot, 1, 0)$. The theory of **algebraically closed fields** (acf) is given by the axioms for fields and

$$\forall x_0\forall x_1...\forall x_{n-1}\exists x: \; x^n + \sum_{i=0}^{n-1} x_i x^i = 0.$$

EXAMPLE 1.3.10. Let $\mathcal{L} = (<, +, -, \cdot, 1, 0)$. The theory of **real closed ordered fields** (rcof) is axiomatized by the fields axioms, the linearly ordered sets axioms and

- $\forall x\forall y\forall z(x < y \rightarrow x + z < y + z)$;
- $\forall x\forall y\forall z((x < y \wedge z > 0) \rightarrow x \cdot z < y \cdot z)$;
- $\forall x_1...\forall x_n(x_1^2 + ... + x_n^2 \neq -1)$, for each $n \in \mathbb{N}$;
- $\forall x\exists y(x = y^2 \vee x + y^2 = 0)$;
- $\forall x_0...\forall x_{2n}\exists y(y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$, for each $n \in \mathbb{N}$,

where y^k means $y \cdot ... \cdot y$ with y occuring k times.

1.4 Definable sets and quantifier elimination

We now turn our attention to sets defined by formulas. This will give a geometric point of view of formulas.

DEFINITION 1.4.1. *Let $\mathcal{M} = (M, ...)$ be an $\mathcal{L}$-structure. We say that $X \subseteq M^m$ is **definable** if and only if there is an $\mathcal{L}$-formula $\phi(v_1, ..., v_m, v_{m+1}, ..., v_{m+n})$ and $b \in M^n$ such that*

$$X = \{a \in M^m : \mathcal{M} \vDash \phi(a, b)\}.$$

*We say that $\phi(v_1, ..., v_m, b)$ **defines** X.*

NOTE 1.4.2. Given a formula $\phi(x)$ and a structure $\mathcal{M}$ we will sometimes write $\{a \in M^n : \phi(a)\}$ to mean $\{a \in M^n : \mathcal{M} \vDash \phi(a)\}$.

We now give a geometric characterization of the definable sets. An important feature is that a set defined by a formula with an existential quantifier can be thought of as the projection of some definable set in a higher dimension.

LEMMA 1.4.3. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure.*
Let $(\mathcal{D}_n)_{n\in\mathbb{N}}$ be the sequence of sets defined by

1. *$M^n \in \mathcal{D}_n$;*
2. *For each n-ary function symbol f, the graph of the function $f^{\mathcal{M}}$ is in $\mathcal{D}_{n+1}$;*
3. *For each n-ary relation symbol R, $R^{\mathcal{M}} \in \mathcal{D}_n$;*
4. *For each $i, j \leq n$, $\{(x_1, ..., x_n) \in M^n : x_i = x_j\} \in \mathcal{D}_n$;*
5. *Each $\mathcal{D}_n$ is closed under complement, union, and intersection;*
6. *If $X \in \mathcal{D}_n$ then $M \times X \in \mathcal{D}_{n+1}$;*
7. *If $X \in \mathcal{D}_{n+1}$ and $\pi : M^{n+1} \to M^n$ is the projection map $(x_1, ..., x_n, x_{n+1}) \mapsto (x_1, ..., x_n)$, then $\pi(X) \in \mathcal{D}_n$;*
8. *If $X \in \mathcal{D}_{n+m}$ and $b \in M^m$, then $\{a \in M^n : (a, b) \in X\} \in \mathcal{D}_n$.*

Then $X \subseteq M^n$ is definable if and only if $X \in \mathcal{D}_n$.

Proof. Consult Proposition 1.3.4 of [3].

□

DEFINITION 1.4.4. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure. Let $A \subseteq M$. The set*

$$\langle A \rangle := \{x \in M : \exists y_1, ..., y_n \in A(x = t^{\mathcal{M}}(y_1, ..., y_n)), \textit{ for some } t \in \mathcal{L}\textit{-terms}\}$$

*is called the **definable closure** of A.*

NOTE 1.4.5. Let $\mathcal{L} = (\{R_i\}_{i\in I}, \{f_j\}_{j\in J}, \{c_k\}_{k\in K})$. Let $\mathcal{M}$ be an $\mathcal{L}$-structure. Let $A \subseteq M$. Then $\langle A \rangle$ is the domain of a substructure of $\mathcal{M}$.

We can attribute a notion of complexity to definable sets (and by extension to formulas) by the number of quantifiers present in the formula that defines the set. Usually the fewer the quantifiers the easier the treatment of the definable set.

DEFINITION 1.4.6. *We say that an $\mathcal{L}$-structure $\mathcal{M}$ has **quantifier elimination** (QE) if for every formula $\phi(\overline{v})$ there is a quantifier-free formula $\psi(\overline{v})$ such that*

$$\mathcal{M} \vDash \forall \overline{v}(\phi(\overline{v}) \Leftrightarrow \psi(\overline{v})).$$

We say that a theory T has QE if every model of T has QE.

We have a simpler sufficient condition for QE

PROPERTY 1.4.7. *Let T be an theory. Suppose that for every quantifier-free $\mathcal{L}$-formula $\theta(\overline{v}, w)$ there is a quantifier-free formula $\psi(\overline{v})$ such that $T \vDash \forall\overline{v}(\exists w\theta(\overline{v}, w) \Leftrightarrow \psi(\overline{v}))$. Then T has quantifier elimination.*

Proof. Consult Lemma 3.1.5 of [3]. $\square$

An immediate feature of a theory with QE is the following

PROPERTY 1.4.8. *Let T be a theory with QE. Let $\mathcal{M}, \mathcal{N} \vDash T$. Then*

$$\mathcal{M} \subseteq \mathcal{N} \Rightarrow \mathcal{M} \preceq \mathcal{N}.$$

Proof. This is obvious by 1.2.6. $\square$

PROPERTY 1.4.9. *Let T be a theory with QE that has an universal axiomatization. Let $\mathcal{N} \vDash T$. Then*

$$\mathcal{M} \subseteq \mathcal{N} \Rightarrow \mathcal{M} \preceq \mathcal{N}.$$

Proof. By 1.3.8 $\mathcal{M} \subseteq \mathcal{N}$ implies $\mathcal{M} \vDash T$. By 1.4.8 $\mathcal{M} \preceq \mathcal{N}$. $\square$

Sometimes it is useful to add new symbols to the language.

DEFINITION 1.4.10. *Let $\mathcal{L}'$ be an extension of a language $\mathcal{L}$. Let $\mathcal{M}'$ be an $\mathcal{L}'$-structure. The $\mathcal{L}$-structure $\mathcal{M}$ obtained from $\mathcal{M}'$ by ignoring the interpretations of the symbols in $\mathcal{L}' \setminus \mathcal{L}$ is called a **reduct** of $\mathcal{M}'$ and $\mathcal{M}'$ is said to be an **expansion** of $\mathcal{M}$.*

The following property illustrates a technique using a new constant symbol in a language.

PROPERTY 1.4.11. *Let T be an $\mathcal{L}$-theory. Let $\psi_1(v), ..., \psi_k(v), \phi(v)$ be $\mathcal{L}$-formulas. Let d be a new constant symbol. The following are equivalent*

1) $T \cup \{\psi_1(d), ..., \psi_k(d)\} \vDash \phi(d)$.

2) $T \vDash \forall v(\bigwedge_{i=1}^{k} \psi_i(v) \Rightarrow \phi(v))$.

Proof. 2) $\Rightarrow$ 1) Obvious.

1) $\Rightarrow$ 2) Let $\mathcal{M} \vDash T$. Independently of the interpretation $d^{\mathcal{M}} \in M$, if we assume $\mathcal{M} \vDash \bigwedge_{i=1}^{k} \psi_i(d^{\mathcal{M}})$, we get $\mathcal{M} \vDash T \cup \{\psi_1(d), ..., \psi_k(d)\}$, and so $\mathcal{M} \vDash \phi(d)$. Since this is valid for all interpretations of d, we have $\mathcal{M} \vDash \forall v(\bigwedge_{i=1}^{k} \psi_i(v) \Rightarrow \phi(v))$. $\square$

Next follows a quantifier elimination criteria that will be useful later.

THEOREM 1.4.12. *Let $\mathcal{L}$ be a language with a constant symbol c and T an $\mathcal{L}$-theory. Let $\phi(\overline{v})$ be an $\mathcal{L}$-formula. The following are equivalent*

1) $T \vDash \forall\overline{v}(\phi(\overline{v}) \Leftrightarrow \psi(\overline{v}))$ for some quantifier-free formula $\psi(\overline{v})$.

2) If $\mathcal{M}, \mathcal{N} \vDash T$ and $\sigma_{\mathcal{M}} : \mathcal{A} \to \mathcal{M}$, $\sigma_{\mathcal{N}} : \mathcal{A} \to \mathcal{N}$ are embeddings, then for all $\overline{a} \in A^n$, $\mathcal{M} \vDash \phi(\sigma_{\mathcal{M}}(\overline{a}))$ if and only if $\mathcal{N} \vDash \phi(\sigma_{\mathcal{N}}(\overline{a}))$.

Proof. 1) $\Rightarrow$ 2) Let $\mathcal{A}$ be a common substructure of $\mathcal{M}$ and $\mathcal{N}$. By 1.2.6, for all quantifier-free formulas ξ and $\overline{a} \in A^\omega$ we have $\mathcal{A} \vDash \xi(\overline{a}) \Leftrightarrow \mathcal{M} \vDash \xi(\sigma_{\mathcal{M}}(\overline{a}))$ and $\mathcal{A} \vDash \xi(\overline{a}) \Leftrightarrow \mathcal{N} \vDash \xi(\sigma_{\mathcal{N}}(\overline{a}))$. In particular

$$\begin{aligned} \mathcal{M} \vDash \phi(\sigma_{\mathcal{M}}(\overline{a})) &\Leftrightarrow \mathcal{M} \vDash \psi(\sigma_{\mathcal{M}}(\overline{a})) \\ &\Leftrightarrow \mathcal{A} \vDash \psi(\overline{a}) \\ &\Leftrightarrow \mathcal{N} \vDash \psi(\sigma_{\mathcal{N}}(\overline{a})) \\ &\Leftrightarrow \mathcal{N} \vDash \phi(\sigma_{\mathcal{N}}(\overline{a})). \end{aligned}$$

2) $\Rightarrow$ 1) We want a quantifier-free formula $\psi(\overline{v})$ such that $T \models \forall \overline{v}(\phi(\overline{v}) \Leftrightarrow \psi(\overline{v}))$. If $T \models \forall \overline{v}\phi(\overline{v})$ then $T \models \forall \overline{v}(\phi(\overline{v}) \Leftrightarrow c = c)$, so ψ can be $c = c$. If $T \models \forall \overline{v}\neg\phi(\overline{v})$ then $T \models \forall \overline{v}(\phi(\overline{v}) \Leftrightarrow c \neq c)$, so ψ can be $c \neq c$. Therefore we can assume that both $T \cup \{\exists \overline{v}\neg\phi(\overline{v})\}$ and $T \cup \{\exists \overline{v}\phi(\overline{v})\}$ are satisfiable. Let

$$\Gamma(\overline{v}) = \{\psi(\overline{v}) \in \mathcal{L}\text{-formula} : \psi(\overline{v}) \text{ is quantifier-free and } T \models \forall \overline{v}(\phi(\overline{v}) \Rightarrow \psi(\overline{v}))\}.$$

Let $d_1, ..., d_n$ be new constant symbols and let $\overline{d} = (d_1, ..., d_n)$. We will show that $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$. This concludes the proof for the following reason: By 1.3.6, there will be a finite subset $\Delta \subseteq T$ and $\psi_1(\overline{d}), ..., \psi_k(\overline{d}) \in \Gamma(\overline{d})$ such that

$$\Delta \cup \{\psi_1(\overline{d}), ..., \psi_k(\overline{d})\} \models \phi(\overline{d}).$$

By 1.4.11, we have

$$\Delta \models \forall \overline{v}(\bigwedge_{i=1}^{k} \psi_i(\overline{v}) \Rightarrow \phi(\overline{v})).$$

In particular

$$T \models \forall \overline{v}(\bigwedge_{i=1}^{k} \psi_i(\overline{v}) \Rightarrow \phi(\overline{v})).$$

Thus establishing

$$T \models \forall \overline{v}(\bigwedge_{i=1}^{k} \psi_i(\overline{v}) \Leftrightarrow \phi(\overline{v})).$$

We proceed with the proof of $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$. Suppose $T \cup \Gamma(\overline{d}) \not\models \phi(\overline{d})$. Let $\mathcal{M}$ be a $(\mathcal{L}, d_1, ..., d_n)$-structure such that $\mathcal{M} \models T \cup \Gamma(\overline{d}) \cup \{\neg\phi(\overline{d})\}$ and let $\mathcal{A}$ be the substructure generated by $\{d_1^{\mathcal{M}}, ..., d_n^{\mathcal{M}}\}$. Let $\Sigma = T \cup \mathrm{Diag}(\mathcal{A}) \cup \{\phi(\overline{d})\}$. If Σ is not satisfiable then

$$T \cup \mathrm{Diag}(\mathcal{A}) \models \neg\phi(\overline{d})$$

and by compactness, there are formulas $\psi_1(\overline{d}), ..., \psi_k(\overline{d}) \in \mathrm{Diag}(\mathcal{A})$ such that

$$T \models \forall \overline{v}(\bigwedge_{i=1}^{k} \psi_i(\overline{v}) \Rightarrow \neg\phi(\overline{v})),$$

or equivalently, putting $\psi(\overline{v}) = \bigwedge_{i=1}^{k} \psi_i(\overline{v})$

$$T \models \forall \overline{v}(\phi(\overline{v}) \Rightarrow \neg\psi(\overline{v})).$$

Note that $\psi(\overline{d})$ is quantifier-free. Thus $\neg\psi(\overline{d}) \in \Gamma(\overline{d})$, implying $\mathcal{M} \models \neg\psi(\overline{d})$. But $\mathrm{Diag}(\mathcal{A}) \models \psi(\overline{d})$, implying $\mathcal{M} \models \psi(\overline{d})$, which is absurd. Thus Σ is satisfiable. Let $\mathcal{N} \models \Sigma$. Since $\mathrm{Diag}(\mathcal{A}) \subseteq \Sigma$, by 1.2.11, $\mathcal{A} \subseteq \mathcal{N}$. Since $\mathcal{N} \models \phi(\overline{d}^{\mathcal{N}})$, by the hypothesis we would have $\mathcal{M} \models \phi(\overline{d}^{\mathcal{M}})$ which is absurd. $\square$

Besides structures with quantifier elimination we will also study structures with the property of o-minimality, where the definable sets have interesting geometrical properties.

DEFINITION 1.4.13. *Let $\mathcal{R} = (R, <, ...)$ be a linearly ordered dense set without end points. We say that $\mathcal{R}$ is* ***o-minimal*** *if every definable set in R is a finite union of points and open intervals. A theory T is o-minimal if every model of T is o-minimal.*

We will prove in the next chapter that any rcof is o-minimal and has QE.

1.5 Brief digression on types

Throughout this section let $\mathcal{M}$ be an $\mathcal{L}$-structure and $A \subseteq M$. Let $\mathcal{L}_A$ denote the extension of the language $\mathcal{L}$ by constant symbols for each $a \in A$ or symbolically $\mathcal{L}_A = (\mathcal{L}, \{a\}_{a \in A})$. Note that $\mathcal{M}$ can naturally be viewed as an $\mathcal{L}_A$-structure by interpreting each new constant symbol in the obvious way. $Th_A(\mathcal{M})$ denotes the $\mathcal{L}_A$-theory of $\mathcal{M}$.

DEFINITION 1.5.1. *Let $\Sigma(x)$ be a set of $\mathcal{L}$-formulas having at most n free variables $x = (x_1, ..., x_n)$. We say that $\Sigma(x)$ is **satisfiable** if there is an $\mathcal{L}$-model $\mathcal{N}$ and an element $c \in N^n$ such that $\mathcal{N} \vDash \phi(c)$ for every $\phi(x) \in \Sigma(x)$. In this case we say that $\mathcal{N}$ **realizes** or **satisfies** $\Sigma(x)$.*

In the setting of ordered fields, $\mathbb{Q}$ doesn't satisfy the intermediate value theorem. For example $x^2 - 2 = 0$ doesn't have a solution in $\mathbb{Q}$. Nevertheless we can ponder about the existence of such a solution in an extension of $\mathbb{Q}$. The following notion allow us to talk about hipothetical elements that satisfy a set of formulas.

DEFINITION 1.5.2. *Let $\Sigma(x)$ be a set of $\mathcal{L}_A$-formulas having at most n free variables $x = (x_1, ..., x_n)$. The set $\Sigma(x)$ is an n-**type** of $\mathcal{M}$ over A if there is $\mathcal{N} \vDash Th_A(\mathcal{M})$ satisfying $\Sigma(x)$. A 1-type is simply called a **type**.*

NOTE 1.5.3. When dealing with types we can omit the structure or the subset whenever it is implicitly understood, so we can call $\Sigma(x)$ an n-type instead of an n-type of $\mathcal{M}$ over A.

Following the comment about the equation $x^2 - 2 = 0$ in the ordered field $\mathbb{Q}$, we know that $\mathbb{R}$ has two elements that solve the equation, namely $\sqrt{2}$ and $-\sqrt{2}$. If we add the condition $x > 0$ we get a unique element that solves the equation.

DEFINITION 1.5.4. *We say that an n-type $\Sigma(x)$ is a **complete** n-**type** if $\phi(x) \in \Sigma(x)$ or $\neg\phi(x) \in \Sigma(x)$ for every $\mathcal{L}_A$-formula $\phi(x)$ with n free variables. We let $S_n^{\mathcal{M}}(A)$ be the set of all complete n-types of $\mathcal{M}$ over A.*

DEFINITION 1.5.5. *Let $b \in M^n$. The **type** of b over A is defined by*

$$\text{tp}(b/A) := \{\phi(v) \in \mathcal{L}_A\text{-formulas} : \mathcal{M} \vDash \phi(b)\}.$$

PROPERTY 1.5.6. *Let $\Sigma(x)$ be a type of $\mathcal{M}$ over A. There is an elementary extension $\mathcal{N}$ of $\mathcal{M}$ realizing $\Sigma(x)$.*

Proof. Consult Proposition 4.1.3 of [3]. □

PROPERTY 1.5.7. *A type $\Sigma(x)$ of $\mathcal{M}$ over A is a complete type realized by $\mathcal{N}$ if and only if there is $b \in N^n$ such that $\Sigma(x) = \text{tp}(b/A)$.*

Proof. Consult Corollary 4.1.4 of [3]. □

In the case of the ordered field $\mathbb{Q}$, $\sqrt{2}$ is uniquely defined in $\mathbb{R}$ by the formulas $x^2 - 2 = 0$ and $x > 0$. So, although the type of $\sqrt{2}$ over $\mathbb{Q}$ is a complete type, it can be uniquely determined by just two formulas. Another example is the following.

PROPERTY 1.5.8. *Let $\mathcal{M}$ be an o-minimal structure, $A \subseteq M$ and $y \in M$. The type $\text{tp}(y/A)$ is determined by the cut y makes in the ordering of A.*

Proof. Consult Proposition 4.1.13 of [3]. □

DEFINITION 1.5.9. *Let $\mathcal{M}$ be a model in some first-order language and k a finite or infinite cardinal. We say that $\mathcal{M}$ is k-**saturated** if for all subsets $A \subseteq M$ such that $|A| < k$, $\mathcal{M}$ realizes all complete types over A. The model $\mathcal{M}$ is called **saturated** if it is $|M|$-saturated.*

The main characteristic of saturated models is that we can do things in the model that we usually could only do in an elementary extension.

LEMMA 1.5.10. *Let T be an $\mathcal{L}$-theory k be an infinite ordinal. Suppose $\mathcal{M} \vDash T$ is k-saturated. If $\mathcal{N} \vDash T$ and $|N| < k$, then there is an elementary embedding of $\mathcal{N}$ into $\mathcal{M}$.*

Proof. Suppose $\{n_\alpha \in N : \alpha < k\}$ enumerates N. Let $A_\alpha = \{n_\beta \in N : \beta < \alpha\}$. We construct a chain of functions $f_\alpha : A_\alpha \to M$ and take its union to end up with the embedding from $\mathcal{N}$ to $\mathcal{M}$. For $\alpha = 0$ let $f_0 = \emptyset$. For a limit ordinal α let $f_\alpha = \bigcup_{\beta<\alpha} f_\beta$. Suppose α is an ordinal such that f_α is a well defined function with the property

$$\mathcal{N} \vDash \phi(a_1, ..., a_n) \Leftrightarrow \mathcal{M} \vDash \phi(f_\alpha(a_1), ..., f_\alpha(a_n))$$

for all $\mathcal{L}$-formulas ϕ and $a_1, ..., a_n \in A_\alpha$. Note that if A_α is the domain of a substructure of $\mathcal{M}$ then f_α is an elementary embedding of $\mathcal{A}_\alpha$ into $\mathcal{N}$. If already $A_\alpha = N$ then put $f_{\alpha+1} = f_\alpha$. Otherwise, let

$$\Gamma_\alpha(v) = \{\phi(v) \in \mathcal{L}_{A_\alpha}\text{-formulas} : \mathcal{N} \vDash \phi(n_\alpha)\}.$$

Since $|A_\alpha| < k$ and $\mathcal{M}$ is k-saturated, $\Gamma(v)$ is realized by some $b \in M$ (where the constant symbols $a \in A_\alpha$ in each $\phi(v)$ have the interpretation $a^{\mathcal{M}} = f_\alpha(a)$). Put

$$f_{\alpha+1} = f_\alpha \cup \{(n_\alpha, b)\}.$$

This function is well defined and preserves truth of formulas. Hence $\bigcup_{\alpha<k} f_\alpha : \mathcal{N} \to \mathcal{M}$ is an elementary embedding. □

Saturated models can be used to test if a theory has quantifier elimination.

