



**HAL**  
open science

# Geometric theories for real number algebra without sign test or dependent choice axiom

Henri Lombardi, Assia Mahboubi

► **To cite this version:**

Henri Lombardi, Assia Mahboubi. Geometric theories for real number algebra without sign test or dependent choice axiom. CCC 2024 - Continuity, Computability, Constructivity From Logic to Algorithms, Sep 2024, Nice, France. pp.1-152. hal-04709177

**HAL Id: hal-04709177**

**<https://inria.hal.science/hal-04709177v1>**

Submitted on 25 Sep 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# Geometric theories for real number algebra without sign test or dependent choice axiom

Henri Lombardi and Assia Mahboubi

last version is available in

<http://hlombardi.free.fr/Real-Geom.pdf>

First proposal, 27th August 2024

## Abstract

In this memoir, we seek to construct a dynamical theory that is as complete as possible to describe the algebraic properties of the real number field in constructive mathematics without a dependent choice axiom.

In the first part, we give a few general points about geometric theories and their dynamical version, dynamical theories.

The second part is devoted to the study of a finitary geometric theory whose ambition is to describe exhaustively the algebraic properties of the real number field, and more generally of a *non* discrete real closed field, at least those that can be expressed in a restricted language close to the language of ordered rings. The result is a theory which, in classical mathematics, turns out to be the theory of local real closed rings. The theory of real closed rings is presented here in a constructive form as a purely natural equational theory, based on the virtual root maps introduced in earlier work. All this constitutes a development, with some minor terminological modifications, of the ideas given in the article [40]. Finally, we ask whether an infinitary axiom of archimedeanity would provide a better understanding of the proposed finitary theory.

In the third part, we introduce a more ambitious theory in which continuous semialgebraic maps are given their own place: new sorts are created for them. This makes it possible to talk inside the theory about the uniform continuity modulus of a continuous semialgebraic map on a bounded closed subset of  $\mathbb{R}^n$ . This new theory is resolutely infinitary. We then obtain a better description of the algebraic properties of  $\mathbb{R}$ , but also a first outline for a constructive theory of certain o-minimal structures.



# Contents

<b>Foreword</b>	<b>3</b>
<b>I Geometric theories</b>	<b>5</b>
<b>Introduction</b>	<b>7</b>
<b>A Finitary geometric theories</b>	<b>11</b>
A.1 Coherent and finitary dynamical theories . . . . .	12
A.2 Dynamic algebraic structures . . . . .	18
A.3 Conservative extensions of a dynamical theory . . . . .	27
A.4 Distributive lattices associated with a dynamic algebraic structure . . . . .	30
A.5 Model theory . . . . .	33
<b>B Infinitary geometric theories</b>	<b>35</b>
B.1 General . . . . .	35
B.2 Barr's Theorem . . . . .	37
<b>II Finitary geometric theories for real algebra</b>	<b>39</b>
<b>Introduction</b>	<b>41</b>
<b>C Ordered fields</b>	<b>43</b>
Introduction . . . . .	43
C.1 About discrete ordered fields . . . . .	44
C.2 Formal Positivstellensätze . . . . .	48
C.3 <i>Non</i> discrete ordered fields . . . . .	51
C.4 A non-archimedean <i>non</i> discrete ordered field . . . . .	54
C.5 <i>Non</i> discrete real closed fields: position of the problem . . . . .	57
C.6 General properties of continuous semialgebraic maps . . . . .	61
C.7 Some questions . . . . .	62
<b>D <math>f</math>-rings</b>	<b>65</b>
Introduction . . . . .	66
D.1 Distributive lattices . . . . .	66
D.2 $\ell$ -groups . . . . .	68
D.3 $f$ -rings . . . . .	72
D.4 Beyond purely equational theories . . . . .	77
D.5 Back to ordered fields . . . . .	80
D.6 The real lattice and spectrum of a commutative ring . . . . .	83

<b>E</b>	<b>Non discrete real closed fields</b>	<b>85</b>
	Introduction . . . . .	86
	E.1 2-closed ordered field (or euclidean field) . . . . .	86
	E.2 Virtual roots . . . . .	87
	E.3 Real closed rings . . . . .	93
	E.4 Non discrete real closed fields . . . . .	99
	E.5 A non-archimedean <i>non</i> discrete real closed field . . . . .	100
	E.6 Use of virtual roots in constructive real algebra . . . . .	104
	E.7 Some questions . . . . .	107
<b>F</b>	<b>The axiom of archimedeanity</b>	<b>111</b>
	F.1 Archimedean <i>non</i> discrete real closed fields . . . . .	111
	F.2 Some questions . . . . .	111
	<b>Conclusion</b>	<b>113</b>
<b>III</b>	<b>Improved version of the theory of <i>non</i> discrete real closed fields</b>	<b>115</b>
	<b>Introduction</b>	<b>117</b>
<b>G</b>	<b>O-minimal structures</b>	<b>119</b>
<b>H</b>	<b>Rings of bounded real maps</b>	<b>121</b>
	H.1 Some reminders of the second part . . . . .	121
	H.2 Dynamical theory of rings of bounded real maps . . . . .	121
	H.3 Dynamical theory of compact real intervals . . . . .	122
<b>J</b>	<b>A reinforced language and the first corresponding axioms</b>	<b>123</b>
	Introduction . . . . .	123
	J.1 The sorts of reinforced language . . . . .	123
	J.2 An abstraction principle . . . . .	124
	J.3 First structures on sorts $Df_{m,n}$ . . . . .	124
<b>K</b>	<b>Decisive axioms</b>	<b>127</b>
	K.1 Upper bound axioms . . . . .	127
	K.2 Axioms for smooth maps . . . . .	129
	K.3 Axioms of real closure or o-minimal closure . . . . .	130
	K.4 O-minimal structures . . . . .	132
	K.5 Some questions . . . . .	133
	<b>General conclusion</b>	<b>135</b>
	<b>References and index</b>	<b>139</b>
	References. Books . . . . .	139
	References. Articles . . . . .	140
	Notations index . . . . .	147
	Terms index . . . . .	150

# Foreword

The memoir we present here is an unfinished development of the article [40]. Compared to that paper, however, we have modified the definition of continuous semialgebraic maps (Definition C.5.5), in the same spirit in which Bishop defines a continuous real map as a uniformly continuous map on any bounded interval.

Despite its unfinished nature and the many questions that we do not currently know how to answer, we hope that this paper will arouse interest for its original approach to the subject.

The paper is written in the style of constructive mathematics à la Bishop, i.e. mathematics with intuitionistic logic (see [Bishop, Bishop & Bridges, Bridges & Richman, CACM, MRR, CCAPM]).

Let us define *real algebra* as the study of the algebraic properties of real numbers, i.e., the properties of  $\mathbb{R}$  formulable in a first-order formal theory on the language of strictly ordered rings defined by the signature

$$\mathbf{Signature:} \quad \boxed{\Sigma_{Aso} = (\cdot = 0, \cdot > 0, \cdot \geq 0 ; \cdot + \cdot, \cdot \times \cdot, - \cdot, 0, 1)}$$

with possibly all or some of the constructive reals as constants. We can also envisage introducing new function symbols for well-defined (from a constructive point of view) maps  $\mathbb{R}^n \rightarrow \mathbb{R}$  whose description is purely algebraic, such as the sup, inf maps and many continuous semialgebraic maps defined on  $\mathbb{Q}$ .

*Real constructive algebra* is not well understood! *Constructive analysis* ( $\simeq$  certified methods in numerical analysis) is much better studied.

From a constructive point of view, real algebra is far removed from the usual classical theory of real closed fields à la Artin-Schreyer-Tarski, in which we assume that we have a sign test for the reals.

Most algorithms in classical real algebra fail with real numbers, because they require a *sign test*.

Even in constructive analysis, there could be interesting spin-offs from further study of real algebra. For example, it would help us to understand how to avoid using the axiom of dependent choice (which is common in Bishop's work).

The understanding of constructive real algebra can also be a first step towards a constructive (and therefore algorithmic) theory of o-minimal structures (cf. [Coste], [van den Dries]). The real line and the  $\mathbb{R}^n$  spaces studied from a purely algebraic point of view can be seen as constituting the simplest of o-minimal structures. The classical (non-algorithmic) theory of o-minimal structures yields pseudo-algorithms which, in order to work correctly, require at least one sign test on the reals (sorts must also be introduced for the definable parts of  $\mathbb{R}^n$ ). And the theory of o-minimal structures has, a priori, a very important area of applications in analysis.

Thus we are looking for as complete a dynamical theory as possible to describe the algebraic properties of the real number field in constructive mathematics without an axiom of dependent choice.

In the study we present here, we also avoid the use of negation. Fred Richman [59] shows that constructive mathematics is more elegant when the axiom of dependent choice is dispensed with. We believe that they are also more elegant if negation is dispensed with.

In the first part, consisting of Chapters [A](#) and [B](#) we give some general information on geometric theories and their dynamical version, dynamical theories. For the most part, we refer to sections 1 to 3 of the article [\[41\]](#).

The second part is devoted to the study of a geometric theory whose ambition is to describe exhaustively the algebraic properties of the real number field, and more generally of a *non* discrete real closed field, at least those expressible in a restricted language, close to the language of ordered rings. This constitutes a development, with some minor terminological modifications, of the ideas given in the article [\[40\]](#).

Chapter [C](#) proposes a definition of the ordered field structure in the absence of a sign test.

Chapter [D](#) deals with  $f$ -rings and some derived structures.

Chapter [E](#) tries to define the structure of a real closed ordered field in the absence of a sign test.

Chapter [F](#) discusses an infinitary geometric theory when we add the axiom that the real number field is *archimedean*.

So, at the end of this second part, we propose for the coveted dynamical theory that of the archimedean local real closed ring structure. The theory of real closed rings is presented here in an elementary, purely equational form, in the style of [\[69\]](#).

In the third part, we add the sorts corresponding to continuous semialgebraic maps on bounded closed semialgebraic subsets. In this way, we hope to obtain a more precise description of real algebra and to be able to sketch a first constructively satisfactory theory for o-minimal structures.

Throughout the text, theorems or lemmas in classical mathematics that have no known constructive proof, and often cannot have one, are indicated with a star.

Finally, the article [\[38\]](#) contains reflections, in a more philosophical framework, similar to those proposed here.

**Acknowledgements** We would like to thank Michel Coste and Marcus Tressl for their patient answers to our many questions.

Henri Lombardi, Assia Mahboubbi, 27th August 2024

**Part I**

**Geometric theories**





# Introduction

This first part is the subject of a more detailed memoir in preparation [39], which can be found at: <http://hlombardi.free.fr/Theories-geometriques.pdf>

We give the main definitions and refer for the main part to sections 1 to 3 of the article [41]

A dynamical theory can be understood as a formalisation of a well-defined piece of intuitive mathematics. This intuitive mathematics, practised by the mathematical community, is studied in a completely computational form independent of any philosophical point of view. But where the classical point of view makes free use of **LEM**<sup>1</sup> and the axiom of choice, dynamical theories replace these non-computational tools with the dynamical point of view of incompletely specified structures, which is the point of view of lazy evaluation in Computer Algebra.

Chapter A deals with finitary dynamical theories.

A finitary geometric theory corresponds to what is known in classical mathematics as a coherent formal theory. But the geometric theory we are considering is governed by intuitionistic logic, whereas the coherent theory is generally governed by classical logic.

What's more, the corresponding dynamical theory is a minimalist version of the geometric theory: it's pure computational machinery without logic, rather similar to Goodstein's recursive arithmetic.

A dynamical theory can also be seen as a partial version of natural deduction, in which the formulas examined are all of a very simple type, without the implication connector (hence without negation) and with very limited use of quantifiers.

The surprise is that dynamical theories are nevertheless very expressive (in classical mathematics any first-order formal theory can be seen as a coherent theory) and that they erase the distinction between classical logic and intuitionistic logic.

In the frequent case where the signature is a countable set and the axioms form a decidable part of the language, the mathematical world outside the theory, which is where we situate ourselves in order to study a given structure, see how the formal system that describes it works, and establish theorems about it, has no interference with the dynamical theory itself. This is confirmed in a general way by the fundamental theorem A.3.6: if we force a finitary geometric theory to behave in a classical way, the dynamical rules written in the initial language that are valid afterwards were already valid before.

This corresponds to the fact that Grothendieck's coherent topos, which are another form of coherent theories, have an intuitionistic internal logic, but that they can nevertheless be understood in different ways depending on whether or not we are in a constructive external mathematical world.<sup>2</sup>

In constructive mathematics, only certain structures come under finite dynamical theories. For example, the discrete field structure, but not the Heyting field structure.<sup>3</sup> In this respect, the restricted viewpoint of dynamical theories opens the way to a relevant classification, invisible in classical mathematics, concerning the degrees of complexity of mathematical beings invented by humans.

---

<sup>1</sup>Law of Excluded Middle.

<sup>2</sup>That is, essentially, whether or not we accept **LEM** in this external world.

<sup>3</sup>A discrete field is a non-trivial ring in which every element is zero or invertible, and a Heyting field is a local ring in which every non-invertible element is zero. Classical mathematics does not know the relevant distinction between the notion of a discrete field and that of a Heyting field.

Chapter B deals with infinitary dynamical theories, in which infinite disjunctions are allowed in the conclusion of a dynamical rule.

An essential restriction must be noted: the free variables present in such a disjunction must be specified in advance and in finite number.

Intuitively, such rules are used in the proof system of dynamical theories by “opening the branches of computation corresponding to the infinite disjunction”. What does this mean precisely? It means that a conclusion will be declared valid if it is valid in each of the branches.

These theories are more expressive than finitary theories and make it possible to axiomatise a very large number of common mathematical structures.

Unlike finitary dynamical theories, the external mathematical world inevitably intervenes to certify the validity of a dynamical rule.

Let’s take a simple example and show what happens if the axioms contain an infinitary rule of the following type

$$\vdash_{x_1, \dots, x_k} \text{OP}_{i \in I} \Gamma_i$$

with an infinite set  $I$  and the  $\Gamma_i$  are lists of atomic formulas with no free variables other than those mentioned (i.e.  $x_1, \dots, x_k$ ). If for each  $i \in I$  we have a valid rule  $\Gamma_i \vdash B(\underline{x})$ , then we declare the rule  $\vdash_{x_1, \dots, x_k} B(\underline{x})$  to be valid.

There is therefore necessarily an intuitive proof external to the dynamical theory to certify that the desired conclusion is valid in each of the branches. In fact, the computation system at work in the dynamical theory cannot handle such an infinite number of proofs. A purely mechanical computation cannot open up an infinite number of branches! For example, with  $I = \mathbb{N}$  the external intuitive proof could be a proof by induction.

Note, on the other hand, that the internal proof must show the validity of the desired conclusion according to the rules of proof “without logic” of the dynamical theory.

**Terminology.** Since we are dealing with constructive mathematics, terminological problems inevitably arise, simply because, for example, the same classical concept generally gives rise to several interesting constructive concepts which are not equivalent, but which are equivalent in classical mathematics.

Below are small tables comparing our terminology (in constructive mathematics) and the most common English terminology (in classical mathematics) for geometric theories. The one found in [Johnstone, Sketches 2, Chapter D1], [Caramello] and in [4].

The comparison is somewhat biased by the fact that dynamical theories do not use logic as such. They are pure computational machines. Thus, although a finitary dynamical theory “generate” a (first-order formal ) consistent theory and although every consistent theory admits a version “finitary dynamical theory”, they are not the same formal objects. Witness the fact that a coherent theory does not work in the same way with classical logic and with intuitionistic logic, whereas a dynamical theory is insensitive to this distinction because, structurally, dynamic proofs are always constructive.

Finitary geometric theories	
Our terminology	Elephant
geometric theory	geometric theory
dynamical theory	
purely equational	algebraic
direct	
Horn	Horn
disjunctive	
propositional	propositional
existential, or regular	regular
existentially rigid	
existential existentially rigid, or cartesian	cartesian
rigid	disjunctive, [29]
finitary dynamical	
intuitionist coherent	
classical coherent	coherent

General (infinitary) geometric theories	
Theory	Theory
dynamical	
geometric	geometric intuitionist
geometric classical	geometric

Dynamical theories	Geometric theories
identical (same signature)	equivalent
essentially identical (same sorts)	
classically essentially identical (same sorts)	definitionally equivalent
essentially equivalent	
classically essentially equivalent?	Morita equivalent



# A. Finitary geometric theories

## Sommaire

---

<b>A.1 Coherent and finitary dynamical theories</b>	<b>12</b>
Coherent theories	12
Finitary dynamical theories	12
Logic replaced by computation	13
Equality predicate	14
Simple extension of a dynamical theory	14
Structural rules	14
Collapsus	16
Classification of dynamical theories	17
Horn theories	17
Disjunctive theories	17
Existential theories	17
Existentially rigid, cartesian theories	17
Rigid theories	17
Propositional theories	17
<b>A.2 Dynamic algebraic structures</b>	<b>18</b>
Definitions, examples	18
Positive diagram of an algebraic structure	21
Constructive versus classical models	21
Morphisms between dynamic algebraic structures of the same type	21
Examples	22
Primitive recursive arithmetic	23
Goodtein's formal system	23
A finitary geometric theory for primitive recursive arithmetic	24
<b>A.3 Conservative extensions of a dynamical theory</b>	<b>27</b>
Essentially equivalent extensions	27
Comparison with intuitionistic logic	28
Fundamental theorem of dynamical theories	28
Skolemisation	29
<b>A.4 Distributive lattices associated with a dynamic algebraic structure</b>	<b>30</b>
Distributive lattices and entailment relations	30
The spectrum of a distributive lattice	30
Stone's antiequivalence	31
The Zariski lattice and spectrum of a commutative ring	31
Other examples	32
First example.	32
More generally	33
Case of an extension $\mathcal{T}_1$ which reflects valid disjunctive rules.	33

Zariski lattices, however, give a lesser image . . . . .	33
<b>A.5 Model theory</b> . . . . .	<b>33</b>
Completeness theorem, simultaneous collapse . . . . .	33
Representation theorem, theories proving the same Horn rules . . . . .	34

---

## A.1. Coherent and finitary dynamical theories

### Coherent theories

A *coherent theory*  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$  is a first-order formal theory based on the language  $\mathcal{L}$  in which the axioms (the elements of  $\mathcal{A}$ ) are all “geometric”, i.e. of the following form:

$$\forall \underline{x} (C \implies \exists \underline{y}^1 D_1 \vee \dots \vee \exists \underline{y}^m D_m) \tag{A.1}$$

where  $C$  and the  $D_j$  are *conjunctions of atomic formulas* of the language  $\mathcal{L}$  of the formal theory, the  $\underline{y}^j$  are lists of variables, and  $\underline{x}$  is the list of other occurring variables (these lists may be empty). The variables in  $C$  are only in the  $\underline{x}$  list. The variables in  $D_j$  are only in the disjoint lists  $\underline{x}$  and  $\underline{y}^j$ . An empty disjunction in the second member can be replaced by the symbol  $\perp$  representing **False**.

We also say *finite geometric theory* instead of coherent theory when we use intuitionist logic.

In the remainder of Chapter A, we almost always omit the qualifier “finitary” before “geometric theory” or “dynamical theory”

### Finitary dynamical theories

Main reference [17]. This article introduces the notions of “dynamical theory” and “dynamical proof”. See also: the article [6, Bezem & Coquand, 2005] which describes a number of advantages provided by this approach, and the precursor articles [55, Prawitz 1971, sections 1.5 and 4.2], [53, Matijasevič 1975] and [33, Lifschitz, 1980].

If  $\mathcal{T}$  is a (finitary) geometric theory, the corresponding (*finitary*) *dynamical theory* differs from it only by an extremely limited use of proof methods:

- Firstly, no formulas other than atomic formulas are ever used: no new predicates using logical connectors or quantifiers are ever introduced. Only lists of atomic formulas from the  $\mathcal{L}$  language are manipulated.
- Secondly, and in accordance with the previous point, axioms are not seen as true formulas, but as *deduction rules*: an axiom such as (A.1) is used as a rule (A.2)

$$\Gamma \vdash \text{Introduce } \underline{y}^1 \text{ such that } \Delta_1 \text{ op } \dots \text{ op Introduce } \underline{y}^m \text{ such that } \Delta_m \tag{A.2}$$

Here the conjunctions of atomic formulas  $C, D_1, \dots, D_m$  of (A.1) have been replaced by the corresponding lists  $\Gamma, \Delta_1, \dots, \Delta_m$ .

- Thirdly, we only prove *dynamical rules*, i.e. theorems which are in the form of the deduction rules above..
- Fourth, the only way to prove a dynamical rule is by a tree computation “without logic”. At the root of the tree are all the hypotheses of the theorem we want to prove. The tree develops by applying the axioms according to pure algebraic computation machinery in the structure. See Examples A.1.1. The precise formal definitions are given in [17], we extend them to the case where there are several types of objects as in the theory of modules on a commutative ring with objects of type “elements of the ring” and objects of type “elements of the module”.

When we apply an axiom such as (A.2), we substitute arbitrary terms  $(t_i)$  from the language for the free variables  $(x_i)$  present in the rule. If the hypotheses, rewritten with these terms, are already proven, then branches of computation are opened in each of which fresh variables corresponding to the dummy variables  $\underline{y}^k$  are introduced (their names may have to be changed to avoid conflict with the free variables present in the  $t_i$  terms) and each conclusion  $B_k$  is valid in its branch.<sup>1</sup>

The very elementary examples A.1.1 show how to validate a dynamic rule in a given dynamical theory. We develop a computation tree using the axioms of the dynamical theory as indicated above and we have won when, at each leaf of the tree, the conclusion is validated.

**Examples A.1.1.** The dynamical theory  $\mathcal{C}d$  of discrete bodies is based on the language of commutative rings and its axioms are those of non-trivial commutative rings (theory  $\mathcal{A}c$  in the example A.2.1) and the dynamic rule for discrete fields:

**CD**  $\vdash x = 0$  **op** **Introduce**  $y$  **such that**  $xy = 1$

1) To demonstrate the dynamic rule

**ASDZ**  $xy = 0 \vdash x = 0$  **op**  $y = 0$

we open two branches in accordance with the axiom **CD**. In the first we have  $x = 0$  and the conclusion is proved. In the second, we introduce a “parameter” (a fresh variable)  $z$  with the relation  $xz = 1$ . The axioms of commutative rings can then be used to prove the equalities  $y = 1 \text{ times } y = (xz)y = (xy)z = 0 \text{ times } z = 0$ . The conclusion is therefore validated for each of the two leaves of the tree.

2) Then, for example, we deduce from the previous dynamic rule the rule

**Anz**  $z^2 = 0 \vdash z = 0$

because this time both leaves of the tree have the same conclusion  $z = 0$ .

3) The theory  $\mathcal{A}l$  of local rings is based on the language of commutative rings and its axioms are those of commutative rings (theory  $\mathcal{A}c0$  in Example A.2.1) and the dynamic rule for local rings

**AL**  $(x + y)z = 1 \vdash$  **Introduce**  $u$  **such that**  $xu = 1$  **op** **Introduce**  $u$  **such that**  $yu = 1$

To prove that a discrete field satisfies the rule **AL**, we open two branches in accordance with the axiom **CD**. In the first, we have  $x = 0$  and the conclusion is proved because  $(x + y)z = 1$  gives  $yz = 1$ . In the second we introduce a “parameter” (a fresh variable)  $v$  with the relation  $xv = 1$ . The conclusion in the rule **AL** is therefore proven at both leaves of the calculation tree. ■

Note also that the validity of the following rule, which could be called “Concrete existence implies formal existence”, is purely tautological.

Let us consider a list  $\Gamma(\underline{x}, \underline{y})$  of atomic formulas in a dynamical theory  $\mathcal{T}$ . Let us denote  $\Gamma(\underline{x}, \underline{t})$  the list of these formulas in which we have substituted for each variable  $y_j$  a term  $t_j$  constructed on the  $x_i$  and on the constants of the theory. Then the following existential rule is valid.

$$\Gamma(\underline{x}, \underline{t}) \vdash \exists y_1, \dots, y_m \Gamma(\underline{x}, \underline{y}).$$

#### • Logic replaced by computation

In practice, proving a dynamical rule within the framework of a dynamical theory always follows an intuitive natural reasoning, and this gymnastics can be seen as a simplified version of Gentzen’s natural deduction. The symbol **op** should be understood as an abbreviation for “open (branches in the calculation)”.

The symbols **op** and **Introduce · such that** have been preferred to  $\mathbf{v}$  and  $\exists$ , to make it clear that their use in deduction rules is not the use of new formulas constructed from atomic formulas.

<sup>1</sup> $B_k$  is the list  $\Delta_k$  in which the  $x_i$  variables have been replaced by the  $t_i$  terms.



The symbol  $\vdash$  has been preferred to  $\vdash$  to avoid confusion with the symbol used for entailment relations in distributional lattices. Note also that it does not have the same interpretation as the analogous symbol used in Gentzen-style sequence calculations.

Thus the language of a dynamical theory contains no logical symbols (connectors or quantifiers) that can be used to construct complicated formulas from atomic formulas. The “logic” is replaced by the symbols  $\vdash$ , **op** and **Introduce · such that** and by the separator “, ”, but these symbols are used to describe a machinery of arborescent calculations and not to form formulas. The non-logical part of a dynamical theory consists of symbols for variables, and the *signature*, which contains symbols for sorts, predicates and functions.

In the following, we replace “**Introduce · such that** ...” with the less cumbersome “ $\exists$  · ...”, which is closer to and yet different from the traditional “ $\exists$  · ...”.

### • Equality predicate

In a dynamical theory each sort must be provided with an equality predicate  $\cdot = \cdot$  and we give the axioms which authorise the substitution of a term  $t$  by a term  $t'$  when  $\vdash t = t'$  is valid in the theory<sup>2</sup> in any occurrence of an atomic formula present in a valid dynamical rule.

We could just as well not give any axioms relating to this substitution and consider that it is simply a legitimate calculation procedure.

### • Simple extension of a dynamical theory

**Definition A.1.2.** It is said that the dynamical theory  $\mathcal{T}' = (\mathcal{L}', \mathcal{A}')$  is a *simple extension of the dynamical theory*  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$  if  $\mathcal{L} \subseteq \mathcal{L}'$  and  $\mathcal{A} \subseteq \mathcal{A}'$ . In this case the dynamical rules formulated in  $\mathcal{L}$  and valid (i.e. demonstrable) in  $\mathcal{T}$  are valid in  $\mathcal{T}'$ .

*Remark A.1.3.* In the previous definition, the expression “simple extension” can be questioned. If  $\mathcal{L}, \mathcal{A}, \mathcal{L}', \mathcal{A}'$  are finite sets, or if they are discrete countable sets, we can consider that everything is intuitively clear. However, it may happen that we wish to use more complicated sets, for example to introduce all the reals as constants in a theory of which one sort is intended to describe the real numbers. In such a case, the word “simple extension” is questionable because there is no canonical monomorphism in Bishop’s category **Set**: in Bishop’s conception, a part of a set corresponds to the categorical notion of a subobject. In this framework, therefore, “simplicity” is not an objective notion, or if you prefer, it has no precise mathematical definition. ■

## Structural rules

Here we give *admissible structural rules* for a dynamical theory. These are *external* deduction rules (different from dynamical rules, which are internal to the theory). They say that if certain dynamical rules are valid, then other dynamical rules are automatically valid.

Here are the admissible structural rules that we feel are the most important.

### Admissible structural rules A.1.4.

#### 0. Free variables, dummy variables

- (a) *Substitution.* In a dynamical rule, you can replace all occurrences of a free variable with a term, provided that you never create a conflict between free and dummy variables.
- (b) *Renaming.* In a dynamical rule, you can rename free variables or dummy variables (those present in the  $\exists$ ) as long as you never create a conflict between free and dummy variables.

<sup>2</sup>This excludes the case where  $t$  contains a variable  $x$  under the dependence of an  $\exists x$ .

## 1. Benefit from work already done

- (a) *Shortcuts.* Once the validity of a dynamical rule has been demonstrated, it can be added to the axioms of the theory.
- (b) *Simultaneous reinforcement of hypothesis and conclusions.* In a dynamical theory, we consider a valid rule

$$\Gamma \vdash \exists y^1 \Delta_1 \text{ op } \dots \text{ op } \exists y^m \Delta_m$$

Let  $A$  be an atomic formula which does not involve any of the existential variables of the second member. Let  $\Gamma'$  be the list  $\Gamma$  followed by  $A$  and  $\Delta'_i$  the list  $\Delta_i$  followed by  $A$ . Then the following rule is also valid:

$$\Gamma' \vdash \exists y^1 \Delta'_1 \text{ op } \dots \text{ op } \exists y^m \Delta'_m$$

## 2. Lists as finite sets

- (a) *Permutation of atomic formulas appearing in a list.*
- (b) *Contraction* If two identical atomic formulas appear in a list, one of the two can be deleted.  
Conversely, you can duplicate an atomic formula in an arbitrary list.
- (c) *Monotony.* Atomic formulas can be added as required to the list to the left of  $\vdash$ .
- (d) *Permutation, contraction and monotony for the op to the right of the  $\vdash$ .*

## 3. Lists of atomic formulas as conjunctions

- (a) *To prove a list of atomic formulas is to prove each of them.* In a theory, consider a dynamical rule  $\Gamma \vdash (A_1, \dots, A_n)$ . This dynamical rule is valid if, and only if, the rules  $\Gamma \vdash A_k$  ( $k \in \llbracket 1..n \rrbracket$ ) are valid.
- (b) *Distributivity of op on the implicit “and” in the lists.* In a theory, we consider a dynamical rule

$$\Gamma \vdash (A_1, \dots, A_n) \text{ op } \exists y^1 \Delta_1 \text{ op } \dots \text{ op } \exists y^m \Delta_m.$$

This dynamical rule is valid if, and only if, the following dynamical rules are valid

$$\Gamma \vdash A_k \text{ op } \exists y^1 \Delta_1 \text{ op } \dots \text{ op } \exists y^m \Delta_m \quad (k \in \llbracket 1..n \rrbracket).$$

## 4. Transitivity and variants

- (a) *Transitivity.* We give an example, leaving it to the reader to give the general formulation. Let us suppose that we have valid dynamical rules in a dynamical theory

$$\begin{aligned} \Gamma(\underline{x}) &\vdash \exists y, z \Delta_1(\underline{x}, y, z) \text{ op } \exists u \Delta_2(\underline{x}, u), \\ \Gamma(\underline{x}), \Delta_1(\underline{x}, y, z) &\vdash \exists r, s, t \Delta_3(\underline{x}, y, z, r, s, t), \\ \Gamma(\underline{x}), \Delta_2(\underline{x}, u) &\vdash \exists v \Delta_4(\underline{x}, u, v) \text{ op } \exists w \Delta_5(\underline{x}, u, w). \end{aligned}$$

Then the rule

$$\Gamma(\underline{x}) \vdash \exists y, z, r, s, t \Delta_3(\underline{x}, y, z, r, s, t) \text{ op } \exists u, v \Delta_4(\underline{x}, u, v) \text{ op } \exists u, w \Delta_5(\underline{x}, u, w).$$

is also valid.

- (b) *Cut.* Consider lists of atomic formulas  $\Gamma(\underline{x}), \Delta_0(\underline{x}), \Delta_1(\underline{x}), \dots, \Delta_m(\underline{x})$  ( $m \geq 1$ ) in a dynamical theory  $\mathcal{T}$ . If the two dynamical rules

$$\Gamma \vdash \Delta_0 \text{ op } \Delta_1 \text{ op } \dots \text{ op } \Delta_m \quad \text{and} \quad \Gamma, \Delta_0 \text{ op } \Delta_1 \text{ op } \dots \text{ op } \Delta_m$$

are valid in  $\mathcal{T}$ , then the rule  $\Gamma \vdash \Delta_1 \text{ op } \dots \text{ op } \Delta_m$  is also valid.

- (c) *Cut with existence.* A more general version is as follows. Consider lists of atomic formulas  $\Gamma(\underline{x}), \Delta_0(\underline{x}, y^0), \Delta_1(\underline{x}, y^1), \dots, \Delta_m(\underline{x}, y^m)$  ( $m \geq 1$ ) dans une dynamical theory  $\mathcal{T}$  ( $m \geq 1$ ) in a dynamical theory  $\mathcal{T}$ . If the two dynamical rules

$$\Gamma \vdash \exists y^0 \Delta_0 \text{ op } \exists y^1 \Delta_1 \text{ op } \dots \text{ op } \exists y^m \Delta_m \text{ and } \Gamma, \Delta_0 \vdash \exists y^1 \Delta_1 \text{ op } \dots \text{ op } \exists y^m \Delta_m$$

are valid in  $\mathcal{T}$ , then the rule  $\Gamma \vdash \exists y^1 \Delta_1 \text{ op } \dots \text{ op } \exists y^m \Delta_m$  is also valid.

## Collapsus

A dynamical rule is called a *collapse rule* when the second member is “False”, which we note  $\perp$ . We can also see  $\perp$  as designating the empty disjunction. Once  $\perp$  has been proved, the universe of discourse collapses, and every atomic formula is then deemed to be “true”, or at least “valid”. This is the application of the rule “ex falso quod libet”, which is the relevant intuitive meaning of False in constructive mathematics. Thus in dynamical theories the rules

$$\text{False}_P \quad \perp \vdash P \quad (\text{ex falso quod libet})$$

are valid for all atomic formulas.

In the language, we also give the logical constant  $\top$  for “True”, with the following Horn rule as its axiom.

$$\text{True} \quad \vdash \top$$

We can also see  $\top$  as designating the empty conjunction.<sup>3</sup> The constants  $\perp$  and  $\top$  are the only logical symbols in dynamical theories.

When a dynamical theory has no collapse rule, it always admits the model reduced to a point<sup>4</sup> where all atomic formulas are evaluated true. This is the final object in the category of models of the theory.

We can say that a dynamical theory without a collapse rule collapses if all the atomic formulas are valid, with the exception of  $\perp$ .

A dynamical theory with a collapse rule is said to collapse when  $\perp$  is provable, and consequently so are all the dynamical rules. In this case the theory admits no model.

To consider collapse in the sense of a single model reduced to a point, rather than in the sense of pure nothingness, is merely a matter of taste which changes nothing in the essence of things.<sup>5</sup>

Instead of saying that a collapsing dynamic algebraic structure has no model, we say (without negation) that any model of this dynamic algebraic structure is trivial, reduced to a point, and that “everything in it is true”.

To formally reconcile these two points of view, the best solution seems to be the following: each sort  $S$  introduced is accompanied by at least two constants in this sort, say  $0_S$  and  $1_S$  to fix ideas, with the axiom  $0_S =_S 1_S \vdash \perp$ . In what follows, this is what would normally happen for the theory of non-trivial distributive lattices and the theory of non-zero commutative rings, as well as in all their extensions. But we prefer to use the following convention.

Throughout this memoir, in the case of a ring or a distributive lattice, we consider that the collapse is always given in the form  $0 = 1$  or a formula of the same style, for example  $0 > 0$  for an ordered field. One disadvantage of using the symbol  $\perp$  is that it takes us out of the realm of Horn theories when we could be staying there. Readers who so wish can add an axiom of the type  $0 = 1 \vdash \perp$ .

<sup>3</sup>When there’s nothing to prove, let’s prove nothing and everything will be OK. Moreover, in a dynamical theory with at least one sort  $S$ ,  $\top$  is equivalent to  $x =_S x$ .

<sup>4</sup>If there are several sorts, each sort is reduced to a point.

<sup>5</sup>In fact, one of the authors must have a horror of the void  $\cdot$ , the silence of this infinite space frightens him  $\cdot$ . Moreover, if total disappearance into nothingness is the true meaning of False, the fact remains that, even before forbidding the existence of models, False begins by reducing them to a single point, which satisfies all the predicates. As Boris Vian’s song says: “on est descendu chez Satan et en bas c’était épatant!”.

## Classification of dynamical theories

### • Horn theories

A dynamical rule which does not contain to the right of the symbol  $\vdash$  either  $\text{op}$ , or  $\exists$  or  $\perp$  is called a *Horn rule*. A dynamical theory is said to be *Horn* when it contains only Horn rules as axioms. In the french version of this paper and in the paper [17], Horn theories are called *théories algébriques*. A special case is provided by purely equational theories, which are Horn theories with a single sort and the only predicate being the equality predicate.