THEOREM 1.5.11. *If $\mathcal{L}$ is a language containing a constant symbol and T is an $\mathcal{L}$-theory, then T has quantifier elimination if and only if whenever $\mathcal{M} \vDash T$, $\mathcal{N} \vDash T$ is $|M|^+$-saturated, $\mathcal{A}$ is a substructure of $\mathcal{M}$ and $\sigma : \mathcal{A} \to \mathcal{N}$ is an embedding, then σ extends to an embedding of $\mathcal{M}$ into $\mathcal{N}$.*

Proof. ($\Rightarrow$) Since T has QE, $\sigma : \mathcal{A} \to \mathcal{N}$ is an elementary embedding. The results follows by making a similar construction as in the proof of 1.5.10, replacing f_0 by σ.

($\Leftarrow$) Let $\mathcal{M}, \mathcal{M}' \vDash T$. Let $\sigma_{\mathcal{M}} : \mathcal{A} \to \mathcal{M}$ and $\sigma_{\mathcal{M}'} : \mathcal{A} \to \mathcal{M}'$ be embeddings. Let $\mathcal{N} \vDash T$ be an $|M|^+$-saturated model and $\tau : \mathcal{M}' \to \mathcal{N}$ an elementary embedding. Since $\mathcal{A} \subseteq \mathcal{M}' \preceq \mathcal{N}$, the map $\sigma_{\mathcal{N}} : \mathcal{A} \to \mathcal{N},\ \ a \mapsto \tau(\sigma_{\mathcal{M}'}(a))$ is an embedding. By hypothesis $\sigma_{\mathcal{N}}$ extends to an embedding $\widetilde{\sigma_{\mathcal{N}}} : \mathcal{M} \to \mathcal{N}$.

We will prove that for every $\overline{a} \in A^n$

$$\mathcal{M}' \vDash \exists w \phi(\sigma_{\mathcal{M}'}(\overline{a}), w) \Leftrightarrow \mathcal{M} \vDash \exists w \phi(\sigma_{\mathcal{M}}(\overline{a}), w)$$

and use 1.4.12 to conclude that there is a quantifier-free formula $\psi(\overline{v})$ such that $T \vDash \forall \overline{v}(\exists w \phi((\overline{v}), w) \Leftrightarrow \psi(\overline{v}))$.

Let $\phi(\overline{v}, w)$ be a quantifier-free formula. Let $\overline{a} \in A^n$. Suppose $\mathcal{M} \vDash \exists w \phi(\overline{a}, w)$ and let $b \in M$ such that $\mathcal{M} \vDash \phi(\overline{a}, b)$. Thus $\mathcal{N} \vDash \phi(\sigma_{\mathcal{N}}(\overline{a}), \widetilde{\sigma_{\mathcal{N}}}(b))$. This implies $\mathcal{N} \vDash \exists w \phi(\tau(\sigma_{\mathcal{M}'}(\overline{a})), w)$. Since $\mathcal{M}' \preceq \mathcal{N}$, $\mathcal{M}' \vDash \exists w \phi(\sigma_{\mathcal{M}'}(\overline{a}), w)$. Reciprocally, assuming $\mathcal{M}' \vDash \exists w \phi(\sigma_{\mathcal{M}'}(\overline{a}), w)$, we can make a similar argument considering an elementary embedding $\tau' : \mathcal{M} \to \mathcal{N}$ and $\sigma'_{\mathcal{N}} : \mathcal{A} \to \mathcal{N},\ \ a \mapsto \tau'(\sigma_{\mathcal{M}}(a))$, to conclude $\mathcal{M} \vDash \exists w \phi(\overline{a}, w)$. □

Chapter 2

QE for the theory of rcof

Trhoughout this chapter let $\mathcal{R} = (R, <, +, -, \cdot, 0, 1)$ be a rcof. It is easy to see that any quantifier-free formula defines on $\mathcal{R}$ a subset

$$V = \{x \in R^n : f_1(x) = ... = f_k(x) = 0,\ g_1(x) > 0, ..., g_l(x) > 0\},$$

where $f_1, ..., f_k, g_1, ..., g_l \in R[X],\ X = (X_1, ..., X_n)$. A set of this form is called a **semialgebraic set**. It is easy to see that the semialgebraic sets are closed under boolean operations. We will see that they are also closed under projections, which proves that the theory of rcof has QE. This result is known as the **Tarski-Seidenberg theorem**. We start with some considerations about the roots of polynomials with coefficients in R. We will consider the algebraic closure $\bar{R}$ of R. This algebraic closure behaves essentially in the same way as $\mathbb{C}$ does to $\mathbb{R}$ in the sense that $\bar{R} = R[i]$, where $i^2 = -1$, and so we can talk about a norm in $\bar{R}$ ($|z|^2 = |a + bi|^2 = a^2 + b^2$, where $a, b \in R$). This norm in $\bar{R}$ is compatible with the usual interval topology in R:

DEFINITION 2.0.1. *An **interval** in R is a set of the form*

$$(a, b) := \{x \in R : a < x < b\} \ \textit{with} \ -\infty \leq a < b \leq +\infty.$$

*We equip R with the interval topology (the intervals form a base), and each product R^m with the corresponding product topology. A **box** in R^m is a cartesian product of m intervals. Note that R^m is a Hausdorff space with this topology.*

NOTATION. The following sets are not intervals

$$\begin{aligned}
(a, b] &:= \{x \in R : a < x \leq b\} \ \text{with} \ -\infty \leq a < b < +\infty;\\
[a, b) &:= \{x \in R : a \leq x < b\} \ \text{with} \ -\infty < a < b \leq +\infty;\\
[a, b] &:= \{x \in R : a \leq x \leq b\} \ \text{with} \ -\infty < a \leq b < +\infty.
\end{aligned}$$

2.1 Roots of polynomials in $R[X]$

In this section we lay out some properties about the roots of polynomials in $R[X]$. Unless specified, whenever we mention a root, we are considering a root in $\bar{R}$. If we mean a root in R we will call it a **real root**. Another word for root is **zero**.

LEMMA 2.1.1. *Let α be a root of the monic polynomial*

$$f(T) = a_0 + a_1 T + ... + a_{d-1} T^{d-1} + T^d \in \bar{R}[T].$$

Then $|\alpha| < 1 + \max\{|a_i| : i = 0, 1, ..., d-1\}$

Proof. $f(\alpha) = 0$ is equivalent to:

$$\alpha^d = -(a_0 + a_1\alpha + ... + a_{d-1}\alpha^{d-1}).$$

Let $M = \max\{|a_i| : i = 0, 1, ..., d-1\}$. Then

$$\begin{aligned} |\alpha|^d &\leq M(1 + |\alpha| + ... + |\alpha|^{d-1}| \\ &= M\frac{|\alpha|^d - 1}{|\alpha| - 1}. \end{aligned}$$

If $|\alpha| > 1 + M$, then

$$\begin{aligned} |\alpha|^d &< M\frac{|\alpha|^d - 1}{M} \\ &= |\alpha|^d - 1 \end{aligned}$$

which is absurd. □

LEMMA 2.1.2 (Continuity of roots). *Let $f(T) = a_0 + a_1T + ... + a_dT^d \in R[T]$ be a polynomial. For every $\epsilon > 0$ there is $\delta > 0$ such that if $|a_i - b_i| \leq \delta$ for $i = 0, ...d$, then for every root β of $g(T) = b_0 + b_1T + ... + b_dT^d \in R[T]$ there is a root α of f such that $|\alpha - \beta| < \epsilon$.*

Proof. Let $f(T) = a_0 + a_1T + ... + a_dT^d$. We can write

$$f(T) = a_d(T - \alpha_1)...(T - \alpha_d) \text{ for some } \alpha_1, ..., \alpha_d \in \bar{R}.$$

Let $\epsilon > 0$ and let

$$\begin{aligned} M &= 2 + 2\max_{0\leq i\leq d-1}\left(\frac{|a_i|}{|a_d|}\right); \\ 0 < \delta &< \min_{0\leq i\leq d-1}\left(\frac{|a_d\epsilon^d|}{|\sum_{k=0}^{d} M^k|}, \frac{|a_d|}{2}, \frac{|a_i|}{|a_d|}, |a_i|\right); \\ g(T) &= b_0 + b_1T + ... + b_dT^d \text{ such that } |a_i - b_i| < \delta. \end{aligned}$$

We have $|b_d| > |a_d|$ or $|b_d| > ||a_d| - \delta|$: Suppose $|b_d| \leq |a_d|$. Then $|a_d| - |b_d| \leq |a_d - b_d| < \delta$. So $|b_d| > |a_d| - \delta$. Since $\delta \leq \frac{|a_d|}{2}$ we have $|b_d| > ||a_d| - \delta|$ as we wanted.

Let β be a root of $g(T)$. We now prove that whether $|b_d| > |a_d|$ or $|b_d| > ||a_d| - \delta|$ we have $\beta < M$. By Lemma 2.1.1,

$$|\beta| < 1 + \max_{0\leq i\leq d-1}\left(\frac{|b_i|}{|b_d|}\right).$$

Suppose $|b_d| > |a_d|$. Then

$$\begin{aligned} \frac{|b_i|}{|b_d|} &< \frac{|b_i|}{|a_d|} \\ &\leq \frac{|b_i - a_i| + |a_i|}{|a_d|} \\ &\leq \frac{|a_i|}{|a_d|} + \frac{\delta}{|a_d|} \\ &\leq 2\frac{|a_i|}{|a_d|}. \end{aligned}$$

So $\beta < M$.

Suppose now $|b_d| > ||a_d| - \delta|$. Then

$$\begin{aligned}\frac{|b_i|}{|b_d|} &< \frac{|b_i - a_i| + |a_i|}{|a_d - \delta|} \\ &< \frac{|a_i| + \delta}{|a_d - \delta|} \\ &\leq \frac{|a_i| + \delta}{|a_d - \frac{|a_d|}{2}|} \\ &\leq 2\frac{|a_i|}{|a_d|} + 1\end{aligned}$$

and so again $\beta < M$.

Observe now that

$$|f(\beta)| = |f(\beta) - g(\beta)| \leq \sum_{i=0}^{d} |a_i - b_i||\beta|^i < \delta \sum_{i=0}^{d} M^i < |a_d|\epsilon^d.$$

On the other hand, $f(\beta) = a_d(\beta - \alpha_1)...(\beta - \alpha_d)$, so at least one of the factors $|(\beta - \alpha_i)|$ has to be less than ϵ. $\square$

We will say something more in the line of the previous lemma. For the rest of this section X will denote a topological space and E a ring of continuous functions $f : X \to R$, equipped with pointwise addition and multiplication. If we endow the product topology to $X \times R$, we can consider the ring of polynomials $E[T]$ where each polynomial

$$f(T) = f_0 + f_1T + ...f_dT^d$$

is interpreted as the continuous function $(x, t) \mapsto f_0(x) + f_1(x)t + ...f_d(x)t^d$. In this way, $X \times R$ is a topological space and $E[T])$ is a ring of continuous functions $f(T) : X \times R \to R$, equipped with pointwise addition and multiplication. The pair $(X \times R, E[T])$ should be thought as an extension of the pair (X, E).

NOTATION. Let $A = (A_0, ..., A_d)$ be a tuple of distinct variables and let

$$f(A, T) = A_0 + A_1T + ... + A_dT^d \in \mathbb{Z}[A, T].$$

Let $a \in \bar{R}^{d+1}$. We denote by

$$Z_{=k}(f(a, T))$$

the proposition "the number of distinct roots (in $\bar{R}$) of $f(a, T)$ is $= k$". We will also use the notations $Z_{<k}(f(a, T))$ and $Z_{\leq k}(f(a, T))$ with the obvious meanings.

LEMMA 2.1.3. *Suppose X is connected. Let $f = f_0 + f_1T + ... + f_dT^d \in E[T]$, and suppose $e \leq d$ is such that for every $x \in X$, $Z_{=e}(f(x, T))$. Then the number of distinct real roots of $f(x, T)$ is also constant as x ranges over X. Writing $\zeta_1(x) < ... < \zeta_k(x)$ for these real roots, the functions $\zeta_i : X \to R$ are continuous.*

Proof. Let $x_0 \in X$ and $z_1, ..., z_e$ be the distinct roots of $f(x_0, T)$. For each $i \in \{1, ..., e\}$ let $B_i \subset \bar{R}$ be a closed ball with $z_i \in B_i$, $B_i \cap B_j = \emptyset$ whenever $i \neq j$ and $B_i \cap R = \emptyset$ whenever $z_i \in \bar{R} - R$. Let U be an open subset of X such that $x_0 \in U$ and, for each $x \in U$, $f(x, T)$ has exactly one root in B_i for each $i \in \{1, ..., e\}$ (Lemma 2.1.2). Let $\xi_i : U \to B_i$ be the function that sends $x \in U$ to the unique root of $f(x, T)$ in B_i.

Claim: ξ_i is continuous

Proof: Let $\delta > 0$. We will prove the existence of an open set $V \subset U$ with $a \in V$ such that for all $x \in V$, $|\xi(x) - \xi(a)| < \delta$. Let $\epsilon > 0$ such that for every $b_0, ..., b_d \in \bar{R}$ with $|b_i - f_i(a)| < \epsilon$, there is a root β of $g(T) = b_0 + b_1T + ... + b_dT^d$ with $|\beta - \xi(a)| < \delta$ (Lemma 2.1.2). Let $V_i \subset U$ be an open set with $a \in V_i$ such that for all $x \in V_i$, $|f_i(x) - f_i(a)| < \epsilon$ (continuity of each function f_i). Let $V = \bigcap V_i$. Since for every $x \in U$ there is a unique root of $f(x, T)$, we have that for every $x \in V$, $|\xi(x) - \xi(a)| < \delta$ as we wanted.

The coefficients of $f(x, T)$ are real so the set $\{\xi_1(x), ..., \xi_e(x)\}$ is closed under "complex" conjugation. This implies that if $\xi_i(x_0) = z_i \in R$ then $\xi_i(x) \in R$ for all $x \in U$. This shows that the number of real roots is locally constant. Since X is connected, we can extend ξ_i to a continuous function $\zeta_i : X \to R$ and so the number of zeros is also constant in X. $\square$

2.2 Semialgebraic cell decomposition

In this section we evidence the relationship between the zero-sets of polynomials and the semialgebraic sets.

NOTE 2.2.1. Let $p(T) = a_0 + a_1T + ... + a_dT^d$ be a polynomial in $\bar{R}[T]$. Suppose $p(T) = (T - T_1)^{n_1}...(T - T_m)^{n_m}$, where T_i's are the distinct roots of p. Then

$$\text{degree}(\ \text{gcd}(p, \frac{\partial p}{\partial T})\ ) = d - m;$$

$$\text{degree}(\ \text{lcm}(p, \frac{\partial p}{\partial T})\ ) = d + m - 1.$$

LEMMA 2.2.2. *Let $A = (A_0, ..., A_d)$ be a tuple of distinct variables and let*

$$f(A, T) = A_0 + A_1T + ... + A_dT^d \in \mathbb{Z}[A, T].$$

Let $e \in \{0, ..., d\} \cup \{\infty\}$. Then the set

$$\{a \in \bar{R}^{d+1} : Z_{=e}(f(a, T))\}$$

is a finite union of sets of the form

$$\{a \in \bar{R}^{d+1} : p_1(a) = ... = p_k(a) = 0,\ \ q(a) \neq 0\}$$

where $p_i(A), q(A) \in \mathbb{Z}[A]$.

Proof. Let $d > 0$ and $a = (a_0, ..., a_d) \in \bar{R}^{d+1}$. Let m be the number of distinct zeros of $f(a, T)$. The degree of $\text{lcm}(f(a, T), \frac{\partial f}{\partial T}(a, T))$ is $d + m - 1$. Let $0 < k < d$. Then

$$\begin{cases} f(a,T)q(x,T) = \frac{\partial f}{\partial T}(a,T)r(x,T), \text{ for some nonzero} \\ x = (x_0, ..., x_{2k+1}) \in \bar{R}^{2k+1}, \text{ where} \\ q(x,T) = x_0 + x_1T + ... + x_{k-1}T^{k-1}, \text{ and} \\ r(x,T) = x_k + x_{k+1}T + ... + x_{2k}T^k \end{cases}$$

is equivalent to the condition $d + m - 1 \leq d + k - 1$, that is to $m \leq k$. This is equivalent to $Z_{\leq k}(f(a, T))$. We have

$$\begin{aligned} &f(a,T)q(x,T) - \frac{\partial f}{\partial T}(a,T)r(x,T) \\ &= \beta_0(a,x) + \beta_1(a,x)T + ... + \beta_{d+k-1}(a,x)T^{d+k-1} \end{aligned}$$

for some bilinear functions $\beta_0, ..., \beta_{d+k-1} : \bar{R}^{d+1} \times \bar{R}^{2k+1} \to \bar{R}$. Hence the previous condition is equivalent to

$$\beta_0(a, x) = ... = \beta_{d+k-1}(a, x) = 0$$

for some nonzero $x \in \bar{R}^{2k+1}$, that is, to the condition that the linear map

$$x \mapsto (\beta_0(a, x), ..., \beta_{d+k-1}(a, x))$$

has nontrivial kernel. This in turn, is equivalent to the vanishing of all $(d + k - 1) \times (d + k - 1)$ minors of the matrix of this linear map. This expresses the set

$$\{a \in \bar{R}^{d+1} : a_d \neq 0 \ \wedge \ Z_{\leq k}(f(a,T))\}$$

as the intersection of $\{a \in \bar{R}^{d+1} : a_d \neq 0\}$ with the zero set of certain polynomials in $\mathbb{Z}[A]$. We obtain the conclusion of the lemma by considering the intersection of the previous set with the complementary of $\{a \in \bar{R}^{d+1} : a_d \neq 0 \ \wedge \ Z_{\leq k-1}(f(a,T))\}$. □

DEFINITION 2.2.3. *A set $A \subseteq X$ is an E-**set** if A is a finite union of sets of the form*

$$\{x \in X : f(x) = 0,\ g_1(x) > 0, ...,\ g_k(x) > 0\}$$

with $f, g_1, ..., g_k \in E$.

We can think about the E-sets as a generalization of the semialgebraic sets. Note that the E-sets form a boolean algebra of subsets of X. An easy application of lemma 2.2.2 is the following:

LEMMA 2.2.4. *Let $f(T) = f_0 + f_1T + ... + f_dT^d \in E[T]$. Then the set*

$$\{x \in X : Z_{=e}(f(x,T))\}$$

is an E-set.

Proof. Let $g(A,T) =: A_0 + A_1T + ... + A^dT^d \in \mathbb{Z}[A,T]$. The set

$$\{\bar{f}(x) = (f_0(x), ..., f_d(x)) \in R^{d+1} : Z_{=e}(g(\bar{f}(x),T))\}$$

is contained in $\{a \in \bar{R}^{d+1} : Z_{=e}(g(a,T))\}$ which by lemma 2.2.2, is given by a finite union of sets of the form

$$\{a \in \bar{R}^{d+1} : p_1(a) = ... = p_k(a) = 0,\ \ q(a) \neq 0\}.$$

Thus

$$\{x \in X : Z_{=e}(f(x,T))\}$$

is given by a finite union of sets of the form

$$\{x \in X : p_1(\bar{f}(x)) = ... = p_k(\bar{f}(x)) = 0,\ \ q(\bar{f}(x)) \neq 0\}$$

Note that for every polynomial p we have $p \circ \bar{f} \in E$. □

Now follows an easy lemma that will be useful to prove the next theorem.

LEMMA 2.2.5 (Thom's lemma). *Let $f_1, ..., f_k \in R[T]$ be nonzero polynomials such that if $f_i' \neq 0$, then $f_i' \in \{f_1, ..., f_k\}$. Let $\epsilon : \{1, ..., k\} \to \{-1, 0, 1\}$, and put*

$$A_\epsilon = \{t \in R : \text{sign}(f_i(t)) = \epsilon(i), i = 1, ..., k\}.$$

Then A_ϵ is empty, a point, or an interval. If $A_\epsilon \neq 0$, then its closure is given by

$$cl(A_\epsilon) = \{t \in R : \text{sign}(f_i(t)) = \{\epsilon(i), 0\}\ i = 1, ..., k\}.$$

Proof. We prove by induction. If $k = 1$ then $f_1' = 0$ so f_1 is constant and the result holds. Suppose the results holds for $k \geq 1$. Let $\{f_1, ..., f_{k+1}\}$ be a set with the conditions of the lemma, and let $\epsilon' : \{1, ..., k, k+1\} \to \{-1, 0, 1\}$ be an application. Let ϵ be the restriction of ϵ' to $\{1, ..., k\}$. We have

$$A_{\epsilon'} = A_\epsilon \cap \{t \in R : \text{sign}(f_{k+1}(t)) = \epsilon'(k+1)\}.$$

If A_ϵ is either empty or a point $A_{\epsilon'}$ is also of that form. Suppose A_ϵ is an interval. If $f'_{k+1} = 0$ then $\{t \in R : \text{sign}(f_{k+1}(t)) = \epsilon'(k+1)\}$ is either empty or the whole R, which proves the result. Suppose $i \in \{1, ..., k\}$ such that $f'_{k+1} = f_i \neq 0$. We have that f'_{k+1} is constant in A_ϵ, and so f_{k+1} is strictly monotone in A_ϵ. It is now easy to see that $A_{\epsilon'}$ is either empty, a point or an interval. $\square$

NOTATION. Let $R_\infty := R \cup \{-\infty, +\infty\}$. Given functions $f, g : X \to R_\infty$ we put

$$(f, g)_X := \{(x, r) \in X \times R : f(x) < r < g(x)\}$$

We write $f < g$ to indicate $f(x) < g(x)$ for all $x \in X$. We will simply write (f, g) instead of $(f, g)_X$ whenever X is implicitly understood.