*Note.* We use the following terminology from [17]. A Horn rule is said to be *direct* when, to the left of the symbol  $\vdash$ , there are only atomic formulas relating to variables different from each other or to constants. The other Horn rules are called *simplification rules*. For example, in the two examples below, the first is direct, the second is not.

$$\bullet \quad x = 0, y = 0 \vdash x + y = 0 \qquad \bullet \quad x + y = 0, x = 0 \vdash y = 0$$

### • Disjunctive theories

A dynamical theory is said to be *disjunctive* if in the axioms there are no  $\exists$  to the right of the  $\vdash$ .

### • Existential theories

A dynamical rule is said to be *simple existential* if the second member (the conclusion) is of the form  $\exists y \Delta$  where  $\Delta$  is a finite list of atomic formulas.

A dynamical theory is said to be *existential* if its axioms are all simple algebraic or existential rules (a Horn rule can also be considered as a special case of a simple existential rule). A typical existential theory is the theory of *Bézout rings* (any finitely generated ideal is principal). In the English literature on categorical logic (studied in the context of classical mathematics), an existential theory is called a *regular theory*. In the french version of this paper an existential theory is called a *théorie existentielle*.

### • Existentially rigid, cartesian theories

Existentially rigid theories are dynamical theories in which the existential axioms are simple and correspond to unique existences. This generalises (very slightly) the disjunctive theories.

An existentially rigid theory is said to be *cartesian*. This generalises (very slightly) Horn theories.

### • Rigid theories

A dynamical theory is said to be *rigid* if it is existentially rigid and if the disjuncts of the second member in the disjunctive axioms are two by two incompatible. For example, the theory of discrete fields is rigid, but the theory of local rings is not. The theory of real closed discrete fields can be stated rigidly, but the theory of algebraically closed discrete fields cannot. See [29], who uses the terminology “disjunctive theory” where we use “rigid theory”.

### • Propositional theories

The (classical or intuitionistic) logic of propositions has a very abstract character, which may seem useless from a dynamic point of view, since it is already present in the form of some of the admissible structural rules A.1.4. However, it is useful for the definition of distributive lattices associated with dynamic algebraic structures (Section A.4.)

The logic of propositions can be presented in a minimal dynamic form as follows, without any sort, which implies that the constants must be interpreted as pure abstract truth values (in classical logic they only hesitate between True and False).

The constants are therefore  $\perp$ ,  $\top$ , and *propositional constants* or *propositions*. To define such a theory  $(\mathcal{L}, \mathcal{A})$ , we give a set  $G$  of propositional constants.<sup>6</sup> and a set  $\mathcal{A}$  of axioms which are disjunctive rules on the language  $\mathcal{L}$

<sup>6</sup>This fixes the language  $\mathcal{L}$  via the signature  $\{G, \top, \perp\}$

First we have the axioms  $\perp \vdash p$  and  $p \vdash \top$ , and the axioms which handle equality in  $G$ :  $p \vdash q$  each time  $p =_G q$ . If  $G$  is not a discrete set, these axioms reflect the structure of the set  $G$  in the informal category  $\mathcal{Set}$ .

The additional axioms given in  $\mathcal{A}$  are of the type  $p_1, p_n \vdash q_1 \text{ op } \dots \text{ op } q_m$  where  $p_i$  and  $q_j$  are constants in  $G$  (with possibly  $m = 0$  or  $n = 0$ ).

Two constants  $p$  and  $q$  are said to be *opposite* or *complementary* if they satisfy the axioms of negation

$$\bullet \vdash p \text{ op } q \qquad \bullet p, q \vdash \perp$$

While classical propositional logic can be interpreted as given by dynamical theories without any sort of the type described above, the same cannot be said for intuitionistic logic. Indeed, the  $\Rightarrow$  connector cannot be described by restricting ourselves to dynamical theories. Obviously, this connector can be introduced into the language, but the external structural rule used to introduce implication in natural deduction cannot be formulated as a dynamical rule.

## A.2. Dynamic algebraic structures

References: [17], [37], [41].

The dynamic algebraic structures are explicitly named in [37]. In [17], they are implicit, but explicit in the form of their presentation. They are also implicit in [36], and, last but not least, in [18, D5, 1985], which has been an essential source of inspiration: one can compute safely in the algebraic closure of a discrete field, even when it is not possible to construct this algebraic closure. It is therefore sufficient to consider the algebraic closure as a dynamic algebraic structure “à la D5” rather than as a usual algebraic structure: *lazy evaluation in D5 provides a constructive semantics for the algebraic closure of a discrete field*.

### Definitions, examples

**Example A.2.1.** Our first example is the purely equational theory of commutative rings (with only one sort, called  $Ac$ ) in which most of the calculations are entrusted to machines outside the formal theory. This possibility is based on the fact that the elements of the ring  $\mathbb{Z}[x_1, \dots, x_n]$  can be reduced to a predefined normal form. This implies that the equality of two terms is equivalent to the identity of their normal forms. Consequently, the binary equality predicate can be replaced by the equality to 0 predicate.

The theory  $\mathcal{Ac}0$  of commutative rings is written on the following signature. There is only one sort, called  $Ac$ .

$$\text{Signature: } \boxed{\Sigma_{Ac} = (\cdot =_{Ac} 0 ; \cdot + \cdot, \cdot \times \cdot, - \cdot, 0_{Ac}, 1_{Ac})}$$

The only axioms are the following (these are direct rules):<sup>7</sup>

$$\begin{aligned} \mathbf{ac0} \quad & \vdash 0_{Ac} =_{Ac} 0 & \mathbf{ac1} \quad & x =_{Ac} 0 \vdash_{x,y:Ac} x \times y =_{Ac} 0 \\ \mathbf{ac2} \quad & x =_{Ac} 0, y =_{Ac} 0 \vdash_{x,y:Ac} x + y =_{Ac} 0 \end{aligned}$$

The term “ $x - y$ ” is an abbreviation for “ $x + (-y)$ ” and the binary predicate “ $\cdot = \cdot$ ” is *defined* by convention: “ $x = y$ ” is an abbreviation for “ $x - y = 0$ ”.

We often consider the theory  $\mathcal{Ac}$  of *non-trivial commutative rings*, which is obtained from  $\mathcal{Ac}0$  by adding the collapse axiom

$$\mathbf{CL}_{=,Ac} \quad 1 =_{Ac} 0 \vdash \perp$$

<sup>7</sup>The names of the rules are written as follows: for the direct rules, all lower case, for the other Horn rules (the simplification rules), the first letter in upper case, and finally the other dynamical rules, all upper case.

**Explanations.**

1. The rules that define the  $\mathcal{AcO}$  theory of commutative rings must be understood precisely as follows. Any term of the theory can be seen as a polynomial with integer coefficients in the present variables. We then use the computational machinery of commutative polynomials with integer coefficients (“external” to the theory), which rewrites any term (formed over constants and variables) as a polynomial with integer coefficients in a predefined normal form.

The distributivity rule  $x(y + z) =_{Ac} xy + xz$ , for example, is then entrusted to an automatic calculation which reduces to 0 the term  $x(y + z) - (xy + xz)$ .

Similarly, the transitivity of binary equality is handled by the rule **ac2** and by the automatic calculation which reduces the term  $(x - y) + (y - z)$  to  $(x - z)$ .

2. In the three rules **ac0**, **ac2** and **ac1** we recognise the axioms of ideals, which make it possible to create a quotient ring structure, and which signify the compatibility of equality with addition and multiplication. In the  $\mathcal{AcO}$  theory, any atomic formula is of the form “ $t(x_1, \dots, x_n) =_{Ac} 0$ ” where  $x_i$ ’s are variables and  $t$  a term of the language. Any atomic formula is therefore immediately equivalent to an atomic formula in which  $t$  is an element of the ring  $\mathbb{Z}[x_1, \dots, x_n]$ , written in the agreed normal form. The  $\mathcal{AcO}$  theory is therefore the “the theory of algebraic identities”, in the old sense of the expression. Precisely, it is easy to check that the validity of a simple Horn rule such as

$$\bullet \quad p_1 =_{Ac} 0, \dots, p_m =_{Ac} 0 \vdash_{x_1, \dots, x_r: Ac} q =_{Ac} 0$$

means exactly that the polynomial  $q \in \mathbb{Z}[x_1, \dots, x_r]$  is in the ideal generated by the polynomials  $p_1, \dots, p_m$  of  $\mathbb{Z}[x_1, \dots, x_r]$ . This property is rather difficult to decide.<sup>8</sup>

The dynamical theory of a purely equational theory does not provide any additional tool to the purely equational theory itself. There is therefore nothing really “dynamic” about purely equational dynamical theories. The really interesting dynamical theories are obtained by adding dynamical axioms to Horn theories.

For the theory  $\mathcal{AcO}$  the validity of more complicated rules than those considered above is handled by the structural rule **3a** page 15.

3. The theory  $\mathcal{AcO}$  as it is presented does not seem “purely equational” at first sight because the axioms are not simple equalities between terms. This is due to our decision to replace equality with the unary predicate “ $\cdot = 0$ ” accompanied by the external computational machinery of polynomials with integer coefficients. This approach has the advantage, in our opinion, of showing the true logical structure of the theory by reducing it to three very simple axioms and by entrusting to an automatic calculation what can be entrusted to it, which has little to do with logic proper. The same remark will subsequently apply to many theories that we will describe as purely equational. ■

**Definition A.2.2.** If  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$  is a dynamical theory, a *dynamic algebraic structure of type  $\mathcal{T}$*  is given by a set  $G$  of *generators* and a set  $R$  of *relations*. A “relation” is by definition an atomic formula  $P(\underline{t})$  constructed on the language  $\mathcal{L} \cup G$  with closed terms  $t_i$  in this language. Such a relation is associated with the axiom “ $\vdash P(\underline{t})$ ” of the dynamic algebraic structure. So, this dynamic algebraic structure is the dynamical theory  $(\mathcal{L} \cup G, \mathcal{A} \cup R)$ , also denoted by  $((G, R), \mathcal{T})$ .

**Example A.2.3.** For example, we obtain a dynamic algebraic structure for a discrete field

$$\mathbf{K} = ((G, R), \mathcal{Cd})$$

by taking  $G = \{a, b\}$  and  $R = \{105 = 0, a^2 + b^2 - 1 = 0\}$ . This dynamic discrete field corresponds to any discrete field of characteristic 3 or 5 or 7 generated by two elements  $\alpha$  and  $\beta$  satisfying  $\alpha^2 + \beta^2 = 1$ .

In addition to the dynamical rules valid in all discrete fields, there are now those obtained by extending the language with the constants taken from  $G$  and by adding to the axioms the relations taken from  $R$ . For example the disjunctive rule

<sup>8</sup>This follows for example from Theorem VIII-1.5 in [MRR].

- $3 = 0$  **op**  $5 = 0$  **op**  $7 = 0$

is valid, and so is the dynamical rule

- $\exists z 15z = 1$  **op**  $\exists z 21z = 1$  **op**  $\exists z 35z = 1$  ■

#### Definitions and notations A.2.4.

Let  $\mathbf{S} = ((G, R), \mathcal{T})$  be a dynamic algebraic structure of type  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ .

- We will indicate that the rule “ $\Gamma \vdash \dots$ ” is valid in the dynamic algebraic structure  $\mathbf{S}$  in the following abbreviated form: “ $\Gamma \vdash_{\mathbf{S}} \dots$ ”. We could also use the notation “ $R, \Gamma \vdash_{\mathcal{T}} \dots$ ”, which means that the proof can use a finite list of axioms extracted from  $R$ .
- The set of closed terms of  $\mathbf{S}$ , i.e. the terms built on  $\mathcal{L} \cup G$ , is denoted by  $\text{Tcl}(\mathbf{S})$ . The set of closed atomic formulas is denoted by  $\text{Atcl}(\mathbf{S})$ .
- An Horn rule  $\vdash P$  for  $P \in \text{Atcl}(\mathbf{S})$  is called a *fact in  $\mathbf{S}$* . The set of valid facts in  $\mathbf{S}$  is called  $\text{Atclv}(\mathbf{S})$ . A fact only concerns syntactically definable objects in the structure. It is clear that  $\mathbf{S}$  proves exactly the same dynamical rules as the dynamic algebraic structure  $\tilde{\mathbf{S}} = ((\text{Tcl}(\mathbf{S}), \text{Atclv}(\mathbf{S})), \mathcal{T})$ .

Concrete algebra very often consists of proving facts or dynamic rules in particular dynamic algebraic structures. It is a little more general than the (inexhaustible) theory of algebraic identities, i.e. the universal algebra behind a large proportion of the great theorems of abstract algebra.

In the case of a Horn theory  $\mathcal{T}$ , a dynamic algebraic structure of type  $\mathcal{T}$  gives a usual algebraic structure, defined by generators and relations, satisfying the required Horn rules.

The dynamic method is often a practical way of constructing algebraic identities (“Positivstellensätze” for example), following as closely as possible the paths indicated in the proofs given in classical mathematics.

In a dynamic algebraic structure a fact  $P(\underline{t})$  is *absolutely true* if it is provable (i.e. if the rule “ $\vdash P(\underline{t})$ ” is valid). It is *absolutely false*, or more precisely *catastrophic* if “ $P(\underline{t}) \vdash \perp$ ” is valid. There are many possibilities in between these two cases: a dynamic algebraic structure does not have a single fixed model, but represents all the possible ideal realisations of the structure in the potential state (this notion remains deliberately vague). Adding a catastrophic fact as an axiom amounts to eliminating all models.<sup>9</sup>

**Example A.2.5.** We consider a presentation  $(G, R)$  in the language of  $\mathcal{Ac}$ . Let  $\mathcal{T}$  be a dynamical theory which extends the theory  $\mathcal{Ac}$  without extending the language, for example the theory  $\mathcal{Cd}$  of discrete fields. Any closed term of the dynamic algebraic structure  $((G, R), \mathcal{T})$  is rewritten as a polynomial  $f(\underline{x}) \in \mathbb{Z}[G]$  with integer coefficients in the “constants”  $x_i \in G$  of the dynamic algebraic structure. The elements of  $R$  are relations  $f(\underline{x}) = 0$ , so that by a slight abuse of language, we can consider  $R$  as a set of elements of  $\mathbb{Z}[G]$ .

We are therefore studying the ring  $\mathbf{A} = \mathbb{Z}[G]/\langle R \rangle$ , or more precisely what happens to this ring when we ask it to satisfy certain new axioms. We will note  $\mathcal{T}(\mathbf{A})$  the dynamic algebraic structure  $((G, R), \mathcal{T})$ .

In many examples, the theory collapses if, and only if,  $\mathbf{A}$  is trivial. For example, the dynamic algebraic structure  $\mathcal{Cd}(\mathbf{A})$  collapses if, and only if,  $1 =_{\mathbf{A}} 0$ . In classical mathematics we say: indeed a non-trivial ring has a prime ideal  $\mathfrak{p}$ , and the field of fractions of the integral ring  $\mathbf{A}/\mathfrak{p}$  is a non-trivial model of  $\mathcal{Cd}(\mathbf{A})$ . More simply, without using model theory or the axiom of the prime ideal, we transform a proof of  $1 = 0$  in  $\mathcal{Cd}(\mathbf{A})$  into a proof of  $1 = 0$  in  $\mathcal{Ac}(\mathbf{A})$  (proof analogous to that of [17, Theorem 2.4]).

<sup>9</sup>In the variant where the collapse reduces all models to a singleton: ... amounts to allowing only the trivial model.

Concerning the facts  $\theta = 0$ <sup>10</sup> valid in the theory  $\mathcal{T}(\mathbf{A})$ , the situation is a little more complicated. The theory of local rings  $\mathcal{A}$  proves  $\theta = 0$  exactly when  $\theta =_{\mathbf{A}} 0$ , hence the great importance of local rings in commutative algebra.

The theory  $\mathcal{C}d$  proves  $\theta = 0$  exactly when  $\theta \in \sqrt{0}$ . This corresponds to the reduced quotient of  $\mathbf{A}$ : if  $\theta = 0$  in  $\mathcal{C}d(\mathbf{A})$  then  $\theta$  is nilpotent in  $\mathbf{A}$ . This is a (relatively weak) abstract form of the Nullstellensatz. The proof is elementary. Naturally, if two theories prove the same facts, they can differ in terms of dynamical rules that are more general than Horn rules. ■

## Positive diagram of an algebraic structure

### Definition and notation A.2.6.

1. Let  $\mathcal{T}_1 = (\mathcal{L}_1, \mathcal{A}_1)$  be a dynamical theory and  $\mathbf{A}$  an algebraic structure over a language  $\mathcal{L} \subseteq \mathcal{L}_1$ . We call *positive diagram of  $\mathbf{A}$  for the language  $\mathcal{L}$* , a presentation  $(G, R)$  of  $\mathbf{A}$  as an algebraic structure over the language  $\mathcal{L}$ . Such a diagram is denoted  $\text{Diag}(\mathbf{A}, \mathcal{L})$ . We then denote  $\mathcal{T}_1(\mathbf{A})$  the dynamic algebraic structure  $(\text{Diag}(\mathbf{A}, \mathcal{L}), \mathcal{T}_1)$ .
2. Let  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$  be a dynamical theory,  $\mathbf{B}$  a model of  $\mathcal{T}$ , and  $\mathcal{T}_1 = (\mathcal{L}_1, \mathcal{A}_1)$  a simple extension of  $\mathcal{T}$ . Consider a presentation  $(G, R)$  of  $\mathbf{B}$  as a dynamic algebraic structure of type  $\mathcal{T}$ . Such a diagram is called *positive diagram of  $\mathbf{B}$  for the dynamical theory  $\mathcal{T}$*  and it is denoted  $\text{Diag}(\mathbf{B}, \mathcal{T})$ . We then note  $\mathcal{T}_1(\mathbf{B})$  the dynamic algebraic structure  $(\text{Diag}(\mathbf{B}, \mathcal{T}), \mathcal{T}_1)$ .

Item 1 can be seen as a special case of item 2, where  $\mathcal{A} = \emptyset$ .

### Remarks A.2.7.

1) Here is a typical example for Item 1. The theory  $\mathcal{T}_1$  is a simple extension of the theory  $\mathcal{A}c$  where equality is the only predicate. Let  $\mathcal{L}$  be the language of  $\mathcal{A}c$  and let  $\mathbf{A}$  be a commutative ring. For generators of  $\text{Diag}(\mathbf{A}, \mathcal{L})$  we can take the elements of the set underlying  $\mathbf{A}$ , and for relations we can restrict ourselves to the equalities  $0_{\mathbf{A}} = 0$ ,  $1_{\mathbf{A}} = 1$ ,  $-a = b$ ,  $a + b = c$  and  $ab = c$  when they are satisfied for elements of  $\mathbf{A}$ . This positive diagram does not contain any  $a \neq b$  inequalities for the simple reason that they are not part of the language of  $\mathcal{A}c$ . This is why we call it a “positive” diagram.

2) An element  $a$  of  $\mathbf{A}$  does not always have a canonical representative in a set à la Bishop, even if the set is discrete. In such a case, to return to the definition of the set underlying  $\mathbf{A}$  according to Bishop, we can take a different constant  $x_b$  for each representative  $b$  of the element  $a$ . We then find in the positive diagram of  $\mathbf{A}$  a relation  $x_b = x_c$  each time  $b =_{\mathbf{A}} c$ . ■

## Constructive versus classical models

Consider a dynamic algebraic structure  $\mathbf{A} = ((G, R), \mathcal{T})$  of type  $\mathcal{T}$  with one or more sorts. To simplify the notation, we assume a single sort. A *model of  $\mathbf{A}$*  is a usual (static) algebraic structure  $M$  described in the language associated with  $\mathbf{A}$  and verifying the axioms of  $\mathbf{A}$  (those of  $\mathcal{T}$  and those given by the presentation of  $\mathbf{A}$ ).

When  $\mathbf{A}$  is defined by the empty presentation, we speak of *models of  $\mathcal{T}$* .

The notion of model is therefore based a priori on an intuitive notion of *algebraic structure* à la Bourbaki. We can describe these algebraic structures as “static” in contrast to the general dynamic algebraic structures. Note that here the set “underlying” the structure is a “naive set” (or several naive sets if there are several sorts) structured by giving predicates and functions (in the naive sense) subject to certain axioms.

From a constructive point of view, the models must satisfy the axioms by respecting the intuitive sense of “or” and “there exists”: to prove that a particular algebraic structure satisfies the axioms, we allow only intuitionistic logic. Note also that the set theory to which we refer is a priori Bishop’s informal set theory.

<sup>10</sup>With  $\theta = t(\xi) \in \mathbf{A}$ , where  $t \in \mathbb{Z}[G]$  and the  $\xi_k$  are the  $x_k$  seen in the quotient  $\mathbf{A}$  of  $\mathbb{Z}[G]$ .



## Morphisms between dynamic algebraic structures of the same type

Consider a disjunctive theory  $\mathcal{T}$ . In this case, a possible natural notion of morphism from a dynamic algebraic structure  $\mathbf{A} = ((G, R), \mathcal{T})$  to a dynamic algebraic structure  $\mathbf{A}' = ((G', R'), \mathcal{T})$  for the disjunctive theory  $\mathcal{T}$  is as follows.

An element of  $\mathbf{Sad}_{\mathcal{T}}(\mathbf{A}, \mathbf{A}')$  is given by a map  $\varphi: G \rightarrow \text{Tcl}(\mathbf{A}')$  which interprets the elements of  $G$  by closed terms of  $\mathbf{A}'$ . This map uniquely extends into a map  $\text{Tcl}(\mathbf{A}) \rightarrow \text{Tcl}(\mathbf{A}')$  respecting the construction of the terms by means of the function symbols present in  $\mathcal{L}$ . In addition, the elements of  $R$  must give valid facts in  $\mathbf{A}'$  according to this interpretation.

The equality between two elements  $\varphi$  and  $\psi$  of the set  $M = \mathbf{Sad}_{\mathcal{T}}(\mathbf{A}, \mathbf{A}')$  is defined as follows: one has  $\varphi =_M \psi$  if, and only if, for all  $x \in G$ , the equality  $\varphi(x) = \psi(x)$  is valid in  $\mathbf{A}'$ .

The composition of morphisms is defined in a natural way for three dynamic algebraic structures  $\mathbf{A}$ ,  $\mathbf{B}$  and  $\mathbf{C}$ .

This gives us a very interesting (informal) category. The objects are dynamic algebraic structures of type  $\mathcal{T}$ . The set of arrows from  $\mathbf{A}$  to  $\mathbf{A}'$  is  $\mathbf{Sad}_{\mathcal{T}}(\mathbf{A}, \mathbf{A}')$ .

This category has arbitrary limits and colimits, constructed very naively at the level of the presentations  $(G, R)$ , based on the naive intuitive set theory that we consider in the ambient mathematical world.

For example, the product in the category  $\mathbf{Sad}_{\mathcal{T}}$  of  $\mathbf{A} = ((G, R), \mathcal{T})$  and  $\mathbf{A}' = ((G', R'), \mathcal{T})$  is the dynamic algebraic structure of type  $\mathcal{T}$  whose presentation is given by  $(G \times G', R \times R')$ . When  $\mathcal{T}$  is the theory of discrete fields, in the disjunctive version where a discrete field is defined as a connected reduced zero-dimensional ring (a function symbol must be introduced for the quasi-inverse). The previous product is a new dynamic algebraic structure of a discrete field, and  $\mathbf{A} \times \mathbf{A}'$  is provided with a usual algebraic structure of a reduced zero-dimensional ring. This situation seems analogous to that of bundles of discrete fields (according to the semantics of Kripke-Joyal), which are discrete fields only in the fibres.

*Remark.* If we are dealing with an existentially rigid theory, we can reduce ourselves to the case of a disjunctive theory by skolemisation of the rigid existential rules. However, it seems that in the case of a dynamical theory with non-rigid existential axioms, things are not very clear. ■

Sometimes we are interested in a more restrictive notion of morphism between two dynamical algebraic structures  $\mathbf{A}$  and  $\mathbf{A}'$  of the same type  $\mathcal{T}$ , for example the notion of local morphism between commutative rings, adapted to a specific context. In such a case, we would like the new morphisms from  $\mathbf{A}$  to  $\mathbf{A}'$  to be treated as given by dynamic algebraic structures for a certain dynamical theory defined from  $\mathcal{T}$ ,  $\mathbf{A}$  and  $\mathbf{A}'$  (as may be the case for local morphisms).

## Examples

1) The disjunctive theory  $\mathcal{A}sdz0$  (resp.  $\mathcal{A}sdz$ ) of *rings without zerodivisor* is obtained from the theory  $\mathcal{A}c0$  (resp.  $\mathcal{A}c$ ) by adding the dynamical rule

$$\mathbf{ASDZ} \quad xy = 0 \vdash x = 0 \text{ op } y = 0$$

2) Reference [ACMC, section VIII-3]. The existential theory  $\mathcal{A}lsdz0$  (resp.  $\mathcal{A}lsdz$ ) of the *rings locally without zerodivisor* is obtained by adding to the theory  $\mathcal{A}c0$  (resp.  $\mathcal{A}c$ ) the axiom  $\mathbf{LSDZ}$ :

$$\mathbf{LSDZ} \quad xy = 0 \vdash \exists u, v (ux = 0, vy = 0, u + v = 1)$$

3) With the signature

$$\mathbf{Signature:} \quad \boxed{\Sigma_{Ai} = (\cdot = 0, \cdot \neq 0; \cdot + \cdot, \cdot \times \cdot, - \cdot, 0, 1)}$$

The theory  $\mathcal{A}i$  of *integral rings* is obtained from the theory  $\mathcal{A}c0$  by adding as axioms the following dynamical rules

- $x \neq 0, y = 0 \vdash x + y \neq 0$
- $\vdash 1 \neq 0$
- $x \neq 0, y \neq 0 \vdash xy \neq 0$
- $xy \neq 0 \vdash x \neq 0$
- $x \neq 0, xy = 0 \vdash y = 0$
- $0 \neq 0 \vdash \perp$
- $\vdash x = 0 \text{ op } x \neq 0$

Note the significant difference between the theories  $\mathcal{A}sdz$  and  $\mathcal{A}i$ , which corresponds to an important distinction in constructive mathematics but invisible in classical mathematics.

## Primitive recursive arithmetic

This subsection shows the interest of using sorts for maps that can be defined constructively in an algebraic structure (for example here the semi-ring of natural numbers) when the language in which the structure is defined does not allow the introduction of function symbols corresponding to these maps in the corresponding geometric theory.

This example motivates us to introduce sorts for certain continuous semialgebraic maps and their continuity moduli in the theory of *non* discrete real closed fields.

Long before the machinery of dynamical theories was set up, R. L. Goodstein explained how to treat a large part of the usually practised mathematics by means of purely computational formal systems, *without logic*.

In the book [Goodstein, 1957] the author, following a suggestion by Skolem, shows how a calculus system “without logic, and without quantifiers” makes it possible to develop a very important part of “arithmetic”, understood in the sense of a formal theory of the natural integers.

The only problem, and it’s a major problem that is likely to put off many a mathematician, is that the usual mathematical statements have to be encoded in the form of primitive recursive maps. This may seem to take us back to the realm of second-order arithmetic and Reverse Mathematics.

In a second book ([Goodstein, 1961]) Goodstein extends his study to recursive analysis. We also highly recommend [Goodstein, 1979].

## Goodstein’s formal system

If we restrict ourselves to primitive recursive arithmetic,<sup>11</sup> we can describe the formal system proposed by Goodstein as follows.

As in the formal theory *Peano*, the variables and constants represent natural numbers. There is a single constant, 0, and a single relation symbol, which is the equality  $x = y$ .

For any primitive recursive map  $f: \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ , defined by simple recurrence using the equations

$$\begin{aligned} f(x_1, \dots, x_k, 0) &= g(x_1, \dots, x_k) \\ f(x_1, \dots, x_k, y + 1) &= h(x_1, \dots, x_k, y, f(x_1, \dots, x_k, y)) \end{aligned}$$

where  $g$  and  $h$  are previously defined primitive recursive maps, we introduce a function symbol corresponding to this definition of  $f$ .

Similarly, for any primitive recursive map defined by composition of previously defined primitive recursive maps, we introduce a function symbol corresponding to this definition.

The function symbols which “initialise” the system are  $S$  for the successor map,  $0_1$  for the null map in one variable and  $\pi_{n,k}$  for the  $k$ -th coordinate map  $\mathbb{N}^n \rightarrow \mathbb{N}$  ( $k \in \llbracket 1..n \rrbracket$ ,  $n \in \mathbb{N}$ ).

In this way we obtain a function symbol of arity  $r$  for each definition of a primitive recursive map  $\mathbb{N}^r \rightarrow \mathbb{N}$ .

Note that we have a formal name  $\underline{n}$ , an abbreviation of  $S(S(\dots(S(0))\dots))$ , for each integer  $n$ .

<sup>11</sup>Goodstein’s book studies broader systems of calculation that include maps defined by multiple recurrences, such as the Ackerman function.

Calculations in primitive recursive arithmetic à la Goodstein consist of establishing “identities” between two functions defined in this way corresponding to two function symbols  $f_i$  and  $f_j$  of the same arity.

$$\forall x_1, \dots, x_k \quad f_i(x_1, \dots, x_k) = f_j(x_1, \dots, x_k)$$

which we can write in the form of a valid rule in the proposed system:

$$\mathbf{Eq}_{i,j} \quad \vdash \quad f_i(x_1, \dots, x_k) = f_j(x_1, \dots, x_k)$$

However, this is not a dynamical theory because the valid rules do not result from a simple axiomatic system of dynamical rules.

In fact, we must obviously take as axioms all the equalities mentioned earlier, which are used to define arbitrary primitive recursive maps, but this is clearly not enough.

Indeed, if the equality  $(\underline{m} + \underline{n}) + \underline{p} = \underline{m} + (\underline{n} + \underline{p})$  can be established for arbitrary  $m, n, p$  integers by simply using the definition of  $+$  by recurrence, the corresponding rule

$$\vdash \quad (x + y) + z = x + (y + z)$$

does not result in a purely finitary way from the axioms of definition of  $+$ .

The same applies, for example, to an equality  $f_i(\underline{m}, \underline{n}) = f_j(\underline{m}, \underline{n})$  which could be found for all integers  $m, n$  by simply applying the axioms defining  $f_i$  and  $f_j$ , whereas the corresponding rule  $\mathbf{Eq}_{i,j}$  cannot in general be established in a purely finitary way if the definitions of  $f_i$  and  $f_j$  use the simple induction scheme.

The computational system allows us to validate composition of maps,<sup>12</sup> because it is subject to the axioms of equality. But to complete primitive recursive arithmetic, we need the *external rules* corresponding to definitions by recurrence. Specifically, for example, from the following two valid rules

- $\vdash \quad u(x, 0) = v(x, 0)$
- $u(x, y) = v(x, y) \quad \vdash \quad u(x, y + 1) = v(x, y + 1)$

we deduce the validity of the rule

- $\vdash \quad u(x, y) = v(x, y)$

(here  $u$  and  $v$  are two terms containing  $x$  and  $y$  as free variables)

The use of these external rules avoids recourse to the corresponding axiom, which can be formulated in a first-order formal theory, but not in a finitary dynamical theory:

$$[\forall x \ u(x, 0) = v(x, 0) \wedge \forall x, y \ ((u(x, y) = v(x, y) \Rightarrow u(x, y+1) = v(x, y+1))] \Rightarrow \forall x, y \ u(x, y) = v(x, y)$$

## A finitary geometric theory for primitive recursive arithmetic

In this subsection we show how to treat Goodstein-style primitive recursive arithmetic within the framework of a dynamical theory.

We now explain how the use of sorts for maps allows us to avoid recourse to these external rules and to define a simple formal system (a finitary Horn theory) for primitive recursive arithmetic.

### 1. Sorts

For each integer  $k$  we introduce the sort  $F_k$  of the primitive recursive maps  $f: N^k \rightarrow N$ . The sort  $F_0$  is the sort of integers denoted  $N$ .

### 2. Predicates.

For each sort  $F_k$ , there is a corresponding equality symbol  $\cdot =_k \cdot$ .

<sup>12</sup>For example,  $g = f_1 \circ (f_2 \circ f_3)$  and  $h = (f_1 \circ f_2) \circ f_3$  which correspond to two different definitions, give rise to the identity  $\vdash \quad g(x) = h(x)$  because according to the definitions  $\vdash \quad g(x) = f_1(f_2(f_3(x)))$  and  $\vdash \quad h(x) = f_1(f_2(f_3(x)))$ .

## 3. Constants.

- (a) The basic constants are (names for)
- 0 of sort  $N$ ,
  - $0_k$  of sort  $F_k$  (for the constant null map,  $k \geq 1$ ),
  - the successor map  $S$  of sort  $F_1$ ,
  - for  $n \geq 1$ , the  $n$  coordinate maps<sup>13</sup>  $\pi_{n,k}$  of sort  $F_n$  ( $1 \leq k \leq n$ ).
- (b) For any primitive recursive map  $f: \mathbb{N}^k \rightarrow \mathbb{N}$  ( $k \geq 1$ ), defined by simple recurrence using the equations

$$\begin{aligned} f(\underline{x}, 0) &= g(\underline{x}) & g: \mathbb{N}^{k-1} &\rightarrow \mathbb{N} \\ f(\underline{x}, S(y)) &= h(\underline{x}, y, f(\underline{x}, y)) & h: \mathbb{N}^{k+1} &\rightarrow \mathbb{N} \end{aligned}$$

where  $g$  and  $h$  are previously defined primitive recursive maps, we introduce a name for  $f$  as a constant of sort  $F_k$ .<sup>14</sup>

- (c) A name is also introduced for any primitive recursive map defined by composition of previously defined primitive recursive maps.
4. *The other function symbols.* The function symbols given in 4b and 4c can be used, if desired, to avoid creating the constants given in 3b and 3c.

- (a) *Evaluations.* For each  $\ell \geq 1$  there is a function symbol for the evaluation  $\text{Ev}_\ell$  of the constant  $f \in F_\ell$  in a  $k$ -uplet of integers. It is a symbol of the type  $F_\ell \times N^\ell \rightarrow N$ . We abbreviate  $\text{Ev}_\ell(f, x_1, \dots, x_\ell)$  to  $f(x_1, \dots, x_\ell)$ .
- (b) *Simple recurrence.* For  $k \geq 1$  we have a function symbol  $R_k$  for the element  $f \in F_k$  defined “by simple recurrence” from an element  $g \in F_{k-1}$  and an element  $h \in F_{k+1}$  (as in 3b, but here,  $f$ ,  $g$  and  $h$  are variables). It is a function symbol of the type  $F_{k-1} \times F_{k+1} \rightarrow F_k$ .
- (c) *Compositions.* For  $k \geq 1$  and  $\ell \geq 1$  we have a function symbol  $C_{\ell,k}$  for the “composition” of the element  $f \in F_\ell$  with  $\ell$  elements  $g_i \in F_k$ . It is a symbol of the type  $F_\ell \times F_k^\ell \rightarrow F_k$ . We abbreviate  $C_{\ell,k}(f, g_1, \dots, g_\ell)$  to  $f \circ (g_1, \dots, g_\ell)$  or  $f(g_1, \dots, g_\ell)$ . We can see  $\text{Ev}_\ell$  as the special case  $C_{\ell,0}$ .

## 5. The axioms are as follows.

- (a) The usual equality axioms for  $=_k$  relations.
- (b) A collapse axiom  $S(0) = 0 \vdash \perp$ . We note 1 rather than  $\underline{1}$  for  $S(0)$ .
- (c) The axioms that establish equalities linking constants and other function symbols. For example:

$$\begin{aligned} &\vdash_{f:F_k} f \circ (\pi_{k,1}, \dots, \pi_{k,k}) = f \\ &\vdash_{f_1, \dots, f_k:F_\ell} 0_k(f_1, \dots, f_k) = 0_\ell \\ &\vdash_{f_1, \dots, f_k:F_\ell} \pi_{k,i}(f_1, \dots, f_k) = f_i \\ \text{prod} &\vdash_{x,y:N} \text{prod} = R_2(0_1, \text{sum} \circ (\pi_{3,3}, \pi_{3,1})) \end{aligned}$$

The last rule gives the recurrence definition of the product (the constant  $\text{prod}$  in  $F_2$ ) from the addition (the constant  $\text{sum}$  in  $F_2$ ).