The next theorem is the central result of this section.

THEOREM 2.2.6. *Given $f_1(T), ..., f_M(T) \in E[T]$, we can expand this set to $f_1(T), ..., f_N(T) \in E[T]$ with $M \leq N$, and partition X into a finite union of E-sets X_i such that for each connected component C of X_i there are continuous real valued functions $\xi_{C,1} < ... < \xi_{C,\mu(C)}$ on C with the following properties:*

1. *each f_i has constant sign (-1,0 or 1) on each of the sets $\Gamma(\xi_{C,j})$ ($1 \leq j \leq \mu(C)$) and $(\xi_{C,j}, \xi_{C,j+1})$ ($0 \leq j \leq \mu(C)$) where $\xi_{C,0} = -\infty$ and $\xi_{C,\mu(C)+1} = +\infty$.*
2. *each of the sets $\Gamma(\xi_{C,j})$ and $(\xi_{C,j}, \xi_{C,j+1})$ is of the form $\{(x, t) \in C \times R : \text{sign}(f_i(x, t)) = \epsilon(i),\ i = 1, ..., N\}$ for some function $\epsilon : \{1, ..., N\} \to \{-1, 0, 1\}$.*

Proof. Take d (big enough) such that every f_m ($1 \leq m \leq M$) can be written as

$$f_m(T) = f_{m,0} + f_{m,1}T + ... + f_{m,d}T^d$$

for some $f_{m,i} \in E$.

For each $\Delta \subseteq \{1, ..., M\} \times \{0, ..., d\}$, let

$$f_\Delta = \prod_{(m,r)\in\Delta} \frac{\partial^r f_m}{\partial T^r} \quad \in E[T].$$

Note that the degree of each f_Δ never exceeds Md^2. Consider also sets of the form

$$Z_{\Delta,e} = \{x \in X : Z_{=e}(f_\Delta)\}.$$

For each Δ fixed, letting e range over $\{0, ..., Md^2, \infty\}$, we obtain a finite partition of X by these $Z_{\Delta,e}$'s, which are E-sets by lemma 2.2.4. Since E-sets form a boolean algebra, we can choose a partition $X = X_1 \cup ... \cup X_k$ (by taking intersections of $Z_{\Delta,e}$'s) such that for every Δ there is some e such that each X_i is contained in some $Z_{\Delta,e}$. Augment $f_1, ..., f_M$ to $f_1, ..., f_N$ ($M \leq N$) such that

$$\{f_1, ..., f_N\} = \{\frac{\partial^r f_m}{\partial T^r} : 1 \leq m \leq M,\ \ 0 \leq r \leq d\}.$$

We will prove that the partition $X = X_1 \cup ... \cup X_k$ and the functions $f_1, ..., f_N$ satisfy the conclusion of the theorem.

Let C be a connected component of some X_i. Let

$$\Delta(C) = \{(m, r) : \frac{\partial^r f_m}{\partial T^r} \text{ does not vanish identically on } C \times R\}.$$

We have that C is contained in $Z_{\Delta(C),e}$ for some e. This e is finite: otherwise, one of the factors in $f_{\Delta(C)}$ would have infinite zeros for some $x \in C$, which is absurd by definition. Lemma 2.1.3 implies the existence of continuous real valued functions $\xi_{C,1} < ... < \xi_{C,\mu(C)}$ on C such that

$$\{(x, t) \in C \times R : f_{\Delta(C)}(x, t) = 0\} = \Gamma(\xi_{C,1}) \cup ... \cup \Gamma(\xi_{C,\mu(C)}).$$

We now prove that these $\xi_{C,i}$ satisfy the conclusion of the theorem.

Claim 1: each function $\frac{\partial^r f_m}{\partial T^r}$ has constant sign on each set $\Gamma(\xi_{C,i})$ $(1 \leq i \leq \mu(C))$ and $(\xi_{C,i}, \xi_{C,i+1})$ $(0 \leq i \leq \mu(C))$ with $\xi_{C,0} = -\infty$ and $\xi_{C,\mu(C)+1} = +\infty$.

Proof: If $(m, r) \notin \Delta(C)$, then $\frac{\partial^r f_m}{\partial T^r}$ vanishes identically on C, which makes the claim obvious. Suppose $(m, r) \in \Delta(C)$. The set C is contained in $Z_{\{(m,r)\},e}$ for some e. The zero-set of $\frac{\partial^r f_m}{\partial T^r}$ on $C \times R$ is given by a finite union of graphs of real valued continuous functions on C, and since $\frac{\partial^r f_m}{\partial T^r}$ is one of the factors in f_Δ, these functions have to be among the $\xi_{C,i}$'s.

We have established that $\frac{\partial^r f_m}{\partial T^r}$ has constant sign on each of the sets mentioned in the claim. Now we prove that, fixed the connected component C, these sets can be defined uniquely by a sign condition on the $\frac{\partial^r f_m}{\partial T^r}$ for $(m, r) \in \{1, ..., M\} \times \{0, ..., d\}$.

Claim 2: Suppose A is either $\Gamma(\xi_{C,i})$ (for some $1 \leq i \leq \mu(C)$) or $(\xi_{C,i}, \xi_{C,i+1})$ (for some $0 \leq i \leq \mu(C)$). Put $\epsilon(m, r) := \text{sign}(\frac{\partial^r f_m}{\partial T^r})$ on A. Let

$$A' = \{(x, t) \in C \times R : \epsilon(m, r) = \text{sign}(\frac{\partial^r f_m}{\partial T^r}(x, t)),\ \ 1 \leq m \leq M,\ \ 0 \leq r \leq d\}.$$

Then $A = A'$

Proof: Clearly $A \subseteq A'$. Suppose $A \neq A'$. Take $(x, t') \in A' \setminus A$. Let $(x, t) \in A$ and assume, without loss of generality, $t < t'$. Observe that the set $\Delta(C)$ has the property that if f_i has a corresponding index in $\Delta(C)$ and f_i' does not vanish identically in $C \times R$ then f_i' also has a corresponding index in $\Delta(C)$. This property and the fact that C is connected implies (by lemma 2.2.5) that the set $\{t \in \mathbb{R} : (x, t) \in A'\}$ must be an interval, and so $\{x\} \times [t, t'] \subseteq A'$. But $(x, t') \notin A$, so A' must have non-empty intersection with $\Gamma(\xi_{C,i})$ and $(\xi_{C,i}, \xi_{C,i+1})$ for some i, hence changing the signal of $f_{\Delta(C)}$, which is absurd since $f_{\Delta(C)}$ is a product of $\frac{\partial^r f_m}{\partial T^r}$'s. □

DEFINITION 2.2.7. *We say that the pair (X, E) has the **Łojasiewicz property** if every E-set has only finitely many connected components and each connected componet is also an E-set.*

COROLLARY 2.2.8. *If (X, E) has the Łojasiewicz property, then $(X \times R, E[T])$ also has the Łojasiewicz property. Moreover, for each $E[T]$-set, its projection onto X is an E-set.*

Proof. Let S be an $E[T]$-set and let $f_1, ..., f_M$ be the polynomials in $E[T]$ involved in the definition of S. Applying theorem 2.2.6, we can augment these polynomials to $f_1, ..., f_N$ and get a partition of X into a finite union of E-sets X_i with the property that for every i, each connected component C of X_i gives a finite partition of $C \times R$ described solely by sign conditions on the f_j's, hence a finite partition of $C \times R$ into $E[T]$-sets. Since (X, E) has the Łojasiewicz property we can assume the X_i's to be connected. And so S has only a finite number of connected components, each of them being an $E[T]$-set. It is obvious that projection of S onto X just gives a finite union of the X_i's which is an E-set. □

Observe that the $R[T_1, ..., T_n]$-sets are exacly the semialgebraic sets of R^n. For $n = 0$, R^n is just a point and $R[T_1, ..., T_n]$ is just R, hence $(R^0, \{0\})$ has the Łojasiewicz property. By induction, using the previous corollary, $(R^n, R[T_1, ..., T_n])$ has the Łojasiewicz property, and the projection of a semialgebraic set in R^{n+1} onto R^n is still a semialgebraic set.

COROLLARY 2.2.9. *Let $\mathcal{R} = (R, <, +, -, \cdot, 0, 1)$ be a rcof. The definable sets are exactly the semialgebraic sets.*

Proof. The atomic formulas define semialgebraic sets. The semialgebraic sets are closed under boolean operations and, by the aforementioned property, they are also closed under projections. By lemma 1.4.3 it is now obvious the result. □

We have shown

THEOREM 2.2.10. *The theory of rcof has QE.*

And in particular

COROLLARY 2.2.11. *Any rcof is o-minimal.*

Chapter 3

O-minimality

In this chapter we present some fundamental results of o-minimality and some interesting applications. Throughout this chapter $\mathcal{R} = (R, <, ...)$ is an o-minimal structure.

PROPERTY 3.0.1. *Let $U \subseteq R$ and $A \subseteq B \subseteq R^m$ be definable sets. Then*

1. $\inf(U)$ *and* $\sup(U)$ *exist in* R_∞*;*

2. *The boundary of U =: $\mathrm{bd}(U)$ is finite, and if $u_1 < ... < u_k$ are the points of $\mathrm{bd}(U)$ then each interval (u_i, u_{i+1}), where $u_0 = -\infty$ and $u_{k+1} = +\infty$, is either contained in U or disjoint from U;*

3. $\mathrm{cl}(A)$ *and* $\mathrm{int}(A)$ *are definable.*

Proof. Consult Lemmas 3.3 and 3.4 of [1]. □

DEFINITION 3.0.2. *A set $X \subseteq R^m$ is called **definably connected** if X is definable and X is not the union of two nonempty definable disjoint subsets that are open in X.*

PROPERTY 3.0.3. *The image of a definably connected set $X \subseteq R^m$ under a definable continuous map $f : X \to R^n$ is definably connected.*

Proof. Suppose $f(X) = A \cup B$, where A, B are definable open sets in $f(X)$ and $A \cap B = \emptyset$. Then $X = f^{-1}(A) \cup f^{-1}(B)$. The sets $f^{-1}(A), f^{-1}(B)$ are definable and disjoint. The function $f' : X \to f(X), x \mapsto f(x)$ is continuous, so $f^{-1}(A), f^{-1}(B)$ are open in X. Since X is a definably connected set, either $f^{-1}(A) = \emptyset$ or $f^{-1}(B) = \emptyset$. □

PROPERTY 3.0.4. *If $(R, <, \cdot, 1)$ is an ordered group, then $(R, \cdot, 1)$ is abelian, divisible and torsion-free.*

Proof. Consult Proposition 4.2 of [1]. □

PROPERTY 3.0.5. *If $(R, <, +, -, \cdot, 0, 1)$ is an ordered ring, then $(R, <, +, -, \cdot, 0, 1)$ is a real closed field.*

Proof. Consult Proposition 4.6 of [1]. □

From these properties and the results in the previous section we have

THEOREM 3.0.6. *An ordered ring is a rcof if and only if it is o-minimal.*

Regardless of whether $\mathcal{R}$ is a rcof, we will see an intuitively similar result to the Tarski-Seidenberg theorem, regarding continuous functions instead of polynomials.

3.1 Monotonicity Theorem and Uniform Finiteness

The monotonicity theorem is a crucial result for the development of o-minimality. We follow closely Chapter 3 of [1].

THEOREM 3.1.1 (Monotonicity Theorem). *Let $f : I \to R$ be a definable function. Then there are constants $a_1, ..., a_k$ such that $I = (a_1, a_2) \cup ... \cup (a_{k-1}, a_k) \cup \{a_1, ..., a_k\}$ and, for each interval (a_i, a_{i+1}), f is constant or strictly monotone and continuous.*

To prove this theorem we rely on the following three lemmas. For these lemmas assume $f : I \to R$ is a definable function.

LEMMA 3.1.2. *There is a subinterval of I where f is constant or injective.*

LEMMA 3.1.3. *If f is injective, then f is strictly monotone on some subinterval.*

LEMMA 3.1.4. *If f is strictly increasing, then f is continuous on some subinterval.*

Assume $I = (a, b)$. Here is how we use the lemmas to prove 3.1.1:

Proof of Monotonicity Theorem: Let $\Phi_0, \Phi_\nearrow, \Phi_\searrow$ be formulas defined by

$$\begin{aligned}
\Phi_0(x) &:= f \text{ "is constant on some subinterval of } I \text{ containing } x\text{"};\\
\Phi_\nearrow(x) &:= f \text{ "is strictly increasing on some subinterval of } I \text{ containing } x\text{"};\\
\Phi_\searrow(x) &:= f \text{ "is strictly decreasing on some subinterval of } I \text{ containing } x\text{"}.
\end{aligned}$$

Let

$$\begin{aligned}
X_0 &:= \{x \in I : \Phi_0(x)\};\\
X_\nearrow &:= \{x \in I : \Phi_\nearrow(x)\};\\
X_\searrow &:= \{x \in I : \Phi_\searrow(x)\};\\
X = X_0 \sqcup X_\nearrow \sqcup X_\searrow.
\end{aligned}$$

If $I \setminus X$ is infinite, then it must contain an interval $J \subset I \setminus X$. Applying the Lemmas 3.1.2, 3.1.3 and 3.1.4 to J, we conclude that there is an interval $J' \subset J$ such that $J' \subset X$ which is absurd. Thus $I \setminus X$ is finite. We can write

$$I = (a_0, a_1) \cup ... \cup (a_{n-1}, a_n) \cup \{a_0, a_1, ..., a_n\},$$

such that $I \setminus X = \{a_1, ..., a_n\}$ and for each $i \in \{0, ..., n-1\}$ either

- for all $x \in (a_i, a_{i+1})$, $\Phi_0(x)$ or
- for all $x \in (a_i, a_{i+1})$, $\Phi_\nearrow(x)$ or
- for all $x \in (a_i, a_{i+1})$, $\Phi_\searrow(x)$.

Suppose the first case happens for some $i \in \{0, ..., n-1\}$. Take $x_0 \in (a_i, a_{i+1})$ and put

$$s := \sup\{x \in (a_i, a_{i+1}) : x_0 < x < a_{i+1},\ f \text{ is constant on } [x_0, x)\}.$$

Then $s = a_{i+1}$, since $s < a_{i+1}$ implies that f is constant on an interval containing s which is absurd. Therefore f is constant on (a_i, a_{i+1}).

Suppose the second case happens for some $i \in \{0, ..., n-1\}$. Take $x_0 \in (a_i, a_{i+1})$ and put

$$s := \sup\{x \in (a_i, a_{i+1}) : x_0 < x < a_{i+1},\ f \text{ is strictly increasing on } [x_0, x)\}.$$

Then $s = a_{i+1}$, since $s < a_{i+1}$ implies that f is strictly increasing on an interval containing s which is absurd. Therefore f is strictly increasing on (a_i, a_{i+1}).

The third case has a similar result as the second case. □

Now we prove the lemmas.

Proof of Lemma 3.1.2: Let us denote $I = (a, b)$. If $f^{-1}(y)$ is infinite for some $y \in f[I]$, since $f^{-1}(y)$ is definable, it must contain an interval, which gives us the result.
Suppose then $f^{-1}(y)$ is finite for every $y \in f[I]$. This implies that $f[I]$ is infinite. Let $g(y) = \min\{x \in I : f(x) = y\}$. Then $g : f[I] \to I$ is definable and clearly injective. This implies that the range of g is infinite, so it must contain an interval. Evidently f is injective on that interval. Replacing I by that interval, we can assume injectivity of f. □

Proof of Lemma 3.1.3: Let $u \in I$. Consider the definable sets

$$I_+(u) = \{x \in (a, u) : f(x) > f(u)\};$$
$$I_-(u) = \{x \in (a, u) : f(x) < f(u)\}.$$

Since f is injective, we can write $(a, u) = I_+(u) \sqcup I_-(u)$. At least one of the subsets must be infinite, so it contains an interval of the form (c, u). This rationale is also valid for (u, b). Thus it is true that every element of I satisfies one of the following formulas $\Phi_{-+}, \Phi_{++}, \Phi_{+-}, \Phi_{--}$:

$$\Phi_{-+}(x) =: \exists c_1, c_2 \in I \forall y((c_1 < y < x \Rightarrow f(y) < f(x)) \wedge (x < y < c_2 \Rightarrow f(y) > f(x)));$$

$$\Phi_{++}(x) =: \exists c_1, c_2 \in I \forall y((c_1 < y < x \Rightarrow f(y) > f(x)) \wedge (x < y < c_2 \Rightarrow f(y) > f(x))).$$

The formulas $\Phi_{+-}(x), \Phi_{--}(x)$ are defined similarly. Let $I_{-+} =: \{x \in I : \Phi_{-+}(x)\}$ and define I_{+-}, I_{++}, I_{--} similarly. We have $I = I_{-+} \sqcup I_{+-} \sqcup I_{++} \sqcup I_{--}$, so there is a subinterval of I on which every element satisifes only one of the above formulas. Replace I by that subinterval. If $I = I_{-+}$ or $I = I_{+-}$, then f is strictly monotone. We now prove that any subset satisfying either Φ_{++} or Φ_{--} must be finite. Suppose by contradiction that $I = I_{++}$. Let $B = \{x \in I : \forall y(x < y \Rightarrow f(x) < f(y)\}$. If B is infinite, then B contains an interval. Replacing I by that interval completes the proof. So let's assume B is finite. Replacing I by $(\max(B), +\infty) \cap I$ we have

$$\forall x \in I \exists y \in I(x < y \wedge f(y) < f(x)). \tag{3.1}$$

Let $c \in I$. We claim that there is $d \in I$ such that for all $y \in (d, b)$ we have $f(y) < f(x)$: Let

$$Y = \{y : y > c \wedge f(y) < f(c)\}$$

and

$$Y' = \{y : y > c \wedge f(y) > f(c)\}.$$

Since f is injective we have

$$(c, b) = Y \sqcup Y'.$$

By o-minimality, either Y or Y' contains an interval (d, b). Suppose by contradiction that Y doesn't contain such interval. We have $c < \sup Y < b$. But by 3.1, there is $w > \sup Y$ such that $f(w) < f(\sup Y) < f(c)$. Hence $w \in Y$ which is absurd.

Let $y(c)$ be the least element of $[c, b)$ such that for all $y \in (y(c), b)$ we have $f(y) < f(c)$. Note that $\Phi_{++}(c)$ implies that $c < y(c)$ and $f(y(c)) < f(c)$.

Let

$$\Psi_{+-}(v) =: \exists v_1, v_2 \in I\, \forall z_1, z_2(v_1 < z_1 < v < z_2 < v_2 \Rightarrow f(z_1) > f(z_2)).$$

Then $y(c)$ satisfies Ψ_{+-} since otherwise there would be an element $z \in (c, y(c))$ such that $f(z) \leq f(y) < f(c)$ for some $y \in (y(c), b)$ which contradict the minimality of $y(c)$.

Since c was arbitrary we have shown $\forall c \in I\, \exists v \in I(v > c \wedge \Psi_{+-}(v))$. We have that $\Psi_{+-}(v)$ holds for all $v \in (d, b)$ for some $d \in I$. Replace I by this interval (d, b).

Instead of B, defining $B' = \{x \in I : \forall y(x > y \Rightarrow f(x) < f(y)\}$, then proceeding with similar arguments, and replacing I by an even smaller subinterval, we conclude that both Ψ_{+-} and Ψ_{-+} hold for all $x \in I$ which is absurd.

The case that Φ_{--} hold for all $x \in I$ is similar. $\square$

Proof of Lemma 3.1.4: Let J be an interval in $f[I]$. We show that $f^{-1}(J)$ is an interval. Clearly $f^{-1}(J) \subseteq (\inf f^{-1}(J), \sup f^{-1}(J))$. Let x be an element of $(\inf f^{-1}(J), \sup f^{-1}(J))$. If $x \notin f^{-1}(J)$ then we could partition J in two intervals which is absurd. Hence f is continuous. $\square$

DEFINITION 3.1.5. *Let $A \subseteq R^{m+1}$ be definable. We say that A is* ***finite over*** *R^m if for each $x \in R^m$ the fiber $A_x = \{y \in R : (x, y) \in A\}$ is finite. We say that A is* ***uniformly finite over*** *R^m if there is $n \in \mathbb{N}$ such that $|A_x| < n$ for every $x \in R^m$.*

LEMMA 3.1.6 (Finiteness Lemma). *Let A be a definable subset of R^2 and suppose A is finite over R. Then A is uniformly finite over R.*

Proof. We will call a pair $(a, b) \in R^2$ **normal** if there is a box $I \times J$ around (a, b) such that either $I \times J$ doesn't intersect A or, when it does, there is a continuous function $f : I \to J$ such that $\Gamma(f) = (I \times J) \cap A$. We will also call a pair $(a, +\infty) \in R \times R_\infty$ normal if there is a box $I \times J$ disjoint from A such that $a \in I$ and $J = (b, +\infty)$ for some b. (analogous for $(a, -\infty) \in R \times R_\infty$).
Note that the following sets are definable

$$\{(a, b) \in \mathbb{R}^2 : (a, b) \text{ is normal }\};$$
$$\{a \in \mathbb{R} : (a, -\infty) \text{ is normal }\};$$
$$\{a \in \mathbb{R} : (a, +\infty) \text{ is normal }\}.$$

We define a function f_n by

$$\text{dom}(f) := \{x \in R : |A_x| \geq n\};$$
$$f_n(x) := n^{th} \text{ element of } A_x.$$

Note that f_n is definable.

Let $a \in R$ and take $n \geq 0$ maximal such that $f_1, ..., f_n$ are defined and continuous on an interval containing a. We call the point a **good** or **bad**, according to

$$a \notin \text{cl}(\text{dom}(f_{n+1})) - \text{ “good”};$$
$$a \in \text{cl}(\text{dom}(f_{n+1})) - \text{ “bad” }.$$

Let $\mathcal{G}$ be the set of good points and $\mathcal{B}$ the set of bad points. Note that if $a \in \mathcal{G}$ then (with n as above) the domain of f_{n+1} is disjoint from an entire interval around a on which $f_1, ..., f_n$ are defined and continuous. This shows that for $a \in \mathcal{G}$ we have

- $|A_x|$ is constant on an interval around a;
- (a, b) is normal for all $b \in R_\infty$.

We want to prove that $\mathcal{G}$ and $\mathcal{B}$ are definable. For this we shall prove

- If $a \in \mathcal{B}$ then there is some $b \in R$ such that the pair (a, b) is not normal.

Let $a \in \mathcal{B}$. Define functions $\lambda_-, \lambda_+, \lambda_0 : B \to R_\infty$ by

$$\begin{aligned}
\lambda_-(a) &:= \lim_{x \to a^-} f_{n+1}(x) \text{ if } f_{n+1} \text{ is defined on a interval } (t, a) \text{ for some } t < a, \\
&:= +\infty \text{ otherwise;} \\
\lambda_+(a) &:= \lim_{x \to a^+} f_{n+1}(x) \text{ if } f_{n+1} \text{ is defined on a interval } (a, t) \text{ for some } t > a, \\
&:= +\infty \text{ otherwise;} \\
\lambda_0(a) &:= f_{n+1}(a) \text{ if } a \in \text{dom}(f_{n+1}), \\
&:= +\infty \text{ otherwise.}
\end{aligned}$$

Let $\beta(a) = \min\{\lambda_-(a), \lambda_+(a), \lambda_0(a)\}$. In this way $\beta(a)$ is the least element such that $(a, \beta(a))$ is not normal. So we have that $\mathcal{G}$ and $\mathcal{B}$ are definable by

$$\begin{aligned}
\mathcal{G} &:= \{a \in R : \forall b \in R_\infty((a, b) \text{ is normal})\}; \\
\mathcal{B} &:= \{a \in R : \exists b \in R_\infty((a, b) \text{ is not normal})\}.
\end{aligned}$$

If $\mathcal{B}$ is finite then the rest of the proof is easy: Let

$$\mathcal{B} = \{a_1, ..., a_k\} \text{ with } -\infty = a_0 < a_1 < ... < a_k < a_{k+1} = +\infty.$$

Let $x \in \mathcal{G}$. Suppose $|A_x| = n$ for some $n \in \mathbb{N}$. Since $|A_y| = n$ for every y in some interval around x, the set $\{x \in R : |A_x| = n\}$ is open and definable. For the same reason the set $\{x \in R : |A_x| \neq n\}$ is also open and definable. So $A_x = (a_i, a_{i+1})$ for some $i = 0, ..., k$. This proves the lemma.

Now let's conclude the proof by showing that $\mathcal{B}$ can't be an infinite set: Suppose by contradiction that $\mathcal{B}$ is infinite. Define

$$\begin{aligned}
\mathcal{B}_- &:= \{x \in \mathcal{B} : \exists y(y < \beta(x) \land (x, y) \in A\}; \\
\mathcal{B}_+ &:= \{x \in \mathcal{B} : \exists y(y > \beta(x) \land (x, y) \in A\}.
\end{aligned}$$

Let $\beta_- : \mathcal{B}_- \to R$ and $\beta_+ : \mathcal{B}_+ \to R$ be defined by

$$\begin{aligned}
\beta_-(x) &:= \max\{y : y < \beta(x) \land (x, y) \in A\}; \\
\beta_+(x) &:= \min\{y : y > \beta(x) \land (x, y) \in A\}.
\end{aligned}$$

Since $\mathcal{B}$ is infinite one of the sets $\mathcal{B}_- \cap \mathcal{B}_+$, $\mathcal{B}_- - \mathcal{B}_+$, $\mathcal{B}_+ - \mathcal{B}_-$, $B - (\mathcal{B}_- \cup \mathcal{B}_+)$ is also infinite. Suppose $\mathcal{B}_- \cap \mathcal{B}_+$ is infinite (the other cases are proved in similar way). Since β, β_-, β_+ are definable, by the Monotoniciy Theorem, there is an interval I contained in $\mathcal{B}_- \cap \mathcal{B}_+$ where each of the functions β, β_-, β_+ are continuous. We can write

$$I = \{x \in I : (x, \beta(x)) \in A\} \sqcup \{x \in I : (x, \beta(x)) \notin A\}.$$

One of the sets in this partition of I must be infinite. Replacing I by that interval we get $\Gamma(\beta|_I) \subseteq A$ or $\Gamma(\beta|_I) \cap A = \emptyset$. By continuity of β, β_-, β_+ in I we have $x, x_1, x_2, y_0, y_1, y_2, y_3 \in R$ such that

$$\begin{aligned}
& x \in (x_1, x_2) \subseteq I \\
& y_0 < \beta_-(x) < y_1 < \beta(x) < y_2 < \beta_+(x) < y_3 \\
\beta_-(x_1, x_2) &\subseteq (y_0, y_1) \\
\beta(x_1, x_2) &\subseteq (y_1, y_2) \\
\beta_+(x_1, x_2) &\subseteq (y_2, y_3).
\end{aligned}$$

This gives either $(x_1, x_2) \times (y_1, y_2) \cap A = \emptyset$ or $(x_1, x_2) \times (y_1, y_2) \cap A = \Gamma(\beta|_{(a,b)})$, implying $(x, \beta(x))$ to be a normal point, which is absurd. □

Combining the Monotonicity Theorem and the Finiteness Lemma we get the following property:

PROPERTY 3.1.7. *Let $A \subseteq R^2$ be a definable set such that A_x is finite for each $x \in R$. Then there are points $a_1 < ... < a_k$ in R such that the intersection of A with each vertical strip $(a_i, a_{i+1}) \times R$ has the form $\Gamma(f_{i,1}) \cup ... \cup \Gamma(f_{i,n(i)}$ for certain definable continuous functions $f_{i,j} : (a_i, a_{i+1}) \to R$ with $f_{i,1}(x) < ... < f_{i,n(i)}(x)$ for x in (a_i, a_{i+1}) (where $a_0 := -\infty$ and $a_{k+1} := +\infty$).*

3.2 Cell decomposition

NOTATION. For each definable set X in R^m we put

$$C(X) := \{f : X \to R : f \text{ is definable and continuous }\};$$
$$C_\infty(X) := C(X) \cup \{-\infty, +\infty\},$$

where we regard $-\infty$ and $+\infty$ as constant functions on X.

DEFINITION 3.2.1. *Let $(i_1, ..., i_m)$ be a sequence of zeros and ones of lenght m. An $(i_1, ..., i_m)$-cell is a definable subset of R^m defined by induction on m as follows:*

1. *A (0)-cell is a point $\{r\} \subseteq R$, a (1)-cell is an interval $(a, b) \subseteq R$;*
2. *Suppose $(i_1, ..., i_m)$-cell is already defined. Then an $(i_1, ..., i_m, 0)$-cell is the graph $\Gamma(f)$ of a funciton $f \in C(X)$, where X is an $(i_1, ..., i_m)$-cell; an $(i_1, ..., i_m, 1)$-cell is a set $(f, g)_X$ where $f, g \in C_\infty(X)$ and X is an $(i_1, ..., i_m)$-cell.*

PROPERTY 3.2.2. *Each cell is homeomorphic to an open cell under a coordinate projection.*

Proof. Let $i = (i_1, ..., i_m)$ be a sequence of zeros and ones. Define $p_i : R^m \to R^k$ as follows: let $\lambda(1) < ... < \lambda(k)$ be the indices $\lambda \in \{1, ..., m\}$ such that $i_\lambda = 1$ and $k = i_1 + ... + i_m$. Put

$$p_i(x_1, ..., x_m) := (x_{\lambda(1)}, ..., x_{\lambda(k)}).$$

We show by induction on m that p_i maps homeomorphically each i-cell A to an open cell $p_i(A)$ in R^k. If $m = 1$ then it is obvious. Let $j = (j_1, ..., j_m, j_{m+1})$ and $j' = (j_1, ..., j_m)$. If $j_{m+1} = 0$ then a j-cell is $\Gamma(f)$ for some $f \in C(X)$, where X is a j'-cell. We have that X is homeomorphic to $\Gamma(f)$ under the projection p_j. By the inductive hypothesis X is homeomorphic to the open cell $p_{j'}(X)$. So $\Gamma(f)$ is homeomorphic to the open cell $p_{j'}p_j(\Gamma(f))$. Suppose now $j_{m+1} = 1$. Then a j-cell is of the form $(f, g)_X$ where $f, g \in C(X)$ and $f < g$. Let $x \in X$ and $f(x) < y < g(x)$. Then $p_j(x, y) = (p_{j'}(x), y)$. So we have $p_j[(f, g)_X] = (f \circ p_{j'}^{-1}, g \circ p_{j'}^{-1})_{p_{j'}(X)}$. Note that $(f \circ p_{j'}^{-1}, g \circ p_{j'}^{-1})_{p_{j'}(X)}$ is an open cell because $p_{j'}(X)$ is an open cell by hypothesis. Since $p_{j'}$ defines an homeomorphism we have $(f, g)_X \simeq (f \circ p_{j'}^{-1}, g \circ p_{j'}^{-1})_{p_{j'}(X)}$. □

PROPERTY 3.2.3. *Each cell is definably connected.*

DEFINITION 3.2.4. *A **decomposition** of R^m is a special kind of partition of R^m into finitely many cells. The definition is by induction on m:*

1. *A decomposition of R is a collection*

$$\{(a_0, a_1), ..., (a_k, a_{k+1}), \{a_1\}, ..., \{a_k\}\}$$

where $a_1, ..., a_k$ are points in R and $a_0 = -\infty$, $a_{k+1} = +\infty$;

2. *A decomposition of R^{m+1} is a finite partition of R^{m+1} into cells A such that the set of projections $\pi(A)$ is a decomposition of R^m. (Here $\pi : R^{m+1} \to R^m$ is the usual projection map).*

DEFINITION 3.2.5. *A decomposition $\mathcal{D}$ of R^m is said to* ***partition*** *a set $S \subseteq R^m$ if each cell in $\mathcal{D}$ is either part of S or disjoint from S*

Now follows three fundamental properties of o-minimal structures:

THEOREM 3.2.6. *Let $A, A_1, ..., A_k \subseteq R^n$ and $Y \subseteq R^{n+1}$ be definable sets. Then*

- *(**Uniform finiteness** - UF_n) If Y is finite over R^m then it is uniformly finite over R^m;*
- *(**Cell decomposition** - CD_n) There is a decomposition of R^n partitioning $A_1, ..., A_k$;*
- *(**Piecewise continuity** - PC_n) Let $f : A \to R$ be a definable function. Then there is a cellular decomposition of R^n adapted to A such that for each cell $C \subseteq A$, $f|_C$ is continuous.*

The proof is by induction. If $n = 1$, UF_1 is the finiteness lemma, CD_1 follows immediately from o-minimality and PC_1 is the monotonicity theorem. Let $n > 1$ and suppose UF_m, CD_m and PC_m hold for every $1 \leq m < n$.

Proof of UF_n. A box $B \subseteq R^m$ will be called Y-**good** if for each point $(x, r) \in Y$ there is an interval I with $r \in I$ such that $Y \cap (B \times I) = \emptyset$ or $Y \cap (B \times I) = \Gamma(f)$ for some continuous function $f : B \to I$. It is obvious that if the latter case happens then f is uniquely determined by Y, B and I, and is definable.

Claim 1: Suppose the box $B \subseteq R^m$ is Y-good; then there are continuous definable functions $f_1 < ... < f_k$ in $C(B)$ such that $Y \cap (B \times R) = \Gamma(f_1) \cup ... \cup \Gamma(f_k)$.

To see this, let us fix $x \in B$ and write $Y_x = \{r_1, ..., r_k\}$ with $r_1 < ... < r_k$. Take intervals I_i around r_i , and continuous functions $f_i : B \to R$ such that $Y \cap (B \times I_i) = \Gamma(f_i)$, for each $1 \leq i \leq k$.

Subclaim 1.1: $f_1 < ... < f_k$.

We will prove only $f_1 < f_2$. The other cases follow in the same way. Suppose there is a point $p \in B$ such that $f_1(p) = f_2(p)$. Then $I_1 \cap I_2 \neq \emptyset$ and $A \cap (B \times I_1) \cap (B \times I_2) = \Gamma(f_1) \cap \Gamma(f_2)$. This implies $\{p \in B : f_1(p) = f_2(p)\} = f^{-1}[I_1 \cap I_2]$. By continuity this set is open. We can write B as a disjoint union of $\{p \in B : f_1(p) = f_2(p)\}$, $\{p \in B : f_1(p) < f_2(p)\}$ and $\{p \in B : f_1(p) > f_2(p)\}$ and these are all definable open sets. Since B is definably connected the subclaim follows easily.

Subclaim 1.2: $Y \cap (B \times R) = \Gamma(f_1) \cup ... \cup \Gamma(f_k)$.

Let $(y, s) \in Y \cap (B \times R)$ be arbitrary. Let $f : B \to R$ be definable continuous such that $f(y) = s$ and $\Gamma(f) \subseteq Y$. We have $f(x) = r_i = f_i(x)$ for some i since $\Gamma(f) \subseteq Y$. By a similar argument as in Subclaim 1.1, we conclude $f = f_i$.

A point $x \in R^m$ will be called Y-**good** if it belongs to a Y-good box $B \subseteq R^m$. Note that the set of Y-good points is definable.

Claim 2: If $A \subseteq R^m$ is a definably connected set and its points are all Y-good then there are continuous functions $f_1 < ... < f_k$ in $C(A)$ such that

$$Y \cap (A \times R) = \Gamma(f_1) \cup ... \cup \Gamma(f_k).$$

Let $k \in \mathbb{N}$. Consider the set $A_k = \{a \in A : |Y_a| = k\}$. By Claim 1 and the definition of good point, for every $a \in A_k$ there is a Y-good box B such that $B \subseteq A_k$. So A_k is open in A. Note that in this case there are continuous functions $f_1 < ... < f_k$ in $C(A_k)$ such that $Y \cap (A_k \times R) = \Gamma(f_1) \cup ... \cup \Gamma(f_k)$. By arbitrariness of k, A_k^c is also open in A. So A_k is both open and closed in A. So if $A_k \neq \emptyset$ then $A_k = A$. Supposing k is in fact such that $k = |Y_x|$ for every $x \in A$, we get Claim 2.

Claim 3: Each open cell in R^m contains a Y-good point.

It is enough to show that each box B in R^m contains a Y-good point. Write

$$B = B' \times (a, b), \quad B' \text{ a box in } R^{m-1}.$$

For each point $p \in B'$ consider the set

$$Y(p) := \{(r, s) \in R^2 : a < r < b \ \wedge \ (p, r, s) \in Y\}.$$

Note that $Y(p)$ is finite ove R. Applying Property 3.1.7 we conclude that the set $\{r \in R : r \text{ is not } Y(p)\text{-good }\}$ is finite. Therefore the definable set

$$\mathrm{Bad}_p(Y) := \{(p,r) \in B : r \text{ is not } Y(p)\text{-good }\}$$

has empty interior. By the inductive hypothesis CD_m there is a decomposition of R^m which partitions B and $\mathrm{Bad}_p(Y)$. Take an open cell C of this partition such that $C \subseteq B$, so that $C \cap \mathrm{Bad}_p(Y) = \emptyset$. Replace B with a box contained in C so we reduce to the case that $\mathrm{Bad}_p(Y) = \emptyset$. In this way, fixed a point $p \in B'$ and applying Claim 2 to the box B' and considering $Y(p)$-good points instead of Y-good points we conclude that there is $k(p) \in \mathbb{N}$ such that for every $r \in (a,b)$ we have $|Y_x| = k(p)$ where $x = (p,r)$. Next we have to show that there is a finite bound on the numbers $k(p)$, $p \in B'$. Choose $r \in (a,b)$ and consider the set

$$Y^r := \{(p,s) : (p,r,s) \in Y\} \subseteq R^m.$$

Since Y is finite over R^m, Y^r is finite over R^{m-1}, so by the inductive hypothesis UF_{m-1}, Y^r is uniformly finite over R^{m-1}. Thus for some $r \in (a,b)$ there is a number $N \in \mathbb{N}$ such that for every $p \in B'$, $|Y_{(p,r)}| \leq N$. Thus we have shown that for every $p \in B'$, $k(p) \leq N$.

For each $i \in \{0,...,N\}$ let $B_i := \{x \in B : |Y_x| = i\}$, and define the functions $f_{i,1},...,f_{i,i}$ on B_i by $f_{i,1}(x) < ... < f_{i,i}(x)$ and $Y_x = \{f_{i,1}(x),...,f_{i,i}(x)\}$. Applying PC_m to each function $f_{i,j}$ separately, and then using CD_m to find a common refinement of the decomposition obtained via PC_m, we get a decomposition $\mathcal{D}$ of R^m partitioning each of the sets B_i, such that for each $A \in \mathcal{D}$, if $A \subseteq B_i$, then $f_{i,j}|_A$ is continuous, $j = 0,...,i$. Since B is open there is an open cell $A \in \mathcal{D}$ with $A \subseteq B$. Now $B = \bigcup_i B_i$, so $A \subseteq B_i$ for some i, therefore the functions $f_{i,1},...,f_{i,i}$ are continuous on A. Hence each point in A is Y-good. This establishes Claim 3.

The proof of the lemma now proceeds as follows. Take a decomposition $\mathcal{D}$ of R^m partitioning the set of Y-good points. Let $A \in \mathcal{D}$. If A is open then by claim 3 it contains a Y-good point, and so all points of A are Y-good. By claim 2 there is a number $N_A \in \mathbb{N}$ such that $Y_x \leq N_A$ for all $x \in A$. If A is not open, we still have a definable homeomorphism p_A to an open cell of lesser dimension (Property 3.2.2) validating also the existence of such a number N_A. Now take $N = \max\{N_A \in \mathbb{N} : A \in \mathcal{D}\}$. Then $|Y_x| \leq N$ for all $x \in R^m$. □

Proof of CD_n. For a definable set $A \subseteq R^{m+1}$ we put

$$\mathrm{bd}_m(A) := \{(x,r) \in R^{m+1} : r \in \mathrm{bd}(A_x)\}$$

and we note that $\mathrm{bd}_m(A)$ is definable and by o-minimality finite over R^m. Recall Property 3.0.1, to note that if r_1, r_2 are two consecutive boundary points of A_x then either $(r_1,r_2) \subseteq A_x$ or $(r_1,r_2) \subseteq A_x^c$. Let $A_1,...,A_k$ be definable subsets of R^{m+1} . Put

$$Y := \mathrm{bd}_m(A_1) \cup ... \cup \mathrm{bd}_m(A_k).$$

Then $Y \subseteq R^{m+1}$ is definable and finite over R^m, so by UF_m there is $M \in \mathbb{N}$ such that $|Y_x| \leq M$ for all $x \in R^m$. For each $i \in \{0,...,M\}$ put $B_i := \{x \in R^m : |Y_x| = i\}$ and define $f_{i,1},...,f_{i,i}$ functions on B_i by

$$Y_x = \{f_{i,1}(x),...,f_{i,i}(x)\},\ \ f_{i,1}(x) < ... < f_{i,i}(x).$$

Further put $f_{i,0} = -\infty$ and $f_{i,i+1} = +\infty$ (functions on B_i). Finally we define for each $\lambda \in \{1,...,k\}$, $i \in \{0,...,M\}$ and $j \in \{1,...,i\}$

$$C_{\lambda,i,j} := \{x \in B_i : f_{i,j}(x) \in (A_\lambda)_x\}\},$$

and for each $\lambda \in \{1,...,k\}$, $i \in \{0,...,M\}$ and $j \in \{0,...,i\}$

$$D_{\lambda,i,j} := \{x \in B_i : (f_{i,j}(x), f_{i,j+1}(x)) \subseteq (A_\lambda)_x\}.$$

Using the inductive assumptions CD_m and PC_m, we now take a decomposition $\mathcal{D}$ of R^m which partitions each set B_i, each set $C_{\lambda,i,j}$ and each set $D_{\lambda,i,j}$, and which has also the following property: if $E \in \mathcal{D}$ is contained in B_i, then $f_{i,1}|_E, ..., f_{i,i}|_E$ are continuous functions. For each $E \in D$ we let $\mathcal{D}_E$ be the following partition of $E \times R$

$$\mathcal{D}_E := \{(f_{i,0}|_E, f_{i,1}|_E), ..., (f_{i,i}|_E, f_{i,i+1}|_E), \Gamma(f_{i,1}|_E), ..., \Gamma(f_{i,i}|_E)\},$$

where $i \in \{0, ..., M\}$ is such that $E \subseteq B_i$. Then $\mathcal{D}^* := \bigcup\{\mathcal{D}_E : E \in \mathcal{D}\}$ is a decomposition of R^{m+1} which partitions each set $A_1, ..., A_k$. $\square$

We will use the following lemma to prove PC_n.

LEMMA 3.2.7. *Let X be a topological space $(R_1, <, ...)$, $(R_2, <, ...)$ dense linear orderings without endpoints. Let $(p, r) \in X \times R_1$ and suppose $f : X \times R_1 \to R_2$ is such that*

(i) For every $x \in X$, $f(x, \cdot) : R_1 \to R_2$ is continuous and monotone on R_1;

(ii) For every $r \in R_1$, $f(\cdot, r) : X \to R_2$ is continuous at p.