- (d) The axioms for the associativity of compositions, including the cases of evaluations. For example:

$$\begin{aligned} \text{asC}_{1,1,1} &\vdash_{f,g,h:F_1} f \circ (g \circ h) = (f \circ g) \circ h \\ \text{asC}_{1,1,0} &\vdash_{f,g:F_1;x:N} (f \circ g)(x) = f(g(x)) \\ \text{asC}_{2,1,1} &\vdash_{f:F_2;g_1,g_2,h_1,h_2:F_1} f \circ (g_1 \circ h_1, g_2 \circ h_2) = (f \circ (g_1, g_2)) \circ (h_1, h_2) \end{aligned}$$

<sup>13</sup>Note that  $\pi_{1,1}$  is the constant which designates the identity in  $F_1$ .

<sup>14</sup>For  $k = 2$  for example this could be the name  $R2(G, H)$  if  $G$  and  $H$  are names for  $g$  and  $h$ .

(e) The axioms for definitions by recurrence. For example,  $R_2$ :

$$\begin{aligned} \mathbf{Rec}_{2,\text{ini}} \quad f = R_2(g, h) &\vdash_{f:F_2;g:F_1;h:F_3} f \circ (\pi_{1,1}, 0_1) = g \\ \mathbf{Rec}_{2,\text{rec}} \quad f = R_2(g, h) &\vdash_{f:F_2;g:F_1;h:F_3} f \circ (\pi_{2,1}, S \circ \pi_{2,2}) = h \circ (\pi_{2,1}, \pi_{2,2}, f) \end{aligned}$$

(f) The axioms for proofs by induction (one for each arity). For example,  $\mathbf{REC}_2$ :

$$\mathbf{REC}_2 \quad \left. \begin{aligned} f_1 \circ (\pi_{1,1}, 0_1) &= f_2 \circ (\pi_{1,1}, 0_1), \\ f_1 \circ (\pi_{2,1}, S \circ \pi_{2,2}) &= h \circ (\pi_{2,1}, \pi_{2,2}, f_1), \\ f_2 \circ (\pi_{2,1}, S \circ \pi_{2,2}) &= h \circ (\pi_{2,1}, \pi_{2,2}, f_2) \end{aligned} \right\} \vdash_{f_1, f_2: F_2; h: F_3} f_1 = f_2$$

Note that in (e) the axioms assert that the map  $f = R_2(g, h)$  verifies the properties expected of a definition by recurrence, whereas in (f) the axiom asserts the uniqueness of the map verifying these properties.

Let's now look at how a usual proof by induction translates into the "language of maps" that we have set up. For example, the distributivity of multiplication over addition. In the usual proof, we prove the equality  $x \times (y + z) = (x \times y) + (x \times z)$  by induction on  $z$  as follows:

- *Initialisation.*

$$x \times (y + 0) \stackrel{1}{=} x \times y \stackrel{2}{=} (x \times y) + 0 \stackrel{3}{=} (x \times y) + (x \times 0)$$

with: 1 : initialisation of  $a + \cdot$ , 2 : initialisation of  $a \times \cdot$ , 3 : initialisation of  $a \times \cdot$ .

- *Induction.*

$$\begin{aligned} x \times (y + S(z)) &\stackrel{4}{=} x \times S(y + z) \stackrel{5}{=} (x \times (y + z)) + x \stackrel{6}{=} \\ ((x \times y) + (x \times z)) + x &\stackrel{7}{=} (x \times y) + ((x \times z) + x) \stackrel{8}{=} (x \times y) + (x \times S(z)) \end{aligned}$$

with 4 : induction of  $a + \cdot$ , 5, 8 : induction of  $a \times \cdot$ , 6 : induction hypothesis, 7 : associativity of  $+$  (demonstrated earlier),

Let's translate all this into the language of maps, for the elements of  $F_3$

$$f = \text{prod}(\pi_{3,1}, \text{sum}(\pi_{3,2}, \pi_{3,3})) \quad \text{and} \quad g = \text{sum}(\text{prod}(\pi_{3,1}, \pi_{3,2}), \text{prod}(\pi_{3,1}, \pi_{3,3})).$$

To validate  $f = g$ , we use the  $\mathbf{REC}_3$  principle. To do this, we validate the three hypotheses. First of all the initialisation, which is  $f(\pi_{2,1}, \pi_{2,2}, 0_1) = g(\pi_{2,1}, \pi_{2,2}, 0_1)$ .

- We have  $f(\pi_{2,1}, \pi_{2,2}, 0_1) = \text{prod}(\pi_{2,1}, \text{sum}(\pi_{2,2}, 0_1))$ . Since  $\text{sum}(\pi_{2,2}, 0_1) = \pi_{2,2}$  according to the initialisation in the recurrence definition of  $\text{sum}$ , we obtain

$$f(\pi_{2,1}, \pi_{2,2}, 0_1) = \text{prod}(\pi_{2,1}, \pi_{2,2}).$$

- We have  $g(\pi_{2,1}, \pi_{2,2}, 0_1) = \text{sum}(\text{prod}(\pi_{2,1}, \pi_{2,2}), \text{prod}(\pi_{2,1}, 0_1))$ . Since  $\text{prod}(\pi_{2,1}, 0_1) = 0_1$  from the recurrence definition of  $\text{prod}$ , we obtain

$$g(\pi_{2,1}, \pi_{2,2}, 0_1) = \text{sum}(\text{prod}(\pi_{2,1}, \pi_{2,2}), 0_1),$$

then  $g(\pi_{2,1}, \pi_{2,2}, 0_1) = \text{prod}(\pi_{2,1}, \pi_{2,2})$  from the recurrence definition of  $\text{sum}$ .

Next we need to validate the passage from  $n$  to  $S(n)$ , i.e. find a suitable element  $h \in F_4$ , i.e. satisfying the equalities

$$\begin{aligned} f(\pi_{3,1}, \pi_{3,2}, S(\pi_{3,3})) &= h(\pi_{3,1}, \pi_{3,2}, \pi_{3,3}, f) \\ g(\pi_{3,1}, \pi_{3,2}, S(\pi_{3,3})) &= h(\pi_{3,1}, \pi_{3,2}, \pi_{3,3}, g) \end{aligned}$$

- We have  $f(\pi_{3,1}, \pi_{3,2}, S(\pi_{3,3})) = \text{prod}(\pi_{3,1}, \text{sum}(\pi_{3,2}, S(\pi_{3,3})))$  which gives according to the induction in the definition by recurrence of sum

$$f(\pi_{3,1}, \pi_{3,2}, S(\pi_{3,3})) = \text{prod}(\pi_{3,1}, S(\text{sum}(\pi_{3,2}, \pi_{3,3}))),$$

then according to the recurrence definition of prod

$$f(\pi_{3,1}, \pi_{3,2}, S(\pi_{3,3})) = \text{sum}(\text{prod}(\pi_{3,1}, \text{sum}(\pi_{3,2}, \pi_{3,3})), \pi_{3,1}) = \text{sum}(f, \pi_{3,1}).$$

- In the same way (using the associativity of addition)

$$g(\pi_{3,1}, \pi_{3,2}, S(\pi_{3,3})) = \text{sum}(\text{sum}(\text{prod}(\pi_{3,1}, \pi_{3,2}), \text{prod}(\pi_{3,1}, \pi_{3,3})), \pi_{3,1}) = \text{sum}(g, \pi_{3,1}).$$

- We have therefore validated the hypotheses with the element  $h \in F_4$  defined by

$$h = h(\pi_{4,1}, \pi_{4,2}, \pi_{4,3}, \pi_{4,4}) := \text{sum}(\pi_{4,4}, \pi_{4,1}).$$

We call *PR $\mathcal{A}$*  the dynamical theory of primitive recursive arithmetic that we have just defined. This dynamical theory demonstrates exactly the same statements as the system developed by Goodstein.

## A.3. Conservative extensions of a dynamical theory

### Essentially equivalent extensions

**Definition A.3.1.** A dynamical theory  $\mathcal{T}'$  is said to be a *conservative extension of the theory  $\mathcal{T}$*  if it is an extension of  $\mathcal{T}$  and if the dynamical rules formulable in  $\mathcal{T}$  and valid in  $\mathcal{T}'$  are valid in  $\mathcal{T}$ .<sup>15</sup>

Two dynamical theories on the same language are said to be *identical* when they prove exactly the same dynamical rules. In other words, the axioms of one are valid dynamical rules in the other. Each is obviously a conservative extension of the other.

The simplest case of conservative extension when the language has grown is that of extensions which are essentially equivalent in the following meaning.

**Definition A.3.2.** An extension  $\mathcal{T}'$  de la dynamical theory  $\mathcal{T}$  is said *essentially equivalent* if it is obtained, up to renamings, by means of the following procedures, used iteratively, each time giving the appropriate axioms (see the details in [41, section 2.3]).

*Essentially identical* extensions are those which are obtained without adding new sorts.

- Add abbreviations.
- Addition of predicates expressing the conjunction or disjunction of already existing predicates. This amounts to accepting  $\wedge$  and  $\vee$  as logical symbols for constructing compound formulas, i.e. accepting a bit of intuitionist logic in the language.
- Add predicates translating a formula  $\exists xP$  where  $P$  is an existing predicate and  $x$  is a variable. Same comment as for the previous point.
- Add a function symbol when a unique existence is valid under certain hypotheses.
- Add a sort that is the product of several sorts.
- Add a sort that is the disjoint union of several sorts.
- Add a subsort of an existing sort, defined as the elements satisfying an existing predicate.

---

<sup>15</sup>The reciprocal is clear.

- Add a quotient sort of an already existing sort, defined by a binary predicate, which is provably an equivalence relation, and which defines the new equality in the quotient sort.
- Add a sort whose objects are (certain) morphisms of one sort into another that shares some algebraic structure with the first.

An essentially equivalent extension is intuitively equivalent in the following meaning.

**Informal definition A.3.3.** Consider a dynamical theory  $\mathcal{T}$  and an extension  $\mathcal{T}'$  of  $\mathcal{T}$ . We say that  $\mathcal{T}'$  is an *intuitively equivalent* extension of  $\mathcal{T}$  if the following three properties are verified.

1.  $\mathcal{T}'$  is a conservative extension of  $\mathcal{T}$ .
2. Any dynamical rule formulated in the language of  $\mathcal{T}'$  is equivalent<sup>16</sup> to a family of dynamical rules formulated in the language of  $\mathcal{T}$ .
2. For any presentation  $(G, R)$  in the language of  $\mathcal{T}$ , the dynamic algebraic structures  $\mathbf{A} = ((G, R), \mathcal{T})$  and  $\mathcal{T}'(\mathbf{A}) := ((G, R), \mathcal{T}')$  have the same models (in constructive mathematics as in classical mathematics).

In the rest of this section we give two very important cases of conservative extensions (Theorems A.3.6 and A.3.8), relating to the use of classical logic, which do not fall into the previous simple case. Before that, we give Theorem A.3.4 relating to the use of constructive (intuitionistic) logic.

## Comparison with intuitionistic logic

Dynamical theories can be considered to be nothing more than truncated versions of intuitionistic natural deduction, in which neither the  $\Rightarrow$  connector nor the  $\forall$  quantifier is introduced.

This is precisely the strength of dynamical theories: not being encumbered with “complicated” formulas such as  $(A \Rightarrow B) \Rightarrow C$ , or  $\forall x \exists y \forall z \dots$ , makes it possible to see things more clearly and to simplify a certain number of non-trivial results, when they can be demonstrated at the basic level of natural deduction, i.e. with the “logic-free” system of dynamic proofs.

**Theorem A.3.4** (conservativity of intuitionistic logic with respect to dynamic proofs). *Consider a finitary dynamical theory  $\mathcal{T}$ . If a consistent formula on the language of  $\mathcal{T}$  is proved using the axioms of  $\mathcal{T}$  and intuitionistic logic, the corresponding dynamical rule can be proved valid directly in the dynamical theory  $\mathcal{T}$ .*

*Proof.* See [11, Coquand, 2005]. □

Thierry Coquand intuitively interprets the proof as the construction of a certain type of model (a *generic model*) of the dynamic algebraic structure under consideration. The proof in [11] is more direct and more intuitive than that of the slightly stronger conservativity result given in Theorem A.3.6.

## Fundamental theorem of dynamical theories

To a dynamical theory  $\mathcal{T}$  corresponds a coherent theory, or finitary geometric theory, obtained by replacing the dynamical rules by the corresponding formulas according to the scheme given on page 12 at the beginning of Section A.1. This coherent theory can be treated according to classical logic or intuitionistic logic. Let us note  $\mathcal{T}^c$  and  $\mathcal{T}^i$  respectively.

We have the fundamental theorem A.3.6 below (cf. for example Theorem 1 in [17]). This theorem is already given for purely equational theories in [55, Prawitz, 1971], and this kind of result is omnipresent in the contemporary literature, in more or less varied forms. We recommend the recent progress on this theme described in [23, 22] which shows that, properly treated, classical

<sup>16</sup>The equivalence in question is an external rule, like the structural rules described above. It may depend on the logic used in the external world.

proofs do not provide significantly longer constructive proofs. The proof in [17] is constructive and relatively intuitive, but leads to an explosion in the size of proofs.

It is based on the following lemma which explains the harmlessness, in certain circumstances, of the rule **LEM** of excluded thirds.

**Lemma A.3.5** (elimination of classical negation).

Let  $\mathcal{T}$  be a finitary dynamical theory, and  $P(.,.)$  be a predicate forming part of the signature (we have taken it here of arity 2 by way of example). Let us introduce “the predicate opposed to  $P$ ”, let us note it  $Q(.,.)$ , with the two dynamical rules which define it in classical mathematics:<sup>17</sup>

$$\text{In-non}_P \vdash P(x, y) \quad \text{op} \quad Q(x, y) \qquad \text{El-non}_P \quad P(x, y), Q(x, y) \vdash \perp$$

Then, the new dynamical theory is a conservative extension of  $\mathcal{T}$ .

Note that this time some constructive models of the first theory may no longer be constructive models of the second. Nevertheless, this is not too serious, as the lemma indicates, and is generalised in the following fundamental theorem.

**Theorem A.3.6** (elimination of cuts).

As far as finitary dynamical theories are concerned, logic, including classical logic (and in particular the **LEM**) only serves to shorten proofs. More precisely a dynamical rule is valid in a dynamical theory  $\mathcal{T}$  if, and only if, it is valid in the corresponding classical coherent theory (the one with the same signature and axioms as  $\mathcal{T}$ ): connectors, quantifiers and classical first-order logic are used in the coherent theory.

*Remark A.3.7.* The preceding theorem, and the following one concerning skolemisation, show that the use of dynamical theories allows Hilbert’s programme to be partly realised, by providing a constructive semantics for certain uses of **LEM** and the axiom of choice. ■

## Skolemisation

We now look at the general process of skolemisation, which consists of getting rid of the  $\exists$  in some valid rules of a dynamical theory by replacing the existing  $\exists$  with functions symbols.

We have already indicated the case where this operation is harmless, according to the following informal remark: when the existent in a valid rule is provably unique, it doesn’t hurt to replace the dummy variable which designates the existent by a function symbol.

On the other hand, replacing the dummy variable that designates the existent with a function symbol when the existent is not provably unique is more problematic. This is called skolemisation. Some constructive models before skolemisation may no longer be suitable after skolemisation, and the new theory may no longer have any known constructive model. And even in classical mathematics, if the models are “almost” the same, it is on condition that the axiom of choice is assumed.

**Theorem A.3.8** (skolemisation). Consider a dynamical theory  $\mathcal{T}$ . We denote  $\mathcal{T}'$  the “skolemised” theory, where we have skolemised all the existential axioms by replacing the  $\exists$  with the introduction of function symbols. Then  $\mathcal{T}'$  is a conservative extension of  $\mathcal{T}$ .

*Proof.* A proof in classical mathematics using an axiom of choice consists in noting that the two theories have “the same models”. A syntactic and constructive proof is given in [7, Bezem & Coquand, 2019]. □

<sup>17</sup>The definition of the predicate opposed to a predicate  $P$  in constructive mathematics is not the same, and it cannot be treated in the framework of dynamical theories, except in the case where the predicate is decidable. The constructive meaning of  $P$  is  $P \Rightarrow \perp$  and the constructive implication cannot be treated by the dynamical method alone.



## A.4. Distributive lattices and spectral spaces associated with a dynamic algebraic structure

For this section, we refer to [CACM, Chapters XI and XIII] [41, sections 1 and 3]

### Distributive lattices and entailment relations

A particularly important rule for distributive lattices, called *cut*, is the following

$$\text{if } x \wedge a \leq b \text{ and } a \leq x \vee b \text{ then } a \leq b. \quad (\text{A.3})$$

If  $A \in \text{P}_{\text{fe}}(\mathbf{T})$  (set of finitely enumerated parts of  $\mathbf{T}$ ) we will note

$$\bigvee A := \bigvee_{x \in A} x \quad \text{and} \quad \bigwedge A := \bigwedge_{x \in A} x.$$

We denote  $A \vdash B$  or  $A \vdash_{\mathbf{T}} B$  the relation defined as follows on the set  $\text{P}_{\text{fe}}(\mathbf{T})$ :

$$A \vdash B \stackrel{\text{d\u00e9f}}{\iff} \bigwedge A \leq \bigvee B.$$

This relationship verifies the following axioms, in which we write  $x$  for  $\{x\}$  and  $A, B$  for  $A \cup B$ .

$$\begin{aligned} x \vdash x & \quad (R) \\ \text{if } A \vdash B \text{ then } A, A' \vdash B, B' & \quad (M) \\ \text{if } (A, x \vdash B) \text{ and } (A \vdash B, x) \text{ then } A \vdash B & \quad (T). \end{aligned}$$

The relationship is said to be *reflexive*, *monotonic* and *transitive*. The third rule (transitivity) can be seen as a rewriting of the rule (A.3) and is also called the *cut* rule.

**Definition A.4.1.** For an arbitrary set  $S$ , a binary relation on  $\text{P}_{\text{fe}}(S)$  which is reflexive, monotonic and transitive is called an *entailment relation*.

The following theorem is fundamental. It states that the three properties of entailment relations are exactly what is needed for the interpretation of an entailment relation as the trace of that of a distributive lattice to be adequate.

**Theorem A.4.2** (fundamental theorem of entailment relations). [46, Satz 7], [10], [ACMC, XI-5.3]. *Let  $S$  be a set with an entailment relation  $\vdash_S$  on  $\text{P}_{\text{fe}}(S)$ . Consider the distributive lattice  $\mathbf{T}$  defined by generators and relations as follows: the generators are the elements of  $S$  and the relations are the*

$$A \vdash_{\mathbf{T}} B$$

*each time  $A \vdash_S B$ . Then, for all  $A, B$  in  $\text{P}_{\text{fe}}(S)$ , we have*

$$\text{if } A \vdash_{\mathbf{T}} B \text{ then } A \vdash_S B.$$

*In particular, two elements  $x$  and  $y$  of  $S$  define the same element of  $\mathbf{T}$  if, and only if, we have  $x \vdash_S y$  and  $y \vdash_S x$ .*

### The spectrum of a distributive lattice

In classical mathematics a *prime ideal*  $\mathfrak{p}$  of a distributive lattice  $\mathbf{T} \neq \mathbf{1}$  is an ideal whose complementary  $\mathfrak{v}$  is a filter (which is then a *prime filter*). We then have  $\mathbf{T}/(\mathfrak{p} = 0, \mathfrak{v} = 1) \simeq \mathbf{2}$ . It is the same to give a prime ideal of  $\mathbf{T}$  or a morphism of distributive lattices  $\mathbf{T} \rightarrow \mathbf{2}$ .

It is easy to check that if  $S$  is a generating part of the distributive lattice  $\mathbf{T}$ , a prime ideal  $\mathfrak{p}$  of  $\mathbf{T}$  is completely characterised by its trace on  $S$  (cf. [10]).

**Definition A.4.3.** The *spectrum* of a distributive lattice  $\mathbf{T}$  is the set  $\text{Spec } \mathbf{T}$  of its prime ideals, with the following topology: a basis of opens is given by the

$$D_{\mathfrak{T}}(a) \stackrel{\text{d\u00e9f}}{=} \{ \mathfrak{p} \in \text{Spec } \mathfrak{T} \mid a \notin \mathfrak{p} \}, \quad a \in \mathbf{T}.$$

Classical mathematics verifies that

$$\left. \begin{aligned} D_{\mathbf{T}}(a \wedge b) &= D_{\mathbf{T}}(a) \cap D_{\mathbf{T}}(b), & D_{\mathbf{T}}(0) &= \emptyset, \\ D_{\mathbf{T}}(a \vee b) &= D_{\mathbf{T}}(a) \cup D_{\mathbf{T}}(b), & D_{\mathbf{T}}(1) &= \text{Spec } \mathbf{T}. \end{aligned} \right\} \quad (\text{A.4})$$

The complementary of  $D_{\mathbf{T}}(a)$  is a closed set which we denote  $\mathfrak{V}_{\mathbf{T}}(a)$ .

The notation  $\mathfrak{V}_{\mathbf{T}}(a)$  is extended as follows: if  $I \subseteq \mathbf{T}$ , then  $\mathfrak{V}_{\mathbf{T}}(I) \stackrel{\text{d\u00e9f}}{=} \bigcap_{x \in I} \mathfrak{V}_{\mathbf{T}}(x)$ . If  $I$  generates the ideal  $\mathfrak{J}$ , then  $\mathfrak{V}_{\mathbf{T}}(I) = \mathfrak{V}_{\mathbf{T}}(\mathfrak{J})$ . It is sometimes said that  $\mathfrak{V}_{\mathbf{T}}(I)$  is *the variety associated with  $I$* .

**Definition A.4.4.** A topological space homeomorphic to a space  $\text{Spec}(\mathbf{T})$  is called a *spectral space*.

The spectral spaces come from the study [68, Stone, 1937].

[Johnstone] calls these spaces *coherent spaces*. [Balbes & Dwinger] calls them *Stone spaces*. This terminology is obsolete, because since [Johnstone] Stone spaces are the spectral spaces associated with distributive lattices which are Boolean algebras.

The name *spectral space* was given by [28, Hochster, 1969], who popularised them in the mathematical community after a prolonged hibernation since 1937.

With classical logic and the axiom of choice, the space  $\text{Spec}(\mathbf{T})$  has “enough points”: we can find the lattice  $\mathbf{T}$  from its spectrum.

A point  $\mathfrak{p}$  in a spectral space  $X$  is said to be the *generic point of the closed set  $F$*  if  $F = \overline{\{\mathfrak{p}\}}$ . This point (when it exists) is necessarily unique because spectral spaces are Kolmogoroff spaces. In fact, the  $\overline{\{\mathfrak{p}\}}$  closed sets are exactly all the irreducible closed sets of  $X$ . The order relation  $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$  will be denoted  $\mathfrak{p} \leq_X \mathfrak{q}$ , and we have the equivalences

$$\mathfrak{p} \leq_X \mathfrak{q} \iff \overline{\{\mathfrak{q}\}} \subseteq \overline{\{\mathfrak{p}\}}. \quad (\text{A.5})$$

The closed points of  $\text{Spec}(\mathbf{T})$  are the maximal ideals of  $\mathbf{T}$ . When  $X = \text{Spec}(\mathbf{T})$  the relation  $\mathfrak{p} \leq_X \mathfrak{q}$  is simply the usual inclusion relation  $\mathfrak{p} \subseteq \mathfrak{q}$  between prime ideals of the distributive lattice  $\mathbf{T}$ .

In the category of spectral spaces we define *spectral morphisms* as maps such that the reciprocal image of any quasi-compact open is a quasi-compact open (in particular they are continuous).

## Stone’s antiequivalence

Stone’s antiequivalence asserts (in modern language) that in classical mathematics the category of distributive lattices is antiequivalent to the category of spectral spaces.

Although spectral spaces have invaded contemporary abstract algebra, it is only in constructive mathematics that this anti-equivalence of classical mathematics is given the attention it deserves.

The aim is to correctly define the distributive lattices corresponding to the spectral spaces in the classical literature, and, if possible, to decipher the classical discourses using spectral spaces into constructive discourses concerning the corresponding distributional lattices.

## The Zariski lattice and spectrum of a commutative ring

The Zariski lattice of a commutative ring can be obtained from rules valid in different extensions of the theory  $\mathcal{A}\mathcal{C}$  of commutative rings.

We choose the theory of local rings because of their fundamental role in Grothendieck schemes.

We consider precisely a dynamical theory of *local rings with units*  $\mathcal{A}\mathcal{L}\mathcal{I}$ , based on the signature

$$\Sigma_{\mathcal{A}\mathcal{L}\mathcal{I}} = (\cdot = 0, U(\cdot); \cdot + \cdot, \cdot \times \cdot, - \cdot, 0, 1).$$

This theory is an extension of the theory of commutative rings. A predicate  $U(x)$  is defined as the invertibility predicate by means of the two suitable axioms. We add the collapse axiom  $\mathbf{CL}_{\mathcal{A}\mathcal{L}\mathcal{I}}$  and the actual axiom of local rings  $\mathbf{AL}$ .

$$\mathbf{CL}_{\mathcal{A}\mathcal{L}\mathcal{I}} \quad U(0) \vdash \perp$$

$$\mathbf{AL} \quad U(x + y) \vdash U(x) \text{ op } U(y)$$

Let  $\mathbf{A}$  be a commutative ring. Consider the entailment relation  $\vdash_{\mathbf{A}, \text{Zar}}$  on the set underlying  $\mathbf{A}$  defined by the following equivalence

$$\begin{array}{ccc} a_1, \dots, a_n \vdash_{\mathbf{A}, \text{Zar}} c_1, \dots, c_m & \stackrel{\text{d\u00e9f}}{\iff} & \\ U(a_1), \dots, U(a_n) \vdash_{\mathcal{A}l(\mathbf{A})} U(c_1) \text{ op } \dots \text{ op } U(c_m) & & \end{array} \quad (\text{A.6})$$

We define the *Zariski lattice of  $\mathbf{A}$* , denoted  $\text{Zar } \mathbf{A}$  or  $\text{Zar}(\mathbf{A})$ , as the distributive lattice generated by the entailment relation  $\vdash_{\mathbf{A}, \text{Zar}}$ .

The corresponding map  $D_{\mathbf{A}} : \mathbf{A} \rightarrow \text{Zar } \mathbf{A}$  is called the *Zariski support of  $\mathbf{A}$* . When  $\mathbf{A}$  is fixed by the context we simply note  $D$ .

The usual *Zariski spectrum* is the dual spectral space of this distributive lattice.

Note that since  $D(a_1) \wedge \dots \wedge D(a_n) = D(a_1 \cdots a_n)$ , the elements of  $\text{Zar } \mathbf{A}$  are all of the form  $D(c_1, \dots, c_m) := D(c_1) \vee \dots \vee D(c_m)$ .

We have the following equivalences. Equivalence between (1) and (2) essentially copies the definition of  $\text{Zar } \mathbf{A}$ . The equivalence with (3) is the subject of a *formal Nullstellensatz*. The Hilbert Nullstellensatz itself is a more difficult result.

**Theorem A.4.5** (Nullstellensatz formel).

Let  $\mathbf{A}$  be a commutative ring, et  $a_1, \dots, a_n, c_1, \dots, c_m \in \mathbf{A}$ . T.F.A.E.

- (1)  $D(a_1), \dots, D(a_n) \vdash_{\text{Zar } \mathbf{A}} D(c_1), \dots, D(c_m)$
- (2)  $U(a_1), \dots, U(a_n) \vdash_{\mathcal{A}l(\mathbf{A})} U(c_1) \text{ op } \dots \text{ op } U(c_m)$
- (3)  $\exists k > 0 \ (a_1 \cdots a_n)^k \in \langle c_1, \dots, c_m \rangle$

We can therefore identify the element  $D(c_1, \dots, c_m)$  of  $\text{Zar } \mathbf{A}$  with the ideal  $\sqrt{\langle c_1, \dots, c_m \rangle}$ . Modulo this identification, the order relation is the inclusion relation.

**Corollary A.4.6.** *The lattice  $\text{Zar } \mathbf{A}$  is generated by the smallest entailment relation on (the set underlying to)  $\mathbf{A}$  satisfying the following relations.*

- $0 \vdash 0_{\mathbf{T}}$
- $1 \vdash 1_{\mathbf{T}}$
- $ab \vdash a$
- $a, b \vdash ab$
- $a + b \vdash a, b$

In other words, the map  $D : \mathbf{A} \rightarrow \text{Zar } \mathbf{A}$  satisfies the relations

$$D(0) = 0, \ D(1) = 1, \ D(ab) = D(a) \wedge D(b), \ D(a + b) \leq D(a) \vee D(b),$$

and any other map  $D' : \mathbf{A} \rightarrow T$  which satisfies these relations factorises via  $\text{Zar } \mathbf{A}$  with a unique morphism of distributive lattices  $\text{Zar } \mathbf{A} \rightarrow T$ .

## Other examples

Remember that a disjunctive rule is a dynamical rule without the  $\exists$  symbol, and that a simple disjunctive rule is a dynamical rule of the following form, with  $m, n \geq 0$ .

$$C_1, \dots, C_n \vdash D_1 \text{ op } \dots \text{ op } D_m \quad (\text{A.7})$$

where  $C_i$ 's and  $D_j$ 's are atomic formulas. (Simple) Horn rules are special cases of (simple) disjunctive rules.

• **First example.** Consider a dynamic algebraic structure  $\mathbf{A} = ((G, R), \mathcal{T})$  for a dynamical theory  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ . If  $P(x, y)$  is a binary predicate in the signature, and if  $Tcl = Tcl(\mathbf{A})$  is the set of closed terms of  $\mathbf{A}$ , we obtain an entailment relation  $\vdash_{\mathbf{A}, P}$  on  $Tcl \times Tcl$  by defining

$$\begin{aligned} (a_1, b_1), \dots, (a_n, b_n) \vdash_{\mathbf{A}, P} (c_1, d_1), \dots, (c_m, d_m) & \stackrel{\text{d\u00e9f}}{\iff} \\ P(a_1, b_1), \dots, P(a_n, b_n) \vdash_{\mathbf{A}} P(c_1, d_1) \text{ op } \dots \text{ op } P(c_m, d_m) & \end{aligned} \quad (\text{A.8})$$

Intuitively, the distributive lattice generated by this entailment relation is the lattice of the “truth values” of the predicate  $P$  in the dynamic algebraic structure  $\mathbf{A}$ .

• **More generally** Consider a dynamic algebraic structure  $\mathbf{A} = ((G, R), \mathcal{T})$  for a dynamical theory  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ . Let  $S$  be a set of closed atomic formulas of  $\mathbf{A}$ . We define *the entailment relation on  $S$  associated with  $\mathbf{A}$*  as follows:

$$\begin{aligned} A_1, \dots, A_n \vdash_{\mathbf{A}, S} B_1, \dots, B_m & \stackrel{\text{d\u00e9f}}{\iff} \\ A_1, \dots, A_n \vdash_{\mathbf{A}} B_1 \text{ op } \dots \text{ op } B_m & \end{aligned} \quad (\text{A.9})$$

We can denote  $\text{Zar}(\mathbf{A}, S)$  the distributive lattice generated by this entailment relation.

In particular, the lattice  $\text{Zar}(\mathbf{A}, \text{Atcl}(\mathbf{A}))$  is called the *absolute Zariski lattice of the dynamic algebraic structure  $\mathbf{A}$* .

• **Case of an extension  $\mathcal{T}_1$  which reflects valid disjunctive rules.** Let  $\mathcal{T}_1$  be an extension of a dynamical theory  $\mathcal{T}$  which proves exactly the same disjunctive rules (for example a conservative extension). Let  $\mathbf{A} = ((G, R), \mathcal{T})$  and  $\mathbf{A}_1 = ((G, R), \mathcal{T}_1)$ . Let  $S$  be a set of closed atomic formulas of  $\mathbf{A}$ . Then the Zariski lattices  $\text{Zar}(\mathbf{A}, S)$  and  $\text{Zar}(\mathbf{A}_1, S)$  are isomorphic.

In particular, when  $\mathcal{T}_1$  is an essentially equivalent extension of  $\mathcal{T}$  the absolute Zariski lattices of  $\mathbf{A}$  and  $\mathbf{A}_1$  are isomorphic.

• **Zariski lattices, however, give a lesser image** of a dynamic algebraic structure. On the one hand, in these Zariski lattices nothing is taken into account a priori that corresponds to valid dynamical rules when they are not disjunctive. On the other hand, adding classical logic and skolemising a dynamical theory do not change the lattices corresponding to  $\text{Atcl}(\mathbf{A})$ , but in this case, the absolute Zariski lattice of  $\mathbf{A}_1$  is the Boolean algebra generated by  $\text{Zar}(\mathbf{A}, \text{Atcl}(\mathbf{A}))$ . To rediscover the richness of dynamical theories seen from a constructive point of view, it is necessary to call upon the theory of bundles or topos.

## A.5. Model theory

### Completeness theorem, simultaneous collapse

First of all, here is the completeness theorem in its minimal form: its intuitive interpretation in classical mathematics is that classical logic gives exhaustive rules for reasoning in accordance with “absolute truth”, based on an ideal mathematical universe in which no doubt is ever allowed, **LEM** is absolutely true and the axiom of choice just the same.

**Theorem\* A.5.1** (G\u00f6del’s completeness theorem, first form).

*A dynamic algebraic structure that does not collapse admits a non-trivial model.*

*Comment.* An equivalent form of the completeness theorem is the following special case (Krull’s lemma): *any non-trivial commutative ring has a non-trivial integral quotient.*

The constructively acceptable form of Krull’s lemma is the following easy result: *when we add the dynamical rule “ $xy = 0 \vdash x = 0 \text{ op } y = 0$ ” to the theory of commutative rings, a dynamical algebraic structure collapses in the former theory if, and only if, it collapses in the latter.*

In other words, the theories  $\mathcal{A}c$  and  $\mathcal{A}sz$  collapse simultaneously. ■

**Theorem\* A.5.2** (G\u00f6del’s completeness theorem, second form).

*Consider a dynamical theory  $\mathcal{T}$  and a dynamic algebraic structure  $\mathbf{A}$  of type  $\mathcal{T}$ . A fact is valid in  $\mathbf{A}$  if, and only if, it is satisfied in all models of  $\mathbf{A}$ .*

A dynamical theory that extends another (by adding sorts and/or predicates and/or axioms) proves *a priori* more results. An interesting case is when it proves the same results while offering greater facilities for proofs. This was the essence of the fundamental theorems A.3.6 and A.3.8. A variant in model theory, but only in classical mathematics, is given by the following theorems.

**Theorem\* A.5.3** (simultaneous collapses and non-trivial models). *Let  $\mathcal{T}$  be a dynamical theory and  $\mathcal{T}'$  an extension which collapses simultaneously with  $\mathcal{T}$ . If a dynamic algebraic structure of type  $\mathcal{T}$  admits a non-trivial model, it also admits a non-trivial model as a dynamic algebraic structure of type  $\mathcal{T}'$ . More precisely, if  $M$  is a non-trivial model of  $\mathcal{T}$ , the dynamic algebraic structure  $(\text{Diag}(M), \mathcal{T}')$  admits a non-trivial model.*

*Comment.* A good constructive version of the completeness theorem is a pure tautology: if a dynamic algebraic structure does not collapse, then ... it does not collapse. Or again: if a first-order formal theory doesn't collapse, then ... it doesn't collapse. And for Theorem A.5.3: if  $\mathcal{T}$  and  $\mathcal{T}'$  collapse simultaneously, then ... they collapse simultaneously. The same would apply to Theorems A.5.2 and A.5.4.

Indeed, what we call a constructive version of a “doubtful” classical theorem is a statement, correct in constructive mathematics, which, in practice, i.e. to demonstrate concrete results, provides the same services as the classical theorem. Indeed, in practice, all these “abstract” theorems are only used, to arrive at concrete results, only in reasoning by the absurd, which uses fictitious models to conclude that they cannot exist. The concrete result, on the other hand, is much closer to the hypothesis of the abstract theorem that has been invoked. A detailed analysis of the whole proof then generally shows that one has tautologised in circles without realising it (see for example [35] for Hilbert's 17th problem). This is one of the reasons why classical mathematics is so often constructive, contrary to the appearance given by its demonstrations. ■

## Representation theorem, theories proving the same Horn rules

**Theorem\* A.5.4** (representation theorem). *Consider a dynamical theory  $\mathcal{T}'$  which extends a Horn theory  $\mathcal{T}$  and proves the same Horn rules. Any algebraic structure of type  $\tau$  is a subdirect product of algebraic structures of type  $\tau'$*

For example  $\mathcal{T}$  is the theory of  $\ell$ -groups and  $\mathcal{T}'$  is the theory of linearly ordered abelian groups. The important and constructive result is that these two theories prove the same Horn rules. The intuitive interpretation in classical mathematics is that every lattice group is a lattice subgroup of a product of linearly ordered groups. When Paul Lorenzen proved this result, he generalised Krull's analogous result that the integral closure of an integral ring  $\mathbf{A}$  is the intersection of the valuation rings of its fraction field that contain  $\mathbf{A}$ .

The following intuitive theorems, which will be useful to us, concern extensions which prove the same Horn rules; they are proved in [39].

**Theorem A.5.5.** *Let  $\mathcal{T}_2$  be a dynamical theory which is a simple extension of a  $\mathcal{T}_1$  theory and which proves the same Horn rules. Consider an essentially equivalent extension  $\mathcal{T}'_1$  of  $\mathcal{T}_1$  obtained without the addition of existential predicates. We assume that there is no syntactic interference at the level of language extensions between  $\mathcal{T}'_1$  and  $\mathcal{T}_2$ . We can therefore construct an essentially equivalent extension  $\mathcal{T}'_2$  of  $\mathcal{T}_2$  by copying for  $\mathcal{T}_2$  what was done for  $\mathcal{T}_1$ . In these conditions,  $\mathcal{T}'_2$  proves the same Horn rules as  $\mathcal{T}'_1$ .*

**Theorem A.5.6.** *Let  $\mathcal{T}_2$  be a dynamical theory which is a simple extension of a  $\mathcal{T}_1$  theory and which proves the same Horn rules. Consider an extension  $\mathcal{T}'_1$  of  $\mathcal{T}_1$  obtained by adding a family of axioms which are all Horn rules. Consider the extension  $\mathcal{T}'_2$  of  $\mathcal{T}_2$  obtained by adding the same axioms. Under these conditions,  $\mathcal{T}'_2$  proves the same Horn rules as  $\mathcal{T}'_1$ .*

# B. Infinitary geometric theories

## Sommaire

---

<b>B.1 General</b> . . . . .	<b>35</b>
Example: nilpotent elements, Krull dimension . . . . .	35
<b>B.2 Barr’s Theorem</b> . . . . .	<b>37</b>
An infinitary geometric theory for primitive recursive arithmetic . . . . .	37
Conclusion . . . . .	38

---

## B.1. General

A very useful general notion of geometric theory is defined, which is not necessarily expressed in finitary terms. This is known as *infinitary geometric theory*. In an infinitary geometric theory, we allow dynamical rules that have an infinite disjunction in the second member. There is one essential restriction: the free variables present in such a disjunction must be specified in advance and in finite number.

Intuitively, we use such rules in the proof system of dynamical theories by “opening the branches of calculation corresponding to the infinite disjunction”. What does this mean precisely? It means that a conclusion will be declared valid if it is valid in each of the branches.

Let’s take a simple example, and show what happens if we have in the axioms an infinitary rule of the type

$$\vdash_{x_1, \dots, x_k} \text{OP}_{i \in I} \Gamma_i$$

with an infinite set  $I$  and the  $\Gamma_i$  are lists of atomic formulas with no free variables other than those mentioned (i.e.  $x_1, \dots, x_k$ ). If for each  $i \in I$  we have a valid rule  $\Gamma_i \vdash B(\underline{x})$ , then we declare the rule  $\vdash_{x_1, \dots, x_k} B(\underline{x})$  to be valid.

There is therefore necessarily an intuitive proof external to the dynamical theory to certify that the desired conclusion is valid in each of the branches. Indeed, the system of calculation “without logic” at work in the dynamical theory cannot handle such an infinity of deductions. A purely mechanical calculus cannot open up an infinite number of branches! For example, with  $I = \mathbb{N}$  the external intuitive proof could be a proof by induction.

Note, on the other hand, that the internal proof must show the validity of the desired conclusion according to the deduction rules “without logic” of the dynamical theory.

The above presentation is only a sketch. All this deserves a more formal definition of what is the legal functioning of an infinitary geometric theory; even if there is an unavoidable informal aspect in the recourse to “external” proofs in intuitive mathematics.

We should also say a few words about the operation of the formal intuitionist and classical theories that extend the infinite dynamical theory (by adding the  $\Rightarrow$  connector and the universal quantifier in the intuitionist case, and by adding **LEM** in the classical case).

As in the case of finitary geometric theories, we will reserve the name of dynamical theory for proofs whose internal part is “without logic”.

### Example: nilpotent elements, Krull dimension

An element  $x$  of a ring is nilpotent if there exists an  $n \in \mathbb{N}^+$  such that  $x^n = 0$ . If we introduce a predicate  $Z(x)$  for “ $x$  is nilpotent”, it will be subject to the natural axioms

$$\mathbf{nil1} \quad \vdash Z(0)$$

$$\mathbf{nil2} \quad Z(x), Z(y) \vdash Z(x + y)$$

$$\mathbf{NIL1} \quad Z(x) \vdash \exists z z(1 + x) = 1$$

$$\mathbf{nil3} \quad Z(x) \vdash Z(xy)$$

$$\mathbf{Nil} \quad Z(x^2) \vdash Z(x)$$

In the corresponding dynamical theory, the only  $t$  terms for which we will be able to demonstrate  $Z(t)$  will be those for which we will be able to demonstrate  $t^n = 0$  for a  $n > 0$ . However, there is no guarantee that in a model of the theory, the predicate  $Z(x)$  corresponds to “ $x$  is nilpotent”.

The only way to be sure is to introduce the infinitary dynamical rule

$$\mathbf{NIL} \quad Z(x) \vdash \mathbf{OP}_{n \in \mathbb{N}^+} x^n = 0$$

This concern is directly related to the Krull dimension of commutative rings. The Krull dimension of a distributive lattice can be formulated in a dynamical theory as follows.

#### Definition B.1.1.

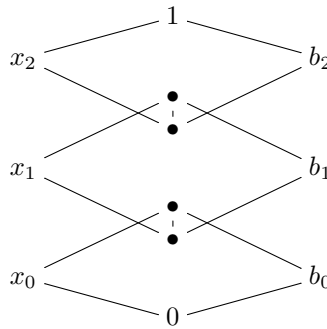
1. Two sequences  $(x_0, \dots, x_n)$  and  $(b_0, \dots, b_n)$  in a distributive lattice  $\mathbf{T}$  are said to be *complementary* if

$$\left. \begin{array}{l} b_0 \wedge x_0 = 0 \\ b_1 \wedge x_1 \leq b_0 \vee x_0 \\ \vdots \quad \vdots \quad \vdots \\ b_n \wedge x_n \leq b_{n-1} \vee x_{n-1} \\ 1 = b_n \vee x_n \end{array} \right\} \quad (\text{B.1})$$

A sequence which has a complementary sequence is said to be *singular*.

2. For  $n \geq 0$  we will say that the distributive lattice  $\mathbf{T}$  is of *Krull dimension*  $\leq n$  if any sequence  $(x_0, \dots, x_n)$  in  $\mathbf{T}$  is singular. Furthermore, the distributive lattice  $\mathbf{T}$  is of Krull dimension  $-1$  if it is trivial, i.e. if  $1_{\mathbf{T}} = 0_{\mathbf{T}}$ .

For example, for  $n = 2$  the equalities and inequalities (B.1) correspond to the following drawing in  $\mathbf{T}$ .



And the dimension  $\leq 2$  corresponds to the following existential axiom.

$$\mathbf{KDIM2} \quad \vdash \exists b_0, b_1, b_2 (x_2 \vee b_2 = 1, x_2 \wedge b_2 \leq x_1 \vee b_1, x_1 \wedge b_1 \leq x_0 \vee b_0, x_0 \wedge b_0 = 0)$$

For the Krull dimension of rings, we need to involve the distributive lattice formed by the radicals of finitely generated ideals and we express for example the dimension  $\leq 2$  as follows, noting  $D_{\mathbf{A}}(x, y) = \sqrt{\langle x, y \rangle} = \{ z \in \mathbf{A} \mid \exists n \in \mathbb{N}^+, z^n \in \langle x, y \rangle \}$ :

For all  $x_0, x_1, x_2 \in \mathbf{A}$  there exist  $b_0, b_1, b_2 \in \mathbf{A}$  such that

$$\left. \begin{aligned} D_{\mathbf{A}}(b_0x_0) &= D_{\mathbf{A}}(0) \\ D_{\mathbf{A}}(b_1x_1) &\subseteq D_{\mathbf{A}}(b_0, x_0) \\ D_{\mathbf{A}}(b_2x_2) &\subseteq D_{\mathbf{A}}(b_1, x_1) \\ D_{\mathbf{A}}(1) &= D_{\mathbf{A}}(b_2, x_2) \end{aligned} \right\} \quad (\text{B.2})$$

Note that  $D_{\mathbf{A}}(b_2x_2) \subseteq D_{\mathbf{A}}(b_1, x_1)$  means that there exist  $a_1, y_1 \in \mathbf{A}$  and  $n \in \mathbb{N}^+$  such that

$$(b_2x_2)^n = a_1b_1 + y_1x_1.$$

We can therefore express “ $\text{Kdim } \mathbf{A} \leq 2$ ” in the context of an infinitary geometric theory. And for example the theorems of Serre or Foster-Swan ([CACM, Chapter XIV]) with the Krull dimension as an assumption can be treated entirely within the framework of geometric theories ([12]).

## B.2. Barr's Theorem

The fundamental theorem of dynamical theories A.3.6 is a solid basis for the constructive decoding of classical proofs. In classical mathematics, we show that a coherent theory proves a dynamical rule by looking at what happens in the models of the theory, which we study with powerful but dubious tools such as the excluded third, the axiom of choice and sometimes even the full power of  $\mathcal{ZFC}$ . However, Theorem A.3.6 assures us that if the rule in question is provable in formal theory with classical logic, it is also provable by the elementary methods “without logic” that constitute dynamic proofs.

The essential part of decoding is therefore to check that the classical proof can be formalised in classical first-order logic. This is not always easy, because after all,  $\mathcal{ZFC}$  theory can be used to prove results that are much more “strange” than Gödel's completeness theorem, and why not results that are downright false if  $\mathcal{ZFC}$  is inconsistent. But in practice, in classical mathematics, even the overuse of ultrafilters or the continuum hypothesis always seems to hide simpler arguments.

**Barr's theorem**, established in classical mathematics (and apparently impossible to prove in constructive mathematics), states that for geometric theories, any result proved with classical logic can also be proved with constructive logic. This is a generalisation of Theorem A.3.6 which is confirmed in practice, even if it is not completely certain from the constructive point of view. A recent study of the problem is made by Rathjen in the article [57] published in the book [Proofs, 2013].

Barr's theorem gives us good reason to believe that the type of decryption provided by Theorem A.3.6 also applies for infinitary geometric theories, with the same caveats as we indicated for finitary theories. The reader can find examples of this type in [CACM, Sections XV-6 and XV-7].

At the end of this chapter we illustrate how Barr's theorem should not be understood.

### An infinitary geometric theory for primitive recursive arithmetic

We now consider the infinitary geometric theory  $\mathcal{PRA}\omega$  obtained from the finitary geometric theory  $\mathcal{PRA}$  by adding the following axiom which forces the sort  $N$  to contain only usual integers.

$$\mathbf{Nat} \quad \vdash_{x:N} \quad \mathbf{OP}_{n \in N} \quad x = \underline{n}$$

In the theory thus obtained, we see that to prove  $\vdash f(x) = g(x)$  with  $f, g$  of sort  $F_1$ , it is sufficient to know how to show that for each  $n \in \mathbb{N}$  the rule  $\vdash f(\underline{n}) = g(\underline{n})$  is valid. Indeed, we then deduce  $x = \underline{n} \vdash f(x) = g(x)$  for each concrete integer  $n$ , and by using the rule **Nat**, we obtain  $\vdash f(x) = g(x)$ .

Now for maps  $f$  and  $g$  defined in  $\mathcal{PRA}$  (i.e. two arbitrary primitive recursive maps),  $f(\underline{n})$  and  $g(\underline{n})$  are two explicit usual integers. Thus two primitive recursive maps are “provably everywhere equal” in the theory if they take the same values in any integer, i.e. if they are concretely equal, i.e. if we have a proof for the fact that they are equal.



But this proof is not always formalisable within the theory (it may, for example, use a double induction). In any case, it is supposed to be produced in intuitive mathematics in the intuitive mathematical world of the natural integers.

An example is provided by the primitive recursive map  $C_{PRA} : \mathbb{N} \rightarrow \mathbb{N}$  which is everywhere zero if the theory  $\mathcal{PRA}$  is consistent (which we are intimately convinced). According to Gödel's incompleteness theorem, the theory  $\mathcal{PRA}$  cannot prove  $\vdash C_{PRA}(x) = 0$ . However, it does prove  $\vdash C_{PRA}(\underline{n}) = 0$  for all  $n$ .

In the same way it seems probable that the geometric theory  $\mathcal{PRA}\omega$ , although it is capable of proving  $\vdash C_{PRA}(x) = 0$ , cannot however prove  $\vdash C_{PRA} = 0_1$ .

The infinitary axiom **Nat** that we add therefore authorises up to a certain point, but only up to a certain point, the use of the  $\omega$ -rule for the equality of primitive recursive maps.

## Conclusion

The study we have just made casts a shadow over Barr's theorem, because it would seem to assert in this case that any primitive recursive map proved null in classical mathematics would be provably null in constructive mathematics.

However, it may be that the intuitive proof of classical mathematics uses dubious principles, such as those formalised in the theory  $\mathcal{ZF}$ , in which case it may lead to quite questionable results.

For example, consider the primitive recursive map  $\text{consisZ}$ , which always takes the value 0 until such time as we eventually find a proof of  $0 = 1$  in  $\mathcal{Z}$ , at which point the map takes the value 1. Thus  $\text{consisZ}$  is a well-defined constant of sort  $F_1$  in  $\mathcal{PRA}$ .

In classical mathematics with a sufficiently strong intuitive set theory (e.g.  $\mathcal{ZF}$ ), it can be shown that  $\text{consisZ}$  is identically zero. And this demonstrates in classical mathematics (using  $\mathcal{ZF}$  in the external intuitive mathematical world) the rule  $\vdash \text{consisZ}(x) = 0$  in the geometric theory  $\mathcal{PRA}\omega$ .

Now this result clearly escapes any constructive proof. And there can be no constructive proof of the rule  $\vdash \text{consisZ}(x) = 0$  in the geometric theory  $\mathcal{PRA}\omega$ .

In fact we need to clarify the statement of Barr's theorem. It does not say that the framework of classical mathematics is conservative for geometric properties in a geometric theory. It only says that when we use the same mathematics outside the formal infinitary theory, adding the connectives, quantifiers and rules of classical logic inside the infinitary geometric theory, does not allow us to prove new properties formulable as geometric rules.

ajouter une conclusion de la première partie

## Part II

# Finitary geometric theories for real algebra



# Introduction

This second part is devoted to the development of a finitary dynamical theory whose ambition is to describe exhaustively the algebraic properties of the real number field, and more generally of a *non* discrete real closed field<sup>1</sup> at least those that are expressible in a restricted language, close to the language of ordered rings. This constitutes a development, with some minor terminological modifications, of the ideas given in the article [40]. The axiom of archimedeanity, introduced in the last chapter, takes us out of the realm of finitary geometric theories.

Chapter C proposes a first definition of the ordered field structure in the absence of a sign test. It also discusses the possibility of a suitable axiomatic for discrete real closed fields, such as the field of real numbers.

Section C.1 gives some reminders about the dynamical theory of discrete ordered fields and that of discrete real closed fields.

Section C.2 discusses the decisive consequences of formal Positivstellensätze, in our framework.

Section C.3 proposes an axiomatic for *non* discrete ordered fields (Definition C.3.7).

Section C.4 describes an example of a non-archimedean discrete Heyting ordered field.

Section C.5 gives a first discussion on acceptable dynamical theories for  $\mathbb{R}$  as a *non* discrete real closed field.

Chapter D deals with dynamical theories which admit extensions essentially equivalent to the theory *Co* of *non* discrete ordered fields.

We start (Section D.1) with the theory of distributive lattices (a *non* discrete ordered field is a distributive lattice for its order relation).

In Section D.2 we deal with  $\ell$ -groups of lattice groups (purely equational theory, valid for addition on the reals).

Then (Section D.3) we move on to *f*-rings (*f*-rings in french litterature), a theory inspired by rings of continuous real maps.

Section D.4 describes dynamical theories in which the predicate  $\cdot > 0$  is added to the signature (strict *f*-rings and variants).

Section D.5 proposes a return to the theory *Co* by confronting it with suitable extensions of the theory of strict *f*-rings.

Chapter E proposes a definition of the structure of a real closed ordered field in the absence of a sign test.

Section E.1 explains how to introduce square roots of the elements  $\geq 0$  in a *non* discrete ordered field. This is done as a warm-up to the more general notion of virtual roots.

Section E.2 introduces virtual root maps and some corresponding dynamical theories: in particular *f*-rings with virtual roots and *non* discrete ordered fields with virtual roots,

Section E.3 deals with real closed rings and Section E.4 proposes a definition for *non* discrete real closed fields as local real closed rings. The theory of real closed rings is presented here in an elementary, purely equational form, in the style of [69].

Chapter F deals with an infinitary geometric theory where we add the axiom that the field of real numbers is *archimedean*.

---

<sup>1</sup>In this text, a negation is italicised when the corresponding statement, true in classical mathematics, implies in constructive mathematics a well-recorded non-constructive principle, such as **LPO** or even **MP**.

Thus, we propose for the coveted dynamical theory the structure of a local real closed ring (possibly archimedean if that proved useful).

In a concluding chapter, we summarise the situation we have arrived at, specifying the important questions, from a constructive point of view, which we do not know how to answer satisfactorily today.

# C. Ordered fields

## Sommaire

---

<b>Introduction</b> . . . . .	<b>43</b>
<b>C.1 About discrete ordered fields</b> . . . . .	<b>44</b>
A natural dynamical theory for discrete ordered fields . . . . .	44
Some valid rules in <i>Cod</i> . . . . .	45
Weaker dynamical theories . . . . .	46
An example with nilpotents . . . . .	47
Adding the function symbol $\vee$ for the lub . . . . .	48
<b>C.2 Formal Positivstellensätze</b> . . . . .	<b>48</b>
The demonstrative force of formal Positivstellensätze . . . . .	49
Concrete Positivstellensatz . . . . .	50
<b>C.3 Non discrete ordered fields</b> . . . . .	<b>51</b>
A first dynamical theory . . . . .	51
The convexity axiom and the theory <i>Co</i> . . . . .	52
Other continuous operations . . . . .	53
<b>C.4 A non-archimedean non discrete ordered field</b> . . . . .	<b>54</b>
<b>C.5 Non discrete real closed fields: position of the problem</b> . . . . .	<b>57</b>
The principle of extension by continuity . . . . .	57
Continuous semialgebraic maps . . . . .	58
Continuous parametrisation of continuous semialgebraic maps . . . . .	58
A reasonable definition . . . . .	59
Rational dynamical theories for real number algebra . . . . .	60
<b>C.6 General properties of continuous semialgebraic maps</b> . . . . .	<b>61</b>
Stability by composition . . . . .	61
Stability by upper bound . . . . .	61
Finiteness properties . . . . .	62
<b>C.7 Some questions</b> . . . . .	<b>62</b>
Continuous variations . . . . .	62

---

## Introduction

This chapter offers a first constructive approach to the classical theory of real closed fields. In fact, the classical theory applies only to real closed fields for which we have a sign test on any element of the field, if it is given in accordance with the definition. In other words, the usual classical theory is a theory of discrete real closed fields. But it is well known that matrix numerical analysis, used in applications of the theory to concrete situations, never uses such a sign test. A constructive approach to a theory of algebraic properties of the real number field requires a dynamical theory of *non* discrete real closed fields.

Section C.1 gives some reminders on the dynamical theory of discrete ordered fields and that of discrete real closed fields.

Section C.2 explains the great utility of formal Positivstellensätze.

Section C.3 proposes an axiomatic for *non* discrete ordered fields (Definition C.3.7). We must abandon the axioms of total order in their usual discrete formulation and replace them with dynamical rules relevant to  $\mathbb{R}$ . We then find that many well-defined continuous rational maps on  $\mathbb{Q}$ , such as the map  $\sup$ , need to be introduced into the language.

Section C.4 describes an example of a *non* discrete non-archimedean Heyting ordered field.

Section C.5 gives a first discussion of acceptable dynamical theories for  $\mathbb{R}$  as a *non* discrete real closed field. We are guided by the continuity extension principle C.5.2 which can be seen as an algebraic version of the completeness of  $\mathbb{R}$ . In this framework Theorem C.5.4 plays a fundamental role for a relevant definition of continuous semialgebraic maps, by reducing the definition to the case of continuous semialgebraic maps in the discrete framework of  $\mathbb{R}_{\text{alg}}$ .

## C.1. About discrete ordered fields

### A natural dynamical theory for discrete ordered fields

We recall here the dynamical theory of *discrete ordered fields*  $\text{Cod}$  given in [17].

**Signature:**  $(\cdot = 0, \cdot > 0, \cdot \geq 0; \cdot + \cdot, \cdot \times \cdot, -, 0, 1)$ .

If we want to give a dynamic discrete ordered field, i.e. a dynamic algebraic structure of type  $\text{Cod}$ , we add to the signature a presentation by generators and relations of the dynamic algebraic structure considered. For example, this can be the empty presentation, or a countable set of generators, without any relations, or it can be based on an existing algebraic structure in which certain relations are required to be preserved, for example all the equality relations between terms constructed on the elements of the structure. Thus any ring defines a dynamic discrete ordered field.

#### Abbreviations

- $x \# 0$  means  $x^2 > 0$
- $x = y$  means  $x - y = 0$
- $x > y$  means  $x - y > 0$
- $x < y$  means  $y > x$
- $x \geq y$  means  $x - y \geq 0$
- $x \# y$  means  $x - y \# 0$
- $x \leq y$  means  $y \geq x$

#### Axioms

##### Direct rules

First we put the axioms of commutative rings, then the rules concerning  $\cdot = 0$  and  $\cdot \geq 0$ , then the rules involving  $\cdot > 0$ .

$$\text{ga0} \quad \vdash \quad 0 = 0$$

$$\text{ac1} \quad x = 0 \quad \vdash \quad xy = 0$$

$$\text{ga2} \quad x = 0, y = 0 \quad \vdash \quad x + y = 0$$

$$\text{gao1} \quad x = 0 \quad \vdash \quad x \geq 0$$

$$\text{ao1} \quad \vdash \quad x^2 \geq 0$$

$$\text{gao2} \quad x \geq 0, y \geq 0 \quad \vdash \quad x + y \geq 0$$

$$\text{ao2} \quad x \geq 0, y \geq 0 \quad \vdash \quad xy \geq 0$$

$$\mathbf{aso1} \quad \vdash 1 > 0$$

$$\mathbf{aso2} \quad x > 0 \vdash x \geq 0$$

$$\mathbf{aso3} \quad x > 0, y \geq 0 \vdash x + y > 0$$

$$\mathbf{aso4} \quad x > 0, y > 0 \vdash xy > 0$$

*Collapse*

$$\mathbf{col}_> \quad 0 > 0 \vdash 1 = 0$$

*Simplification rules*

$$\mathbf{Gao} \quad x \geq 0, x \leq 0 \vdash x = 0$$

$$\mathbf{lv} \quad xy = 1 \vdash x^2 > 0$$

*Dynamical rules*

$$\mathbf{IV} \quad x > 0 \vdash \exists y xy = 1$$

$$\mathbf{OT} \quad \vdash x \geq 0 \text{ op } x \leq 0$$

$$\mathbf{ED}_> \quad \vdash x = 0 \text{ op } x^2 > 0$$

The dynamical theory *Crcd* of discrete real closed fields is obtained from the theory *Cod* by adding as axioms the dynamical rules  $\mathbf{RCF}_n$ .<sup>1</sup>

$$\mathbf{RCF}_n \quad a < b, P(a)P(b) < 0 \vdash \exists x (P(x) = 0, a < x < b) \quad (P(x) = \sum_{k=0}^n a_k x^k)$$

The rules **gao1** and **gao2** express, in the context of abelian groups, the reflexivity and transitivity of the order relation (compatible with the group law). The rule **Gao** corresponds to anti-symmetry for the order relation.

The rules  $\mathbf{ED}_>$  and **OT** express that the equality is discrete and the order total. They are not satisfied constructively for  $\mathbb{R}$ . For Bishop's reals, the rule  $\mathbf{ED}_>$  is equivalent to the omniscience principle **LPO** and the rule **OT** is equivalent to the principle **LLPO**. Note also that the principle "any regular element of  $\mathbb{R}$  is invertible" is equivalent to the Markov principle<sup>2</sup> **MP**.

Given the form "without negation" adopted here for collapse, the trivial ring is a discrete ordered field, and the collapse axiom  $\mathbf{col}_>$  is a consequence of **IV**.

By means of the direct rules alone we see that  $1 = 0 \vdash (x = 0, x \geq 0, x > 0)$ . This justifies taking  $1 = 0$  as a substitute for **L**. And the collapse rule looks like a simplification rule.

## Some valid rules in *Cod*

*Four valid simplification rules*

$$\mathbf{Anz} \quad x^2 = 0 \vdash x = 0$$

$$\mathbf{Aso1} \quad x > 0, xy \geq 0 \vdash y \geq 0$$

$$\mathbf{Aonz} \quad c \geq 0, x(x^2 + c) \geq 0 \vdash x \geq 0$$

$$\mathbf{Aso2} \quad x \geq 0, xy > 0 \vdash y > 0$$

*Two valid dynamical rules*

$$\mathbf{OTF} \quad x + y > 0 \vdash x > 0 \text{ op } y > 0$$

$$\mathbf{OTF}^\times \quad xy < 0 \vdash x < 0 \text{ op } y < 0$$

Note that the rule **Aso1** implies that elements  $> 0$  are regular.

<sup>1</sup>A theorem essentially equivalent to these rules is proved by Bishop for the field  $\mathbb{R}$ , but using the axiom of dependent choice.

<sup>2</sup>Equivalence suggested by Fred Richman.



**Lemma C.1.1.** *The following rule is provable with direct axioms.*

$$\mathbf{Aonz2} \quad c \geq 0, x(x^2 + c) \geq 0, x < 0 \vdash 0 > 0$$

**Theorem C.1.2.** *With the exception of the rules  $\mathbf{ED}_>$  and  $\mathbf{OT}$ , all the above rules are constructively valid for  $\mathbb{R}$ , without using the axiom of dependent choice.*

*Proof.* Everything is clear except perhaps the rule  $\mathbf{Aonz}$ . For  $x \in \mathbb{R}$ , we can prove  $x \geq 0$  by reducing  $x < 0$  to the absurd. This is what  $\mathbf{Aonz2}$  does (take  $c = 0$ ).  $\square$

*Remark C.1.3.* The rules  $\mathbf{ED}_>$  and  $\mathbf{OTF}^\times$  imply the rule  $\vdash x = 0 \text{ op } x < 0, \text{ op } x > 0$ , and a fortiori  $\mathbf{OT}$ . See also D.4.1, D.4.4 and D.5.4.  $\blacksquare$

If  $\mathbf{K}$  is a discrete ordered field, we denote  $\mathbf{Cod}(\mathbf{K})$  the dynamic algebraic structure of type  $\mathbf{Cod}$  having for presentation the *positive diagram of  $\mathbf{K}$* . A non-trivial model of  $\mathbf{Cod}(\mathbf{K})$  is a non-trivial discrete ordered field  $\mathbf{L}$  given with a morphism  $\mathbf{K} \rightarrow \mathbf{L}$ . Similarly, if  $\mathbf{A}$  is a commutative ring (or an ordered ring), we denote  $\mathbf{Cod}(\mathbf{A})$  the dynamic algebraic structure of type  $\mathbf{Cod}$  having for presentation the *positive diagram of  $\mathbf{A}$* . A model of  $\mathbf{Cod}(\mathbf{A})$  is a discrete ordered field  $\mathbf{L}$  given with a morphism  $\mathbf{A} \rightarrow \mathbf{L}$  (of commutative ring, or of ordered ring).

## Weaker dynamical theories

The rule  $\mathbf{Aonz}$  implies  $x^3 \geq 0 \vdash x \geq 0$ , therefore also, under  $\mathbf{Gao}$ ,  $x^3 = 0 \vdash x = 0$ , and a fortiori  $\mathbf{Anz}$ .

### Definition C.1.4.

Theories based on the language of ordered rings  $(\cdot = 0, \cdot \geq 0; \cdot + \cdot, \cdot \times \cdot, -\cdot, 0, 1)$ .

1. The direct theory  $\mathcal{Apo}$  of *preordered rings*. The axioms are those of commutative rings and the direct rules  $\mathbf{gao1}$ ,  $\mathbf{gao2}$ ,  $\mathbf{ao1}$ ,  $\mathbf{ao2}$ .
2. The Horn theory  $\mathcal{Ao}$  of *ordered rings*. The axioms are those of pre-ordered rings and the simplification rule  $\mathbf{Gao}$ .
3. The Horn theory  $\mathcal{Aonz}$  of *strictly reduced ordered rings*<sup>3</sup> is obtained by adding the simplification rule  $\mathbf{Aonz}$  to the theory  $\mathcal{Ao}$ .
4. The dynamical theory  $\mathcal{Ato}$  of *linearly ordered rings*<sup>4</sup> is obtained by adding the dynamical rule  $\mathbf{OT}$  to the theory  $\mathcal{Ao}$ .
5. The dynamical theory  $\mathcal{Atonz}$  of *reduced linearly ordered rings* is obtained by adding the dynamical rule  $\mathbf{Anz}$  to the theory  $\mathcal{Ato}$ . This theory proves the rules  $\mathbf{Aonz}$  and  $\mathbf{ASDZ}$  (Lemma C.1.6)

Theories based on the language of strictly ordered rings: we add the predicate  $\cdot > 0$ .

6. The direct theory  $\mathcal{Apro}$  of *proto-ordered rings* (cf. [17]). The axioms are those of commutative rings, all the direct rules stated for  $\mathbf{Cod}$  ( $\mathbf{gao1}$ ,  $\mathbf{gao2}$ ,  $\mathbf{ao1}$ ,  $\mathbf{ao2}$ ,  $\mathbf{aso1}$  to  $\mathbf{aso4}$ ) and the collapse rule  $\mathbf{col}_>$ .
7. The Horn theory  $\mathcal{Aso}$  of *strictly ordered rings* is the theory  $\mathcal{Apro}$  to which we add the simplification rules  $\mathbf{Gao}$ ,  $\mathbf{Aso1}$  and  $\mathbf{Aso2}$ . It can also be seen as constructed from  $\mathcal{Ao}$  by adding the predicate  $\cdot > 0$  in the language, the direct rules  $\mathbf{aso1}$  to  $\mathbf{aso4}$  and the simplification rules  $\mathbf{Aso1}$  and  $\mathbf{Aso2}$ .

<sup>3</sup>The rule  $\mathbf{Aonz}$  is stronger than the rule  $\mathbf{Anz}$ , so “strictly reduced” is used rather than “reduced”. However, see Item 3 of Lemma C.1.6.

<sup>4</sup>An order relation is *linear* or *total* when two elements are always comparable.

8. The Horn theory **Asonz** of *reduced strictly ordered rings* (“quasi-ordered rings” in [17]) is obtained by adding the simplification rule **Aonz** to **Aso**. It can also be seen as the theory **Apro** to which we add the simplification rules **Gao**, **Aonz**, **Aso1** and **Aso2**.
9. The dynamical theory **Asto** of *strictly linearly ordered rings* is the theory **Aso** to which we add the dynamical rule **OT**. It can also be seen as constructed from **Ato** by adding the predicate  $\cdot > 0$  in the language, the direct rules **aso1** to **aso4** and the simplification rules **Aso1** and **Aso2**.
10. The dynamical theory **Aito** of *linearly ordered integral rings* is obtained by adding the dynamical rule **ED<sub>></sub>** to **Asto**. The rules **Aonz**, **OTF** and **OTF<sup>×</sup>** are valid in this theory.

In Items 6, 7 and 8, the meaning of  $x > 0$  is not fixed a priori. This can range from “ $x$  is regular and  $\geq 0$ ” to “ $x$  is invertible and  $\geq 0$ ”.

The direct theory **Apro** is the one in which the collapse is the clearest, directly given by an algebraic certificate, as specified in the following lemma.

Recall that in a ring, a *cone* is a part  $C$  which contains squares and which is stable by addition and product:  $C + C \subseteq C$ ,  $C \times C \subseteq C$ .

**Lemma C.1.5** (algebraic certificate of collapse). *Let  $\mathbf{K}$  be a dynamic algebraic structure of type **Apro** given by a presentation  $(G; R_{>0}, R_{\geq 0}, R_{=0})$  with the following meaning:  $G$  is the set of generators of the structure,  $R_{>0}$ ,  $R_{\geq 0}$  and  $R_{=0}$  are three parts of  $\mathbb{Z}[G]$ , the elements of  $R_{>0}$  (resp.  $R_{\geq 0}$ ,  $R_{=0}$ ) are assumed  $> 0$  (resp.  $\geq 0$ ,  $= 0$ ) in the structure. The dynamic algebraic structure  $\mathbf{K}$  collapses if, and only if, we have in  $\mathbb{Z}[G]$  an equality*

$$s + p + z = 0$$

where  $s$  is in the multiplicative monoid generated by  $R_{>0}$ ,  $p$  is in the cone generated by  $R_{>0} \cup R_{\geq 0}$  and  $z$  in the ideal generated by  $R_{=0}$ .

**Lemma C.1.6.** (See also Lemma D.4.1.)

1. The dynamical theory **Aso** proves the simplification rule **lv** and the collapsus **col<sub>></sub>**.
2. The dynamical theory **Ato** proves the following simplification rules.

$$\mathbf{Afr4} \quad y \geq 0, xy = 1 \vdash x \geq 0$$

$$\mathbf{Afr5} \quad c \geq 0, x(x^2 + c) \geq 0 \vdash x^3 \geq 0$$

3. The theory **Atonz** proves the rules **Aonz** and **ASDZ**.

*Proof.* Items 1 and 2 are easy. For Item 3, **Aonz** follows from **Afr5**. Let’s look at **ASDZ**. Let  $a, b$  be such that  $ab = 0$ ; if  $|a| \leq |b|$ , we have  $0 \leq |a|^2 \leq |ab| = 0$  so  $a = 0$ , and in the case where  $|b| \leq |a|$  we get  $b = 0$ .  $\square$

In the **Aso** theory, the rule **Afr4** is a weakened variant of **Aso1**. In the **Ao** theory, the rule **Afr5** is a weakened variant of **Aonz**.

In a linearly ordered ring, if we define “ $x > 0$ ” by “ $x$  is regular and  $\geq 0$ ”, all the rules that define **Aso** are satisfied (and  $x \neq 0$  is a priori stronger than the simple negation of  $x = 0$ ). This explains the interest of the Horn theory **Aso**. A lattice variant, the **Asr** theory of strict  $f$ -rings, will be defined later.

## An example with nilpotents

**Example C.1.7** (a non-reduced linearly ordered ring). The example we now give is the one that should be kept in mind in order to fully understand the difference between linearly ordered rings and linearly ordered domains.