Then f is continuous at (p, r).

Proof. Let $(p, r) \in X \times R_1$ and J an interval in R_2 containing $f(p, r)$. By (i) there are $r_- < r < r_+$ such that $f(p, r_-), f(p, r_+) \in J$. By (ii) there is a neighbourhood U of p such that $f(U \times \{r_-\})$ and $f(U \times \{r_+\})$ are contained in J. Let $x \in U$ and $r_- < r' < r_+$. Assume $f(x, \cdot)$ is increasing (the decreasing case goes the same way). Then $f(x, r_-) < f(x, r') < f(x, r_+)$, and since both $f(x, r_-)$ and $f(x, r_+)$ are in J we have $f(x, r') \in J$. $\square$

Proof of PC_n. Let $A \subseteq R^{m+1}$ be definable and $f : A \to R$ a definable function. We have to show that f is "cellwise" continuous. By CD_{m+1} there is a finite partition of A into cells. So we can consider A to be a cell. If A is not open, then we consider the definable homeomorphism $p_A : A \to U$, with $U \subseteq R^n$ an open cell for some $1 \le n \le m$. By the inductive assumption PC_n we have a decomposition of U into finitely many cells $U_1, ..., U_k \subseteq R^n$ such that $f \circ p_A^{-1}|_{U_1}, ..., f \circ p_A^{-1}|_{U_k}$ are continuous. This gives a decomposition $A = p_A^{-1}(U_1) \cup ... \cup p_A^{-1}(U_k)$, such that $f|_{p_A^{-1}(U_1)}, ..., f|_{p_A^{-1}(U_k)}$ are continuous.

Suppose now that A is an open cell. Call a point $(p, r) \in A$ **well-behaved** if there is a box $C \subseteq R^m$ and an interval $I = (a, b)$ such that

(i) $(p, r) \in C \times I$ and $C \times I \subseteq A$;

(ii) for all $x \in C$, $f(x, \cdot)$ is continuous and monotone on I;

(iii) $f(\cdot, r)$ is continuous at p.

Denote by A^* the set of well-behaved points. This set is definable.

Claim: A^* is dense in A.

Let C be a box in R^m and $I = (a, c)$ an interval such that $C \times I \subseteq A$. We will show that $C \times I$ intersects A^*. For each $x \in C$ fixed we can apply PC_1 to $f(x, *)$ to obtain a maximum element $\lambda(x) \in (a, c]$ such that $f(x, \cdot)|_{(a, \lambda(x))}$ is monotone and continuous. The function $\lambda : C \to R$ is definable, hence by PC_m there is a box C' contained in C such that $\lambda|_{C'}$ is continuous. Replacing, if necessary, C' by a smaller box, we can assume for every $x \in C'$, $\lambda(x) \ge b$ for some $b \in (a, c)$. Now applying PC_m to $f(\cdot, r)$ for some $r \in (a, b)$ there is a box $B \subseteq C'$ such that $f(\cdot, r)|_B$ is continuous. So for any $p \in B$, (p, r) is a well-behaved point. This proves the claim.

Now, using CD_{m+1}, we take a decomposition $\mathcal{D}$ of R^{m+1} that partitions both A and A^*. Let $D \in \mathcal{D}$ be an open cell contained in A. This implies $D \subseteq A^*$. We'll show that f is continuous on D. Let (p, r) be an arbitrary point in D. Let $C \times I \subseteq D$ be a neighbourhood of (p, r) such that for every $x \in C$, $f(x, \cdot)$ is continuous and monotone on I. Note that for every $(p, r') \in D$, the function $f(\cdot, r')$ is continuous at p and in particular, this is true for $r' \in I$. So by Lemma 3.2.7, $f|_{C \times I}$ is continuous at (p, r), which proves continuity of f at (p, r). $\square$

DEFINITION 3.2.8. *Let X be a definable subset of R^m. A subset $U \subseteq X$ is said to be a* ***definably connected component*** *of X if it is definable and a maximal definably connected subset of X.*

PROPERTY 3.2.9. *Let X be a nonempty definable subset of R^m. Then X has only finitely many definably connected components. These sets are open and closed in X and form a finite partition of X.*

Proof. Let $\{C_1, ..., C_n\}$ be a decomposition of X into k disjoint cells. For each $I \subseteq \{1, ..., k\}$ let $C_I = \bigcup_{i \in I} C_i$. Let C' be one of the $2^k - 1$ sets C_I be maximal with respect to being definably connected. Let Y be a definably connected set such that $Y \cap C' \neq \emptyset$. We will prove $Y \subseteq C'$. For this let $C_Y := \bigcup\{C_i : C_i \cap Y \neq \emptyset\}$. Since the $C_i' s$ cover X we have $Y \subseteq C_Y$, and so the set C_Y is definably connected. The set $C' \cap C_Y$ is nonempty since it contains $C' \cap Y$, and so $C' \cup C_Y$ is definably connected. By maximality $C_Y \subseteq C'$, and so $Y \subseteq C'$ as we wanted. It follows that C' is a definably connected component of X. The closure of a definably connected subset of X is also definably connected so C' is closed. Sets of the form C' obviously partition X finitely. Since each one of these sets is closed, it follows that each one of these sets is also open. $\square$

Chapter 4

The theory of restricted analytic fields

We have seen that every rcof has quantifier elimination and as a consequence we verified o-minimality. What if we consider an extension of rcof, coupling it with some class of functions? This type of considerations has already a vast field of knowledge and it is still a very active area of research. Let $\mathbb{R}\{X_1, ..., X_m\}$ denote the subring of real power series that converge in a neighbourhood of I^m, with $I = [-1, 1]$. For $f \in \mathbb{R}\{X_1, ..., X_m\}$ we let $\widetilde{f} : \mathbb{R}^m \to \mathbb{R}$ be given by:

$$\widetilde{f}(x) = \begin{cases} f(x), & \text{for } x \in I^m, \\ 0, & \text{for } x \notin I^m. \end{cases}$$

We call the $\widetilde{f}$'s **restricted analytic functions**.
Let $\mathcal{L}_{\text{an}} = (<, 0, 1, +, -, \cdot, \{f\}_{f \in \mathbb{R}\{X_1,...,X_m\}})$ be the language of ordered rings augmented by a new function symbol for each function $\widetilde{f}$. Let $\mathbb{R}_{\text{an}} = (\mathbb{R}, <, 0, 1, +, -, \cdot, \{\widetilde{f}\}_{f \in \mathbb{R}\{X_1,...,X_m\}})$ be the reals with its natural $\mathcal{L}_{\text{an}}$-structure and let T_{an} be the theory of $\mathbb{R}_{\text{an}}$. We will show that T_{an} admits an universal axiomatization in the language $(\mathcal{L}_{an}, ^{-1}, (\sqrt[n]{\ })_{n=2,3,...})$.

Recall the definition of a real analytic function as well as some important properties.

DEFINITION 4.0.1. *Let U be an open subset of $\mathbb{R}^m$. We say that a function $f : U \to \mathbb{R}$ is a* ***real analytic function*** *if for every $(a_1, ..., a_m) \in U$ there is a neighbourhood V of $(a_1, ..., a_m)$ and a sequence of coefficients $c_i \in \mathbb{R}$ with $i = (i_1, ..., i_m) \in \mathbb{N}^m$ such that for every $x = (x_1, ..., x_m) \in V$*

$$f(x) = \sum c_i (x - x_1)^{i_1} ... (x - x_m)^{i_m}$$

An analytic function is infinitely differentiable and its power expansion coincides with the Taylor series.

PROPERTY 4.0.2. *Considering the same notation as in definition 4.0.1, we can write the coefficients c_i as*

$$c_i = \frac{1}{|i|!} \frac{\partial^{|i|} f}{\partial x_1^{i_1} ... \partial x_m^{i_m}}(a) = \frac{1}{|i|!} \frac{\partial^{|i|} f}{\partial x^i}(a)$$

where $|i| = i_1 + ... + i_m$.

Proof. Consult Remark 2.2.4 of [12]. □

PROPERTY 4.0.3. *If $f : U \subset \mathbb{R}^n \to \mathbb{R}$, $g : V \subset \mathbb{R}^n \to \mathbb{R}$ are analytic, then $f + g$ and $f \cdot g$ are real analytic on $U \cap V$.*

Proof. Consult Proposition 2.2.2 of [12]. □

PROPERTY 4.0.4. *If $f : U \subset \mathbb{R}^m \to \mathbb{R}$, $g_1, ..., g_k : V \subset \mathbb{R}^n \to \mathbb{R}$ are analytic such that $g = (g_1, ..., g_m) : V \to \mathbb{R}^m$ with $g(V) \subset U$, then $f \circ g : V \to \mathbb{R}$ is analytic.*

Proof. Consult Proposition 2.2.8 of [12]. □

Another useful fact is that the implicit function theorem applied to a real analytic function gives a real analytic function.

PROPERTY 4.0.5. *Let $U \subset \mathbb{R}^m$ and $V \subset \mathbb{R}$ be open sets. Suppose $F : U \times V \to \mathbb{R}$ is analytic and for some $(a, b) \in U \times V$, $\frac{\partial F}{\partial x_{m+1}}(a, b) \neq 0$. Then there is an open neighbourhood $W \subset U$ of a and an analytic function $f : W \to V$ such that*

$$F(x, f(x)) = F(a, b), \text{ for every } x \in W$$

Proof. Consult Theorem 2.3.5 of [12]. $\square$

In the next sections we introduce the concepts and results to prove the following theorem

THEOREM 4.0.6. *The theory T_{an} is axiomatized by the axioms of ordered fields, the axiom saying that each positive element has an n^{th} root for each $n = 2, 3, ...$, and the universal axioms:*

- ***AC1:*** *For $f, g \in \mathbb{R}\{X_1, ..., X_m\}$, with $m \in \mathbb{N}$ and $x = (x_1, ..., x_m)$*

$$\widetilde{f+g}(x) = \widetilde{f}(x) + \widetilde{g}(x);$$
$$\widetilde{fg}(x) = \widetilde{f}(x) \cdot \widetilde{g}(x);$$
$$\bigwedge_{i=1}^{m} |x_i| \leq 1 \to \widetilde{0}(x) = 0 \wedge \widetilde{1}(x) = 1;$$
$$\bigvee_{i=1}^{m} |x_i| > 1 \to \widetilde{0}(x) = 0 \wedge \widetilde{1}(x) = 0,$$

where $\widetilde{0}$ and $\widetilde{1}$ are the function symbols corresponding to the elements 0 and 1 of $\mathbb{R}\{X_1, ..., X_m\}$;

- ***AC2:***

$$\bigwedge_{i=1}^{m} |x_i| \leq 1 \to \widetilde{X_j}(x) = x_j;$$
$$\bigvee_{i=1}^{m} |x_i| > 1 \to \widetilde{X_j}(x) = 0,$$

where X_j is considered as an element of $\mathbb{R}\{X_1, ..., X_m\}$, for $j = 1, ..., m$;

- ***AC3:*** *For $f \in \mathbb{R}\{X_1, ..., X_n\}$ and $g_1, ..., g_n \in \mathbb{R}\{X_1, ..., X_m\}$ such that $g_i(0) = 0$, $f(g_1, ..., g_n) \in \mathbb{R}\{X_1, ..., X_m\}$ and $g(I^m) \subset I^n$, where $g = (g_1, ..., g_n) : \mathbb{R}^m \to \mathbb{R}^n$:*

$$\bigwedge_{i=1}^{m} |x_i| \leq 1 \to f(\widetilde{g_1, ..., g_n})(x) = \widetilde{f}(g_1(x), ..., g_n(x));$$

- ***AC4:*** *For $f, g \in \mathbb{R}\{X_1, ..., X_m\}$, $0 < \epsilon \in \mathbb{R}$, $a = (a_1, ..., a_m) \in I^m$, such that $g = f_a(\epsilon X_1, ..., \epsilon X_m)$, where $f_a = \sum \frac{1}{|i!|} \frac{\partial^{|i|}}{\partial X^i}(a) X^i \in \mathbb{R}\langle X_1, ..., X_m \rangle$ is the Taylor series of f at a:*

$$(\bigwedge_{i=1}^{m} |x_i| \leq 1 \wedge \bigwedge_{i=1}^{m} |\widetilde{a}_i + \widetilde{\epsilon} x_i| \leq 1) \to \widetilde{f}(\widetilde{a}_1 + \widetilde{\epsilon} x_1, ..., \widetilde{a}_m + \widetilde{\epsilon} x_m) = \widetilde{g}(x).$$

NOTE 4.0.7. Let K be a non-trivial ordered field, viewed as an $\mathcal{L}_{an}$-structure, satisfying AC1 from Theorem 4.0.6. We show that K must contain a copy of $\mathbb{R}$. Note that, since $\widetilde{1}^K = 1^K$, the interpretation of the symbols $\widetilde{q}$, corresponding to $q \in \mathbb{Q}$ viewed as elements of $\mathbb{R}\{X_1, ..., X_m\}$, are exactly the rationals embedded in K. Let $x \in \mathbb{R}$ such that $x > 0$. Then $x = \sqrt{x}\sqrt{x}$. By AC1, $\widetilde{x}^K = \widetilde{\sqrt{x}}^K \widetilde{\sqrt{x}}^K > 0$. Now suppose $x, y \in \mathbb{R}$ such that

$x > y$. Then $x - y > 0$ and by the previous reasoning $\widetilde{(x-y)}^K > 0$, and so $\widetilde{x}^K > \widetilde{y}^K$. Thus the interpretation of the symbols $\widetilde{x}$ with $x \in \mathbb{R}$ viewed as an element of $\mathbb{R}\{X_1, ..., X_m\}$ in K must preserve the natural order present in $\mathbb{R}$. This implies that K contains a copy of $\mathbb{R}$.

4.1 Valuations

Valuations are an important tool in the context of this paper.

DEFINITION 4.1.1. *Let K be a field. We say that an integral domain $\mathcal{O} \subseteq K$ is a* ***valuation ring*** *if*

$$\forall x \in K(x \notin \mathcal{O} \rightarrow x^{-1} \in \mathcal{O}).$$

We denote its units by $\mathcal{O}^\times$.

DEFINITION 4.1.2. *Let K be a field and Γ a totally ordered abelian group. A surjective map $v : K \rightarrow \Gamma \cup \{\infty\}$ is called a* ***valuation*** *if*

- $v(x) = \infty \leftrightarrow x = 0$;
- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \min(v(x), v(y))$.

where ∞ is larger than any element of Γ and $\alpha + \infty = \infty + \alpha = \infty$, for every $\alpha \in \Gamma$. The additive subgroup $v(K^\times)$ is called the ***value group****. The pair (K, v) is called a* ***valued field****.*

Now follows some properties that can help grasp the notion of valuation as well as some useful identities.

PROPERTY 4.1.3. *Let (K, v) be a valued field. Then*

i) $v(x) = v(-x)$

ii) $v(x^{-1}) = -v(x)$.

iii) $v(x + y) = \min\{v(x), v(y)\}$ *if and only if* $v(x) \neq v(y)$.

iv) $v(x) = v(y) \Leftrightarrow x - y \in \mu(K)$.

DEFINITION 4.1.4. *Let (K, v) be a valued field. The* ***ring of valuation*** *of v is given by*

$$\mathcal{O}_v := \{x \in K : v(x) \geq 0\}.$$

PROPERTY 4.1.5. *Let (K, v) be a valued field. Then*

1 $\mathcal{O}_v$ *is a subdomain of* K*;*

2 $m_v := \{x \in \mathcal{O}_v : v(x) > 0\}$ *is the unique maximal ideal of* $\mathcal{O}_v$*;*

3 $\mathcal{O}_v^\times = \{x \in \mathcal{O}_v : v(x) = 0\}$ *is the set of units of* $\mathcal{O}_v$*.*

Proof. For (2) consult Corollary 6.4 of [7]. The rest of the proof is elementary. □

NOTE 4.1.6. We refer to m_v as the set of **infinitesimals**. If K is a real closed field, we refer to $\mathcal{O}_v$ as the **reals**.

PROPERTY 4.1.7. *Let K be a field and $\mathcal{O} \subset K$ a valuation ring. There is an ordered abelian group Γ and a valuation $v : K \rightarrow \Gamma \cup \{\infty\}$ such that*

$$\mathcal{O} = \mathcal{O}_v.$$

Moreover, this valuation is unique in the sense that if Γ' is another ordered abelian group and $w : K \rightarrow \Gamma' \cup \{\infty\}$ is a valuation on K such that $\mathcal{O}_w = \mathcal{O}$, then there is an isomorphism of ordered groups $\phi : \Gamma \rightarrow \Gamma'$ such that for every $x \in K^\times$, $w(x) = \phi(v(x))$.

Proof. **Existence**: Let $\Gamma = K^\times/\mathcal{O}^\times$. Its elements $x\mathcal{O}^\times$ are of the form $\{xy : y \in \mathcal{O}^\times\}$. Define an operation by $x\mathcal{O}^\times + y\mathcal{O}^\times = (xy)\mathcal{O}^\times$. This operation is obviously associative and commutative, with identity $1\mathcal{O} = \mathcal{O}$, and inverse $-(x\mathcal{O}^\times) = x^{-1}\mathcal{O}^\times$. This makes $(\Gamma, +, \mathcal{O})$ an abelian group. Define a relation $\leq$ on Γ by

$$x\mathcal{O}^\times < y\mathcal{O}^\times \leftrightarrow x^{-1}y \in \mathcal{O} \setminus \mathcal{O}^\times$$

which is equivalent to

$$x\mathcal{O}^\times \leq y\mathcal{O}^\times \leftrightarrow x^{-1}y \in \mathcal{O}$$

- $\leq$ is transitive: Suppose $x\mathcal{O}^\times < y\mathcal{O}^\times < z\mathcal{O}^\times$. We have $x^{-1}y, y^{-1}z \in \mathcal{O} \setminus \mathcal{O}^\times$, so $x^{-1}yy^{-1}z = x^{-1}z \in \mathcal{O}$ and also $y^{-1}x \notin \mathcal{O}$. Suppose by contradiction $x^{-1}z \in \mathcal{O}^\times$. We get $z^{-1}x \in \mathcal{O}^\times$, which implies $y^{-1}zz^{-1}x = y^{-1}x \in \mathcal{O}^\times$, and hence a contradiction.

- $\leq$ is antisymmetric: Suppose $x\mathcal{O}^\times \leq y\mathcal{O}^\times$ and $y\mathcal{O}^\times \leq x\mathcal{O}^\times$. Then $x^{-1}y, y^{-1}x \in \mathcal{O}$ and so $xy^{-1} \in \mathcal{O}^\times$ which is equivalent to $x\mathcal{O}^\times = y\mathcal{O}^\times$.

- $\leq$ is a total order: Suppose $y\mathcal{O}^\times \nleq x\mathcal{O}^\times$. We get $y^{-1}x \notin \mathcal{O}$, so $(y^{-1}x)^{-1} = x^{-1}y \in \mathcal{O} \setminus \mathcal{O}^\times$, which gives $x\mathcal{O}^\times < y\mathcal{O}^\times$.

- $\leq$ is compatible with $+$: Suppose $x\mathcal{O}^\times < y\mathcal{O}^\times$. We have $x^{-1}y = (xz)^{-1}yz \in \mathcal{O} \setminus \mathcal{O}^\times$ which gives $x\mathcal{O}^\times + z\mathcal{O}^\times < y\mathcal{O}^\times + z\mathcal{O}^\times$.

So $(\Gamma, \leq, +, \mathcal{O})$ is an ordered abelian group. Define $v : K \to \Gamma \cup \{\infty\}$ by $v(x) = x\mathcal{O}^\times$ if $x \neq 0$ and $v(0) = \infty$. We have

- $v(xy) = xy\mathcal{O}^\times = x\mathcal{O}^\times + y\mathcal{O}^\times = v(x) + v(y)$.

- $v(x + y) \geq \min(v(x), v(y))$: Suppose $v(x) \leq v(y)$. So $x^{-1}y \in \mathcal{O}$. Since $1 \in \mathcal{O}$, we have $1 + x^{-1}y = x^{-1}(x + y) \in \mathcal{O}$, which gives $v(x) \leq v(x + y)$.

So v is a valuation on K. Now it is very easy to see that $\mathcal{O}_v = \mathcal{O}$, since $0 = v(1) \leq v(x)$ if and only if $x \in \mathcal{O}$.

Uniqueness: Let Γ' be an ordered abelian group and $w : K \to \Gamma' \cup \{\infty\}$ be a valuation on K such that $\mathcal{O} = \mathcal{O}_w$. The application $w^\times : K^\times \to \Gamma'$ defined by $w^\times(x) = w(x)$ is an homomorphism of groups between $(K^\times, \cdot)$ and $(\Gamma', +)$. We have $\mathrm{Ker}(w^\times) = \mathcal{O}^\times$. So we get an isomorphism $\phi : K/\mathcal{O}^\times \to \Gamma'$, defined by $\phi(x\mathcal{O}^\times) = w(x)$ which gives the uniqueness property. ☐

DEFINITION 4.1.8. *Let (K, v) be a valued field. The field*

$$K_v := \mathcal{O}_v/m_v$$

is called the ***residue class field*** *of v.*

EXAMPLE 4.1.9. Let

$$\mathrm{Fin}(K) := \{x \in K : \text{ there is } q \in \mathbb{Q} \text{ such that } |x| < q\}.$$

Then

1. $\mathrm{Fin}(K)$ is a valuation ring;

2. The maximal ideal of $\mathrm{Fin}(K)$ is given by the infinitesimals of K, which we denote by μ;

Proof. **(1)**: Let $x \in K$. Then, for some $q \in \mathbb{Q}$, either $x \leq q$ or $x^{-1} \leq q$, otherwise we can choose a rational $q > 1$ such that $x > q$ and $x^{-1} > q$. This implies $|xx^{-1}| = |x||x^{-1}| > q^2 \geq 1$ which is absurd.

(2): Let I be the unique maximal ideal of $\mathrm{Fin}(K)$. For every infinitesimal $y \in \mathrm{Fin}(K)$, $\mathrm{Fin}(K)y$ is a proper ideal since $y^{-1} \notin \mathrm{Fin}(K)$, so $\mathrm{Fin}(K)y \subset I$. This means that I contains every infinitesimal. Let $x \in \mathrm{Fin}(K) - \mu$ and suppose by contradiction $x \in I$. We have $x^{-1} \in \mathrm{Fin}(K)$. Let u be any element of $\mathrm{Fin}(K)$. Then $ux^{-1} \in \mathrm{Fin}(K)$ and so $ux^{-1}x = u \in I$, implying $\mathrm{Fin}(K) = I$ which is absurd. ☐

We will call the valuation implicit in example 4.1.9 the **usual valuation**.

DEFINITION 4.1.10. *Let (K, v) be a valued field. Consider*

$$\begin{aligned} \text{res} : &\mathcal{O}_v[x] \to K_v[x] \\ &f(x) = a_0 + a_1 x + ... + a_n x^n \mapsto \textit{res}(f)(x) = \bar{a_0} + \bar{a_1} x + ... + \bar{a_n} x^n \end{aligned}$$

where $\bar{a}_i$ is the class of a_i in K_v. This map is called ***residue map****.*

DEFINITION 4.1.11. *Let (K, v) be a valued field. We say that K satisfies the* ***hensel property*** *if whenever $f(x) \in \mathcal{O}_v[x]$ and $\bar{\alpha} \in K_v$ is such that $res(f)(\bar{\alpha}) = \bar{0}$ and $\text{res}(f')(\bar{\alpha}) \neq \bar{0}$, there is $\beta \in \mathcal{O}_v$ such that $\beta \in \bar{\alpha}$ and $f(\beta) = 0$. In this case the valued field K is called* ***henselian****.*

An important property of henselian valued fields is the following

THEOREM 4.1.12. *Let (K, v) be a henselian valued field. If the residue field $\mathcal{O}_v/m_v$ is real closed and the value group $v(K)$ is divisible, then K is real closed.*

Proof. Consult Theorem 8.6 of [8]. □

This gives in particular a non-standard model of rcof.

4.2 Ordered fields as $\mathcal{L}_{an}$-structures

Let K be a non-empty ordered field. We have seen in 4.0.7 that if K satisfies the axiom AC1 from Theorem 4.0.6, then K contains a copy of $\mathbb{R}$. In this section we assume that K satisfies a more flexible version of the axioms AC1, AC2 and AC3 to prove some important properties and to show a natural way of interpreting the function symbols $\widetilde{f} \in \mathbb{R}\{X_1, ..., X_n\}$ in K. This will allow us to see K as an $\mathcal{L}_{an}$-structure containing $\mathbb{R}_{an}$ as a substructure. We will denote this structure by K_{an}. This natural interpretation is essentially the content of axiom AC4. It will allow us to show that the flexible versions of AC1, AC2 and AC3 that we assumed for K are actually equivalent to those axioms and to prove quantifier elimination of $Th(K_{an})$ in an extended language. Once these results are established the proof of Theorem 4.0.6 will be an easy consequence.

Let $\mathbb{R}\langle X_1, ..., X_n\rangle$ denote the ring of power series in $X_1, ..., X_n$ over $\mathbb{R}$ which converge in a neighbourhood of 0. Denote the infinitesimals of K by μ and let v be the usual valuation on K.

For each $f \in \mathbb{R}\langle X_1, ..., X_n\rangle$, $n \in \mathbb{N}$, suppose we can associate a function $f_K : \mu^n \to K$ such that

C1) $(f + g)_K = f_K + g_K$ and $(f \cdot g)_K = f_K \cdot g_K$ for $f, g \in \mathbb{R}\langle X_1, ..., X_n\rangle$. The constant functions $0 : x \mapsto 0$ and $1 : x \mapsto 1$ are respectively associated to $1_K : x \to 1^K$ and $0_K : x \mapsto 0^K$.

C2) $(X_i)_K : \mu^n \to K$ is the i^{th} coordinate function $(x_1, ..., x_n) \mapsto x_i$, for $X_i \in \mathbb{R}\langle X_1, ..., X_n\rangle$;

C3) If $f \in \mathbb{R}\langle X_1, ..., X_n\rangle$ and $g_1, ..., g_n \in (X_1, ..., X_m)\mathbb{R}\langle X_1, ..., X_m\rangle$ (i.e., the g_i have constant term zero), then
$$f(g_1, ..., g_n)_K(x) = f_K(g_1(x), ..., g_n(x)), \quad \text{for all } x \in \mu^m.$$

Observe that, as in Note 4.0.7, C1 implies that $\mathbb{R} \subset K$. Since K contains $\mathbb{R}$, K_v is arquimedian and contains $\mathbb{R}$. In the other way $\mathbb{R}$ contains a copy of every arquimedian field. So $K_v = \mathbb{R}$.

From C1, C2 and C3 we prove the following two lemmas:

LEMMA 4.2.1. *Let $f \in R\langle X_1, ..., X_n\rangle$. Then*

$$f_K(\mu^n) \subset f(0) + \mu \cancel{\in Fin(K)}.$$

Proof. Let $0 < \epsilon \in \mathbb{R}$. The power series $f - f(0) + \epsilon \in \mathbb{R}\langle X_1, ..., X_n\rangle$ has constant term $\epsilon > 0$. Let $F(x, y) = y^2 - (f(x) - f(0) + \epsilon)$. Then $F(0, \sqrt{\epsilon}) = 0$ and $\frac{\partial F}{\partial y}(0, \sqrt{\epsilon}) = 2\sqrt{\epsilon}$. By the Implicit Function Theorem there exists $g \in \mathbb{R}\langle X_1, ..., X_n\rangle$ such that $F(x, g(x)) = 0$ for x in some neighbourhood of 0. We can write $g^2 = f - f(0) + \epsilon$.

We get $f = f(0) - \epsilon + g^2$ and so by C1, $f_K = f(0) - \epsilon + (g_K)^2$. Thus $f_K(x) \geq f(0) - \epsilon$, for all $x \in \mu^n$. In a similar way we get $f_K(x) \leq f(0) + \epsilon$, for all $x \in \mu^n$. Since ϵ was arbitrary, this proves the lemma. $\square$

LEMMA 4.2.2. *The valued field (K, v) is henselian.*

Proof. Let $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathcal{O}_v[x]$. For each $0 \leq i \leq n$, let $a_i = r_i + \xi_i$, where $r_i \in \mathbb{R}$ and $\xi_i \in \mu$. We have

$$f(x) = (r_0 + r_1 x + ... + r_n x) + (\xi_0 + \xi_1 x + ... + \xi_n x^n).$$

Then $\mathrm{res}(f)(x) = r_0 + r_1 x + ... + r_n x^n$. Suppose $\alpha \in \mathbb{R}$ is such that $\mathrm{res}(f)(\alpha) = 0$ and $\mathrm{res}(f')(\alpha) \neq 0$. Let

$$F(x, y) = (r_0 + r_1 x + ... + r_n x^n) + (y_0 + y_1 x + ... + y_n x^n).$$

Then $F(\alpha, 0, ..., 0) = 0$ and $\frac{\partial F}{\partial x}(\alpha, 0, ..., 0) = \mathrm{res}(f')(\alpha) \neq 0$. By the implicit function theorem there is $g \in \mathbb{R}\langle y_0, ..., y_n\rangle$ such that $g(0, ..., 0) = \alpha$ and $F(g(y_0, ..., y_n), y_0, ..., y_n) = 0$. In particular $g(\xi_0, ..., \xi_n)$ is a root of $f(x)$ and by Lemma 4.2.1, $g(\xi_0, ..., \xi_n) \cancel{\in \mathcal{O}_v}$. $\square$

With this we get

COROLLARY 4.2.3. *If each positive element of K has an n^{th} root, for $n = 2, 3, ...$, then K is real closed.*

Proof. Let $x \in K$ be a positive element. Let n be an integer greater than 2. Then $v((x)^{\frac{1}{n}}) = \frac{1}{n} v(x)$ which implies that the value group is divisible. Since $K_v = \mathbb{R}$, by Theorem 4.1.12, K is real closed. $\square$

For each open $U \subset \mathbb{R}^n$ let

$$U_K := \{x \in K^n : x - a \in \mu^n \text{ for some } a \in U\} = \bigcup_{a \in U} a + \mu^n.$$

For open, nonempty $U \subset \mathbb{R}^n$, let $\mathrm{An}(U)$ be the $\mathbb{R}$-algebra of real analytic functions $f : U \to \mathbb{R}$. We assign to each $f \in \mathrm{An}(U)$ a function $f_K : U_K \to K$ as follows: given $a \in U$ let

$$f_a(X) = \sum \frac{1}{i!} \frac{\partial^{|i|} f}{\partial X^i}(a) X^i \in \mathbb{R}\langle X\rangle$$

be the Taylor series of f at a. Then we put

$$f_K(a + x) = (f_a)_K(x)$$

for $x \in \mu^n$.

PROPERTY 4.2.4. *Regarding functions of the form $f_K : U_K \to K$, for open, nonempty $U \subset \mathbb{R}^n$ and $f \in An(U)$ we have*

C1)$_U$ $(f + g)_K = f_K + g_K$ *and* $(f \cdot g)_K = f_K \cdot g_K$ *for* $f, g \in An(U)$, *and* c_K *is the constant function* $x \mapsto c$ *for* $c \in \mathbb{R} \subset An(U)$;

C2)$_U$ *If* $(X_i)_K : \mu^n \to K$ *is the* i^{th} *coordinate function* $(x_1, ..., x_n) \mapsto x_i$, *from* U *to* $\mathbb{R}$, *then* $(X_i)_K$ *is the* i^{th} *coordinate function from* U_K *to* K.

C3)$_{U,V}$ *If* $f \in An(U)$ *and* $g_1, ..., g_n \in \mathbb{R}[X_1, ..., X_m]$, *and* $V \subset \mathbb{R}^m$ *is open and nonempty with* $g(V) \subset U$ *for* $g = (g_1, ..., g_n) : V \to \mathbb{R}^n$, *the function* $f \circ g \in An(V)$ *satisfies*

$$(f \circ g)_K(x) = f_K(g_1(x), ..., g_n(x)), \quad \text{for all } x \in V_K$$

Proof. C1)$_U$: Let $a \in U$ and $x \in \mu^n$. Then

$$\begin{aligned}(f+g)_K(a+x) &= ((f+g)_a)_K(x)\\ &= (f_a+g_a)_K(x)\\ &= (f_a)_K(x)+(g_a)_K(x).\end{aligned}$$

C3)$_{U,V}$: Let $a \in V$ and $x \in \mu^n$. We use the fact that $(f \circ g)_a = f_{g(a)}(g_a - g(a))$.

$$\begin{aligned}(f\circ g)_K(a+x) &= ((f\circ g)_a)_K(x)\\ &= (f_{g(a)})_K(x)((g_a)_K(x) - g(a)_K)\\ &= (f_{g(a)})_K(x)((g_a)_K(x)) - (f_{g(a)})_K(x)g(a)_K\\ &= (f_a)_K(g_1(x),...,g_n(x))\\ &= f_K(g_1(a+x),...,g_n(a+x)).\end{aligned}$$

□

Recall that $\mathbb{R}\{X_1,...,X_n\}$ is the subring of $\mathbb{R}\langle X_1,...,X_n\rangle$ whose elements converge on a neighbourhood of I^n, $I = [-1,1]$. We now present a way to assign for each series $f \in \mathbb{R}\{X_1,...,X_n\}$ a function $\widetilde{f}_K : K^n \to K$. Let $\widehat{f} \in \mathrm{An}(U)$ be any analytic function on an open set $U \subset \mathbb{R}^n$ containing I^n, such that $\widehat{f}(x) = f(x)$ for $x \in I^n$. Put

$$\widetilde{f}_K(x) = \begin{cases} \widehat{f}_K(x) & \text{for } x \in I(K)^n \\ 0 & \text{for } x \notin I(K)^n \end{cases}$$

where $I_K = \{x \in K : -1 \le x \le 1\}$.

In this way we can turn K as an $\mathcal{L}_{an}$-structure such that $\mathbb{R}_{an} \subset K$. We denote it by K_{an}. Sometimes we will also be interested to consider K as an $\mathcal{L}_{an}(^{-1})$-structure, where $^{-1}$ is a unary function symbol interpreted as multiplicative inverse, with $0^{-1} = 0$.

In the seminal paper [10] it is proved that $(\mathbb{R}_{an},^{-1})$ admits quantifier elimination. The proof can be adapted to $(K_{an},^{-1})$, provided K is real closed:

THEOREM 4.2.5. *Suppose K is a non-empty real closed ordered field containing $\mathbb{R}$. For every $\mathcal{L}_{an}(^{-1})$-formula $\phi(x_1,...,x_m)$ there is a quantifier-free $\mathcal{L}_{an}(^{-1})$-formula $\phi'(x_1,...,x_m)$ such that $(K_{an},^{-1}) \vDash \phi \leftrightarrow \phi'$.*

As a corollary we get

COROLLARY 4.2.6. *If K is a non-empty real closed ordered field containing $\mathbb{R}$, then $\mathbb{R}_{an} \preceq K_{an}$*

Proof. We have that $(\mathbb{R}_{an},^{-1})$ is a substructure of $(K_{an},^{-1})$. By Theorem 4.2.5, this implies $\mathbb{R}_{an} \preceq K_{an}$. □

Now we are ready to prove Theorem 4.0.6.

Proof of Theorem 4.0.6. Let T be the set of axioms described in the theorem. Let K be an $\mathcal{L}_{an}$-strucutre such that $K \vDash T$. The axioms AC1, AC2, AC3 and the existence of n^{th}-root for each positive element $x \in K$ imply that K is real closed (Corollary 4.2.3). AC4 implies that $\mathbb{R}_{an}$ is a substructure of K and, with the fact that K is real closed, it also gives QE of K in the language $(L_{an},^{-1})$ (Theorem 4.2.5). So $Th(K) = T_{an}$ and since $K \vDash T$ was chosen arbitrarily, this implies that T is an axiomatization of T_{an}. □

By section 4 of [2] we have quantifier elimination in the language $\mathcal{L}_{an}(^{-1})$ for the theory T_{an} adding the axiom

$$\forall x(x \cdot x^{-1}) = 1.$$

Adding the unary function symbols $\sqrt[n]{\ }$ for $n = 2,3,...$ to the language $\mathcal{L}_{an}(^{-1})$ and write the axioms

$$\forall x(x > 0 \Rightarrow ((\sqrt[n]{x})^n = x \wedge \sqrt[n]{x} > 0)) \wedge (x \le 0 \Rightarrow \sqrt[n]{x} = 0),$$

for each $n = 2,3,...$ to the axioms of T_{an} we get an universal axiomatization for T_{an}.

Chapter 5

The theory of $\mathbb{R}_{an}(\exp)$

In this chapter we prove that the theory of restricted analytic fields with exponentiation defined everywhere ($\mathbb{R}_{an}(\exp)$) is o-minimal. Along the way we show that $Th(\mathbb{R}_{an}(\exp))$ has quantifier elimination in the language $\mathcal{L}_{an}(\exp, \log)$.

5.1 Power series fields

We will see in the next section that every model of T_{an} can be viewed as a subfield of a very specific form of power series field. Throughout this section k denotes a field and Γ is an ordered abelian group. We will consider formal power series, objects of the form

$$x = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma,$$

where $\gamma \in \Gamma$ ("exponents") and $a_\gamma \in k$ ("coefficients"), such that the **support** of x, defined as $\text{supp}(x) := \{\gamma \in \Gamma : a_\gamma \neq 0\}$, is a well-ordered subset of Γ. We will denote the set of formal power series by $k((t^\Gamma))$.

We define an addition and multiplication on $k((t^\Gamma))$. Let $x = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ and $y = \sum_{\gamma \in \Gamma} b_\gamma t^\gamma$. Then

- $x + y = \sum_{\gamma \in \Gamma} (a_\gamma + b_\gamma) t^\gamma$;
- $x \cdot y = \sum_{\gamma \in \Gamma} (\sum_{\gamma_1 + \gamma_2 = \gamma} a_{\gamma_1} b_{\gamma_2}) t^\gamma$.

With these two operations $k((t^\Gamma))$ is a field (consult [13]) We consider k as a subfield of $k((t^\Gamma))$ by identifying $c \in k$ with ct^0. Consider the map ord : $k((t^\Gamma))^\times \to \Gamma,\ \text{ord}(x) = \min \text{supp}(x)$. The map ord defines a valuation on $k((t^\Gamma))$ with valuation ring

$$k[[t^\Gamma]] = \{x \in k((t^\Gamma)) :\ \text{if } \gamma \in \text{supp}(x) \text{ then } \gamma \geq 0\}$$

maximal ideal

$$\mu = \{x \in k((t^\Gamma)) :\ \text{if } \gamma \in \text{supp}(x) \text{ then } \gamma > 0\}$$

and residue field k. This valuation is henselian (consult [14]). If k is an ordered field, then we consider $k((t^\Gamma))$ with the following order: Let $x = \sum a_\gamma t^\gamma$ and $y = \sum b_\gamma t^\gamma$. Then $x < y$ if $a_\gamma < b_\gamma$ where γ is least such that $a_\gamma \neq b_\gamma$.

NOTE 5.1.1 (Ring of power series). Let $k[[X_1, ..., X_n]]$ denote the ring of power series $\sum c_i X^i$ where $i = (i_1, ..., i_n) \in \mathbb{N}^n$, $c_i \in k$ and $X^i = X_1^{i_1} \cdots X_n^{i_n}$. Let $\mu^n = \mu \times ... \times \mu \subset k[[t^\Gamma]]^n$. If $a = (a_1, ..., a_n) \in \mu^n$ and $f = \sum c_i X^i \in k[[X_1, ..., X_n]]$, then $f(a) = \sum c_i a^i$ is a well-defined element of $k((t^\Gamma))$ since only finitely many terms $c_i a^i$ contribute a nonzero coefficient to a given monomial t^γ and the union of the supports of the elements $c_i a^i$ is well-ordered (consult [13]). It is easy to see that the map $f(X) \mapsto f(a)$ is a k-algebra homomorphism from $k[[X_1, ..., X_n]]$ into $k((t^\Gamma))$.

5.2 Models of T_{an} as power series fields

In this section we will prove a key fact about valuations in models of T_{an}.

Let $\mathcal{M} \subset \mathcal{N}$ be models of T_{an}. If $y \in N \setminus M$, we denote by $M\langle y\rangle$ the definable closure of $M \cup \{y\}$. Note that $M\langle y\rangle \preceq \mathcal{N}$. Since T_{an} is o-minimal, $\text{tp}(y/M)$ is determined by the cut y makes in the ordering of M (see 1.5.8).

We denote the field generated by $M \cup \{y\}$ by

$$M(y) := \{f(y)/g(y) : f, g \in M[X],\ g(y) \neq 0\}$$

We want to prove that $v(M\langle y\rangle^\times) = v(\overline{M(y)}^\times)$, where $\overline{M(y)}$ is the real closure of $M(y)$.

NOTE 5.2.1. $v(\overline{M(y)}^\times) = \langle v(M(y)^\times)\rangle$, where $\langle v(M(y)^\times)\rangle$ denotes the divisible hull of $v(M(y)^\times)$.

Proof. Let $\langle M(y)\rangle$ be the field generated by $M(y)$ and all n^{th}-roots of positive elements in $M(y)$. Then $v(\langle M(y)\rangle^\times) = \langle v(M(y)^\times)\rangle$. By Corollary 4.2.3, $\langle M(y)\rangle = \overline{M(y)}$ and so $\langle v(M(y)^\times)\rangle = v(\overline{M(y)}^\times)$. □

DEFINITION 5.2.2. *Let (K, v) be an ordered valued field and $\Gamma = v(K^\times)$. We call $s : \Gamma \to K$ a **section** if it is an homomorphism of groups, considering K as a multiplicative group, and $v(s(g)) = g$ for all $g \in \Gamma$.*

NOTE 5.2.3. Let K be an ordered field such that every positive element of K has an n^{th}-root for all $n \in \mathbb{N}$. Then there is always a section $s : v(K^\times) \to K$.

Proof. Let $(g_j)_{j\in J}$ be a basis for $\Gamma = v(K^\times)$ as a $\mathbb{Q}$-vector space. Let $b_j > 0$ such that $b_j = v(g_j)$ for each $j \in J$. Define a section s by $s(\sum q_j g_j) = \prod b_j^{q_j}$. □

LEMMA 5.2.4. *Let $\mathcal{M}, \mathcal{N} \vDash T_{an}$ with $\mathcal{M} \subset \mathcal{N}$. Let $\Gamma = v(M^\times)$. Let $s : \Gamma \to M$ be a section and suppose we have an $\mathcal{L}_{an}$-embedding $\tau : M \to \mathbb{R}((t^\Gamma))_{an}$ such that $\tau(s(g)) = t^g$ for all $g \in \Gamma$. If $y \in N \setminus M$ and $v(M(y)^\times) = \Gamma$, then we can extend τ to an $\mathcal{L}_{an}$-embedding from $M\langle y\rangle$ into $\mathbb{R}((t^\Gamma))_{an}$.*

Proof. Identify M as a subset of $\mathbb{R}((t^\Gamma))$. We will find an element $w \in \mathbb{R}((t^\Gamma))$ making the same cut in the ordering of M as y does, which by property 1.5.8 proves the lemma. For this we construct a sequence of approximations to y, $(x_\alpha \in M : \alpha < \gamma)$ for some limit ordinal γ yet to be determined. Recall that the residue field of N and M are both $\mathbb{R}$.