This is the linearly ordered ring  $\mathbb{Q}[\alpha]$  where  $\alpha > 0$  and  $\alpha^6 = 0$  ( $\alpha$  is an infinitesimal  $> 0$  nilpotent). Let  $c$  be an element such that  $c^2 = 0$  (for example  $c = \alpha^5$ ). The system of constraints

$$x^2 = c^2, x \geq 0,$$

which could be suggested to characterise  $|c|$  without using the sign test in the case of an ordered field, now admits an infinite number of solutions: all  $r\alpha^3 + y\alpha^4$  where  $r > 0$  in  $\mathbb{Q}$  and  $y$  arbitrary in  $\mathbb{Q}[\alpha]$ . ■

## Adding the function symbol $\vee$ for the lub

In a linearly ordered set, and even more so in a discrete ordered field, every pair of elements has a least upper bound (lub): the greater of the two. We therefore change nothing essential in the theory of *Cod* by adding a function symbol  $\cdot \vee \cdot$  subject to the three axioms which define the sup of two elements, when it exists for a of given order relation.

**Definition C.1.8.** The dynamical theory of *discrete ordered fields with sup*, denoted *Codsup*, is the dynamical theory of discrete ordered fields to which we add a function symbol  $\cdot \vee \cdot$  and for axioms the following Horn rules **sup1**, **sup2** and **Sup**.

$$\mathbf{sup1} \vdash x \vee y \geq x \qquad \mathbf{Sup} \quad z \geq x, z \geq y \vdash z \geq x \vee y$$

$$\mathbf{sup2} \vdash x \vee y \geq y$$

From the theories *Ato*, *Asto*, *Aito* and *Crcd* the theories *Atosup*, *Astosup*, *Aitosup* and *Crcdsup* are defined in the same way.

In the case of discrete ordered fields and discrete real closed fields we could also have replaced the Horn rule **Sup** by the following direct rule **sup**, so as to add only direct rules to *Cod*.

$$\mathbf{sup} \vdash ((x \vee y) - x) ((x \vee y) - y) = 0$$

We can also think of the theory *Crcdsup* as the theory *Codsup* to which we add the axioms of real closure **RCF<sub>n</sub>**.

*Remark C.1.9.* The theories *Cod* and *Codsup* are essentially identical. The same applies to the other pairs of theories in Definition C.1.8. ■

## C.2. Formal Positivstellensätze

The formal Positivstellensatz of classical mathematics ([Bochnak, Coste & Roy, Theorem 4.4.2]) admits the following constructive version (see [17]).

**Formal Positivstellensatz C.2.1** (concrete formal Positivstellensatz for ordered fields, 1).

Let  $\mathbf{R}$  be a dynamic algebraic structure in the language of strictly ordered rings.

1. The dynamical theories *Apro*, *Aso*, *Cod* and *Crcd* collapse simultaneously.
2. The dynamical theories *Asonz*, *Aito*, *Cod* and *Crcd* prove the same Horn rules.

The strength of this theorem lies in the fact that the collapse of a dynamic algebraic structure of type *Apro* is given by an *algebraic certificate of collapse* (Lemma C.1.5), which we call a *Positivstellensatz*.

As a special case, for a commutative ring  $\mathbf{R}$ , the dynamic algebraic structure *Crcd*( $\mathbf{R}$ ) collapses if, and only if,  $-1$  is a sum of squares in  $\mathbf{R}$ .

In classical mathematics, thanks to Gödel's completeness theorem A.5.1, we deduce from previous Item 1 the abstract formal *Positivstellensatz* in the following form (see [17]).

*A system of sign conditions imposed on elements of a ring  $\mathbf{A}$  admits an algebraic certificate of impossibility if, and only if, the only model of *Cod*( $\mathbf{A}$ ) is trivial, if, and only if, the only model of *Crcd*( $\mathbf{A}$ ) is trivial.*

Item 2 of C.2.1 also admits “abstract” classical versions via model theory, in application of Theorem A.5.4 (see [17]).

We now examine what happens to the previous results in the absence of the predicate “ $\cdot > 0$ ” in the presentation of a dynamic algebraic structure.

**Formal Positivstellensatz C.2.2** (concrete formal Positivstellensatz, 1bis). *Let  $\mathbf{R}$  be a dynamic algebraic structure in the language of ordered rings.*

1. The dynamical theories  $\mathcal{A}o$ ,  $\mathcal{A}pro$ ,  $\mathcal{A}to$ ,  $\mathcal{C}od$  and  $\mathcal{C}rcd$  collapse simultaneously.
2. The dynamical theories  $\mathcal{A}onz$ ,  $\mathcal{A}tonz$ ,  $\mathcal{C}od$  and  $\mathcal{C}rcd$  prove the same Horn rules.

*NB.* The language used for the presentation must not mention the predicate  $\cdot > 0$ . There is no collapse axiom in  $\mathcal{A}o$  and  $\mathcal{A}to$ , and a dynamic algebraic structure of type  $\mathcal{A}o$  or  $\mathcal{A}to$  is said to collapse when it proves  $1 = 0$ .

*Proof.* 1. Consider a dynamic algebraic structure  $\mathbf{A}$  for  $\mathcal{A}o$ . The same presentation gives a dynamic algebraic structure  $\mathbf{A}'$  for  $\mathcal{A}pro$ . Suppose that  $\mathbf{A}'$  proves  $1 = 0$ . The collapse for  $\mathbf{A}'$  (of type  $\mathcal{A}pro$ ) has the form of a very precise algebraic certificate (a Positivstellensatz). This certificate is written  $1 + p = 0$ , where  $p$  is  $\geq 0$  by virtue of the presentation and the axioms of  $\mathcal{A}o$ . We therefore have both  $1 \geq 0$  and  $1 \leq 0$  in  $\mathbf{A}$ , so  $1 = 0$  by virtue of  $\mathcal{G}ao$ . Conversely, if  $\mathbf{A}$  proves  $1 = 0$ , then a fortiori the same will be true for  $\mathbf{A}'$ .

Finally, we apply Positivstellensatz C.2.1 and note that  $\mathcal{A}to$  is an intermediate theory between  $\mathcal{A}o$  and  $\mathcal{C}od$ .

2. Consider a dynamic algebraic structure  $\mathbf{A}$  for  $\mathcal{A}onz$ . It suffices to prove the result for a fact of the form  $x \geq 0$  (because  $x = 0$  is equivalent to  $x \geq 0$  and  $x \leq 0$ ). This fact is valid in  $\mathcal{C}od$  if, and only if, the fact  $x < 0$  collapses the dynamic algebraic structure  $\mathcal{C}od(\mathbf{A})$ . According to Positivstellensatz C.2.1, this corresponds to an algebraic certificate of the form  $x^{2n} + p = xq$ , where  $p$  and  $q$  are  $\geq 0$  by virtue of the presentation and the axioms of  $\mathcal{A}o$ . This gives  $x(x^{2n} + p) \geq 0$ , then  $x^k(x^{2k} + p_1) \geq 0$  for a suitable odd integer  $k$ . The rule  $\mathcal{A}onz$  tells us that  $x^k \geq 0$  in  $\mathbf{A}$ . This same rule shows that  $x^3 \geq 0$  implies  $x \geq 0$ , and consequently  $x^k \geq 0$  implies  $x \geq 0$  for all odd  $k$ .  $\square$

A consequence of Item 1 in classical mathematics (via Theorem A.5.3) is that a field  $\mathbf{K}$  in which  $-1$  is not a sum of squares can be ordered. On the other hand, the only known computational meaning of this result of classical mathematics is that the theory  $\mathcal{C}od(\mathbf{K})$  collapses if, and only if,  $-1$  is a sum of squares in  $\mathbf{K}$ .

From a classical point of view, since the theory  $\mathcal{C}od(\mathbb{R})$  does not collapse, we can provide  $\mathbb{R}$  with an order relation which extends the usual order relation and which is a total order. But the only constructive meaning of this result of classical mathematics is that  $-1$  is not a sum of squares in  $\mathbb{R}$ .

## The demonstrative force of formal Positivstellensätze

The dynamical theories we explore in the following to describe the algebraic properties of real numbers are extensions of  $\mathcal{A}sonz$  (if the predicate  $\cdot > 0$  is present) or  $\mathcal{A}onz$  (in the opposite case). Moreover, the theories explored are always weaker than  $\mathcal{C}rcd$ . And any Horn rule valid in the dynamical theory  $\mathcal{C}rcd$  is valid in  $\mathcal{A}sonz$  (in  $\mathcal{A}onz$  if the predicate  $\cdot > 0$  is absent).

Now  $\mathbb{R}$  constitutes a constructive model of the  $\mathcal{A}sonz$  theory for the language based on the signature  $(\cdot = 0, \cdot > 0, \cdot \geq 0; \cdot + \cdot, \cdot \times \cdot, -, 0, 1)$  (Theorem C.1.2).

Thus from the point of view of Horn rules alone, the formal Positivstellensätze tell us that the theory  $\mathcal{C}rcd$  is entirely satisfactory, including for  $\mathbb{R}$ , which does however satisfy neither  $\mathcal{C}ol_{>}$  nor  $\mathcal{O}T$ . However, to temper this optimistic statement, here is the precise result. Note also that it applies only to Horn rules, not to other dynamical rules.

**Theorem C.2.3.** *Consider a Horn rule formulated in the dynamic algebraic structure  $\mathbf{R} = \mathcal{A}sonz(\mathbb{R})$ . If the constants involved in the rule are in a discrete subfield  $\mathbf{R}_0$  of  $\mathbb{R}$ , for the rule to be valid in  $\mathbf{R}$ , it is sufficient for it to be valid in  $\mathcal{C}rcd(\mathbf{R}_0)$ .*

The existential rules satisfied in  $\mathbb{R}$  and introduced in the dynamical theories under consideration will as far as possible be treated in the framework of provably unique existences and can therefore be skolemised without damage, providing theories without existential axioms which are essentially equivalent to those which would have required existential axioms.

*Remark C.2.4.* We can also apply Theorem A.3.6 with the dynamical theory  $\mathbf{Co0}(\mathbb{R})$  (Definition C.3.2). We will then introduce a predicate  $x \succ y$  opposed to  $x < y$ . The new dynamical theory will treat  $\mathbb{R}$  as a discrete ordered field and any dynamical rule proved in the new theory but not using  $x \succ y$  will also be valid in  $\mathbb{R}$ . The disadvantage is of course that  $\mathbb{R}$  is not a constructive model of the new theory. Another drawback is the mysterious status of the new predicate  $x \succ y$ , which is weaker than  $x \geq y$  in the new dynamical theory. In conclusion, the advantage that Theorem A.3.6 seems to provide (the use of classical logic is harmless) does not seem to go beyond the considerations we have developed on the proper use of the formal Positivstellensatz. ■

## Concrete Positivstellensatz

First, we recall Tarski's fundamental theorem. For a simple Cohen-Hormander proof, see [Bochnak, Coste & Roy, Section 1.4] or [17, Lemma 3.12]. Some instructive comments can be found in [43, Theorems 10, 11, 12].

**Theorem C.2.5** (elimination of quantifiers). *The first-order intuitionistic formal theory associated with the dynamical theory  $\mathbf{Crcd}$  admits the elimination of quantifiers. It is complete and decidable. In particular, it exhaustively describes all the purely algebraic properties of  $\mathbb{R}_{\text{alg}}$  (those formulated to first-order in the language of ordered rings).*

This paragraph gives a theorem equivalent to Krivine-Stengle's Positivstellensatz, stated here in the language of dynamic algebraic structures.

A constructive proof of Positivstellensatz C.2.6 can be found in [17] or [34]. It is based on the formal Positivstellensatz and on Lemma 3.12 of [17], a variant of Tarski's theorem.

For a more conceptual approach and better complexity bounds see [LPR]. For the construction of the real closure of a discrete ordered field see [42, 43].

**Positivstellensatz C.2.6** (concrete Positivstellensatz).

*Let  $\mathbf{K}$  be a discrete ordered field and  $\mathbf{R}$  be a discrete real closed field containing  $\mathbf{K}$ , (for example the real closure of  $\mathbf{K}$ ). Let  $\mathbf{A} = ((G, \text{Rel}), \text{Cod}(\mathbf{K}))$  be a dynamic algebraic structure where  $G = (x_1, \dots, x_n)$  and where  $\text{Rel}$  is finite.*

1. *The dynamic algebraic structure  $\mathbf{A}$  collapses if, and only if, it is impossible to find a model of  $\mathbf{A}$  contained in  $\mathbf{R}$ .*
2. *The collapse if it occurs is given by an algebraic certificate according to Item 1 of Theorem C.2.1 and Lemma C.1.5.*
3. *We have an algorithm which decides whether  $\mathbf{A}$  collapses and which in the case of a negative answer gives the description of a system  $(\xi_1, \dots, \xi_n)$  in  $\mathbf{R}^n$  which satisfies the constraints given in the relations  $\text{Rel}$ .*

This statement is not valid in this general form if we take  $\mathbf{K} = \mathbf{R} = \mathbb{R}$  because there is no sign test in  $\mathbb{R}$  and the algorithms which explicitate Positivstellensatz C.2.6<sup>5</sup> make crucial use of this sign test.

Here's a small example of the problems we run into. On  $\mathbb{R}$ , as on an arbitrary local ring<sup>6</sup> in which  $x \# 0$  denotes the invertibility predicate, we have the equivalence

$$\exists y \ x^2 y = x \iff x = 0 \text{ or } x \# 0. \quad (\text{C.1})$$

<sup>5</sup>These algorithms are provided by the constructive proof of the theorem.

<sup>6</sup>For the constructive treatment of local rings, the Jacobson radical and Heyting fields see for example [CACM, section IX-1].

Let's assume that  $x(1 - xy) = 0$ . If  $xy$  is invertible, then  $x$  is invertible, and if  $1 - xy$  is invertible, then  $x = 0$ . This proof translates formally into the corresponding dynamical theory by establishing the following three valid rules:

- $x^2y = x \vdash x = 0 \quad \text{op} \quad x \neq 0$ ,
- $x = 0 \vdash \exists y x^2y = x$ ,
- $x \neq 0 \vdash \exists y x^2y = x$ .

This simple case of eliminating the quantifier  $\exists$  shows that the calculations lead to dead ends from the point of view of decidability, since “ $x = 0$  or invertible” is undecidable in  $\mathbb{R}$ .

Nevertheless, in the final section of the article [26], we find a fully satisfactory constructive form for the 17th Hilbert problem on  $\mathbb{R}$ . And other cases of constructively provable Positivstellensätze on  $\mathbb{R}$  are also treated.

### C.3. Non discrete ordered fields

As a first approximation, and following a suggestion by Heyting, we could choose as a first-order formal theory for the algebraic properties of  $\mathbb{R}$  the *Asonz* theory (seen as a first-order formal theory) to which we add the geometric axioms **IV** and **OTF** as well as the following axiom **HOF**, non-geometric and therefore undesirable.

**HOF**     $(x > 0 \Rightarrow 1 = 0) \Rightarrow x \leq 0$     (Heyting axiom for ordered field)

This amounts to replacing the axioms **col<sub>></sub>** and **OT** by the axioms **OTF** and **HOF**. We then have a local ring structure, because the rules **lv** and **IV** imply that “ $x \neq 0$ ” means “ $x$  is invertible”, so **OTF** implies that for all  $x$ ,  $x$  or  $1 - x$  is invertible. In this context, the axiom **HOF** means that the Jacobson radical is reduced to 0.

*Remark C.3.1.* Note that the axiom **HOF**, which can be formulated to first-order even though it is not part of dynamical theories, is satisfied indirectly in the following form: *in a dynamic algebraic structure of type Asonz, if a closed term  $t$  verifies  $t > 0 \vdash \perp$ , then it also verifies  $\vdash t \leq 0$ .* This follows from the formal Positivstellensatz.

In fact we even have: *if a closed term  $t$  verifies  $t \geq 0 \vdash \perp$ , then it also verifies  $\vdash t < 0$ .* This means that Markov's principle, which is expressed on  $\mathbb{R}$  by the implication  $\neg(t \geq 0) \Rightarrow t < 0$  holds as an *external* deduction rule<sup>7</sup> admissible in the dynamical theory *Asonz*( $\mathbb{R}$ ).

The same remarks apply to dynamical theories which extend *Asonz* while simultaneously collapsing. ■

#### A first dynamical theory

Apart from the undesirable character of **HOF**, the formal theory considered at the beginning of the section has a major drawback, which is that it cannot prove the existence of the upper bound of two elements: see on this subject [13].

It is therefore legitimate to explore the possibilities offered by the addition of a law for this upper bound, with the appropriate rules. We now propose a minimalist dynamical theory for *non* discrete ordered fields by introducing the function symbol  $\vee$  into the language.

**Definition C.3.2.** A first minimal dynamical theory for *non* discrete ordered fields, denoted **Co0**, is based on the following signature. There is only one sort, named *Co0*.

**Signature :**  $\Sigma_{Co0} = (\cdot = 0, \cdot \geq 0, \cdot > 0 \cdot ; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, - \cdot, 0, 1)$

<sup>7</sup>We must add the word *external* here, as this is not a valid rule in the dynamic algebraic structure itself. It refers to the fact that we deduce the validity of one rule from that of another rule.

The axioms are those of *Asonz*, the axioms **IV** and **OTF**, and the natural axioms for  $\vee$ : **sup1**, **sup2**, **Sup**, **grl** and **afr**. They are all listed below ( $x^+$  is an abbreviation of  $x \vee 0$ ).

<b>ga0</b> $\vdash 0 = 0$	<b>ac1</b> $x = 0 \vdash xy = 0$
<b>ga2</b> $x = 0, y = 0 \vdash x + y = 0$	
<b>gao1</b> $x = 0 \vdash x \geq 0$	<b>ao1</b> $\vdash x^2 \geq 0$
<b>gao2</b> $x \geq 0, y \geq 0 \vdash x + y \geq 0$	<b>ao2</b> $x \geq 0, y \geq 0 \vdash xy \geq 0$
<b>aso1</b> $\vdash 1 > 0$	<b>aso3</b> $x > 0, y \geq 0 \vdash x + y > 0$
<b>aso2</b> $x > 0 \vdash x \geq 0$	<b>aso4</b> $x > 0, y > 0 \vdash xy > 0$
<b>sup1</b> $\vdash x \vee y \geq x$	<b>grl</b> $\vdash x + (y \vee z) = (x + y) \vee (x + z)$
<b>sup2</b> $\vdash x \vee y \geq y$	<b>afr</b> $\vdash x^+ (y \vee z) = (x^+ y) \vee (x^+ z)$
<b>Gao</b> $x \geq 0, x \leq 0 \vdash x = 0$	<b>lv</b> $xy = 1 \vdash x^2 > 0$
<b>Anz</b> $x^2 = 0 \vdash x = 0$	<b>Aso1</b> $x > 0, xy \geq 0 \vdash y \geq 0$
<b>Aonz</b> $c \geq 0, x(x^2 + c) \geq 0 \vdash x \geq 0$	<b>Aso2</b> $x \geq 0, xy > 0 \vdash y > 0$
<b>Sup</b> $z \geq x, z \geq y \vdash z \geq x \vee y$	
<b>IV</b> $x > 0 \vdash \exists y xy = 1$	<b>OTF</b> $x + y > 0 \vdash x > 0 \text{ op } y > 0$

*Remarks C.3.3.*

- 1) Note that the collapse “ $0 > 0 \vdash 1 = 0$ ” is deduced from **IV**.
- 2) If we add the axioms **OT** and **col<sub>></sub>** to the theory *Co0* we find a theory which is essentially identical to *Cods<sub>sup</sub>* or *Cod*. In fact, we just need to add the axiom **ED<sub>></sub>**: see Lemma D.4.1. ■

**Examples C.3.4.** Many natural subfields of  $\mathbb{R}$  are *non* discrete, for example the enumerable field  $\mathbb{R}_{\text{PR}}$  of real numbers computable in primitive recursive time, or the enumerable field  $\mathbb{R}_{\text{Ptime}}$  of real numbers computable in polynomial time, or the *non* enumerable field  $\mathbb{R}_{\text{Rec}}$  of recursive real numbers. A satisfactory dynamical theory for the algebraic properties of the real numbers will have to accept as models these natural subfields of  $\mathbb{R}$ . ■

The subfields  $\mathbb{R}_{\text{PR}}$  and  $\mathbb{R}_{\text{Ptime}}$  can be handled on a machine in a nicer way than the field  $\mathbb{R}_{\text{Rec}}$ . These are enumerable fields (albeit *non* discrete), whose elements do not need to be accompanied by “certificates” external to the dynamical theory under consideration (a general recursive map exists constructively only if it is accompanied by a “certificate”: a constructive proof of the fact that it is total).

Note that the “complete” character of  $\mathbb{R}$  seems to come more from analysis than from algebra. Note also that the “field” of Puiseux series on  $\mathbb{R}$  does not seem to satisfy **OTF** (for any attempt at a reasonable definition for the order relation).

## The convexity axiom and the theory *Co*

In addition to the lub map, other “rational” maps pose the same kind of problem.

In the theory of real closed rings, in classical mathematics, (see the articles [63, 56] and Section E.3), the following axiom “of convexity”<sup>8</sup> is satisfied

<sup>8</sup>There are two very distinct uses of the term “convex” in the present text. On the one hand, an ordered ring can be declared convex, as here. On the other hand, a subgroup of an ordered group can be declared convex as page 70.

**CVX**  $0 \leq a \leq b \vdash \exists z \, zb = a^2$  (convexity)

Note that if  $zb = a^2$  then  $(z \wedge a)b = zb \wedge ab = a^2 \wedge ab = a(a \wedge b) = a^2$ . Similarly  $(z \vee 0)b = a^2$ . Consequently, an equivalent axiom which ensures the uniqueness of  $z$  is given by the following dynamical rule:

**FRAC**  $0 \leq a \leq b \vdash \exists z (zb = a^2, 0 \leq z \leq a)$

This rule is valid for  $\mathbb{R}$  because  $z$  can be defined as a continuous map of  $(a, b)$  on its domain of definition.

**Lemma C.3.5.** *The uniqueness of  $z$  (when it exists) in the rule **FRAC** is guaranteed in the Horn theory  $\mathcal{A}tonz$  and in  $\mathcal{C}o0$ . The same calculation shows that uniqueness is guaranteed in the Horn theory  $\mathcal{A}frnz$  (Lemma D.4.7).*

*Proof.* Suppose  $yb = zb = a^2$ ,  $0 \leq z \leq a$  and  $0 \leq y \leq a$ . We have  $(y - z)b = 0$ ,  $|y - z| \leq a \leq b$  and thus  $|y - z|^2 \leq |y - z|b = 0$ .  $\square$

**Lemma C.3.6.** *The addition of the axiom **FRAC** to the theory  $\mathcal{C}o0$  can be replaced by the introduction of a function symbol  $\text{Fr}$  with the axioms*

$$\mathbf{fr1} \vdash \text{Fr}(a, b) |b| = (|a| \wedge |b|)^2 \qquad \mathbf{fr2} \vdash 0 \leq \text{Fr}(a, b) \leq |a| \wedge |b|$$

*The same applies to the theories  $\mathcal{A}tonz$  and  $\mathcal{A}frnz$ .*

*Proof.* The rule **FRAC** is equivalent to the following rule

$$\bullet \vdash \exists z (z|b| = (|a| \wedge |b|)^2, 0 \leq z \leq |a| \wedge |b|)$$

We have therefore simply skolemised an existential rule in the case of unique existence (Lemma C.3.5). This gives us an essentially identical extension (see page 27). Moreover, once the function symbol  $\text{Fr}$  and the axioms **fr1** and **fr2** are added, the rule **FRAC** clearly becomes unnecessary.  $\square$

**Definition C.3.7.** The dynamical theory  $\mathcal{C}o$  of non discrete ordered fields<sup>9</sup> is the extension of the theory  $\mathcal{C}o0$  obtained by adding the function symbol  $\text{Fr}$  and the axioms **fr1** and **fr2**.

This is a one sort dynamical theory with the signature

$$\mathbf{Signature} : \boxed{\Sigma_{\mathcal{C}o} = (\cdot = 0, \cdot \geq 0, \cdot > 0; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, \cdot \wedge \cdot, \text{Fr}(\cdot, \cdot), 0, 1)}$$

The non discrete subfields of  $\mathbb{R}$  of Example C.3.4 are models of  $\mathcal{C}o$ , and also of certain extensions of  $\mathcal{C}o$  which we define later, such as  $\mathcal{C}rc1$  or  $\mathcal{C}orv$ .

*Remark C.3.8.* In formal Positivstellensatz C.2.1 statement, we can add the  $\mathcal{C}odsup$  theory which is essentially identical to the  $\mathcal{C}od$  theory, and the  $\mathcal{C}o$  theory which is intermediate between  $\mathcal{A}sonz$  and  $\mathcal{C}odsup$ . For more information, see formal Positivstellensatz D.5.6.  $\blacksquare$

## Other continuous operations

Here is another paradigmatic example with a continuous function defined everywhere

$$f(x, y) = \frac{(ax + by)xy}{x^2 + y^2} \tag{C.2}$$

<sup>9</sup>In [40], a slightly different, slightly stronger definition was given, see Remark C.3.9.



This rational map <sup>10</sup> is the prototype of a family, parametrised by  $a, b$ , of continuous real maps  $\mathbb{R}^2 \rightarrow \mathbb{R}$  (or of a continuous real map  $\mathbb{R}^4 \rightarrow \mathbb{R}$ ).

A dynamical rule defines this map:

$$\vdash \exists z \quad (z(x^2 + y^2) = (ax + by)xy, |z| \leq |ax + by|) \quad (\text{C.3})$$

and it does not seem valid in the basic theory *Co0*.

In this example, if  $a = b = 1$ , the fraction is of the type  $z = u/v$  with  $u^2 \leq v^3$ . It is characterised by the relationships  $zv = u$  and  $|z|^2 \leq |v|$ . The following dynamical rules are satisfied for  $\mathbb{R}$ , and also for discrete real closed fields:

$$\text{FRAC}_n \quad |u|^n \leq |v|^{n+1} \vdash \exists z (zv = u, |z|^n \leq |v|) \quad (n \geq 1)$$

Intuitively, this rule means that the fraction  $u/v$  is well-defined. In the case of a discrete ordered field we reason case by case: if  $v \neq 0$  it is clear, if  $v = 0$  the rule forces  $z = 0$ . More generally we check that existence, if assumed, is uniquely proved in the theory *Afrmz* (page 78) as follows.

If  $zv = u = yv$ ,  $|z|^n \leq |v|$ ,  $|y|^n \leq |v|$ , we pose  $w = |z - y|$  and we obtain

$$w|v| = 0, \leq |z| + |y| \leq 2|v|^{\frac{1}{n}}, w^n \leq 2^n|v|, 0 \leq w^{n+1} \leq 2^n|v|w = 0,$$

therefore  $w^{n+1} = 0$  and finally  $w = 0$ .

Another argument is that the Horn rule

$$\bullet \quad zv = u, yv = u, |z|^n \leq |v|, |y|^n \leq |v| \vdash z = y$$

is satisfied in *Cod*, and that *Afrmz* and *Cod* prove the same Horn rules (formal Positivstellensatz D.5.6).

In the Horn theory *Aonz* the rule **FRAC** follows from **FRAC**<sub>1</sub> by posing  $u = a^2$  and  $v = b$ .

Conversely, the rules **FRAC** <sub>$n$</sub>  can be deduced from the rule **FRAC** in a fairly general framework (see Lemma D.4.8). In the following we will only use the rule **FRAC**.

*Remark C.3.9.* It would have been more logical to ask, in the definition of the theory *Co*, in addition to the validity of the rule **FRAC**, that of the rules **FRAC** <sub>$n$</sub>  (this was the choice made in the article [40], definition 2.13). More generally, for any map  $f: \mathbb{Q}^n \rightarrow \mathbb{Q}$  which extends by continuity<sup>11</sup> a fraction  $h/p$ , where  $h$  and  $p$  are semipolynomials,<sup>12</sup> the zeros of  $p$  being of empty interior, we should ask that the rule analogous to **FRAC** <sub>$n$</sub>  which says that “ $f$  exists” be valid, and more precisely introduce a corresponding function symbol with the appropriate axioms. But we did not want to complicate too much the definition of the theory *Co* of non discrete ordered fields insofar as we have essentially in view the theory of non discrete real closed fields, in which the rule **FRAC** is sufficient. ■

## C.4. A non-archimedean non discrete ordered field

In this section we describe an example of a non discrete non-archimedean Heyting ordered field.

Let  $\varepsilon$  be an indeterminate. Let  $\mathbf{Z} = \mathbb{Q}[[\varepsilon]]$  be the ring of formal series with rational coefficients and  $\mathbf{Q} = \mathbb{Q}((\varepsilon)) := \mathbb{Q}[[\varepsilon]][1/\varepsilon]$ . In classical mathematics  $\mathbf{Z}$  is a local integral henselian ring and  $\mathbf{Q}$  is its field of fractions. Let  $\mathbf{Z}$  have the order relation for which  $\varepsilon$  is an infinitesimal  $> 0$  (i.e.  $0 < \varepsilon$  and  $\varepsilon < r$  for any rational  $r > 0$ ). Let  $\mathbf{Z}$  be the linearly ordered ring thus obtained. The localised  $\mathbf{Z}[1/\varepsilon]$  with the order relation compatible with that of  $\mathbf{Z}$  will again be denoted  $\mathbf{Q}$ . This is probably the simplest example of a non-archimedean Heyting ordered field.

<sup>10</sup>It is a priori defined for  $(x, y) \neq (0, 0)$  and extends by continuity into  $f(0, 0) = 0$ . We can then see that it is uniformly continuous on any cube  $[-a, +a]^4$ .

<sup>11</sup>More precisely: the fraction  $h/p$  with coefficients in  $\mathbb{Q}$ , defined for  $p(x) \neq 0$ , must extend into a continuous map  $\mathbb{Q}^n \rightarrow \mathbb{Q}$ .

<sup>12</sup>A sup-inf combination of polynomials.

These classical statements are still valid in constructive mathematics, provided that suitable definitions are used. For example, we will see that, modulo suitable definitions,  $\mathbf{Q}$  is a model of the  $\mathbf{Co}$  theory.

From a constructive point of view, there is no sign test on  $\mathbf{Z}$  or on  $\mathbf{Q}$ . And it is not immediate to define an order structure corresponding to the intuition given by classical mathematics.

Here's how to treat this example constructively. An element of  $\mathbf{Z}$  is given by a formal series  $\xi = \sum_{j=0}^{+\infty} x_j \varepsilon^j$  with  $x_j \in \mathbb{Q}$ . Any  $c \in \mathbb{Q}$  can be considered as an element of  $\mathbf{Z}$  according to the usual procedure. The coefficient  $x_j$  is denoted  $c_j(\xi)$ . Conventionally,  $c_j(\xi) = 0$  is given for  $j < 0$  in  $\mathbb{Z}$  and for all  $\xi \in \mathbf{Z}$ .

For a series  $\xi = \sum_{j=0}^{\infty} x_j \varepsilon^j$  in  $\mathbf{Z}$  we define for each  $k \geq 0$  a *potential sign in exponent*  $k$ , denoted  $\kappa_k(\xi) \in \{-1, 0, 1\}$  as follows, by induction on  $k$ :

- $\kappa_0(\xi)$  is the sign of  $x_0$ ;
- if  $\kappa_k(\xi) \neq 0$  then  $\kappa_{k+1}(\xi) = \kappa_k(\xi)$ , otherwise  $\kappa_{k+1}(\xi)$  is the sign of  $x_{k+1}$ ;
- we conventionally pose  $\kappa_j(\xi) = 0$  for  $j < 0$  in  $\mathbb{Z}$  and for all  $\xi \in \mathbf{Z}$ .

At least intuitively we have the following result: if  $\kappa_k(\xi) = 1$ , then  $\xi > 0$ ; if  $\kappa_k(\xi) = -1$ , then  $\xi < 0$ ; if  $\kappa_k(\xi) = 0$ , then the sign of  $\xi$  is a priori unknown.

The set  $\mathbf{Z}$  has the usual ring structure (for formal series) and the equality  $\xi = \zeta$  occurs exactly when the series are identical. This is equivalent to  $\forall k \geq 0 \kappa_k(\xi - \zeta) = 0$ . This ring is the projective limit of the sequence of surjective morphisms  $\pi_{k+1,k}: \mathbb{Q}[\varepsilon]/\langle \varepsilon^{k+1} \rangle \rightarrow \mathbb{Q}[\varepsilon]/\langle \varepsilon^k \rangle$  ( $k \in \mathbb{N}$ ), via the natural morphisms  $\pi_k: \mathbf{Z} \rightarrow \mathbb{Q}[\varepsilon]/\langle \varepsilon^k \rangle$  obtained by truncation of the series to order  $k$ .

The foundations of the constructive theory of residually discrete henselian local rings, including the construction of the henselisation of a residually discrete local ring, are treated in the article [3].

Everything necessary for the constructive treatment of the ordered ring  $\mathbf{Z}$  is now introduced in detail.

1. We define  $\xi > 0$  by  $\boxed{\exists k \kappa_k(\xi) = 1}$  and  $\xi \geq 0$  by  $\boxed{\forall k \kappa_k(\xi) \geq 0}$ .

Then we have:

- $\xi = 0$  if, and only if,  $\xi \geq 0$  and  $\xi \leq 0$ ;
- the rules **OTF** and **OTF<sup>×</sup>** are valid in  $\mathbf{Z}$ ;
- Heyting's axiom " $\neg(x > 0) \Rightarrow -x \geq 0$ " is satisfied.

2. *Absolute value and map sup.* We define the map "absolute value"  $\xi \mapsto |\xi|$  by posing  $\boxed{c_k(|\xi|) := \kappa_k(\xi)c_k(\xi)}$  for all  $k$ . Finally  $\boxed{\xi \vee \zeta := (\xi + \zeta + |\xi - \zeta|)/2}$ .

3. We then check that  $\mathbf{Z}$  is a strict  $f$ -ring (theory  $\mathcal{A}sr$ , Chapter D), in other words, by adding the fact that  $\mathbf{Z}$  is reduced, all the Horn rules valid in the theory  $\mathbf{Codsup}$  are satisfied in  $\mathbf{Z}$  (see the formal Positivstellensatz D.5.6, Item 4).

4. *Valuation.*

- (a) We define  $v(\xi) = k \stackrel{\text{def}}{\iff} (\kappa_k(\xi) = \pm 1, \kappa_{k-1}(\xi) = 0)$ .
- (b) We define  $v(\xi) > k \stackrel{\text{def}}{\iff} \kappa_k(\xi) = 0$ .
- (c) Intuitively, we read  $v(\xi) > k$  as "the valuation of  $\xi$  is  $> k$ ". In fact,  $v(\xi)$  is not an element of  $\mathbb{N}$  but of a suitable compactification of  $\mathbb{N}$  containing  $+\infty$ .<sup>13</sup>
- (d) We have precisely the following description for  $\alpha < \beta$ ;

$$\alpha < \beta \iff \exists k \begin{cases} (\kappa_k(\alpha) = -1, \kappa_k(\beta) \geq 0) & \vee \\ (\kappa_k(\alpha) \leq 0, \kappa_k(\beta) = +1) & \vee \\ (v(\alpha) = v(\beta) = k, c_k(\alpha) < c_k(\beta)) & \end{cases} \quad (\text{C.4})$$

<sup>13</sup>This is the metric space obtained by taking on  $\mathbb{N}$  the metric  $d(k, \ell) = \sup(2^{-k}, 2^{-\ell})$  and completing (this sends  $\infty$  to 0).

- (e) We have  $v(\xi^2) = 2v(\xi)$  (equality defined by  $v(\xi^2) > 2k - 1 \Leftrightarrow v(\xi^2) > 2k \Leftrightarrow v(\xi) > k$ ).
- (f) We deduce that  $\mathbf{Z}$  is a reduced ring (it is thus a constructive model of the *Asmz* theory).
- (g) Finally,  $\mathbf{Z}$  is a *valuation ring* in the following sense: it is a reduced strict  $f$ -ring in which two strictly positive elements  $\alpha$  and  $\beta$  are always comparable for divisibility. In other words, the following rule **Val1** is valid.<sup>14</sup>

**Val1**  $\alpha > 0, \beta > 0 \vdash \exists \xi \alpha \xi = \beta$  **op**  $\exists \xi \beta \xi = \alpha$

A neighbouring rule that is also valid in  $\mathbf{Z}$  is the following.