Let $x_0 = \text{res}(y)$. Suppose x_α is defined for some ordinal α. Let $g_\alpha = v(y - x_\alpha)$ and $a_\alpha = \text{res}(\frac{y - x_\alpha}{t^{g_\alpha}})$. Put $x_{\alpha+1} = x_\alpha + a_\alpha t^{g_\alpha}$. Note that $v(y - x_{\alpha+1}) = \min\{v(y - x_\alpha), a_\alpha t^{g_\alpha}) = g_\alpha = v(y - x_\alpha)$.

Consider now a limit ordinal α such that for all $\beta < \alpha$, x_β is defined. If there isn't $z \in M$ such that for all $\beta < \alpha$, $v(y - x_\beta) < v(y - z)$ then let $\alpha = \gamma$. Otherwise pick such z and put $x_\alpha = z$. Iterate until there isn't such element. This gives us the sequence $(x_\alpha : \alpha < \gamma)$.

Note that for two limit ordinals $\alpha, \beta < \gamma$ such that $\alpha < \beta$, we have $v(y - x_\alpha) < v(y - x_\beta)$.

Fix $\alpha, \beta < \gamma$ such that $\alpha < \beta$ and write $x_\alpha = \sum a_{\alpha,g} t^g$, $x_\beta = \sum a_{\beta,g} t^g$. Note that

$$\begin{aligned} v(x_\beta - x_\alpha) &= v(x_\beta - y + y - x_\alpha) \\ &= \min\{v(x_\beta - y), v(y - x_\alpha)\} \\ &= g_\alpha \end{aligned}$$

This implies $a_{\alpha,g} = a_{\beta,g}$ for $g < g_\alpha$. Now we define $w = \sum b_g t^g$ by putting $b_g = a_{\alpha,g}$ whenever $g < g_\alpha$ for some $\alpha < \gamma$, and $b_g = 0$ otherwise. The support of w is well-ordered since any decreasing sequence (g_n) in $\text{supp}(w)$ is contained, ignoring the first few elements if necessary, in $\text{supp}(x_\alpha)$ for some $\alpha < \gamma$. So w is well defined. Note that for every $\alpha < \gamma$, $v(y - x_\alpha) < v(y - w)$. This element w defines the same cut in M as y does: Suppose not. Let $z \in M$ such that $w < z < y$. But then $v(y - w) < v(y - z)$, which would contradict the existence of some $\alpha < \gamma$ such that $v(y - z) < v(y - x_\alpha)$. □

Now follows a general fact about extensions of real closed fields.

LEMMA 5.2.5. *Let K and L be real closed fields with $K \subset L$. Let $y \in L \setminus K$. If $v(K(y)^\times) \neq v(K^\times)$, then there is some element $a \in K$ such that $v(y - a) \notin v(K^\times)$.*

Proof. There are polynomials $p(X), q(X) \in K[X]$ such that $v(\frac{p(y)}{q(y)}) = v(p(y) - v(q(y)) \notin v(K^\times)$. Thus there is a polynomial $p(X) \in K[X]$ such that $v(p(y)) \notin v(K^\times)$. Since K is real closed

$$p(y) = \prod_{i=1}^{m}(y - a_i) \prod_{j=1}^{n}((y - b_j)^2 + c_j^2)$$

for some $a_1, ..., a_m, b_1, ..., b_n, c_1, ..., c_n \in K$. Suppose that for all $i = 1, ..., m$ and $j = 1, ..., n$, $v(y - a_i), v(y - b_j) \notin v(K^\times)$. Then for some j, $v((y - b_j)^2 + c_j^2) \notin v(K^\times)$. We have $v(y - b_j) = v(c_j)$ since otherwise $v((y - b_j)^2 + c_j^2) = \min\{2v(y - b_j), 2v(c_j)\}$, which is absurd. Moreover $v((y - b_j)^2 + c_j^2) > 2v(c_j)$. On the other hand $(y - b_j)^2 + c_j^2 > c_j^2 > 0$ which imply $v((y - b_j)^2 + c_j^2) \leq 2v(c_j)$, a contradiction. □

NOTE 5.2.6. Let M, N, Γ, s and τ be as in 5.2.4. Let $y \in N \setminus M$ and suppose $v(M(y)^\times) \neq \Gamma$. We construct an embedding $\tau' : M\langle y\rangle \to \mathbb{R}((t^{\Gamma'}))_{an}$ for a reasonable group Γ'. By 5.2.5 there is some $a \in M$ such that $v(y - a) \notin \Gamma$. Without loss of generality we assume $v(y) \notin \Gamma$. We also assume $y > 0$. We let Γ' be the divisible subgroup of $v(N)$ generated by Γ and $v(y)$. We extend s to $s' : \Gamma' \to M\langle y\rangle$ by $s'(g + qv(y)) = s(g)y^q$ for $g \in \Gamma$ and $q \in \mathbb{Q}$. Let $m \in M$ with $m > 0$. Note that since $v(y) \notin v(M^\times)$, we have $m < y$ (in $\mathcal{N}$) if and only if $v(m) > v(y)$. On the other hand if $m < t^{v(y)}$ then $v(m) > v(y)$, and reciprocally if $m < t^{v(y)}$ then $v(m) < v(y)$, so $v(m) > v(y)$ if and only if $m < t^{v(y)}$. In other words, $t^{v(y)}$ makes the same cut in M as y does, so $\langle \tau(M) \cup \{t^{v(y)}\}\rangle \subset \mathbb{R}((t^{\Gamma'}))$ is isomorphic to $M\langle y\rangle$.

The $\mathcal{L}_{an}$-embedding $\tau' : M\langle y\rangle \to \mathbb{R}((t^{\Gamma'}))_{an}$ defined by $\tau'(m) = \tau(m)$ for $m \in M$ and $\tau'(y) = t^{v(y)}$ extends τ and for arbitrary $h = g + qv(y) \in \Gamma'$ with $g \in \Gamma$ and $q \in \mathbb{Q}$, we have

$$\begin{aligned}
\tau'(s'(g + qv(y)) &= \tau'(s(g)y^q) \\
&= \tau(s(g))\tau'(y^q) \\
&= t^g t^{qv(y)} \\
&= t^{g+qv(y)}.
\end{aligned}$$

Note that $v(M\langle y\rangle^\times) = \Gamma'$.

COROLLARY 5.2.7. *Let $\mathcal{M} \models T_{an}$ and $v(M^\times) = \Gamma$. For every section $s : \Gamma \to M$ there is an $\mathcal{L}_{an}$-embedding $\tau : M \to \mathbb{R}((t^\Gamma))_{an}$ such that $\tau(s(g)) = t^g$ for all $g \in \Gamma$.*

Proof. Let $M_0 = \mathbb{R}_{an} \preceq \mathcal{M}$, $\Gamma_0 = 0$, $s_0(0) = 1$ and τ_0 the identity. Iterate 5.2.4 and 5.2.6 accordingly. □

The main result of this section

COROLLARY 5.2.8. *Let $\mathcal{M}, \mathcal{N} \models T_{an}$ and suppose $M \subset N$. Let $y \in N \setminus M$. Then $v(M\langle y\rangle^\times) = \langle v(M(y)^\times)\rangle$.*

Proof. Let $\Gamma = v(M^\times)$. Embed $\mathcal{M}$ into $\mathbb{R}((t^\Gamma))_{an}$ through τ and let s be its section such that $\tau(s(g)) = t^g$. If $v(M(y)^\times) = \Gamma$, then by 5.2.4 we can extend τ to an embedding of $M\langle y\rangle$ into $\mathbb{R}((t^\Gamma))_{an}$, giving $v(M\langle y\rangle^\times) = \Gamma$. If $v(M(y)^\times) \neq \Gamma$, let Γ' be the divisible subgroup of $v(N^\times)$ generated by $v(M(y)^\times)$. Then 5.2.6 allows us to extend τ to an embedding of $M\langle y\rangle$ into $\mathbb{R}((t^{\Gamma'}))_{an}$, giving $v(M\langle y\rangle^\times) = \Gamma'$. □

NOTE 5.2.9. Let $\mathcal{M}, \mathcal{N} \models T_{an}$ and suppose $M \subset N$. Let $\Gamma = v(M^\times)$. Let $y \in N \setminus M$. By 5.2.8 $v(M\langle y\rangle^\times) = \langle v(M(y)^\times)\rangle$. If $v(M(y)^\times) = v(M^\times)$, then $v(M\langle y\rangle^\times) = v(M(y)^\times)$. If $v(M(y)^\times) \neq v(M^\times)$, following the construction from 5.2.6,

$$v(M\langle y\rangle^\times) = \{g + qv(y) : g \in \Gamma,\ q \in \mathbb{Q}\}.$$

Thus the $\mathbb{Q}$-linear dimension of $v(M\langle y\rangle^\times)$ over $v(M^\times)$ is either 0 or 1.

5.3 The theory of $\mathbb{R}_{an}$(exp) and quantifier elimination

Let $\mathcal{L}_{an}(\exp)$ be the language $\mathcal{L}_{an}$ with a new unary function symbol exp. Let $T_{an}(\exp)$ be the theory obtained by adding to T_{an} the universal closures of the following axioms

E1) $\exp(x+y) = \exp(x)\exp(y)$

E2) $x < y \to \exp(x) < \exp(y)$

E3) $x > 0 \to \exists y \exp(y) = x$

E4$_n$) $x > n^2 \to \exp(x) > x^n$, for each $n \in \mathbb{N}$

E5) $-1 \leq x \leq 1 \to \exp(x) = E(x)$, where E is the function symbol of $\mathcal{L}_{an}$ corresponding to the exponential power series $\sum \frac{1}{n!} X^n \in \mathbb{R}\{X\}$

Let $\mathcal{L}_{an}(\exp, \log)$ be the language $\mathcal{L}_{an}(\exp)$ with a new unary function symbol log. Let $T_{an}(\exp, \log)$ be the theory obtained by adding to $T_{an}(\exp)$ the universal closures of the following axiom

L) $(x > 0 \to \exp(\log(x)) = x) \wedge (x \leq 0 \to \log(x) = 0)$.

In this section we will prove that $T_{an}(\exp)$ has quantifier eimination in the language $\mathcal{L}_{an}(\exp, \log)$.

Let $K \models T_{an}$. We write $F \subset_{an} K$ to indicate that F is an $\mathcal{L}_{an}$ substructure of K.

DEFINITION 5.3.1. *We say that $F \subset_{an} K$ is* ***log-closed*** *if for every $x \in F$, $\log(x) \in F$.*

DEFINITION 5.3.2. *If $L \models T_{an}(\exp)$, $F \subset_{an} K$, and F is log-closed, we say that $\sigma : F \to L$ is a* ***log-preserving embedding*** *if σ is an $\mathcal{L}_{an}$-embedding and $\log(\sigma(x)) = \sigma(\log(x))$ for all $x \in F$.*

The quantifier elimination result will be an easy consequence of the following theorem

THEOREM 5.3.3. *Suppose $K \models T_{an}(\exp)$, $F_0 \subset_{an} K$ is log-closed and $F_0 \models T_{an}$. If L is a $|K|^+$-saturated model of $T_{an}(\exp)$ and $\sigma_0 : F_0 \to L$ is a log-preserving $\mathcal{L}_{an}$-embedding, then σ_0 can be extended to a log-preserving $\mathcal{L}_{an}(\exp)$-embedding of K into L.*

COROLLARY 5.3.4. *$T_{an}(\exp)$ admits quantifier elimination in the language $\mathcal{L}_{an}(\exp, \log)$.*

Proof. We use 1.5.11 to prove that T_{an}(exp, log) has QE. Let $K, L \models T_{an}(\exp, \log)$ and suppose L is $|K|^+$-saturated. Let F be a substructure of K and let $\sigma_0 : F \to L$ be an embedding. It is sufficient to show that F is a model of T_{an} since 5.3.3 implies that σ_0 is extended to a log-preserving $\mathcal{L}_{an}(\exp)$-embedding $\sigma : K \to L$, which is an $\mathcal{L}_{an}$(exp, log)-embedding and so by 1.5.11 $T_{an}(\exp, \log)$ has quantifier elimination.

By 4.0.6 it is sufficient to show that F is closed under $^{-1}$ and n^{th}-root for all positive elements. For $x > 0$, $x^{-1} = \exp(-\log(x))$ and $\sqrt[n]{x} = \exp(\frac{\log x}{n})$. For $x < 0$, $x^{-1} = -\exp(-\log(-x))$. ☐

COROLLARY 5.3.5. *$T_{an}(\exp)$ is a complete axiomatization of $Th(\mathbb{R}_{an}(\exp))$ and admits a universal axiomatization in the language $\mathcal{L}_{an}(\exp, \log)$.*

Proof. Let $\mathcal{M} \models T_{an}(\exp)$. $\mathcal{M}$ contains an $\mathcal{L}_{an}$-substructure isomorphic to $\mathbb{R}$ so we consider without loss of generality $\mathbb{R}_{an}(\exp) \subseteq \mathcal{M}$. By quantifier elimination, $\mathbb{R}_{an}(\exp) \preceq \mathcal{M}$. This proves that $T_{an}(\exp)$ is complete.

Since T_{an} has a universal axiomatization replacing $E3)$ by the equivalent axiom

$$\forall x > 0(\exp(\log(x)) = x)$$

we see that $T_{an}(\exp, \log)$ admits a universal axiomatization. ☐

Theorem 5.3.3 will follow from three lemmas on extensions of embeddings.

For $F \subset_{an} K$ and $y \in K \setminus F$, we let $F\langle y\rangle$ denote the T_{an}-definable closure of $F \cup \{y\}$ in K.

Throughout the rest of this section let K, L, F_0 and σ_0 be as in 5.3.3. The first lemma says that σ_0 can be extended to $F_0\langle x\rangle$ for $x \in K \setminus F_0$ in the case that $v(F_0(x)^\times) = v(F_0^\times)$, moreover it is proved that $F_0\langle x\rangle$ is log-closed. We then iterate that process until we get a log-closed field $F \supset F_0$, a log-preserving $\mathcal{L}_{an}$-embedding $\sigma : F \to L$ extending σ_0 and for all $x \in K \setminus F$, $v(F(x)^\times) \neq v(F^\times) = v(F_0^\times)$. The second lemma extends σ_0 to a field F closed to log and exp. Finally the third lemma considers the case that F is closed to log and exp, and for all $x \in K \setminus F$, $v(F(x)^\times) \neq v(F^\times)$, extending σ_0 to a log-preserving $\mathcal{L}_{an}$-embedding $\sigma : F' \to L$, where $F' \supset F\langle x\rangle$ and F' is log-closed.

The following property of valuations will be useful:

PROPERTY 5.3.6. *Let F_1 and F_2 be ordered fields with $F_1 \subset F_2$ and $v(F_1) = v(F_2)$. Let $w \in F_2 \setminus F_1$. Then there is an infinitesimal $\epsilon \in F_2$ and $z \in F_1$ such that*

$$w = z(1 + \epsilon)$$

Proof. Let $z' \in F_1$ such that $v(z') = v(w)$. Then there are $r \in (F_2)_v$ and an infinitesimal $\epsilon' \in F_2$ such that $w = z'(r + \epsilon')$. Let $z = z'/r$ and $\epsilon = \epsilon'/r$. This gives $w = z(1 + \epsilon)$. $\square$

LEMMA 5.3.7. *Suppose $x \in K \setminus F_0$ and $v(F_0(x)^\times) = v(F_0^\times)$. Let $F = F_0\langle x\rangle$. Then F is log-closed and σ_0 can be extended to a log-preserving $\mathcal{L}_{an}$-embedding $\sigma : F \to L$.*

Proof. Since $F_0 \models T_{an}$, $v(F_0^\times)$ is divisible and so is $v(F_0(x)^\times)$. By 5.2.8 and the divisibility of $v(F_0(x)^\times)$ we have $v(F_0\langle x\rangle^\times) = \langle v(F_0(x)^\times)\rangle = v(F_0(x)^\times)$. Thus $v(F^\times) = v(F_0^\times)$.

We now prove that F is log-closed. Let $0 < w \in F$. Since $v(F^\times) = v(F_0^\times)$, by 5.3.7, there are $z \in F_0^\times$ and an infinitesimal $\epsilon \in F$ such that $w = z(1 + \epsilon)$. Then

$$\log(w) = \log(z) + \log(1 + \epsilon)$$

Since F_0 is log-closed, $\log(z) \in F_0$. Since log is analytic at 1, there is $l \in \mathbb{R}\{X\}$ such that for $v(\delta) > 0$, $\log(1 + \delta) = l(\delta)$. Thus $\log(1 + \epsilon) \in F$ and so $\log(w) \in F$. Hence F is log-closed.

Let $z \in L$ realize the type $\mathrm{tp}(y/M)$. Then we have an $\mathcal{L}_{an}$-isomorphism σ of $M\langle y\rangle$ onto $M\langle z\rangle$ fixing σ. Thus σ can be seen as an $\mathcal{L}_{an}$-embedding of $M\langle y\rangle$ onto L extending σ_0.

For $w \in F$ choose z and ϵ as above. Then $\sigma(w) = \sigma(z)\sigma(1 + \epsilon)$. Since σ_0 is log-preserving, $\sigma(\log(z)) = \sigma_0(\log(z) = \log(\sigma_0(z)) = \log(\sigma(z))$. Since σ is an $\mathcal{L}_{an}$-embedding, $\sigma(\log(1 + \epsilon)) = \sigma(l(\epsilon)) = l(\sigma(\epsilon)) = \log(1 + \sigma(\epsilon)) = \log(\sigma(1 + \epsilon))$. Thus

$$\begin{aligned}
\sigma(\log(w)) &= \sigma(\log(z)) + \sigma(l(\epsilon)) \\
&= \log(\sigma(z)) + l(\sigma(\epsilon)) \\
&= \log(\sigma(z(1 + \epsilon))) \\
&= \log(\sigma(w)).
\end{aligned}$$

$\square$

LEMMA 5.3.8. *Suppose that $v(F_0(x)^\times) \neq v(F_0^\times)$ for all $x \in K \setminus F_0$. Suppose x is an element of F_0 such that $\exp(x) \notin F_0$. Let $F = F_0\langle \exp(x)\rangle$. Then F is log-closed and there is an extension of σ_0 to a log-preserving $\mathcal{L}_{an}$-embedding $\sigma : F \to L$ with $\sigma(\exp(x)) = \exp(\sigma(x))$.*

Proof. First we show that $v(\exp(x)) \notin v(F_0^\times)$. Suppose not. There are $z \in F_0$ and an infinitesimal $\epsilon \in F$ such that $\exp(x) = z(1 + \epsilon)$. Recalling $\log(1 + \epsilon) = l(\epsilon)$, where $l \in \mathbb{R}\{X\}$, we have $x = \log(z)l(\epsilon) \in F_0$ which is absurd.

Now we show that F is log-closed. We can write $v(F^\times) = v(F_0^\times) \oplus \mathbb{Q}v(\exp(x))$. Let $w \in F$. There are $z' \in F_0$ and $q \in \mathbb{Q}$ such that $v(w) = v(z') + qv(\exp(x)) = v(z'\exp(qx))$. Thus there are $r \in \mathbb{R}$ and an infinitesimal $\epsilon' \in F$ such that $w = z'\exp(qx)(r + \epsilon')$. Putting $\epsilon = \epsilon'/r$ and $z = z'r$ we get

$$w = z(1 + \epsilon)\exp(qx).$$

Thus

$$\log(w) = \log(z) + qx + l(1 + \epsilon) \in F$$

Now we show an extension of σ_0 to a log-preserving $\mathcal{L}_{an}$-embedding commuting with exp. For this we show that $\exp(\sigma_0(x))$ realizes the image under σ_0 of the cut of $\exp(x)$ over F_0. Let $0 < z \in F_0$. Then

$$\begin{aligned} z < \exp(x) &\Leftrightarrow \log(z) < x \\ &\Leftrightarrow \sigma_0(\log(z)) < \sigma_0(x) \\ &\Leftrightarrow \log(\sigma_0(z)) < \sigma_0(x) \\ &\Leftrightarrow \sigma_0(z) < \exp(\sigma_0(x)) \end{aligned}$$

Thus σ_0 can be extended to an $\mathcal{L}_{an}$-embedding $\sigma : F \to L$ with $\sigma(\exp(x) = \exp(\sigma(x))$. The map σ is also log-preserving: let $w \in F$ and write as above $w = z\exp(xq)(1+\epsilon)$. Then

$$\begin{aligned} \sigma(\log(w)) &= \sigma(\log(z)) + \sigma(xq) + \sigma(l(\epsilon)) \\ &= \log(\sigma(z)) + \log(\exp(\sigma(xq))) + l(\sigma(\epsilon)) \\ &= \log(\sigma(z\exp(\sigma(xq))(1+\epsilon))) \\ &= \log(\sigma(w)). \end{aligned}$$

$\square$

LEMMA 5.3.9. *Suppose that F_0 is closed under exponentiation and $v(F_0(x)^\times) \neq v(F_0^\times)$ for all $x \in K \setminus F_0$. Let $x \in K \setminus F_0$. There is a log-closed $F \models T_{an}$ such that*

$$F_0(x) \subseteq F \subseteq_{an} K$$

and a log-preserving embedding $\sigma : F \to L$ extending σ_0.

Proof. We outline the proof

(i) We construct a sequence $(x_n)_{n\in\mathbb{N}} \subset K$ such that for all $n \in \mathbb{N}$, $v(x_n) < v(x_{n+1}) < 0$, $v(x_n) \notin v(F_0^\times)$ and $x_n > 0$.