**Val2**  $\beta \geq \alpha \geq 0, \beta > 0 \vdash \exists \xi \alpha = \beta \xi$

Let's prove these rules. From  $\beta > 0$  we deduce that there is a  $k$  such that  $\beta = \varepsilon^k \gamma$  with  $v(\gamma) = 0$ . We will see in Item 5 that  $\gamma \in \mathbf{Z}^\times$ . Therefore  $\varepsilon^k = \gamma^{-1} \beta$ . For **Val1** we also have a  $\ell$  such that  $\alpha = \varepsilon^\ell \delta$  with  $\delta \in \mathbf{Z}^\times$ . Hence the disjunction depending on whether  $\ell \geq k$  or  $k > \ell$ . For **Val2**, from  $0 \leq \alpha \leq \beta$  we deduce  $\kappa_{k-1}(\alpha) = 0$ , so  $\alpha = \varepsilon^k \delta = \beta \gamma^{-1} \delta$  for a  $\delta \in \mathbf{Z}$ .

Note also that the following implication is satisfied.

$$v(\alpha) = v(\beta) = k \Rightarrow \exists \xi \in \mathbf{Z}^\times \quad \alpha = \beta \xi$$

- (h) The *valuation group* is the ordered group defined as the symmetrisation of the monoid of divisibility  $\mathbf{Z}^\times / \mathbf{Z}^+$  where  $\mathbf{Z}^+ = \{ \alpha \in \mathbf{Z} \mid \exists k > 0 \ v(\alpha) = k \}$ . This valuation group is isomorphic to  $(\mathbb{Z}, +, \geq)$ , and is generated by (the class of)  $\varepsilon$ . In the usual terminology, we say that  $\mathbf{Z}$  is a *discrete valuation ring* (DVR), but here the word "discrete" does not have the usual meaning given to it in constructive mathematics.
5. *Convergent series.* If we have an infinite sequence  $(\xi_n)_{n \in \mathbb{N}}$  in  $\mathbf{Z}$  and if the sequence of  $v(\xi_n)$  tends to  $+\infty$ , then the infinite sum  $\sum_{n \in \mathbb{N}} \xi_n$  is well-defined. In particular, if  $v(\xi) > 0$  the sum  $\zeta = 1 + \sum_{n \in \mathbb{N}} \xi^n$  is well-defined and we have  $\zeta(1 - \xi) = 1$ . From this we can deduce the following properties.
- (a) The ring  $\mathbf{Z}$  is a local ring, whose residual field is discrete, isomorphic to  $\mathbb{Q}$ .
- (b) We have  $\mathbf{Z}^\times = \{ \xi \in \mathbf{Z} \mid \kappa_0(\xi) = \pm 1 \}$  and  $\text{Rad}(\mathbf{Z}) = \{ \xi \in \mathbf{Z} \mid \kappa_0(\xi) = 0 \}$ .
- (c) If  $c(\beta) = k$ , we write  $\beta = \varepsilon^k \gamma$  with  $\gamma = c_0(1 - \alpha)$  and  $v(\alpha) > 0$ , therefore:  $\varepsilon^k = \beta \gamma^{-1} = \beta c_0^{-1} (1 + \text{sum}_{n \in \mathbb{N}} \alpha^n)$ .
- (d) The ring  $\mathbf{Z}$  is henselian. Precisely, if  $P \in \mathbf{Z}[X]$  satisfies the conditions  $v(P(0)) > 0$  and  $v(P'(0)) = 0$ , there exists a (unique)  $\xi \in \mathbf{Z}$  such that  $P(\xi) = 0$  and  $v(\xi) > 0$ . To construct the series  $\xi$ , we use Newton's method.
- (e) The ring  $\mathbf{Z}$  is the henselisation of the residually discrete local ring  $(\mathbb{Q}[\varepsilon])_{1 + \varepsilon \mathbb{Q}[\varepsilon]}$ .
6. Finally, we show that the rule **FRAC** is valid in  $\mathbf{Z}$ . The hypothesis is given by two elements  $\xi, \zeta \in \mathbf{Z}$  which verify  $0 \leq \xi \leq \zeta$  and we look for a  $\rho$  such that  $0 \leq \rho \leq \xi$  and  $\rho \zeta = \xi^2$ . According to Lemma D.4.7, the uniqueness of  $\rho$  (if existence) is guaranteed in strict  $f$ -rings, as in the theory **CoO** (Lemma C.3.5).

We note that  $0 \leq \xi \leq \zeta$  implies that  $v(\xi) \geq v(\zeta)$ . We define  $c_k(\rho)$  as follows.

- If  $\kappa_k(\zeta) = 0$ , then  $\kappa_k(\xi) = 0$ , which forces  $\kappa_k(\rho) = 0$ , so  $c_k(\rho) = 0$ .
- If  $v(\zeta) = k$ , we have  $\zeta = z_k \varepsilon^k (1 + \varepsilon \alpha)$  with  $z_k > 0$  and  $\alpha \in \mathbf{Z}$ , and  $\xi = \varepsilon^k \beta$  with  $\beta \in \mathbf{Z}$ . Then we must have the equality  $\rho = z_k^{-1} \beta^2 \varepsilon^k (1 + \varepsilon \alpha)^{-1}$ . As this equality implies  $\kappa_{k-1}(\rho) = 0$ , it is compatible with the coefficients of  $\rho$  calculated up to exponent  $k - 1$ . This equality makes it possible to define  $c_{k+m}(\rho)$  for all  $m > 0$ .

<sup>14</sup>We give here a definition for the case of a strict  $f$ -ring. A more general definition could be given for a residually discrete local ring with a suitable  $\cdot \neq 0$  predicate.

- Finally if  $\kappa_{k-1}(\zeta) = \kappa_k(\zeta) = 1$ , we look for the exponent  $\ell < k$  such that  $\kappa_{\ell-1}(\zeta) = 0$  and  $\kappa_\ell(\zeta) = 1$ , and we are brought back to the previous case via the calculation of the series  $\rho$ .

So  $\rho$  is well-defined.

Let's summarise the results.

**Proposition C.4.1.** *The ring  $\mathbf{Z}$  is an henselian residually discrete local ring and a reduced strict  $f$ -ring. Moreover it satisfies the rules **OTF**, **FRAC**, **Val1** and **Val2**.*

The test on  $\mathbf{Z}$  for  $\forall \alpha (\alpha^2 > 0 \vee \alpha = 0)$  is equivalent to **LPO**.

Nor can we prove constructively that  $\mathbf{Z}$  is a ring without zerodivisor: the hypothesis  $\xi\zeta = 0$  is equivalent to  $|\xi| \wedge |\zeta| = 0$ , but the implication  $|\xi| \wedge |\zeta| = 0 \Rightarrow ((|\xi| = 0) \vee (|\zeta| = 0))$  is equivalent to the principle **LPPO**.

Finally, we cannot prove that every regular element  $\geq 0$  is strictly positive: this is equivalent to the Markov principle **MP**. The total ring of fractions of  $\mathbf{Z}$  is therefore a somewhat mysterious object, a ring which contains  $\mathbf{Q}$  and which fortunately is of no obvious mathematical interest.

*Note.* The articles [30, 31] propose a constructive theory of valuation rings (without order relation) only in the case of integral rings with a decidable divisibility relation. It would be useful to generalise the results (obtained constructively) to valuation rings in the sense given for  $\mathbf{Z}$ , and to other similar cases (we need a separation relation on the ring)<sup>15</sup> can be used as a basis. ■

It is easy to deduce the following theorem from Proposition C.4.1.

**Theorem C.4.2.** *The ring  $\mathbf{Q} = \mathbf{Z}[1/\varepsilon]$  satisfies all the axioms of the theory **Co** as well as the ordered Heyting axiom. It is a residually discrete local ring with  $\text{Rad}(\mathbf{Q}) = 0$  (thus a Heyting field in the terminology of [CACM] or [MRR]). In short, it is a non-archimedean Heyting field, and a non discrete ordered field in the sense of **Co** theory.*

*Note.* An element of  $\mathbf{Q} = \mathbf{Z}[1/\varepsilon]$  is written  $\varepsilon^{j_0}\alpha$  with  $\alpha \in \mathbf{Z}$  and  $j_0 \in \mathbb{Z}$ , it can be encoded in the form  $\gamma = (j_0, \alpha)$ . The equality  $(j_0, \alpha) = (j'_0, \alpha')$  is defined as follows:

- if  $j_0 \leq j'_0$ ,  $\varepsilon^{j'_0 - j_0}\alpha = \alpha'$ ;
- si  $j'_0 \leq j_0$ ,  $\varepsilon^{j_0 - j'_0}\alpha' = \alpha$ .

We then define, for  $\gamma = (j_0, \alpha)$ :

- $\kappa_k(\gamma) = \kappa_{k-j_0}(\alpha)$  (so  $\kappa_k(\gamma) = 0$  for  $k < j_0$ ) ;
- $c_k(\gamma) = c_{k-j_0}(\alpha)$  (so  $c_k(\gamma) = 0$  for  $k < j_0$ ) ;
- $v(\gamma) = v(\alpha) - j_0$  (so  $v(\gamma) \geq -j_0$ ). ■

## C.5. Non discrete real closed fields: position of the problem

Our dream is to repeat the feat that Artin, Schreier and Tarski achieved for the description of the algebraic properties of  $\mathbb{R}$  through the theory of discrete real closed fields, but in a constructive framework, in intuitionistic logic without **LEM**, taking into account the fact that  $\mathbb{R}$  is not discrete, and avoiding the axiom of dependent choice.

*Remark C.5.1.* We can consider that our quest is the following: to fix a signature  $\Sigma$  which allows us to describe as precisely as possible the structure of a non discrete real closed field, to describe on this signature a dynamical theory which is essentially equivalent to a theory weaker than **Crcd**, while being the strongest possible among the dynamical theories which admit  $\mathbb{R}$  as a constructive model, without using the axiom of dependent choice. This Holy Grail seems out of reach in absolute terms, as there is no clear criterion for knowing whether a dynamical rule is constructively satisfied on  $\mathbb{R}$ .<sup>16</sup> ■

<sup>15</sup>See also the article [3].

<sup>16</sup>Moreover, the axiom of dependent choice is not allowed in proofs.

## The principle of extension by continuity

The “completion” property of  $\mathbb{R}$  is expressed naturally in the following form, without interference from the axiom of dependent choice.

**Theorem C.5.2.** *If a map  $f: \mathbb{Q}^n \rightarrow \mathbb{R}$  is uniformly continuous on all bounded subsets it extends uniquely into a map  $\tilde{f}: \mathbb{R}^n \rightarrow \mathbb{R}$  uniformly continuous on all bounded subsets.*

This theorem is a theorem of analysis and cannot be expressed directly in the context of a dynamical theory which aims at the algebraic properties of  $\mathbb{R}$ , because the property “to be uniformly continuous” is not geometric.

Nevertheless, it is essentially this theorem that guides us in our quest expressed in Remark C.5.1. We will replace the property “be uniformly continuous” by a formulation where uniform continuity is controlled a priori and no longer hides  $\forall\exists$ .

Moreover, the only maps that we can envisage inside in a purely algebraic framework are semialgebraic maps.

We must therefore rely on relevant properties of continuous semialgebraic maps, which we develop in the following paragraph.

## Continuous semialgebraic maps

First of all we recall that the uniform continuity over any bounded subset of a continuous semialgebraic map  $\mathbf{R}^n \rightarrow \mathbf{R}$ , where  $\mathbf{R}$  is a discrete real closed field, is controlled à la Łojasiewicz precisely as follows.

**Lemma C.5.3.** *Let  $\mathbf{R}$  be a discrete real closed field and  $K \subseteq \mathbf{R}^n$  be a bounded semialgebraic closed subset.*

1. *Let  $g: K \rightarrow \mathbf{R}$  be a continuous semialgebraic map. Then  $g$  has a uniform continuity modulus which is expressed à la Łojasiewicz as follows (with  $c \in \mathbf{R}$  and  $\ell$  integer  $\geq 1$ )*

$$\forall \underline{\xi}, \underline{\xi}' \in K \quad |g(\underline{\xi}) - g(\underline{\xi}')|^\ell \leq |c| \|\underline{\xi} - \underline{\xi}'\|. \quad (\text{C.5})$$

2. *Let  $f: \mathbf{R}^n \rightarrow \mathbf{R}$  be a continuous semialgebraic map. Then  $f$  has a uniform continuity modulus over any bounded subset which is expressed à la Łojasiewicz as follows (with  $c \in \mathbf{R}$  and integers  $k, \ell \geq 1$ )*

$$\forall \underline{\xi}, \underline{\xi}' \in \mathbf{R}^n \quad |f(\underline{\xi}) - f(\underline{\xi}')|^\ell \leq |c| (1 + \|\underline{\xi}\| + \|\underline{\xi}'\|)^k \|\underline{\xi} - \underline{\xi}'\|. \quad (\text{C.6})$$

*Proof.* This is a consequence of Theorem 2.6.6 of [Bochnak, Coste & Roy] which states that on a locally closed semialgebraic set, if there are two continuous semialgebraic maps  $F$  and  $G$  such that  $G$  vanishes at the zeros of  $F$ , there exists an exponent  $N$  and a continuous semialgebraic map  $h$  such that  $G^N = hF$ . In the compact case,  $h$  is bounded by a constant; in the general case,  $h$  is bounded by a polynomial map. We apply this with  $F(\underline{x}, \underline{x}') = \|\underline{x} - \underline{x}'\|$  and  $G(\underline{x}, \underline{x}') = |f(\underline{x}) - f(\underline{x}')|$ .  $\square$

### • Continuous parametrisation of continuous semialgebraic maps

We now present a parametrisation result saying that, *from the point of view of continuous semialgebraic maps, everything comes continuously from what happens on the subfield  $\mathbb{R}_{\text{alg}}$  of algebraic real numbers*. In other words, any continuous semialgebraic map  $\mathbf{R}^n \rightarrow \mathbf{R}$  is a point with coordinates in  $\mathbf{R}$  of an equicontinuous family defined on  $\mathbb{R}_{\text{alg}}$ .

The idea is in fact a simple generalisation of the following remark. The family of univariate polynomials  $f(x) = ax^2 + bx + c$  (family parametrised by  $(a, b, c) \in \mathbb{R}^3$ ) is never just the polynomial in four variables  $g(a, b, c, x) = ax^2 + bx + c$  defined on  $\mathbb{Q}$ , where we take  $(a, b, c)$  as parameters and  $x$  as variable, all in  $\mathbb{R}$ : so we don't have to worry too much about the *non* discrete character of  $\mathbb{R}$ , since everything is defined on  $\mathbb{Q}$ . Each individual map  $f(x)$  (depending on parameters taken from  $\mathbb{R}^3$ ) is a real point of a family defined on  $\mathbb{R}_{\text{alg}}$ . This real point comes from the extension by continuity at  $\mathbb{R}^4$  of a continuous map  $\mathbb{R}_{\text{alg}}^4 \rightarrow \mathbb{R}_{\text{alg}}$ .

**Theorem C.5.4.** *Let  $\mathbf{R}$  be a discrete real closed field and  $f: \mathbf{R}^n \rightarrow \mathbf{R}$  be a continuous semialgebraic map. There exists an integer  $r \geq 0$ , a continuous semialgebraic map  $g: \mathbf{R}^{r+n} \rightarrow \mathbf{R}$  defined on  $\mathbb{R}_{\text{alg}}$ , and an element  $\underline{y} \in \mathbf{R}^r$  such that*

$$\forall x_1, \dots, x_n \in \mathbf{R} \quad f(x_1, \dots, x_n) = g(y_1, \dots, y_r, x_1, \dots, x_n).$$

This result seems to be part of folklore. We give here a proof inspired by the advices of Michel Coste and Marcus Tressl. However, it is not entirely constructive. This would require, for example, a constructive re-reading of Chapter 7 of [Bochnak, Coste & Roy]. See Question C.7.1.

*Proof.* The map  $f$  has a closed graph  $F$  which is a semialgebraic union of basic semialgebraic closed sets  $F_i = \{(\underline{x}, y) \in \mathbf{R}^{n+1} \mid p_i(\underline{x}, y) \geq 0\}$ . The coefficients of  $p_i$  are in  $\mathbf{R}$  but can be seen as specialisations of parameters  $c_k$  ( $k \in \llbracket 1..m \rrbracket$ ) so that we have polynomials  $P_i(c, \underline{x}, y)$  with parameters  $c_k$ . The inequalities  $P_i(c, \underline{x}, y) \geq 0$  define for  $i$  a fixed semialgebraic closed set  $G_i \subseteq \mathbf{R}^{m+n+1}$ . The union of  $G_i$ 's, denoted  $G$ , is a semialgebraic which is not sufficiently relevant. We add a parameter  $c_0$  and we will now restrict the domain of variation of  $c_k$  to a “suitable” semialgebraic set  $S$ . Suitable means that the following formula is satisfied

$$\forall \underline{\xi}, \underline{\xi}' \in \mathbf{R}^n \quad \forall \zeta, \zeta' \in \mathbf{R} \quad ((c, \underline{\xi}, \zeta) \in G, (c, \underline{\xi}', \zeta') \in G) \Rightarrow |\zeta - \zeta'|^\ell \leq |c_0| (1 + \|\underline{\xi}\| + \|\underline{\xi}'\|)^k \|\underline{\xi} - \underline{\xi}'\|.$$

where  $k$  and  $\ell$  are integers for which the map  $f$  satisfies these inequalities (for a certain specialisation of  $c_0$ ). Note that  $S \subseteq \mathbf{R}^{m+1}$ . It is clear that the semialgebraic set  $S$  is defined on  $\mathbb{R}_{\text{alg}}$ . Let  $H$  be the semialgebraic subset of  $\mathbf{R}^{m+n+2}$  formed by the points of  $G$  whose  $m+1$  first coordinates (the parameters) form a point of  $S$ . The semialgebraic set  $H$  is the graph of a map  $h: S \times \mathbf{R}^n \rightarrow \mathbf{R}$ , which is seen as a family of maps  $\mathbf{R}^n \rightarrow \mathbf{R}$  parametrised by  $S$ . For any point  $s \in S$  the corresponding graph  $H_s$  is that of a continuous semialgebraic map  $f_s: \mathbf{R}^n \rightarrow \mathbf{R}$  whose uniform continuity modulus is controlled by  $|c_0|$ ,  $k$  and  $\ell$ . The initial map  $f$  corresponds to a point  $s_0 \in S$  with coordinates in  $\mathbf{R}$ . By means of a cylindrical algebraic decomposition of  $\mathbf{R}^{m+1}$  adapted to  $S$ , we insert  $s_0$  in a cell  $\Gamma$  defined on  $\mathbb{R}_{\text{alg}}$  semialgebraically homeomorphic to  $\mathbf{R}^q$  for a  $q \geq 0$  ( $q = 0$  implies that  $s_0$  has coordinates in  $\mathbb{R}_{\text{alg}}$ ). Moreover the homeomorphism is defined on  $\mathbb{R}_{\text{alg}}$ . We then obtain a semialgebraic map  $\varphi: \mathbf{R}^{q+n} \rightarrow \mathbf{R}$  defined on  $\mathbb{R}_{\text{alg}}$  which has the following properties:

- There is an element  $\gamma = (\gamma_1, \dots, \gamma_q) \in \mathbf{R}^q$  such that  $\varphi(\gamma, \underline{\xi}) = f(\underline{\xi})$  for all  $\underline{\xi} \in \mathbf{R}^n$ .
- For any element  $\alpha = (\alpha_1, \dots, \alpha_q) \in \mathbf{R}^q$ , the map  $\underline{\xi} \mapsto \varphi(\alpha, \underline{\xi})$  is continuous semialgebraic. The map  $\varphi$  is locally bounded.

Under these hypotheses, Remark 7.4.9 of [Bochnak, Coste & Roy], assures us that there exists a semialgebraic partition  $A_1 \cup \dots \cup A_k$  of the space of parameters  $\mathbf{R}^q$ , defined on  $\mathbb{R}_{\text{alg}}$ , such that the map  $\varphi$  restricted to each of the  $A_i \times \mathbf{R}^n$  is continuous. For example the point  $\gamma = (\gamma_1, \dots, \gamma_q)$  belongs to  $A_1$ . By means of a cylindrical algebraic decomposition of  $\mathbf{R}^q$  adapted to  $A_1$ , we insert  $\gamma$  in a cell  $\Delta$  defined on  $\mathbb{R}_{\text{alg}}$  semialgebraically homeomorphic to  $\mathbf{R}^r$  for an  $r \geq 0$ . Moreover the homeomorphism is defined on  $\mathbb{R}_{\text{alg}}$ . This provides the continuous semialgebraic map  $g: \mathbf{R}^{r+n} \rightarrow \mathbf{R}$  defined on  $\mathbb{R}_{\text{alg}}$  requested in the statement.  $\square$

#### • A reasonable definition

We therefore propose the following definition in constructive mathematics, made legitimate by Theorem C.5.4.

**Definition and notation C.5.5.** Let  $\mathbf{R}$  be an ordered subfield<sup>17</sup> of  $\mathbb{R}$  containing the field of algebraic reals  $\mathbb{R}_{\text{alg}}$  and a map  $f: \mathbf{R}^n \rightarrow \mathbf{R}$ .

1. (elementary case) The map  $f$  is semialgebraic continuous if there exists a continuous semialgebraic map  $g: \mathbb{R}_{\text{alg}}^n \rightarrow \mathbb{R}_{\text{alg}}$  of which  $f$  is the extension by continuity. Precisely we must have the following two properties:  $f$  is an extension of  $g$ , and  $f$  has the same uniform modulus of continuity as  $g$ , given in Item 2 of Lemma C.5.3.

<sup>17</sup>Precisely  $\mathbf{R}$  is a subobject of  $\mathbb{R}$  for the non discrete ordered field defined by the theory  $\mathcal{C}\mathcal{o}$ . Moreover, for the simple existential rule **IV**, we require that an element of  $\mathbf{R}$  invertible in  $\mathbb{R}$  be invertible in  $\mathbf{R}$ .

2. (general case) The map  $f$  is semialgebraic continuous if there exist an integer  $r \geq 0$ , elements  $y_1, \dots, y_r \in \mathbf{R}$  and a map  $h: \mathbf{R}^{r+n} \rightarrow \mathbf{R}$  which belongs to the previous elementary case such that

$$\forall x_1, \dots, x_n \in \mathbf{R} \quad f(x_1, \dots, x_n) = h(y_1, \dots, y_r, x_1, \dots, x_n).$$

We denote  $\text{Fsa}_n(\mathbf{R})$  the ring of these maps (it is a reduced strict  $f$ -ring for the natural order relation).

Some important properties of these function spaces will be established in Section C.6.

## Rational dynamical theories for real number algebra

Recall that the field  $\mathbb{R}_{\text{alg}}$  of the algebraic reals is a discrete real closed field in the constructive sense.

Following on from Remark C.5.1 and Definition C.5.5, here are the properties we have in mind for a dynamical theory  $\text{Crc}$  of (*non* discrete) real closed fields, described here in a rather informal way.

### Expected properties C.5.6.

1. The theory  $\text{Crc}$  is an extension of  $\text{Co}$ .
2. The fields  $\mathbb{R}$ ,  $\mathbb{R}_{\text{PR}}$ ,  $\mathbb{R}_{\text{Ptime}}$  and  $\mathbb{R}_{\text{Rec}}$  (cf. Example C.3.4) are constructive models of  $\text{Crc}$  (without using the axiom of dependent choice).
3. The theory  $\text{Crc}$  becomes essentially equivalent to  $\text{Crcd}$  when we add to it the axiom  $\text{ED}_{>}$ .
4. The continuous semialgebraic maps  $\mathbb{R}_{\text{alg}}^n \rightarrow \mathbb{R}_{\text{alg}}$  are nicely defined in the language of  $\text{Crc}$  and the Horn rules they satisfy are valid in the theory.
5. Continuity extension principles (as broad as possible) are satisfied in a suitable form in the dynamical theory.
6. Gluing principles (the broadest possible) for maps defined on a finite covering by semialgebraic openings, or by semialgebraic closures, are satisfied in a suitable form in the dynamical theory.

The following points are open to discussion. Item 7 will be dropped if we want to describe more “structure” on  $\mathbb{R}$ , for example for an  $o$ -minimal structure. Item 8 will be abandoned for example if we wish to introduce all the reals as constants of the theory: in a general dynamical theory  $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ ,  $\mathcal{L}$  and  $\mathcal{A}$  are only supposed to be naive sets (à la Bishop).

7. All function symbols in  $\text{Crc}$  define on  $\mathbb{R}$  continuous semialgebraic maps of their variables (Definition C.5.5).
8. The language of  $\text{Crc}$  is enumerated in a natural way and in this framework the axioms are decidable in a primitive recursive way.

A slightly crude way of getting a relatively satisfactory answer is to take seriously Item 4 above. The result is as follows.

**Definition C.5.7.** The dynamical theory  $\text{Crc1}$  is obtained from the dynamical theory  $\text{Co}$  by adding a function symbol and suitable axioms for each continuous semialgebraic map  $f: \mathbb{R}_{\text{alg}}^n \rightarrow \mathbb{R}_{\text{alg}}$ .

*Explanation.* More precisely, we proceed as follows. We know from the finiteness theorem ([Bochnak, Coste & Roy, Theorem 2.7.1]) that the graph  $G_f = \{(\underline{x}, y) \mid \underline{x} \in \mathbf{R}^n, y = f(\underline{x})\}$  of  $f$  (which is assumed to be semialgebraically continuous) is a semialgebraic closed set of  $\mathbb{R}_{\text{alg}}^{n+1}$  which can be

described as the zero set of a *semipolynomial map*  $F: \mathbb{R}_{\text{alg}}^{n+1} \rightarrow \mathbb{R}_{\text{alg}}$ , i. e. a map written in the form

$$\sup_i (\inf_{ij} p_{ij}) \quad \text{where } p_{ij} \in \mathbb{R}_{\text{alg}}[x_1, \dots, x_n, y]$$

We can decide whether such a semialgebraic closed set  $G_f$  described in this way is that of a continuous semialgebraic map, and if so calculate a uniform continuity modulus à la Łojasiewicz. Whenever such a (description of) semipolynomial map defines a continuous semialgebraic map, we introduce a function symbol  $\text{fsa}_F$  with the corresponding axiom

$$\mathbf{Df}_F \vdash F(\underline{x}, \text{fsa}_F(\underline{x})) = 0.$$

Furthermore, for an arbitrary term  $t(\underline{x})$  in the language thus defined, if this term defines a map everywhere zero on  $\mathbb{R}_{\text{alg}}^n$  ( $n \geq 0$ ), we introduce the corresponding axiom  $\vdash t(\underline{x}) = 0$ .

For example, for the map  $\text{fsa}_F$  we will have an axiom of continuity which repeats that which is satisfied for the algebraic reals.

$$\mathbf{Cont}_F \vdash |\text{fsa}_F(\underline{x}) - \text{fsa}_F(\underline{x}')|^\ell \leq |c| (1 + \|\underline{x}\| + \|\underline{x}'\|)^k \|\underline{x} - \underline{x}'\|.$$

Indeed, an inequality between two terms,  $t_1 \leq t_2$ , is equivalent to making the term  $(t_2 - t_1)^-$  equal to 0. ■

Naturally, such a dynamical theory is frustrating at first sight, because it is not very natural and it is undoubtedly difficult to practise from an effective point of view.

However, we shall see that a more natural way, with the addition of few function symbols, which we propose later, leads to the theory *Corv* essentially identical to *Crc1*.

All this is closely related to the theory of real closed rings and its rewriting in concrete form in [69].

## C.6. General properties of continuous semialgebraic maps

In this section we give some remarkable properties of the rings  $\mathbf{Fsac}_n(\mathbf{R})$  (continuous semialgebraic maps  $\mathbf{R}^n \rightarrow \mathbf{R}$  according to Definition C.5.5) over the field  $\mathbf{R} = \mathbb{R}$ . More generally we can consider an ordered subfield  $\mathbf{R}$  of  $\mathbb{R}$  containing  $\mathbb{R}_{\text{alg}}$  and in which any continuous semialgebraic map defined on  $\mathbb{R}_{\text{alg}}$  takes its values in  $\mathbf{R}$  at the points whose coordinates are in  $\mathbf{R}$ , for example  $\mathbb{R}_{\mathbf{PR}}$ ,  $\mathbb{R}_{\mathbf{Ptime}}$  or  $\mathbb{R}_{\mathbf{Rec}}$ .

These properties known for discrete real closed fields are extended to  $\mathbb{R}$  because we take the precaution of only taking properties whose formulation does not imply the discrete nature of the order.

### Stability by composition

For example we compose  $f, g \in \mathbf{Fsac}_3(\mathbf{R})$  with  $h \in \mathbf{Fsac}_2(\mathbf{R})$ . Suppose that

- $f$  is given in the form  $f(x, y, z) = \tilde{f}(a, b, x, y, z)$ , for  $a, b \in \mathbf{R}$  and  $\tilde{f}: \mathbf{R}^5 \rightarrow \mathbf{R}$  extends by continuity  $\bar{f}: \mathbb{R}_{\text{alg}}^5 \rightarrow \mathbb{R}_{\text{alg}}$ ,
- $g$  is given by the form  $g(x, y, z) = \tilde{g}(c, x, y, z)$ , for  $c \in \mathbf{R}$  and  $\tilde{g}: \mathbf{R}^4 \rightarrow \mathbf{R}$  extends by continuity  $\bar{g}: \mathbb{R}_{\text{alg}}^4 \rightarrow \mathbb{R}_{\text{alg}}$ ,
- $h$  is given by the form  $h(u, v) = \tilde{h}(d, u, v)$ , for  $d \in \mathbf{R}$  and  $\tilde{h}: \mathbf{R}^3 \rightarrow \mathbf{R}$  is a continuous extension of  $\bar{h}: \mathbb{R}_{\text{alg}}^3 \rightarrow \mathbb{R}_{\text{alg}}$ ,
- then  $h \circ (f, g): \mathbf{R}^3 \rightarrow \mathbf{R}$  is of the form  $k(x, y, z) = \tilde{k}(a, b, c, d, x, y, z)$  for  $(a, b, c, d) \in \mathbf{R}^4$  and  $\tilde{k}: \mathbf{R}^7 \rightarrow \mathbf{R}$  extends by continuity the map  $\bar{k}: \mathbb{R}_{\text{alg}}^7 \rightarrow \mathbb{R}_{\text{alg}}$  defined by

$$\bar{k}(a, b, c, d, x, y, z) = h(d, f(a, b, x, y, z), g(c, x, y, z)).$$



## Stability by upper bound

For example we have  $f \in \text{Fsac}_4(\mathbf{R})$  and we want to show that there is a  $g \in \text{Fsac}_2(\mathbf{R})$  such that  $g(x, y) = \sup_{z, t \in [0, 1]} f(x, y, z, t)$ . If  $f$  is given in the form  $f(x, y, z, t) = \tilde{f}(a, b, x, y, z, t)$ , for  $a, b \in \mathbf{R}$ , where  $\tilde{f}: \mathbf{R}^6 \rightarrow \mathbf{R}$  extends by continuity  $\bar{f}: \mathbf{R}_{\text{alg}}^6 \rightarrow \mathbf{R}_{\text{alg}}$ , consider the continuous semialgebraic map  $\bar{g}: \mathbf{R}_{\text{alg}}^4 \rightarrow \mathbf{R}_{\text{alg}}$  defined by  $\bar{g}(a, b, x, y) = \sup_{z, t \in [0, 1]} \bar{f}(a, b, x, y, z, t)$ .<sup>18</sup> It extends by continuity into a map  $\tilde{g}: \mathbf{R}^4 \rightarrow \mathbf{R}$  and we define  $g(x, y) = \tilde{g}(a, b, x, y)$ . The fact that  $g$  is indeed the desired lub is due to the fact that the lub on a compact is a continuous function of the parameters and that  $\mathbf{R}_{\text{alg}}$  is dense in  $\mathbf{R}$ .

## Finiteness properties

In classical mathematics, any continuous semialgebraic map  $f: \mathbb{R} \rightarrow \mathbb{R}$  has a finite table of signs and variations. But this table does not depend continuously on the parameters, for example when  $f(x) = g(a_1, \dots, a_n, x)$  for parameters  $a_1, \dots, a_n \in \mathbb{R}^n$ , where  $g$  is the continuity extension of a continuous semialgebraic map  $\bar{g}: \mathbb{R}_{\text{alg}}^{n+1} \rightarrow \mathbb{R}_{\text{alg}}$ .

However, when  $f$  is a monic polynomial, a constructive approach to the question is to use virtual root maps. For example we can see Items [3h](#), [3i](#), [3j](#) and [3k](#) of Theorem [E.2.6](#) as well as Proposition [E.6.3](#).

Analogous results should be established in constructive mathematics for arbitrary continuous semialgebraic maps, at least for Proposition [E.6.3](#), but restricted to maps on the interval  $[-1, 1]$  (on  $\mathbb{R}$  this would not be possible). It may be necessary to use an infinite **OP**.

## C.7. Some questions

**Question C.7.1.** Give a complete constructive proof of Theorem [C.5.4](#).

**Question C.7.2.** Show that the Horn rule **FRAC** is not valid in [Co0](#). Similarly, show that the Horn rule [\(C.3\)](#) which is equivalent to the existence of the map [\(C.2\)](#) page [53](#) is not valid in [Co0](#).

**Question C.7.3.** Determine which algebraic properties of  $\mathbb{R}$  allow us to prove the constructively satisfying forms of Positivstellensätze proved for  $\mathbb{R}$  in [\[26\]](#). See in particular Question [E.7.12](#).

## Continuous variations

Continuous semialgebraic maps  $\mathbb{R}^n \rightarrow \mathbb{R}$  could have been defined as follows. This was the definition adopted in [\[40, Definition 3.3\]](#).

**Definition C.7.4.** Let  $\mathbf{R}$  be a commutative ring. A map  $f: \mathbf{R}^n \rightarrow \mathbf{R}$  is said to be *algebraic on*  $\mathbf{R}[x_1, \dots, x_n] = \mathbf{R}[x]$  if there is a polynomial  $g(x, y) = \sum_{k=0}^m g_k(x)y^k \in \mathbf{R}[x, y]$ , with at least one of the coefficients of a  $g_k(x)$  invertible, such that  $g(\xi, f(\xi)) = 0$  for all  $(\xi) \in \mathbf{R}^n$ .

**Definition C.7.5** (alternative definition to [C.5.5](#)). Let  $\mathbf{R}$  be a subfield of  $\mathbb{R}$ . A map  $f: \mathbf{R}^n \rightarrow \mathbf{R}$  is said to be *semialgebraic continuous* if, on the one hand, it is algebraic on  $\mathbf{R}[x]$  and if, on the other hand, it has a uniform continuity modulus on everything bounded à la Łojasiewicz, given by an inequality [C.6](#) as in Lemma [C.5.3](#).

This definition is legitimate for subfields of  $\mathbb{R}$  because

- it is valid in classical mathematics,
- it has a clear constructive meaning,
- semialgebraic maps which are continuous in the sense of Definition [C.5.5](#) are also continuous in the sense of Definition [C.7.5](#).

---

<sup>18</sup>Here,  $a, b$  are variables.

**Question C.7.6.** If a map  $f: \mathbb{R}^n \rightarrow \mathbb{R}$  is algebraic on  $\mathbb{R}[x]$  and if it is uniformly continuous on all bounded subsets, does it have a uniform continuity modulus à la Łojasiewicz, as in Lemma C.5.3? NB: the answer is positive in classical mathematics, but it seems much trickier in constructive mathematics.

**Question C.7.7.** Is a semialgebraic map that is continuous in the sense of Definition C.7.5 also continuous in the sense of Definition C.5.5?

Yes in classical mathematics, but the problem arises in constructive mathematics, and seems very difficult. It may be that, by preferring the Definition C.5.5 to Definition C.7.5, we are in a situation similar to that which led Bishop to define the continuity of a map  $\mathbb{R} \rightarrow \mathbb{R}$  as meaning uniform continuity on any bounded interval.



# D. $f$ -rings

## Sommaire

---

<b>Introduction</b> . . . . .	<b>66</b>
<b>D.1 Distributive lattices</b> . . . . .	<b>66</b>
Distributive lattice theory . . . . .	66
Ideals and filters in a distributive lattice . . . . .	66
Quotients . . . . .	67
<b>D.2 <math>\ell</math>-groups</b> . . . . .	<b>68</b>
Definition of the purely equational theory $\mathit{Gr}\ell$ . . . . .	68
Some rules derived in $\mathit{Gr}\ell$ . . . . .	69
Quotient structures . . . . .	70
Representation theorem . . . . .	70
<b>D.3 <math>f</math>-rings</b> . . . . .	<b>72</b>
Purely equational theory of $f$ -rings . . . . .	72
Note on $\ell$ -rings . . . . .	73
Some derived rules . . . . .	73
Quotient structures . . . . .	74
Solid ideals (or $\ell$ -ideals) . . . . .	74
Irreducible $\ell$ -ideals . . . . .	74
Formal Positivstellensatz and representation theorem . . . . .	74
Localisations of $f$ -rings . . . . .	75
Generalities . . . . .	75
Gluing $f$ -rings . . . . .	76
Real schemes . . . . .	76
Rewriting terms in $f$ -rings . . . . .	76
$f$ -rings of maps, semipolynomials . . . . .	77
<b>D.4 Beyond purely equational theories</b> . . . . .	<b>77</b>
$f$ -rings without zerodivisor . . . . .	77
Local $f$ -rings . . . . .	78
Strict $f$ -ring . . . . .	78
Reduced $f$ -rings . . . . .	78
Some derived rules . . . . .	78
The rule <b>FRAC</b> in $\mathit{Afmz}$ . . . . .	79
<b>D.5 Back to ordered fields</b> . . . . .	<b>80</b>
Real $f$ -rings . . . . .	80
Formal Positivstellensätze with sup . . . . .	81
<b>D.6 The real lattice and spectrum of a commutative ring</b> . . . . .	<b>83</b>

---

## Introduction

This chapter takes up the problem of *non* discrete ordered fields from scratch.

All the theories introduced admit extensions essentially equivalent to the theory *Co* of *non* discrete ordered fields (Definition C.3.7).

We start (Section D.1) with the theory of distributive lattices (a *non* discrete ordered field is a distributive lattice for its order relation).

In Section D.2 we deal with  $\ell$ -groups or lattice groups (purely equational theory, valid for addition on the reals).

Then (Section D.3) we move on to *f*-rings (*f*-rings in french litterature), a theory inspired by rings of continuous real maps.

Section D.4 describes dynamical theories in which we add the predicate  $\cdot > 0$  (strict *f*-rings and variants).

Section D.5 proposes a return to the theory *Co* by confronting it with suitable extensions of the theory of strict *f*-rings.

In this chapter we say “group” for “abelian group”. And the rings are commutative unitary as throughout the memoir.

## D.1. Distributive lattices

References: [10, 12, 15, 46]

### Distributive lattice theory

The theory of lattices *Tr0* with the only sort *Tr* is a purely equational theory based on the following signature,<sup>1</sup>

$$\text{Signature: } \boxed{\Sigma_{Tr} = (\cdot = \cdot ; \cdot \wedge \cdot, \cdot \vee \cdot, 1, 0)}$$

In addition to the axioms of equality we have the following axioms

- |  |  |
|--|--|
| • $\vdash 0 \wedge x = 0$                                | • $\vdash 1 \vee x = 1$                          |
| • $\vdash x \wedge x = x$                                | • $\vdash x \vee x = x$                          |
| • $\vdash x \wedge y = y \wedge x$                       | • $\vdash x = y \vee x$                          |
| • $\vdash (x \wedge y) \wedge z = x \wedge (y \wedge z)$ | • $\vdash (x \vee y) \vee z = x \vee (y \vee z)$ |
| • $\vdash (x \wedge y) \vee x = x$                       | • $\vdash (x \vee y) \wedge x = x$               |

We define  $x \geq y$  as an abbreviation of  $x = x \vee y$ . This is an extension of the theory of ordered sets.

The theory *Tr* of *non-trivial lattices* is obtained by adding the collapse axiom

$$\mathbf{CL}_= \quad 1 = 0 \quad \vdash \quad \perp$$

The theory *Trdi* of *distributive lattices* is obtained by adding the following distributivity axiom (the dual axiom is deduced from this)

- $\vdash (x \wedge y) \wedge z = (x \wedge z) \vee (y \wedge z)$

<sup>1</sup>More precisely, we can prefer  $\cdot =_{Tr} \cdot, \cdot \wedge_{Tr} \cdot, \cdot \vee_{Tr} \cdot, 0_{Tr}$  and  $1_{Tr}$ .

## Ideals and filters in a distributive lattice

An *ideal*  $\mathfrak{b}$  of a distributive lattice  $(\mathbf{T}, \wedge, \vee, 0, 1)$  is a part that satisfies the constraints:

$$\left. \begin{array}{l} 0 \in \mathfrak{b} \\ x, y \in \mathfrak{b} \implies x \vee y \in \mathfrak{b} \\ x \in \mathfrak{b}, z \in \mathbf{T} \implies x \wedge z \in \mathfrak{b} \end{array} \right\} \quad (\text{D.1})$$

We denote  $\mathbf{T}/(\mathfrak{b} = 0)$  the quotient lattice obtained by forcing the elements of  $\mathfrak{b}$  to be zero. Ideals can also be defined as kernels of morphisms.

A *principal ideal* is an ideal generated by a single element  $a$ , and is denoted by  $\downarrow a$ . We have  $\downarrow a = \{x \in \mathbf{T} \mid x \leq a\}$ . The ideal  $\downarrow a$ , subject to the laws  $\wedge$  and  $\vee$  of  $\mathbf{T}$  is a distributive lattice in which the maximum element is  $a$ . The canonical injection  $\downarrow a \rightarrow \mathbf{T}$  is not a morphism of distributive lattices because the image of  $a$  is not equal to  $1_{\mathbf{T}}$ . On the other hand, the map  $\mathbf{T} \rightarrow \downarrow a$ ,  $x \mapsto x \wedge a$  is a surjective morphism, which therefore defines  $\downarrow a$  as a quotient structure  $\mathbf{T}/(a = 1)$ .

The notion of *filter* is the opposite notion (obtained by reversing the order relation) to that of ideal.

Let  $\mathfrak{a}$  be an ideal and  $\mathfrak{f}$  a filter of  $\mathbf{T}$ . We say that  $(\mathfrak{a}, \mathfrak{f})$  is a *saturated pair* in  $\mathbf{T}$  if

$$(g \in \mathfrak{f}, x \wedge g \in \mathfrak{a}) \implies x \in \mathfrak{a}, \text{ and } (a \in \mathfrak{a}, x \vee a \in \mathfrak{f}) \implies x \in \mathfrak{f}.$$

A saturated pair is a pair  $(\varphi^{-1}(0), \varphi^{-1}(1))$  for a morphism  $\varphi: \mathbf{T} \rightarrow \mathbf{T}'$  of distributive lattices. When  $(\mathfrak{a}, \mathfrak{f})$  is a saturated pair, we have the equivalences

$$1 \in \mathfrak{a} \iff 0 \in \mathfrak{f} \iff; (\mathfrak{a}, \mathfrak{f}) = (\mathbf{T}, \mathbf{T})$$

If  $A$  and  $B$  are two parts of  $\mathbf{T}$  we note

$$A \vee B = \{a \vee b \mid a \in A, b \in B\} \quad \text{and} \quad A \wedge B = \{a \wedge b \mid a \in A, b \in B\}. \quad (\text{D.2})$$

Then the ideal generated by two ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  is equal to  $\mathfrak{a} \vee \mathfrak{b}$ . The set of ideals of  $\mathbf{T}$  itself forms a distributive lattice<sup>2</sup> for inclusion, with the lower bound of  $\mathfrak{a}$  and  $\mathfrak{b}$  being the ideal  $\mathfrak{c} = \mathfrak{a} \wedge \mathfrak{b}$ . Thus the operations  $\vee$  and  $\wedge$  defined in (D.2) correspond to the sup and inf in the lattice of ideals.

When we consider the lattice of filters, we must pay attention to what the inversion of the order relation produces:  $\mathfrak{f} \cap \mathfrak{g} = \mathfrak{f} \vee \mathfrak{g}$  is the inf of the filters  $\mathfrak{f}$  and  $\mathfrak{g}$ , whereas their sup is the lattice generated by  $\mathfrak{f} \cup \mathfrak{g}$ , equal to  $\mathfrak{f} \wedge \mathfrak{g}$ .

## Quotients

A *quotient distributive lattice*  $\mathbf{T}'$  of  $\mathbf{T}$  is given by a binary relation  $\preceq$  over  $\mathbf{T}$  satisfying the following properties:

$$\left. \begin{array}{l} a \leq b \implies a \preceq b \\ a \preceq b, b \preceq c \implies a \preceq c \\ a \preceq b, a \preceq c \implies a \preceq b \wedge c \\ b \preceq a, c \preceq a \implies b \vee c \preceq a \end{array} \right\} \quad (\text{D.3})$$

**Proposition D.1.1.** *Let  $\mathbf{T}$  be a distributive lattice and  $(J, U)$  be a pair of parts of  $\mathbf{T}$ . Consider the quotient  $\mathbf{T}'$  of  $\mathbf{T}$  defined by the relations  $x = 0$  for the  $x \in J$  and  $y = 1$  for the  $y \in U$ . Then we have  $a \leq_{\mathbf{T}'} b$  if, and only if, there exists a finite part  $J_0$  of  $J$  and a finite part  $U_0$  of  $U$  such that:*

$$a \wedge \bigwedge U_0 \leq_{\mathbf{T}} b \vee \bigvee J_0 \quad (\text{D.4})$$

We will note  $\mathbf{T}'/(J = 0, U = 1)$  this quotient lattice  $\mathbf{T}'$ .

<sup>2</sup>In fact it is necessary to introduce a restriction to really obtain a set, so that we have a well-defined procedure for constructing the ideals concerned. For example, we can consider the set of ideals obtained from the principal ideals by certain predefined operations, such as countable meetings and intersections.

In commutative algebra, if  $\mathfrak{a}$  and  $\mathfrak{b}$  are two ideals of a ring  $\mathbf{A}$  we have an “exact sequence” of  $\mathbf{A}$ -modules (with  $j$  and  $p$  ring homomorphisms)

$$0 \rightarrow \mathbf{A}/(\mathfrak{a} \cap \mathfrak{b}) \xrightarrow{j} (\mathbf{A}/\mathfrak{a}) \times (\mathbf{A}/\mathfrak{b}) \xrightarrow{p} \mathbf{A}/(\mathfrak{a} + \mathfrak{b}) \rightarrow 0$$

which can be read in everyday language: the system of congruences  $x \equiv a \pmod{\mathfrak{a}}$ ,  $x \equiv b \pmod{\mathfrak{b}}$  has a solution if, and only if,  $a \equiv b \pmod{\mathfrak{a} + \mathfrak{b}}$  and in this case the solution is unique modulo  $\mathfrak{a} \cap \mathfrak{b}$ . It is remarkable that this Chinese remainder theorem generalises to a system of congruences if, and only if, the ring is *arithmetic* ([CACM, Theorem XII-1.6]), i.e. if the lattice of ideals is distributive (the Chinese remainder theorem “contemporary” concerns the special case of a family of two-by-two comaximal ideals, and it works without any hypothesis on the base ring).

Other epimorphisms in the category of commutative rings are localisations. And there is a gluing principle analogous to the Chinese remainder theorem for localisations, which is extremely fruitful (the local-global principle).

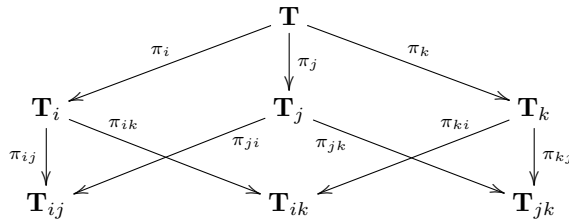
In the same way we can recover a distributive lattice from a finite number of its quotients, if the information they contain is “sufficient”. This can be seen either as a procedure for gluing (going from local to global), or as a version of the Chinese remainder theorem for distributive lattices. Let’s take a closer look.

**Definition D.1.2.** Let  $\mathbf{T}$  be a distributive lattice,  $(\mathfrak{a}_i)_{i=1,\dots,n}$  (resp.  $(\mathfrak{f}_i)_{i=1,\dots,n}$ ) a finite family of ideals (resp. filters) of  $\mathbf{T}$ . We say that the ideals  $\mathfrak{a}_i$  cover  $\mathbf{T}$  if  $\bigcap_i \mathfrak{a}_i = \{0\}$ . Similarly we say that the filters  $\mathfrak{f}_i$  cover  $\mathbf{T}$  if  $\bigcap_i \mathfrak{f}_i = \{1\}$ .

For an ideal  $\mathfrak{b}$  we write  $x \equiv y \pmod{\mathfrak{b}}$  as an abbreviation for  $x \equiv y \pmod{\mathfrak{b} = 0}$ .

**Proposition D.1.3.** Let  $\mathbf{T}$  be a distributive lattice,  $(\mathfrak{a}_i)_{i=1,\dots,n}$  be a finite family of principal ideals ( $\mathfrak{a}_i = \downarrow s_i$ ) of  $\mathbf{T}$  and  $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$ .

1. If  $(x_i)$  is a family of elements of  $\mathbf{T}$  such that for each  $i, j$  we have  $x_i \equiv x_j \pmod{\mathfrak{a}_i \vee \mathfrak{a}_j}$ , then there exists a unique  $x$  modulo  $\mathfrak{a}$  satisfying:  $x \equiv x_i \pmod{\mathfrak{a}_i}$  ( $i = 1, \dots, n$ ).
2. Let us note  $\mathbf{T}_i = \mathbf{T}/(\mathfrak{a}_i = 0)$ ,  $\mathbf{T}_{ij} = \mathbf{T}_{ji} = \mathbf{T}/(\mathfrak{a}_i \vee \mathfrak{a}_j = 0)$ ,  $\pi_i : \mathbf{T} \rightarrow \mathbf{T}_i$  and  $\pi_{ij} : \mathbf{T}_i \rightarrow \mathbf{T}_{ij}$  the canonical projections. If  $(\mathfrak{a}_i)_{i=1,\dots,n}$  covers  $\mathbf{T}$ , then  $(\mathbf{T}, (\pi_i)_{i=1,\dots,n})$  is the projective limit of the diagram  $((\mathbf{T}_i)_{1 \leq i \leq n}, (\mathbf{T}_{ij})_{1 \leq i < j \leq n}; (\pi_{ij})_{1 \leq i \neq j \leq n})$  (see figure below).
3. Now let  $(\mathfrak{f}_i)_{i=1,\dots,n}$  be a finite family of principal filters, let  $\mathbf{T}_i = \mathbf{T}/(\mathfrak{f}_i = 1)$ ,  $\mathbf{T}_{ij} = \mathbf{T}_{ji} = \mathbf{T}/(\mathfrak{f}_i \cup \mathfrak{f}_j = 1)$ ,  $\pi_i : \mathbf{T}_i \rightarrow \mathbf{T}_i$  and  $\pi_{ij} : \mathbf{T}_i \rightarrow \mathbf{T}_{ij}$  the canonical projections. If  $\mathfrak{f}_i$  covers  $\mathbf{T}$ ,  $(\mathbf{T}, (\pi_i)_{i=1,\dots,n})$  is the projective limit of the diagram  $((\mathbf{T}_i)_{1 \leq i \leq n}, (\mathbf{T}_{ij})_{1 \leq i < j \leq n}; (\pi_{ij})_{1 \leq i \neq j \leq n})$ .



## D.2. $\ell$ -groups

### Definition of the purely equational theory $\mathcal{Grl}$

The theory  $\mathcal{Grl}$  of  $\ell$ -groups (or *reticulated groups*, or *lattice groups*) is defined as follows. There is only one sort, named  $\mathcal{Grl}$ .

$$\text{Signature : } \boxed{\Sigma_{\mathcal{Grl}} = (\cdot = 0 ; \cdot + \cdot, - \cdot, \cdot \vee \cdot, 0)}$$

The symbol  $\vee$  used for the binary upper bound must not be confused with the symbol  $\mathbf{v}$  for the logical disjunction.





**Gauss**  $x \geq 0, y \geq 0, z \geq 0, x \perp y, x \leq y + z \vdash x \leq z$

## Quotient structures

The kernels of morphisms of ordered (abelian) groups are the *convex subgroups*: a subgroup  $H$  is convex if, and only if, it verifies the property

$$(x \in H, y \in G, 0 \leq y \leq x) \Rightarrow y \in H.$$

If a subgroup is convex, the order relation “pass to quotient” in  $G/H$ .

The kernels of  $\ell$ -group morphisms are the *solid subgroups*. A subgroup is solid if, and only if, it is a convex  $\ell$ -subgroup, or convex and stable by  $x \mapsto |x|$  ([Bigard, Keimel & Wolfenstein, theorem 2.2.1]).

The solid subgroup generated by an element  $a$  is  $\mathcal{C}(a) := \{x \mid \exists n \in \mathbb{N}, |x| \leq n|a|\}$ .

Solid finitely generated subgroups are all principal:  $\mathcal{C}(|a| + |b|) = \mathcal{C}(|a| \vee |b|)$  is the solid subgroup generated by  $a$  and  $b$ . The principal solid subgroups form a distributive lattice (with  $\mathcal{C}(a) \cap \mathcal{C}(b) = \mathcal{C}(|a| \wedge |b|)$ ), except that a maximum element is missing, which can be added formally.

The Krull dimension of this distributive lattice is called the *dimension, or height, of the  $\ell$ -group*. This is a constructive definition equivalent to the classical definition in classical mathematics, but does not require the existence of prime convex subgroups (see [CACM, section XIII-6] for the Krull dimension of distributive lattices). In the case of linearly ordered groups, this corresponds to the *rank* of the group.

## Representation theorem

In classical mathematics, any lattice group is a subgroup of a product of linearly ordered groups.

The method of proof explained in [CACM, Principle XI-2.10] gives a constructive equivalent of this property: to prove a concrete fact in a lattice group, we can always act as if we were in the presence of a product of linearly ordered groups.

In fact, we have a better (more formal) formulation in the language of dynamical theories: *both dynamical theories (with and without the axiom of total order) prove the same Horn rules*. Let’s look at this in more detail.

**Definition D.2.1.** The dynamical theory *Gtosup* of linearly ordered groups with  $\text{sup}$ <sup>3</sup> is the dynamical theory of  $\ell$ -groups to which we add the dynamical rule **OT** saying that the order is total.

$$\mathbf{OT} \vdash x \geq 0 \quad \mathbf{op} \quad x \leq 0$$

Note that compared with the usual theory of linearly ordered groups *Gto* (whose definition we leave to the reader) we have introduced into the signature the law  $\cdot \vee \cdot$  which is well-defined. The *Gtosup* theory is essentially identical to the *Gto* theory.

**Formal Positivstellensatz D.2.2** (for  $\ell$ -groups).

*The dynamical theories Grl and Gtosup prove the same Horn rules.*

*Proof.* The reader can refer to the proof of the formal Positivstellensatz D.3.2, and change the very little that needs to be changed.  $\square$

For example, the reader can easily prove the rules **Grl2** and **Grl4<sub>n</sub>** using Positivstellensatz D.2.2, which would otherwise be much less simple.

A corollary in classical mathematics of Positivstellensatz D.2.2 is the the following theorem (as a special case of Theorem A.5.4).

---

<sup>3</sup>Or totally ordered groups with  $\text{sup}$ .

**Corollary\* D.2.3** (representation theorem). See [44, Lorenzen, 1939], and the developments [45, 47] commented in [14]. Any  $\ell$ -group  $G$  is a subproduct of linearly ordered groups<sup>4</sup> quotients of  $G$ .

*Remark D.2.4.* The theory of algorithmic complexity in the space of continuous real maps on the interval  $[0, 1]$  makes natural use of the divisible  $\ell$ -group structure (2-divisibility is sufficient). This space of functions is seen essentially as a Riesz space, and the multiplication of maps is relegated to the background. See for example [32, definition 3.2.1]. Note also that in this theory formulas are replaced by circuits (a short circuit can encode a very long formula). In this case we are in analysis rather than abstract algebra. ■

An example of the application of the formal Positivstellensatz for  $\ell$ -groups is given in [CACM, Fact XI-2.12] which we reproduce below.

**Fact D.2.5** (other identities in  $\ell$ -groups).

Let  $x, y, x', y', z, t \in G$ ,  $n \in \mathbb{N}$ ,  $x_1, \dots, x_n \in G$ .

1.  $x + y = |x - y| + 2(x \wedge y)$
2.  $(x \wedge y)^+ = x^+ \wedge y^+$ ,  $(x \wedge y)^- = x^- \vee y^-$ ,  $(x \vee y)^+ = x^+ \vee y^+$ ,  $(x \vee y)^- = x^- \wedge y^-$ .
3.  $2(x \wedge y)^+ \leq (x + y)^+ \leq x^+ + y^+$ .
4.  $|x + y| \leq |x| + |y|$ ;  $|x| + |y| = |x + y| + 2(x^+ \wedge y^-) + 2(x^- \wedge y^+)$ .
5.  $|x - y| \leq |x| + |y|$ ;  $|x| + |y| = |x - y| + 2(x^+ \wedge y^+) + 2(x^- \wedge y^-)$ .
6.  $|x + y| \vee |x - y| = |x| + |y|$ .
7.  $|x + y| \wedge |x - y| = ||x| - |y||$ .
8.  $|x - y| = (x \vee y) - (x \wedge y)$ .
9.  $|(x \vee z) - (y \vee z)| + |(x \wedge z) - (y \wedge z)| = |x - y|$ .
10.  $|x^+ - y^+| + |x^- - y^-| = |x - y|$ .
11.  $x \leq z \implies (x \wedge y) \vee z = x \wedge (y \vee z)$ .
12.  $x + y = z + t \implies x + y = (x \vee z) + (y \wedge t)$ .
13.  $nx \geq \bigwedge_{k=1}^n (ky + (n-k)x) \implies x \geq y$ .
14.  $\bigvee_{i=1}^n x_i = \sum_{k=1}^n (-1)^{k-1} \sum_{I \in \mathcal{P}_{k,n}} \bigwedge_{i \in I} x_i$ .
15.  $x \perp y \iff |x + y| = |x - y| \iff |x + y| = |x| \vee |y|$ .
16.  $x \perp y \iff |x + y| = |x| + |y| = |x| \vee |y|$ .
17.  $(x' \perp y, x' \perp y, x' \perp y', x' \perp y', x + y = x' + y') \implies (x = x', y = y')$ .
18. We define  $\text{Tri}(\underline{x}) = [\text{Tri}_1(\underline{x}), \text{Tri}_2(\underline{x}), \dots, \text{Tri}_n(\underline{x})]$ , where

$$\text{Tri}_k(x_1, \dots, x_n) = \bigwedge_{I \in \mathcal{P}_{k,n}} \left( \bigvee_{i \in I} x_i \right) \quad (k \in \llbracket 1..n \rrbracket).$$

We also have the following.

- (a)  $\text{Tri}_k(x_1, \dots, x_n) = \bigvee_{j \in \mathcal{P}_{n-k+1,n}} \left( \bigwedge_{j \in J} x_j \right)$ ,  $(k \in \llbracket 1..n \rrbracket)$ .
- (b)  $\text{Tri}_1(\underline{x}) \leq \text{Tri}_2(\underline{x}) \leq \dots \leq \text{Tri}_n(\underline{x})$ .

<sup>4</sup>Any  $\ell$ -group  $G$  is a substructure of a product of linearly ordered quotient groups of  $G$ . In other words, there is a lattice subgroup of a product of linearly ordered groups which, as a lattice group, is isomorphic to the original lattice group. The English terminology is: any lattice group is a *subdirect product* of linearly ordered groups.



Rules for compatibility of  $\vee$  with equality

$$\mathbf{sup1}_= \quad x = 0 \vdash (x + y) \vee z = y \vee z$$

$$\mathbf{sup2}_= \quad x = 0 \vdash y \vee (x + z) = y \vee z$$

Equality rules

$$\mathbf{sdt1} \quad \vdash x \vee x = x$$

$$\mathbf{grl} \quad \vdash x + (y \vee z) = (x + y) \vee (x + z)$$

$$\mathbf{sdt2} \quad \vdash x = y \vee x$$

$$\mathbf{afr} \quad \vdash x^+ (y \vee z) = (x^+ y) \vee (x^+ z)$$

$$\mathbf{sdt3} \quad \vdash (xy) \vee z = x(yz)$$

## Note on $\ell$ -rings

The theory  $\mathcal{Arl}$  of  $\ell$ -rings (or lattice rings) is defined by replacing the rule  $\mathbf{afr}$  by the rules  $\mathbf{ao1}$  and  $\mathbf{ao2}$  of ordered rings, valid in  $\mathcal{Afr}$ .

$$\mathbf{ao1} \quad \vdash x^2 \geq 0$$

$$\mathbf{ao2} \quad x \geq 0, y \geq 0 \vdash xy \geq 0$$

**Lemma D.3.1.** *In the theory of  $\ell$ -rings, the following rules are all equivalent.*

$$\mathbf{afr} \quad \vdash a^+ (b \vee c) = (a^+ b) \vee (a^+ c)$$

$$\mathbf{Afr} \quad a \geq 0 \vdash a(b \vee c) = ab \vee ac$$

$$\mathbf{afr}' \quad \vdash a^+ (b \wedge c) = (a^+ b) \wedge (a^+ c)$$

$$\mathbf{Afr}' \quad a \geq 0 \vdash a(b \wedge c) = ab \wedge ac$$

$$\mathbf{afr0} \quad \vdash b^- \wedge a^+ b^+ = 0$$

$$\mathbf{Afr0} \quad b \wedge c = 0, a \geq 0 \vdash b \wedge ac = 0$$

$$\mathbf{afr1} \quad \vdash a^+ a^- = 0$$

$$\mathbf{Afr1} \quad a \wedge b = 0 \vdash ab = 0$$

$$\mathbf{afr2} \quad \vdash |a| |b| = |ab|$$

$$\mathbf{afr6a} \quad \vdash a^2 = (a^+)^2 + (a^-)^2$$

$$\mathbf{afr3a} \quad \vdash (ab)^+ = a^+ b^+ + a^- b^-$$

$$\mathbf{afr6b} \quad \vdash a^2 = |a|^2$$

$$\mathbf{afr3b} \quad \vdash (ab)^- = a^+ b^- + a^- b^+$$

$$\mathbf{sup} \quad \vdash ((x \vee y) - x) ((x \vee y) - y) = 0$$

$$\mathbf{afr4} \quad \vdash c^+ |a| = |c^+ a|$$

$$\mathbf{Afr2} \quad b \perp c \vdash ab \perp ac$$

$$\mathbf{afr5} \quad \vdash (a \wedge b)(a \vee b) = ab$$

In other words, each of these rules can be used to define  $f$ -rings by adding it to the theory  $\mathcal{Arl}$ . The fact that  $\mathbf{afr}$  implies  $\mathbf{ao1}$ ,  $\mathbf{ao2}$  and the rules indicated in Lemma D.3.1 results from the formal Positivstellensatz D.3.2.

In the case of a non-unitary  $f$ -ring the rule  $\mathbf{afr0}$  is stronger than the others (see [Bigard, Keimel & Wolfenstein], proposition 9.1.10<sup>6</sup>).

## Some derived rules in the theory $\mathcal{Afr}$

In addition to the rules derived for  $\ell$ -groups and those indicated in Lemma D.3.1, here are some very useful classical rules in which multiplication is involved.

$$\mathbf{Afr4} \quad b \geq 0, ab = 1 \vdash a \geq 0$$

$$\mathbf{Afr5} \quad c \geq 0, a(a^2 + c) \geq 0 \vdash a^3 \geq 0$$

$$\mathbf{afr7} \quad \vdash ab^+ = (ab \wedge (a^2 + 1)b) \vee (-(a^2 + 1)b \wedge 0)$$

<sup>6</sup>The book deals more generally with ordered rings which are not necessarily commutative or unitary. The condition  $\mathbf{afr0}$  must then be split to take account of the non-commutativity.

*Remark.* The rule **afr7** is used to demonstrate the possibility of writing terms in a simplified form in a free  $f$ -ring: see Lemma D.3.7. ■

## Quotient structures

### • Solid ideals (or $\ell$ -ideals)

By definition, the kernels of  $f$ -ring morphisms are called *solid ideals* or  *$\ell$ -ideals*.

An ideal is solid if, and only if, it is solid as a subgroup.

The solid ideal generated by an element  $a$  is

$$\mathcal{I}(a) := \{ x \mid \exists y, |x| \leq |ya| \}.$$

We have  $\mathcal{I}(a) = \mathcal{I}(|a|)$  and  $\mathcal{I}(a) \cap \mathcal{I}(b) = \mathcal{I}(|a| \wedge |b|)$ . Finally, the  $\ell$ -ideal generated by  $a_1, \dots, a_n$  is

$$\mathcal{I}(a_1, \dots, a_n) = \mathcal{I}(|a_1| + \dots + |a_n|) = \mathcal{I}(|a_1| \vee \dots \vee |a_n|).$$

### • Irreducible $\ell$ -ideals

We say that a solid ideal  $I$  of an  $f$ -ring  $\mathbf{A}$  is *irreducible* if the quotient  $f$ -ring is linearly ordered. In other words, for any  $x \in \mathbf{A}$ ,  $x^+ \in I$  or  $x^- \in I$ .

By Lemma D.4.1, every prime solid ideal is irreducible.

Moreover, a convex prime ideal (as an additive subgroup)  $\mathfrak{p}$  is solid: we must see that it is stable by  $\vee$ . If  $a, b \in \mathfrak{p}$  we have  $(a-b)^+$  or  $(a-b)^- \in \mathfrak{p}$ . And the identities  $b+(a-b)^+ = a \vee b = a+(a-b)^-$  are valid in  $\ell$ -groups (and a fortiori in  $f$ -rings) because they are valid in linearly ordered groups (formal Positivstellensatz D.2.2).

## Formal Positivstellensatz and representation theorem for $f$ -rings

Recall that the dynamical theory of linearly ordered rings with sup is the dynamical theory of linearly ordered rings to which we add a function symbol  $\cdot \vee \cdot$  which must satisfy the following Horn rules.

$$\mathbf{sup1} \vdash x \vee y \geq x$$

$$\mathbf{Sup} \quad z \geq x, z \geq y \vdash z \geq x \vee y$$

$$\mathbf{sup2} \vdash x \vee y \geq y$$

We can also see  $\mathcal{A}tosup$  as the theory of  $f$ -rings to which we add as an axiom the dynamical rule **OT** (saying that the order is total).

$$\mathbf{OT} \vdash x \geq 0 \quad \mathbf{op} \quad x \leq 0$$

Given the unique existence of the lub in a linearly ordered ring, the theories  $\mathcal{A}to$  and  $\mathcal{A}tosup$  are essentially identical. In particular, they prove the same dynamical rules (when formulated without using  $\vee$ ).

The theorem for  $f$ -rings analogous to Positivstellensatz D.2.2 is as follows. It is a result of the same type as Item 2 of Positivstellensatz C.2.2.

### Formal Positivstellensatz D.3.2 (for $f$ -rings).

The theories  $\mathcal{A}fr$  and  $\mathcal{A}tosup$  prove the same Horn rules.

*Proof.* Consider a Horn rule proved in the dynamical theory  $\mathcal{A}tosup$ . We can assume without loss of generality that the conclusion of the rule is an equality  $t = 0$  for a suitable term  $t$ . In the corresponding calculation, in the presence of a term  $u$ , we are authorised by **OT** to open two branches. One where  $u \geq 0$ , the other where  $u \leq 0$ . At each node of the dynamic proof, we are in fact working in an  $f$ -ring defined by generators and relations: the generators are given in the presentation and in the hypotheses of the Horn rule to be proved; the same applies to the relations,

with the addition of those which we have added, in the branch we are in, to the branches which precede the node. Suppose that at a given moment, for two terms  $a$  and  $b$ , we have opened a branch where  $a \geq b$  and another where  $a \leq b$ . Let's put  $c = b - a$ . In the first branch we have added the hypothesis  $c^- = 0$ , in the second the hypothesis  $c^+ = 0$ . If in each of the branches we can prove  $t = 0$ , this means that in the  $f$ -ring corresponding to the node in question, we have on the one hand  $t \in \mathcal{I}(c^-)$ , and on the other hand  $t \in \mathcal{I}(c^+)$ . Now in an  $f$ -ring we have  $\mathcal{I}(c^+) \cap \mathcal{I}(c^-) = \mathcal{I}(c^+ \wedge c^-) = \{0\}$ .  $\square$

Let's use Positivstellensatz D.3.2 for proving Horn Rules Afr4 and Afr5.

$$\mathbf{Afr4} \quad y \geq 0, xy = 1 \vdash x \geq 0$$

$$\mathbf{Afr5} \quad c \geq 0, x(x^2 + c) \geq 0 \vdash x^3 \geq 0$$

In both cases, we open two branches, one where  $x \geq 0$ , and the result is clear, the other where  $x \leq 0$ . For Afr4 we deduce that  $1 \leq 0$ , then  $1 = 0$ , then  $x = 0$ . For Afr5 we deduce that  $x^3 \geq -xc \geq 0$ .

Similarly, we prove afr7 by examining separately the cases " $b \geq 0$ ", " $b \leq 0, a \geq 0$ " and " $b \leq 0, a \leq 0$ ". As a consequence of the formal Positivstellensatz D.3.2 we obtain in classical mathematics the following representation theorem (as a special case of Theorem A.5.4).

**Corollary\* D.3.3** (representation theorem). *Any  $f$ -ring  $\mathbf{A}$  is a subproduct of linearly ordered rings quotients of  $\mathbf{A}$ .*

The following theorem is of the same type as Item 1 of Positivstellensatz C.2.2. This result can be seen as a second form of the formal Positivstellensatz for  $f$ -rings. We say that a dynamic algebraic structure of type  $\mathcal{Afr}$  collapses when the rule  $\vdash 1 = 0$  is valid.

**Theorem D.3.4** (simultaneous collapse, for the signature  $(\cdot = 0, \cdot \geq 0; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, - \cdot, 0, 1)$ ). *The theories  $\mathcal{Afr}$ ,  $\mathcal{Crcdsup}$  and all intermediate theories collapse simultaneously.*

*Proof.* The theories  $\mathcal{Afr}$  and  $\mathcal{Atosup}$  collapse simultaneously according to Positivstellensatz D.3.2. The theories  $\mathcal{Ato}$  and  $\mathcal{Crcd}$  collapse simultaneously according to Item 1 of Positivstellensatz C.2.2. Finally, the theories  $\mathcal{Ato}$  and  $\mathcal{Crcd}$  are essentially identical to the theories  $\mathcal{Atosup}$  and  $\mathcal{Crcdsup}$  respectively.  $\square$

## Localisations of $f$ -rings

### • Generalities

Consider a monoid  $S$  in an  $f$ -ring and construct the solution of the universal problem (in the category of  $f$ -rings) consisting in inverting the elements of  $S$ .

To do this, we need only consider the usual localised ring  $S^{-1}\mathbf{A}$  and define the law  $\vee$  correctly. Since inverting  $s$  or inverting  $s^2$  amounts to the same thing, we can consider only fractions with denominator  $\geq 0$ . We then define

$$\frac{a}{s} \vee \frac{b}{t} := \frac{at \vee bs}{st} \quad (s, t \geq 0).$$

*Note.* We have no choice, because since  $s, t \geq 0$ , we must have  $st \left( \frac{a}{s} \vee \frac{b}{t} \right) = st \frac{a}{s} \vee st \frac{b}{t} = at \vee bs$  in  $S^{-1}\mathbf{A}$ . It remains to be seen that the law is well-defined and that it continues to satisfy the required axioms. For example, let's check that it is well-defined. Suppose that  $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ , i.e. that  $a_1 s_2 s_3 = a_2 s_1 s_3$  for an  $s_3 \geq 0$  in  $S$ . Then we can easily check that the two elements  $\frac{a_i}{s_i} \vee \frac{b}{t}$  given by the definition above are equal in  $S^{-1}\mathbf{A}$ . This is the same calculation that was used to justify addition in  $S^{-1}\mathbf{A}$  when we were young.<sup>7</sup> Just replace  $+$  by  $\vee$ , with the precaution of having denominators  $\geq 0$ .  $\blacksquare$

<sup>7</sup>When we fell over in admiration of Claude Chevalley who dared to invert zerodivisors, and nothing awful resulted, quite the contrary.