(ii) Moreover, this sequence $(x_n)_{n\in\mathbb{N}}$ is $\mathbb{Q}$-linearly independent over $v(F_0^\times)$.

(iii) Defining $F_{n+1} = F_n\langle x_n\rangle$, $F = \bigcup F_n$ is log-closed.

(iv) We construct a sequence $(y_n)_{n\in\mathbb{N}} \subset L$ such that for each $i \in \mathbb{N}$, y_i realizes the image under σ_0 of the cut of x_i over F_0. For all $n \in \mathbb{N}$, $v(y_n) < v(y_{n+1}) < 0$, $v(y_n) \notin v(F_0^\times)$ and $y_n > 0$.

(v) We construct a sequence of $\mathcal{L}_{an}$-embeddings, $(\sigma_n : F_n \to L)_{n\in\mathbb{N}}$, each term extending the previous one, such that $\sigma_n(x_i) = y_i$ for each $n \in \mathbb{N}$ and each $i < n$. The $\mathcal{L}_{an}$-embedding $\sigma = \bigcup \sigma_n : F \to L$ is log-preserving.

Proof of (i): Let $x \in K \setminus F_0$. We can assume without loss of generality that $x > 0,\ v(x) < 0$ and by 5.2.5 we can also suppose that $v(x) \notin v(F_0^\times)$. Put $x_0 = x$. Suppose that x_n is defined and for all $k \leq n$, x_k is also defined. Note that, given x_k, $v(F_0(\log(x_k))^\times) \nsubseteq v(F_0^\times)$, since, otherwise, $\log(x_k) \in F_0$ and because F_0 is closed under exponentiation, $x_k \in F_0$, a contradiction.

We build an auxiliary sequence $(\beta_n)_{n\in\mathbb{N}} \subset F_0$. Given x_n, using 5.2.5, we define $\beta_n \in F_0$ such that $v(\log(x_n) - \beta_n) \notin v(F_0^\times)$. We define $x_{n+1} = |\log(x_n) - \beta_n|$, so $\log(x_n) = \beta_n + \epsilon_n x_{n+1}$, where $\epsilon_n \in \{-1, 1\}$.

Note that $v(x_n) < v(\log(x_n))$: Since $v(x_n) < 0$, we have

$$\begin{aligned} \forall m \in \mathbb{N}\ \ x_n > m^2 &\Rightarrow \forall m \in \mathbb{N}\ \ \exp(x_n) > x_n^m \\ &\Rightarrow \forall m \in \mathbb{N}\ \ x_n > m\log(x_n) \\ &\Rightarrow \forall m \in \mathbb{N}\ \ \frac{x_n}{\log(x_n)} > m \end{aligned}$$

where the first implication is due to axiom E4$_m$ for each $m \in \mathbb{N}$. This implies $v(\frac{x_n}{\log(x_n)}) < 0$, so $v(x_n) < v(\log(x_n))$.

Note that $v(\log(x_n)) \leq v(x_{n+1})$: If $v(\log(x_n)) \neq v(\beta_n)$, then $v(x_{n+1} = v(\log(x_n) - \beta_n) = \min\{v(\log(x_n)), v(\beta_n)\} = v(\log(x_n)$, where the last equality is justified by the contradiction that would rise from equality with $v(\beta_n)$. If $v(\log(x_n)) = v(\beta_n)$, then $\log(x_n) = \beta_n(1+\delta)$ for some δ such that $v(\delta) > 0$. This implies $v(\log(x_n) - \beta_n) = v(\beta_n) + v(\delta)$. Thus $v(\log(x_n)) \leq v(x_{n+1})$.

Note that $v(x_{n+1}) < 0$: otherwise, $v(\exp(x_{n+1})) = 0$ and

$$\begin{aligned} v(x_n) &= v(\exp(\log(x_n))) \\ &= v(\exp(\beta_n)\exp(\epsilon_n x_{n+1})) \\ &= v(\exp(\beta_n)) + v(\exp(x_{n+1})) \\ &= v(\exp(\beta_n)) \in v(F_0^\times), \text{ which is absurd.} \end{aligned}$$

Proof of (ii): Suppose not. Let $m, n \in \mathbb{N}$ such that

$$v(x_m) = \sum_{i=m+1}^{n} q_i x_i + v(w)$$

where $q_i \in \mathbb{Q}$ and $w \in F_0$. Let $c \in K$ such that $v(c) = 0$ and

$$x_m = cw \prod_{i=m+1}^{n} x_i^{q_i}.$$

Thus

$$\log(x_m) = \beta_m + \epsilon_m x_{m+1} = \log(c) + \log(w) + \sum_{i=m+1}^{n} q_i \log(x_i).$$

Rearranging, we get

$$\epsilon_m x_{m+1} = \log(c) + \log(w) - \beta_m + \sum_{i=m+1}^{n} q_i \log(x_i).$$

We have for all $m \in \mathbb{N}$, $v(x_{m+1}) < v(\log(x_{m+1}) \leq v(x_{m+2}) < v(\log_{m+2})$, so, for all $i \geq m+1$, $v(x_{m+1}) < v(\log(x_i))$. Also $v(\log(c)) = 0 > v(x_{m+1})$. Since

$$v(x_{m+1}) \geq \min\{v(\log(c)), v(\log(w) - \beta_m), v(\log(x_{m+1}), ..., v(\log(x_n))\},$$

we have $v(x_{m+1} = v(\log(w) - \beta_m) \in v(F_0^\times)$, a contradiction.

Proof of (iii): By (ii) we have

$$F_{n+1} = F_0 \oplus \mathbb{Q}v(x_0) \oplus ... \oplus \mathbb{Q}v(x_n)$$

Let $0 < w \in F_{n+1}$. By 5.3.7 there are $u \in F_0$, $q_0, ..., q_n \in \mathbb{Q}$ and an infinitesimal $\epsilon \in F_{n+1}$ such that $w = u(1+\epsilon)\prod_{i=0}^{n} x_i^{q_i}$. Then

$$\begin{aligned} \log(w) &= \log(u) + \log(1+\epsilon) + \sum_{i=0}^{n} q_i \log(x_i) \\ &= \log(u) + l(\epsilon) + \sum_{i=0}^{n} q_i(\epsilon_i x_{i+1} + \beta_i) \in F_{n+2}. \end{aligned}$$

where $l \in \mathbb{R}\{X\}$, such that for all $x \in [-1, 1]$, $l(x) = \log(1+x)$.

Proof of (iv): Let $y_0 \in L$ realize the image under σ_0 of the cut of x over F_0. Assuming y_n is defined and realizes $tp(x_n/F_0)$, put

$$\epsilon_n y_{n+1} = \log(y_n) - \sigma_0(\beta_n),$$

where ϵ_n is already defined in terms of x_n and β_n. We must prove that y_{n+1} realizes $tp(x_{n+1}/F_0)$. Without loss of generality we can assume $\epsilon_n = 1$. Let $w \in F_0$. Then

$$\begin{aligned} w < x_{n+1} &\Leftrightarrow w + \beta_n < x_{n+1} + \beta_n = \log(x_n) \\ &\Leftrightarrow \sigma_0(w) + \sigma_0(\beta_n) < \sigma_0(\log(x_n)) = \log(\sigma(x_n)) = \log(y_n) = y_{n+1} + \sigma_0(\beta_n) \\ &\Leftrightarrow \sigma_0(w) < y_{n+1}. \end{aligned}$$

The proof that For all $n \in \mathbb{N}$, $v(y_n) < v(y_{n+1}) < 0$, $v(y_n) \notin v(F_0^\times)$ and $y_n > 0$ is the same as in (i) for (x_n).

Proof of (v): Suppose $\sigma_n : F_n \to L$ is defined.

We prove that y_n realize the image under σ_0 of the cut of x_n over F_n.

Let $w \in F_n$. By (ii) $v(F_n^\times) = v(F_{n-1}^\times) \oplus \mathbb{Q}v(x_{n-1})$. Let $z \in F_{n-1}$, $\epsilon \in F_n$ with $v(\epsilon) > 0$ and $q \in \mathbb{Q}$ such that

$$w = z(1+\epsilon)x_{n-1}^q.$$

Then

$$\begin{aligned} x_n < w &\Leftrightarrow x_{n-1}^{-q} < z(1+\epsilon)x_n^{-1} \\ &\Leftrightarrow x_{n-1} < z^q(1+\epsilon)^q x_n^{q-1} \\ &\Leftrightarrow \log(x_{n-1}) - \beta_{n-1} < q\log(z) - \beta_{n-1} + q\log(1+\epsilon) + (q-1)\log(x_n) \\ &\Leftrightarrow \epsilon_{n-1}x_n < q\log(z) - \beta_{n-1} + q\log(1+\epsilon) + (q-1)\log(x_n). \end{aligned}$$

We have $v(x_n) > v(\log(x_n)) > v(\log(1+\epsilon))$ and similarly $v(y_n) > v(\log(y_n)) > v(\log(\sigma_n(1+\epsilon)))$. Thus

$$\begin{aligned} x_n < w &\Leftrightarrow \epsilon_{n-1}x_n < q\log(z) - \beta_{n-1} + q\log(1+\epsilon) + (q-1)\log(x_n) \\ &\Leftrightarrow \epsilon_{n-1}x_n < q\log(z) - \beta_{n-1} \\ &\Leftrightarrow \log(x_{n-1}) - \beta_{n-1} < q\log(z) - \beta_{n-1} \\ &\Leftrightarrow \log(y_{n-1}) - \sigma_0(\beta_{n-1}) < q\log(\sigma_n(z)) - \sigma_0(\beta_{n-1}) \\ &\Leftrightarrow \log(y_{n-1}) < q\log(\sigma_n(z)) + q\log(\sigma_n(1+\epsilon)) + (q-1)\log(y_n) \\ &\Leftrightarrow y_{n-1} < \sigma_n(z^q)\sigma_n(1+\epsilon^q)y_n^{q-1} \\ &\Leftrightarrow y_n < \sigma_n(w). \end{aligned}$$

We define $\sigma_{n+1} : F_{n+1} \to L$ as the unique $\mathcal{L}_{an}$-embedding up to isomorphism extending σ_n and $\sigma_{n+1}(x_n) = y_n$. Let $\sigma = \bigcup_{n=1}^\infty \sigma_n : F \to L$.

We prove that σ is log-preserving by induction: Assume that σ_n is log-preserving. Let $0 < w \in F_{n+1}$ and $z \in F_n$, $\epsilon \in F_{n+1}$ with $v(\epsilon) > 0$, $q \in \mathbb{Q}$ such that $w = z(1+\epsilon)x_n^q$. Then

$$\begin{aligned} \sigma(\log(w)) &= \sigma(\log(z) + \log(1+\epsilon) + q\log(x_n)) \\ &= \log(\sigma(z)) + \sigma(l(\epsilon)) + q\sigma(\epsilon_n x_{n+1} + \beta_n) \\ &= \log(\sigma(z)) + l(\sigma(\epsilon)) + q(\epsilon_n y_{n+1} + \sigma(\beta_n)) \\ &= \log(\sigma(z)) + \log(1+\sigma(\epsilon)) + q\log(y_n) \\ &= \log(\sigma(w)). \end{aligned}$$

□

5.4 *O*-minimality and Hardy fields

In this section we will show that $\mathbb{R}_{an}$(exp) is *o*-minimal.

Let $\mathcal{L} = (<, +, -, \cdot, 0, 1, ...)$ be an expansion of the languange of ordered rings with only function and constant symbols. $\mathcal{R} = (\mathbb{R}, <, +, -, 0, 1, ...)$ be an $\mathcal{L}$-structure expanding the ordered field of real numbers and let $T = Th(\mathcal{R})$.

We refer to $\mathcal{L}$-terms with parameters from $\mathbb{R}$ as $\mathbb{R}$-terms.

Now follows an equivalent characterization of o-minimality for T, whenever T has quantifier elimination.

LEMMA 5.4.1. *Suppose T has quantifier elimination. Then T is o-minimal if and only if for each $\mathbb{R}$-term $t(x)$ in one variable x, there is $m \in \mathbb{R}$ such that either $t(x) > 0$, $t(x) < 0$ or $t(x) = 0$ for all $x > m$.*

Proof. ($\Rightarrow$) This is clear by the Monotonicity Theorem 3.1.1.

($\Leftarrow$) Let S be a definable set. By quantifier elimination S is a boolean combination of sets of the form $\{x : t(x) = 0\}$, $\{x : t(x) > 0\}$ and $\{x : t(x) < 0\}$, where t is an $\mathbb{R}$-term in one variable. Thus, there is an $m \in \mathbb{R}$ such that either $(m, +\infty) \subseteq S$ or $(m, +\infty) \cap S = \emptyset$. Note that fractional linear transformations $x \mapsto \frac{ax+b}{cx+d}$ are definable as $\{(x, y) \in \mathbb{R}^2 : \exists z((cx + d)z = 1 \wedge y = (ax + d)z)\}$. Applying fractional linear transformations to S, we conclude that there is $m > 0$ such that

i) Either $(m, +\infty) \subseteq S$ or $(m, +\infty) \cap S = \emptyset$;

ii) Either $(-\infty, m) \subseteq S$ or $(-\infty, m) \cap S = \emptyset$;

and for each $r \in \mathbb{R}$, there is $\epsilon > 0$ such that

iii) Either $(r, r + \epsilon) \subseteq S$ or $(r, r + \epsilon) \cap S = \emptyset$;

iv) Either $(r - \epsilon, r) \subseteq S$ or $(r - \epsilon, r) \cap S = \emptyset$.

This implies that bd(S) is closed, bounded and contains only isolated points. Hence bd(S) is finite. Thus S is a finite union of points and intervals. $\square$

This lemma hints about the importance of the germs of functions at infinity. By o-minimality the germs of functions at infinity are actually C^∞ functions "at infinity" (consult 3.2, chapter 2 of [1]).

DEFINITION 5.4.2. *If $f, g : \mathbb{R} \to \mathbb{R}$, we say that f and g have the same **germ** at $+\infty$ if there is $m \in \mathbb{R}$ such that $f(x) = g(x)$ for all $x > m$.*

We denote by G the ring of germs at $+\infty$ of functions $f : \mathbb{R} \to \mathbb{R}$. We use the term "ultimately" whenever we want to say "for all sufficiently large real numbers".

DEFINITION 5.4.3. *A subring A of G is called a G-**domain** if for each $f \in A$ either ultimately $f(x) > 0$, ultimately $f(x) < 0$, or ultimately $f(x) = 0$.*

Note that if A is a G-domain, then A is an integral domain. We will consider the following ordering for a G-domain A: $f > 0$ if and only if ultimately $f(x) > 0$.

DEFINITION 5.4.4. *If a G-domain is also a field, then it is called a G-**field**.*

Note that if A is a G-domain then it has a unique fraction field in G. We identify $\mathbb{R}$ with the G-field of germs of constant functions. We consider the ring of polynomials $\mathbb{R}[x]$ as G-domain in the obvious way and its fraction field $R(x)$ as a G-field.

If f is an n-ary function symbol of $\mathcal{L}$ we define $f_G : G^n \to G$ by $f_G(f_1, ..., f_n)$ as the germ at $+\infty$ of the function $x \mapsto f(f_1(x), ..., f_n(x))$. For each term $t(x_1, ..., x_n)$ we define $t_G : G^n \to G$ by letting $t_G(f_1, ..., f_n)$ be the germ of the function $x \mapsto t(f_1(x), ..., f_n(x))$.

DEFINITION 5.4.5. *A G-field closed under f_G for every function symbol f in $\mathcal{L}$ is called an $\mathcal{R}$-**field**.*

Now we can state an easy consequence that links the abstract view of the $\mathcal{L}$-structure $\mathcal{R}$ as a G-field and its possible o-minimality.

LEMMA 5.4.6. *If T has quantifier elimination and there is an $\mathcal{R}$-field containing the identity function $x \mapsto x$, then $\mathcal{R}$ is o-minimal.*

Proof. We have that for every $\mathbb{R}$-term $t(x)$ either ultimately $t(x) > 0$, or ultimately $t(x) < 0$, or ultimately $t(x) = 0$. Since T has quantifier elimination, by Lemma 5.4.1 $\mathcal{R}$ is o-minimal. $\square$

From now on we make two assumptions on T.

i) T has quantifier elimination.

ii) T has a universal axiomatization.

Note that if $\mathcal{N} \models T$ and $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} \preceq \mathcal{N}$ (1.3.8 and 1.4.8).

Note also that these two assumptions on T hold in $T_{an}({}^{-1}, (\sqrt[n]{\ })_{n=2,3,\ldots})$ and $T_{an}(\exp, \log)$.

LEMMA 5.4.7. *IF K is an $\mathcal{R}$-field then, viewed as an $\mathcal{L}$-structure, $K \models T$.*

Proof. Consult Lemma 5.8 of [2]. □

DEFINITION 5.4.8. *If K is an $\mathcal{R}$-field and $g \in G$, we say that g is **comparable** to K if for each $f \in K$ either ultimately $g(x) < f(x)$, or ultimately $g(x) > f(x)$, ultimately $g(x) = f(x)$.*

LEMMA 5.4.9. *Suppose T is o-minimal. Let K be an $\mathcal{R}$-field. If $g \in G$ is comparable to K then*

$$K\langle g\rangle := \{t_G(f_1, ..., f_n, g) : t(x_1, ..., x_{n+1}) \textit{ is a term and } f_1, ..., f_n \in K\}$$

is the smallest $\mathcal{R}$-field containing $K \cup \{g\}$.

Proof. Consult Lemma 5.9 of [2]. □

Now we turn to Hardy fields.

DEFINITION 5.4.10. *We say that an element $g \in G$ is a C^1**-germ** if the function $g : \mathbb{R} \to \mathbb{R}$ is ultimately C^1.*

DEFINITION 5.4.11. *For a C^1-germ $g \in G$, we define its **derivative** g' as the derivative of the C^1-function $g : (m, +\infty) \to \mathbb{R}$ for some $m > 0$.*

DEFINITION 5.4.12. *A **Hardy field** is a G-field K such that every $f \in K$ is a C^1-germ and $f' \in K$. We say that K is a $\mathcal{R}$-**Hardy field** if it is an $\mathcal{R}$-field which is also a Hardy field.*

Note that, if $\mathcal{R}$ is o-minimal then the ring $H(\mathcal{R})$ of $\mathbb{R}$-definable functions $f : \mathbb{R} \to \mathbb{R}$ is an $\mathcal{R}$-Hardy field. We state, without proof, two facts about Hardy fields.

LEMMA 5.4.13. *Let K be a Hardy field and $f \in K$. Then*

i) $e^f \in G$ is comparable to K.

ii) If $f > 0$, then $\log(f)$ is comparable to K.

Proof. Consult Lemma 5.1.2 of [2]. □

The next lemma asserts that every $\mathcal{R}$-Hardy field can be extended to an $\mathcal{R}$-Hardy field that is closed under exponentiation and under taking logarithms of positive elements.

LEMMA 5.4.14. *Suppose T is o-minimal. Let K be an $\mathcal{R}$-Hardy field and $f \in K$. Then $K\langle e^f\rangle$ is an $\mathcal{R}$-Hardy field, and if $f > 0$, then $K\langle\log(f)\rangle$ is an $\mathcal{R}$-Hardy field.*

Proof. Consult Lemma 5.1.3 of [2]. □

THEOREM 5.4.15. *$(\mathbb{R}_{an}, \exp)$ is o-minimal.*

Proof. Let $\mathcal{R} = (\mathbb{R}_{an}, {}^{-1}, (\sqrt[n]{\ })_{n=2,3,\ldots})$. The structure $\mathcal{R}$ is o-minimal and its theory has quantifier elimination and an universal axiomatization. Let $H(\mathcal{R})$ be the Hardy field of definable functions. By 5.4.14 we can extend $H(\mathcal{R})$ to an $\mathcal{R}$-field $\widetilde{H(\mathcal{R})}$ that is closed under exponentiation and under taking logarithms of positive elements. Thus $\widetilde{H(\mathcal{R})}$ is an $(\mathcal{R}, \exp, \log)$-Hardy field containing the identity function id: $\mathbb{R} \to \mathbb{R},\ x \mapsto x$. Recall that the theory of $(\mathcal{R}, \exp, \log)$ admits quantifier elimination. Thus $(\mathcal{R}, \exp, \log)$ is o-minimal by 5.4.6, and in particular $(\mathbb{R}_{an}, \exp)$ is o-minimal. □

Bibliography

[1] L. van den Dries. *Tame Topology and O-minimal Structures*. Cambridge University Press, 1998

[2] L. van den Dries, A. Macintyre and D. Marker. *p-adic and real subanalytic sets*. Ann. of Math. **140**(1994), 183-205

[3] D. Marker. *Model Theory: An Introduction*. Cambridge University Press, 1993

[4] W. Hodges. *Model Theory*. Springer-Verlag, 2002

[5] P. Ribenboim. *The Theory of Classical Valuations*. Springer-Verlag, 1999

[6] S. Lang. *Algebra*. Springer-Verlag, 2002

[7] O. Endler. *Valuation Theory*. Springer-Verlag, 1972

[8] A. Prestel. *Lectures on Formally Real Fields*. Springer-Verlag, 1984

[9] *https://encyclopediaofmath.org/wiki/Real_analytic_function*. Acessed 01/04/2021

[10] J. Denef and L. van den Dries, *p-adic and real subanalytic sets*. Ann. of Math. **128**(1988), 79-138

[11] *https://www.planetmath.org/henselianfield*. Accessed 15/04/2021

[12] S. Krantz and H. Parks, *A Primer of Real Analytic Functions*. Birkhäuser, 2002

[13] B.H. Neumann, *On ordered division rings*. Trans. Amer. Math. Soc. **66**(1949), 202-252

[14] I. Kaplansky, *maximal fields with valuations*. Duke Math. J. **9**(1942), 303-321