An  $f$ -ring  $\mathbf{A}$  can always be considered as immersed in a  $\mathbb{Q}$ - $f$ -algebra. Indeed, according to **Gr13<sub>n</sub>**, the “integers”  $n.1_{\mathbf{A}}$  are regular and therefore  $\mathbf{A}$  injects itself into the  $\mathbb{Q}$ -algebra  $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbf{A}$  which is an  $f$ -ring as a localisation of  $\mathbf{A}$ .<sup>8</sup>

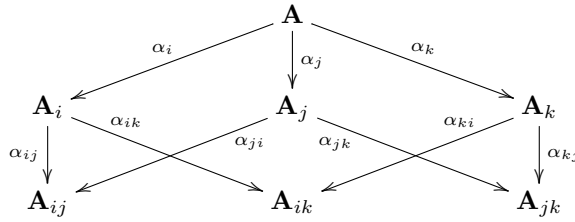
### • Gluing $f$ -rings

**Concrete local-global principle D.3.5** (concrete gluing of  $f$ -rings).

Let  $S_1, \dots, S_n$  be comaximal monoids of a ring  $\mathbf{A}$ . Let  $\mathbf{A}_i$  denote  $\mathbf{A}_{S_i}$ ,  $\mathbf{A}_{ij}$  denote  $\mathbf{A}_{S_i S_j}$ , and assume that an  $f$ -ring structure with a  $\vee_i$  law is given on each  $\mathbf{A}_i$ . It is further assumed that the images in  $\mathbf{A}_{ij}$  of the laws  $\vee_i$  and  $\vee_j$  coincide. Then there exists a unique  $f$ -ring structure on  $\mathbf{A}$  which induces by localisation in each  $S_i$  the structure defined on  $\mathbf{A}_i$ . This  $f$ -ring is identified with the projective limit of the diagram

$$((\mathbf{A}_i)_{i < j \in \llbracket 1..n \rrbracket}, (\mathbf{A}_{ij})_{i < j \in \llbracket 1..n \rrbracket}; (\alpha_{ij})_{i \neq j \in \llbracket 1..n \rrbracket}),$$

where  $\alpha_{ij}$  are localisation morphisms, in the category of  $f$ -rings.



*Proof.* The ring  $\mathbf{A}$  is the limit of the projective system formed by  $\mathbf{A}_i$  and  $\mathbf{A}_{ij}$  in the category of commutative rings, and therefore also in the category of sets. It follows that there is a unique law  $\vee$  on  $\mathbf{A}$  which gives the  $\vee_i$  on the  $\mathbf{A}_i$  by the canonical maps  $\mathbf{A} \rightarrow \mathbf{A}_i$ . It remains to check that it satisfies the axioms of the  $\vee$  law for an  $f$ -ring. This follows from the fact that these axioms are given by equalities between terms, and from the fact that the natural map  $\varphi: \mathbf{A} \rightarrow \prod_i \mathbf{A}_i$ , on the one hand preserves the laws of the  $f$ -ring structure, and on the other hand is injective.  $\square$

### • Real schemes

*Remark D.3.6.* A corollary of the gluing Principle **D.3.5** is that the notion of a Grothendieck  $f$ -scheme is well-defined. An  $f$ -scheme seems to be the most natural definition for the notion of a real scheme. Indeed, it allows nilpotents and therefore a good theory of multiplicities in real schemes. But this topic apparently remains largely unexplored.  $\blacksquare$

## Rewriting terms in $f$ -rings

Reference: [19].

Contrary to the theory of commutative rings in which the terms are rewritten in a unique normal form, we do not have such a satisfactory result for  $f$ -rings. We do, however, have a simplified form, similar to the conjunctive normal form in distributive lattices.

**Lemma D.3.7.** Let  $\mathbf{A}$  be an  $f$ -ring and  $t$  be a term written over indeterminates  $x_1, \dots, x_n$  and constants in  $\mathbf{A}$ . This term can be rewritten as

$$\sup_{i \in I} (\inf_{j \in J_i} (f_{i,j}(\underline{x})))$$

for a suitable finite family of polynomials  $f_{i,j} \in \mathbf{A}[X_1, \dots, X_n]$ .

*Proof.* Given the usual rewritings in distributive lattices and given that  $x \mapsto -x$  exchanges  $\vee$  and  $\wedge$ , it is sufficient to know how to rewrite  $a + (b \vee c)$  and  $a(b \vee c)$  in the desired form. This follows from the equality rules **gr1**, **gr16** and **afr7**.  $\square$

<sup>8</sup>This is true even if  $\mathbf{A}$  is trivial: the only case where the  $\mathbb{Q}$ -algebra in question does not contain  $\mathbb{Q}$  as a subring.

Since the theory  $\mathcal{Afr}$  is purely equational, the preceding lemma is equivalent to its statement restricted to special cases where  $\mathbf{A}$  is an  $f$ -ring free over a finite set.

**Definition and notation D.3.8.** Let  $\mathbf{B} = ((G, R), \mathcal{Afr})$  be a dynamic algebraic structure of  $f$ -ring. Since the theory  $\mathcal{Afr}$  is Horn,  $\mathbf{B}$  admits a generic model, denoted  $\text{AFR}(\mathbf{B})$ , which is the usual  $f$ -ring defined by the generators  $G$  and the relations  $R$ .

**Lemma D.3.9.**

1. The elements of the ring  $\text{AFR}(\mathbf{B})$  can all be written in the form given in Lemma D.3.7 with the  $f_{ij} \in \mathbb{Z}[G]$ .
2. If  $\mathbf{C}$  is a commutative ring, take for  $(G, R)$  the positive diagram of  $\mathbf{C}$ . Then  $\text{AFR}(\mathbf{C})$  is the  $f$ -ring freely generated by the commutative ring  $\mathbf{C}$ , and the elements of  $\text{AFR}(\mathbf{C})$  are written in the form  $\sup_{i \in I} (\inf_{j \in J_i} a_{ij})$  with elements  $a_{ij}$  of  $\mathbf{C}$ .

### $f$ -rings of maps, semipolynomials

For any set  $E$  and any  $f$ -ring  $\mathbf{A}$  the ring of maps  $f: E \rightarrow \mathbf{A}$  is provided with a natural structure of  $f$ -ring (it is the product structure).

**Definition and notation D.3.10.** Let  $\varphi: \mathbf{A} \rightarrow \mathbf{B}$  be a morphism of  $f$ -rings. The ring of  $\mathbf{A}$ -semipolynomials in  $n$  variables<sup>9</sup> on  $\mathbf{B}$  is the  $f$ -subring of maps  $f: \mathbf{B}^n \rightarrow \mathbf{B}$  generated by the constants in  $\varphi(\mathbf{A})$  and the coordinate maps. It will be noted  $\text{Sipd}_n(\mathbf{A}, \mathbf{B})$ . We shorten  $\text{Sipd}_n(\mathbf{A}, \mathbf{A})$  to  $\text{Sipd}_n(\mathbf{A})$ .

The definition extends to the case where  $\mathbf{A}$  and/or  $\mathbf{B}$  are linearly ordered rings, which are considered to be  $f$ -rings.

Note that it is not really restrictive to suppose that  $\varphi$  is injective, which makes it possible to look at  $\mathbf{A}$  as an  $f$ -subring of  $\mathbf{B}$ .

**Lemma D.3.11.** *It is assumed that  $\mathbf{A} \subseteq \mathbf{B}$ . Any element of  $\text{Sipd}_n(\mathbf{A}, \mathbf{B})$  is rewritten as  $\sup_{i \in I} (\inf_{j \in J_i} (f_{i,j}))$  for a suitable finite family of polynomials  $f_{i,j} \in \mathbf{A}[x_1, \dots, x_n]$ .*

*Proof.* Very close to proof of Lemma D.3.7. □

**Examples D.3.12.**

1. The two elements  $x \vee (1 - x)$  and  $1 \vee x \vee (1 - x)$  define the same map in  $\text{Sipd}_1(\mathbb{Z})$ , but not in  $\text{Sipd}_1(\mathbb{Q})$ .
2. Let  $\mathbf{K} = \mathbb{Q}(\epsilon)$  with  $\epsilon$  infinitesimal positive and  $\mathbf{R}$  the real closure of  $\mathbf{K}$ . The semipolynomial  $f = x^+ \wedge -(x^2 - \epsilon)(x^3 - \epsilon)$  defines the null map on  $\mathbf{K}$  but does not define a null map on  $\mathbf{R}$ : the interval  $[\epsilon^{1/2}, \epsilon^{1/3}]$  is invisible on  $\mathbf{K}$ . This example can be simplified by taking  $\mathbf{K} = \mathbb{Q}[\epsilon]$  with a suitable nilpotent  $\epsilon > 0$ . ■

## D.4. Beyond purely equational theories

### $f$ -rings without zerodivisor

**Lemma D.4.1.** *An  $f$ -ring without zerodivisor is linearly ordered. In other words, if we add the axiom **ASDZ** to the theory  $\mathcal{Afr}$ , the rule **OT** is valid. In other words, the resulting theory  $\mathcal{Afrsdz}$  is essentially identical to the theory  $\mathcal{Atonz}$  of linearly ordered rings without zerodivisor (see Item 3 of Lemma C.1.6).*

**ASDZ**  $xy = 0 \vdash x = 0 \text{ op } y = 0$

**OT**  $\vdash x \geq 0 \text{ op } x \leq 0$

<sup>9</sup>Semipolynomials are often called ‘‘SIPD’’ or ‘‘sup-inf-polynomially-defined maps’’.



*Proof.* Since  $x^+x^- = 0$ , we obtain the valid rule

$$\vdash x^+ = 0 \quad \mathbf{op} \quad x^- = 0$$

□

## Local *f*-rings

**Lemma D.4.2.** *Let  $\mathbf{A}$  be a local *f*-ring and  $x \in \mathbf{A}^\times$ , then  $x$  is  $\geq 0$  or  $\leq 0$ .*

*Proof.* Given  $x \in \mathbf{A}^\times$ , we write  $x = x^+ - x^-$ , so  $x^+ \in \mathbf{A}^\times$  or  $x^- \in \mathbf{A}^\times$ . Now  $x^+x^- = 0$ . In the first case we obtain  $x^- = 0$ , in the second case  $x^+ = 0$ . □

## Strict *f*-ring

The following theory merges the theories  $\mathcal{A}fr$  and  $\mathcal{A}so$ . This theory is essentially identical to the one defined in the article [40].

**Definition D.4.3.** The language of the Horn theory  $\mathcal{A}sr$  of *strict f*-rings is given by the following signature.

$$\mathbf{Signature} : \boxed{\Sigma_{\mathcal{A}sr} = (\cdot = 0, \cdot \geq 0, \cdot > 0 ; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, - \cdot, 0, 1)}$$

The axioms are as follows.

- the rules of the purely equational theory  $\mathcal{A}fr$ ,
- the direct rules from **aso1** to **aso4**, (page 45)
- the Horn rules **col<sub>></sub>**, **lv**, **Aso1** and **Aso2**, (page 45)
- finally, we have the three rules **sup1**, **sup2** and **Sup** (page 48) to link  $\cdot \geq 0$  and  $\cdot \vee \cdot$ .

We have put the predicate “ $\cdot \geq 0$ ” directly into the language rather than defining it from  $\cdot \vee \cdot$ .

The meaning of  $x > 0$  is not fixed a priori by the axioms. It can range from “ $x$  is regular and  $\geq 0$ ” to “ $x$  is invertible and  $\geq 0$ ”.

**Lemma D.4.4.** *Consider the Horn theory of strictly lattice rings to which we add the axiom **OTF**. Then the rule **OTF<sup>×</sup>** is also valid (these rules are recalled below).*

$$\mathbf{OTF} \quad x + y > 0 \vdash x > 0 \quad \mathbf{op} \quad y > 0 \qquad \mathbf{OTF}^\times \quad xy < 0 \vdash x < 0 \quad \mathbf{op} \quad y < 0$$

*Proof.* Assume  $xy < 0$ , hence  $x^2y^2 > 0$ , hence, by **Aso2**,  $x^2 > 0$ .

Note that  $x^2 = (x^+)^2 + (x^-)^2$ . So by **OTF**, it is sufficient to treat the cases  $(x^+)^2 > 0$  and  $(x^-)^2 > 0$  separately.

If  $(x^+)^2 > 0$ , we have  $xx^+ = (x^+)^2 > 0$ , so by **Aso2**,  $x > 0$ . And again by **Aso2**, we get  $y < 0$ . If  $(x^-)^2 > 0$ , we have  $-xx^- = (x^-)^2 > 0$ , so by **Aso2**,  $x < 0$ . □

## Reduced *f*-rings

Here we examine the Horn theory  $\mathcal{A}frnz$  of *reduced f*-rings. We therefore add to  $\mathcal{A}frnz$  the axiom **Anz** of reduced rings, which is a simplification rule.

$$\mathbf{Anz} \quad a^2 = 0 \vdash a = 0$$

The Horn theory  $\mathcal{A}srnz$  of *reduced strict f*-rings is the theory obtained from the theory  $\mathcal{A}sr$  by adding as axiom the Horn rule **Anz**.

- **Some derived rules**

Let us prove in the theory  $\mathcal{Afrnz}$  the four rules **Afrnz1**, **Afrnz2**, **Afrnz3**, and **Aonz** (this last one was introduced page 45).

$$\mathbf{Afrnz1} \quad x^3 \geq 0 \vdash x \geq 0$$

We write  $x = x^+ - x^-$ . Since  $x^+ x^- = 0$  we have  $x^3 = (x^+)^3 - (x^-)^3 \geq 0$ . Multiplying by  $x^-$  gives  $(x^-)^4 \leq 0$ , so  $(x^-)^4 = 0$ . Now the ring is reduced:  $x^- = 0$  and  $x \geq 0$ .  $\square$

Note that from **Afrnz1** we deduce the same rule for an arbitrary odd exponent which replaces the exponent 3.

We also have the following reciprocal of the rule **Afr1**.

$$\mathbf{Afrnz2} \quad ab = 0 \vdash |a| \wedge |b| = 0$$

Indeed if  $ab = 0$ , then  $(|a| \wedge |b|)^2 \leq |a|, |b| = 0$ , therefore  $|a| \wedge |b| = 0$ .  $\square$

Thus, for  $a, b \geq 0$ ,  $ab = 0$  is equivalent to  $a \wedge b = 0$ .

$$\mathbf{Afrnz3} \quad a \geq 0, b \geq 0, a^2 = b^2 \vdash a = b$$

Indeed  $|a - b|^2 \leq |a - b| |a + b| = |a^2 - b^2|$ .

Finally

$$\mathbf{Aonz} \quad c \geq 0, x(x^2 + c) \geq 0 \vdash x \geq 0$$

Indeed, by **Afr5** we have  $x^3 \geq 0$ , hence  $x \geq 0$  by **Afrnz1**.  $\square$

It is now easy to obtain the following result.

**Lemma D.4.5.** *In the theory  $\mathcal{Afr}$  the rules **Afrnz1**, **Afrnz2**, **Afrnz3**, **Aonz** and **Anz** are equivalent.*

Here is a simple example of the application of Positivstellensatz D.5.6.

**Lemma D.4.6.** *In a reduced  $f$ -ring, the element  $c = a \vee b$  is characterised by the following equalities and inequalities*

$$c \geq a, c \geq b, (c - a)(c - b) = 0.$$

More precisely, the theory  $\mathcal{Afrnz}$  proves the following Horn rule

$$\bullet \quad x \geq a, x \geq b, (x - a)(x - b) = 0 \vdash x = a \vee b.$$

*Proof.* In fact, as the rule is valid for the theory **Codsup**, this follows from Item 3 of Formal Positivstellensatz D.5.6.  $\square$

- **The rule FRAC in  $\mathcal{Afrnz}$**

Recall the rules **FRAC** and **FRAC<sub>n</sub>**.

$$\mathbf{FRAC} \quad 0 \leq a \leq b \vdash \exists z (zb = a^2, 0 \leq z \leq a)$$

$$\mathbf{FRAC}_n \quad |u|^n \leq |v|^{n+1} \vdash \exists z (zv = u, |z|^n \leq |v|) \quad (n \geq 1)$$

Note that the rule **FRAC**, applied with  $a = 1$  implies the invertibility of any element  $\geq 1$ .

We now recall for the theory  $\mathcal{Afrnz}$  the analogue of Lemma C.3.6 for the theory **Co0**.

**Lemma D.4.7.** *The addition of the axiom **FRAC** to the theory  $\mathcal{Afrnz}$  can be replaced by the introduction of a function symbol **Fr** with the axioms **fr1** and **fr2** which we recall below*

$$\mathbf{fr1} \quad \vdash \text{Fr}(a, b) |b| = (|a| \wedge |b|)^2$$

$$\mathbf{fr2} \quad \vdash 0 \leq \text{Fr}(a, b) \leq |a| \wedge$$

*Proof.* As in Lemma C.3.6, we can see that it is a question of skolemising an existential rule. This gives an essentially identical theory if we have unique existence. The proof is that of Lemma C.3.5. Assume  $yb = zb = a^2$ ,  $0 \leq y \leq a$  and  $0 \leq z \leq a$ . We have  $(y - z)b = 0$ ,  $|y - z| \leq a \leq b^{10}$  and thus  $|y - z|^2 \leq |y - z|b = 0$ .  $\square$

**Lemma D.4.8.** *In the theory  $\mathcal{Afrnz}$  the rule  $\mathbf{FRAC}_2$  is deduced from the rule  $\mathbf{FRAC}$  and from the rule asserting the existence of the sixth root  $\geq 0$  of an element  $\geq 0$ .*

*Proof.* Assume  $u^2 \leq v^3$  and we want to find a  $z$  such that  $zv = u$  and  $z^2 \leq v$ .

First assume  $u \geq 0$  and show that there is a  $z$  such that  $zv = u$ . The rule  $\mathbf{FRAC}$  implies that the fraction  $t = \frac{u^4}{v^3}$  is well-defined with  $0 \leq t \leq u^2$ . Again  $\mathbf{FRAC}$  gives the fact that the fraction  $w = \frac{t^2}{u^2}$  with  $0 \leq w \leq t \leq u^2$  is well-defined. We then obtain  $u^2 w v^6 = t^2 v^6 = u^8$ . So  $u^2(w v^6 - u^6) = 0$ . Now  $w \leq u^2$ , so  $|w v^6 - u^6| \leq u^2(v^6 + u^4)$ , hence  $|w v^6 - u^6|^2 \leq |w v^6 - u^6| u^2(v^6 + u^4) = 0$ . Given the rule  $\mathbf{Anz}$ , we get  $w v^6 = u^6$ . Take  $z = w^{\frac{1}{6}}$  and  $zv = u$ . Furthermore,  $z^6 \leq u^2 \leq v^3$  implies  $z^2 \leq v$ .

For an arbitrary  $u$  we write  $u = u^+ - u^-$ ; we have  $u^2 = (u^+)^2 + (u^-)^2 \leq v^3$ . We obtain a  $z_1$  such that  $z_1 v = u^+$  and a  $z_2$  such that  $z_2 v = u^-$ , we put  $z = z_1 - z_2$  and we have  $zv = u$ . We also get  $z^2 \leq 2v$ . Since  $z^2 v^2 = u^2 \leq v^3$ , we have  $v^2(z^2 - v) \leq 0$ . The inequalities  $0 \leq z^2 \leq 2v$  imply  $|z^2 - v| \leq v$ , hence  $(z^2 - v)^2 \leq v^2$  and  $(z^2 - v)^3 \leq v^2(z^2 - v) \leq 0$ , which implies  $z^2 - v \leq 0$ .  $\square$

## D.5. Back to ordered fields

### Real $f$ -rings

The real number field satisfies all the Horn rules of the theory of discrete real closed fields, but not all the dynamical rules. Recall the following dynamical rules satisfied by discrete ordered fields.

$$\begin{array}{ll} \mathbf{IV} & x > 0 \vdash \exists y xy = 1 & \mathbf{ED}_{\#} & \vdash x^2 > 0 \quad \mathbf{op} \quad x = 0 \\ \mathbf{OTF} & x + y > 0 \vdash x > 0 \quad \mathbf{op} \quad y > 0 & \mathbf{OT} & \vdash x \geq 0 \quad \mathbf{op} \quad x \leq 0 \\ \mathbf{FRAC} & 0 \leq a \leq b \vdash \exists z (zb = a^2, 0 \leq z \leq a) \end{array}$$

The real number field verifies  $\mathbf{IV}$ ,  $\mathbf{OTF}$  and  $\mathbf{FRAC}$  but neither  $\mathbf{ED}_{\#}$ , nor  $\mathbf{OT}$ .

The following lemma prepares the definition of the dynamical theory  $\mathcal{Afr}$ .

**Lemma D.5.1.** *In the theory  $\mathcal{Afrnz}$  to which we add the rule  $\mathbf{FRAC}$ , if we define “ $x > 0$ ” as an abbreviation of “ $x \geq 0 \wedge \exists z zx = 1$ ”, the predicate  $\cdot > 0$  satisfies all the axioms of  $\mathcal{Asrnz}$  where it is present as well as the rule  $\mathbf{IV}$ .*

*Proof.* Rules  $\mathbf{IV}$ ,  $\mathbf{aso1}$ ,  $\mathbf{aso2}$ ,  $\mathbf{aso4}$ ,  $\mathbf{col}_{\#}$  are trivially valid. Let’s look at the rule  $\mathbf{aso3}$ : an element greater than or equal to a positive invertible element is invertible. This follows from the rule  $\mathbf{FRAC}$  because if  $b \geq a > 0$ , we have a  $z$  such that  $zb = a^2$ , so  $b$  is invertible. For  $\mathbf{Aso1}$ ,  $\mathbf{Aso2}$  and  $\mathbf{lv}$ , we begin by validating the rule  $x > 0, xu = 1 \vdash u \geq 0$ : indeed  $u = xu^2 \geq 0$ . The rest follows.  $\square$

**Definition D.5.2.** We now define the dynamical theory  $\mathcal{Afr}$  of strongly real  $f$ -rings (or to abbreviate, strongly real rings) on the following signature.

$$\mathbf{Signature} : \boxed{\Sigma_{\mathcal{Afr}} = (\cdot = 0, \cdot \geq 0, \cdot > 0; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, - \cdot, \text{Fr}(\cdot), 0, 1)}$$

The axioms of the  $\mathcal{Afr}$  theory are as follows:

- the axioms of  $\mathcal{Afrnz}$ ;

<sup>10</sup>We are in an  $\ell$ -group for addition, we can reason case by case, separately with  $0 \leq y \leq z \leq a$  and  $0 \leq z \leq y \leq a$ . In both cases we obtain  $0 \leq |z - y| \leq a$ .

- the axioms which define  $x > 0$  as an abbreviation of “ $x \geq 0 \wedge \exists z xz = 1$ ”;
- the axioms **fr1** and **fr2**.

This definition is justified by the fact that the theory of local strongly real rings is essentially identical to the theory *Co* of *non* discrete ordered field: Item 3 of Lemma D.5.4.

**Lemma D.5.3.** *The dynamical theory  $\mathcal{A}fr$  is essentially identical to the theory  $\mathcal{A}srnz$  to which we add the axioms **IV** and **FRAC**<sup>11</sup>.*

*Proof.* The theory  $\mathcal{A}srnz$  contains in its signature the predicate “ $\cdot > 0$ ” which is not present in  $\mathcal{A}frnz$ . When we add the axiom **IV**, we have  $x > 0$  if, and only if,  $x$  is  $\geq 0$  and invertible. Lemma D.5.1 therefore implies that the theory  $\mathcal{A}frnz$  to which we add the axiom **FRAC** is essentially identical to the theory  $\mathcal{A}srnz$  to which we add the axioms **IV** and **FRAC**. Finally, Lemma D.4.7 shows that adding the axiom **FRAC** to  $\mathcal{A}frnz$  is equivalent to adding the function symbol **Fr** with the axioms **fr1** and **fr2**.  $\square$

A strongly real ring is therefore a reduced  $\mathbb{Q}$ -*f*-algebra in which any element greater than an invertible positive element is itself invertible. Moreover, the validity of the rule **FRAC** adds a little something.

**Lemma D.5.4.**

1. The Horn theory  $\mathcal{A}srnz$  to which we add as axioms the dynamical rules **IV** and **OTF** is essentially identical to the theory *Co0*.
2. The dynamical theory  $\mathcal{A}fr$  to which we add the axiom **ED<sub>#</sub>** is essentially identical to the theory *Codsup* of discrete ordered fields with sup (or to *Cod*).
3. The dynamical theory  $\mathcal{A}fr$  to which we add the axiom **OTF** is essentially identical to the theory *Co* of *non* discrete ordered fields: a strongly real local ring is a *non* discrete ordered field.<sup>12</sup>

*Proof.* 1. Comparing the theories *Co0* (Definition C.3.2) and  $\mathcal{A}srnz$ , we find in the first the additional axioms **Aonz**, **IV** and **OTF** and the collapse axiom is missing. But collapse follows from **IV** and **Aonz** is deduced from **Anz** (Lemma D.4.5).

NB: The axiom **IV** implies that  $x > 0$  is equivalent to “ $x$  is  $\geq 0$  and invertible”. The axiom **OTF** adds the fact that the ring is local.

2. The new theory is an extension of *Co0* from Item 1. To move on to *Codsup* we need only add **ED<sub>#</sub>** and **OT**. Since every element is zero or invertible, we are dealing with a discrete field, and the rule **ASDZ** is valid. Lemma D.4.1 then says that the rule **OT** is also valid.

3. Results from Item 1 and Lemmas D.4.7, D.5.1 and D.5.5.  $\square$

**Lemma D.5.5.** *In a reduced *f*-ring where the rule **FRAC** is valid, the following rule **AFRL** replaces the rule **OTF** when we define the predicate  $a > 0$  as an abbreviation of  $a \geq 0 \wedge \exists z az = 1$ .*

$$\mathbf{AFRL} \quad z(x+y) = 1, x+y \geq 0 \vdash \exists u (ux = 1, x \geq 0) \quad \mathbf{op} \quad \exists v (vy = 1, y \geq 0)$$

*Proof.* *Direct implication.* Assume **A** is local and prove the rule **AFRL**. Since  $x+y$  is invertible,  $x$  or  $y$  is invertible. For example  $x \in \mathbf{A}^\times$ . By Lemma D.4.2 we have  $x \geq 0$  or  $x \leq 0$ . If  $x \leq 0$ , then  $y \geq x+y \geq 0$ , therefore  $y \in \mathbf{A}^\times$  (Lemma D.5.1). *Reciprocal.* If  $x+y$  is invertible, then  $x+y \geq 0$  or  $x+y \leq 0$  (Lemma D.4.2). In the first case, **AFRL** shows that  $x$  or  $y$  is invertible. In the second case,  $-x$  or  $-y$  is invertible.  $\square$

<sup>11</sup>This implies that the theory  $\mathcal{A}fr$  defined here is slightly stronger than the one defined in [40].

<sup>12</sup>We could have avoided introducing the predicate  $x > 0$  in  $\mathcal{A}fr$  because it is defined as an abbreviation. The rule **OTF** should be replaced by the rule **AFRL** in Item 2. The theory would then be a Horn theory. This is hardly surprising since the theory of real closed rings is purely equational and a *non* discrete real closed field is a local real closed ring.

## Formal Positivstellensätze with sup

For simultaneous collapse, we have already given Theorem D.3.4.

**Formal Positivstellensatz D.5.6** (formal Positivstellensatz, 2).

The following dynamical theories prove the same Horn rules.

1. On the signature  $(\cdot = 0, \cdot \geq 0 ; \cdot + \cdot, \cdot \times \cdot, -, 0, 1)$ : the theory  $\mathcal{Aonz}$  of strictly reduced ordered rings (Definition C.1.4), the theory  $\mathcal{Crcdsup}$  of discrete real closed fields with sup and intermediate theories (for example  $\mathcal{Afrnz}$ ,  $\mathcal{Atonz}$ ,  $\mathcal{Cod}$  or  $\mathcal{Co0}$ ).
2. On the signature  $(\cdot = 0, \cdot \geq 0, \cdot > 0 ; \cdot + \cdot, \cdot \times \cdot, -, 0, 1)$ : the  $\mathcal{Asonz}$  theory of reduced strictly ordered rings, the  $\mathcal{Crcdsup}$  theory and intermediate theories (for example  $\mathcal{Asrnz}$ ,  $\mathcal{Cod}$  or  $\mathcal{Co0}$ ).
3. On the signature  $(\cdot = 0, \cdot \geq 0 ; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, -, 0, 1)$ : the  $\mathcal{Afrnz}$  theory of reduced  $f$ -rings, the  $\mathcal{Crcdsup}$  theory and intermediate theories (e.g.  $\mathcal{Asrnz}$ ,  $\mathcal{Co0}$ ).
4. On the signature  $(\cdot = 0, \cdot \geq 0, \cdot > 0 ; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, -, 0, 1)$ : the theory  $\mathcal{Asrnz}$  of reduced strict  $f$ -rings, the theory  $\mathcal{Crcdsup}$  and intermediate theories (for example  $\mathcal{Co}$  and  $\mathcal{Codsup}$ ).
5. On the signature  $(\cdot = 0, \cdot \geq 0 ; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, -, \text{Fr}(\cdot, \cdot), 0, 1)$ : the  $\mathcal{Afr}$  theory of strongly real rings, the theory  $\mathcal{Crcdsup}$  and intermediate theories (for example  $\mathcal{Co}$  and  $\mathcal{Codsup}$ ).

*Proof.* 1 and 2. The theory  $\mathcal{Crcdsup}$  is essentially identical to  $\mathcal{Crcd}$ . So Positivstellensätze C.2.2 and C.2.1 give Items 1 and 2.

3. Since the theories  $\mathcal{Atonz}$  and  $\mathcal{Crcd}$  prove the same Horn rules, Theorem A.5.5 tells us that the theories  $\mathcal{Atosupnz}$  and  $\mathcal{Crcdsup}$  prove the same Horn rules. To have Item 3, it suffices to show that  $\mathcal{Afrnz}$  and  $\mathcal{Atosupnz}$  prove the same Horn rules. As the theories  $\mathcal{Afrnz}$  and  $\mathcal{Atosupnz}$  prove the same Horn rules (formal Positivstellensatz D.3.2) we conclude with Theorem A.5.6.

4. Same reasoning as in the previous item.

5. Note that  $\mathcal{Codsup}$  validates the rules **IV** and **FRAC**, which can be replaced by the introduction of  $\text{Fr}$  with its two axioms (Lemma D.4.7). On the other hand, the dynamical theory  $\mathcal{Afr}$  is essentially identical to the theory  $\mathcal{Asrnz}$  to which we add the axioms **IV** and **FRAC** (Item 2 of Lemma D.5.1). Item 5 therefore results from Item 4.  $\square$

*Remark D.5.7.* In the theories  $\mathcal{Afr}$  and  $\mathcal{Co}$ , we have added the function symbol  $\text{Fr}$  with the axioms **fr1** and **fr2**, which increases the Horn rules formulable in these theories. Nevertheless the use of the symbol  $\text{Fr}$  can be eliminated in the Horn rules in favour of the axiom **FRAC** (see the addition of a function symbol page 27 and Lemma C.3.6). As this axiom is satisfied in the stronger theory  $\mathcal{Cod}$ , Positivstellensatz D.5.6 is not affected by the presence of  $\text{Fr}$ . We could also accept the presence of the function symbol  $\text{Fr}$  with the axioms **fr1** and **fr2** in the theory  $\mathcal{Codsup}$ .  $\blacksquare$

**Corollary D.5.8.** Consider the dynamical theory  $\mathcal{Asrnz} = \mathcal{Asrnz}(\mathbb{Q})$  of reduced strict  $f$ -rings.

1. Let  $\mathbf{K}$  be a discrete ordered field and  $\mathbf{R}$  its algebraic closure. Let  $\mathbf{A} = ((G, \text{Rel}), \mathcal{Asrnz}(\mathbf{K}))$  be a dynamic algebraic structure with  $G = (x_1, \dots, x_n)$  and  $\text{Rel}$  finite. We have an algorithm which decides whether  $\mathbf{A}$  collapses and which in case of a negative answer gives the description of a system  $(\xi_1, \dots, \xi_n)$  in  $\mathbf{R}^n$  which satisfies the constraints given in the relations  $\text{Rel}$ .
2. We have an algorithm that decides whether a Horn rule of  $\mathcal{Asrnz}$  is valid. If the answer is negative, the algorithm gives the description of a system  $(\xi_1, \dots, \xi_n)$  in  $\mathbf{R}_{\text{alg}}^n$  which contradicts the Horn rule.
3. The same results are valid with  $\mathcal{Afr} = \mathcal{Afr}(\mathbb{Q} \cap [0, 1])$  instead of  $\mathcal{Asrnz}$ . In this case we add the function symbol  $\text{Fr}$  with the two accompanying axioms to  $\mathcal{Crcdsup}$ .

*Proof.* We have just seen (formal Positivstellensatz D.5.6) that the Horn theory  $\mathcal{A}smz$  (resp.  $\mathcal{A}fir$ ) proves the same Horn rules as  $\mathcal{C}rcdsup$  (resp. by adding Fr). Moreover, we see that a Horn rule of  $\mathcal{C}rcdsup$  (possibly by adding Fr) is equivalent to a family of Horn rules of  $\mathcal{C}rcd$ . We can therefore conclude with the concrete Positivstellensatz C.2.6.  $\square$

The ring  $\text{Sipd}_n(\mathbf{A})$  of semipolynomials over  $\mathbf{A}$  in  $n$  variables is explained in Definition D.3.10, the  $f$ -ring  $\text{AFR}(\mathbf{A})$  generated by  $\mathbf{A}$  is defined in D.3.8.

**Theorem D.5.9.** Fix  $n$  and denote  $\mathbf{K}[x] = \mathbf{K}[x_1, \dots, x_n]$ .

1. Let  $\mathbf{K}$  be a discrete ordered field and  $\mathbf{R}$  its real closure. The ring  $\text{Sipd}_n(\mathbf{K}, \mathbf{R})$  is identified with the  $f$ -ring generated by  $\mathbf{K}[x]$ . More precisely: the structure of  $\mathbf{K}$  gives to  $\mathbf{K}[x]$  a dynamic algebraic structure of  $f$ -ring and the unique  $\mathbf{K}$ -morphism of  $f$ -rings from  $\text{AFR}(\mathbf{K}[x])$  to  $\text{Sipd}_n(\mathbf{K}, \mathbf{R})$  is an isomorphism.
2. Let  $\mathbf{K}$  be a discrete ordered field and  $\mathbf{R}$  its real closure. If every semialgebraic open of  $\mathbf{R}^n$  contains points of  $\mathbf{K}^n$ , the ring  $\text{Sipd}_n(\mathbf{K})$  is identified with  $\text{AFR}(\mathbf{K}[x])$ .
3. (incomplete proof) If  $\mathbf{K}$  is a  $\mathbb{Q}$ -algebra contained in  $\mathbb{R}$ , the ring  $\text{Sipd}_n(\mathbf{K})$  identifies with  $\text{AFR}(\mathbf{K}[x])$ .

*Proof.* It must be shown that if an expression of the form given in Lemma D.3.11 defines the identically zero map, this can be proved using only the Horn rules of reduced  $f$ -rings.

1. By the Positivstellensatz, the fact that a semipolynomial is zero at any point in  $\mathbf{R}^n$  has an algebraic certificate on  $\mathbf{K}$ . Now  $\mathcal{A}frnz$  and  $\mathcal{C}rcdsup$  prove the same Horn rules. (For more details on this kind of subject see [26]).

2. Results from the previous item because under the considered hypothesis, a  $\mathbf{K}$ -semipolynomial not zero everywhere on  $\mathbf{R}^n$  is not zero everywhere on  $\mathbf{K}^n$ .

3. If  $\mathbf{K}$  is discrete, this follows from Item 1, because a  $\mathbf{K}$ -semipolynomial zero on  $\mathbf{K}$  is zero on  $\mathbb{Q}$  and therefore on  $\mathbb{R}$  and a fortiori on the real closure of the field of fractions of  $\mathbf{K}$ . Apparently, it takes a bit of effort to obtain the result constructively in all generality, whereas it is clear in classical mathematics. It's the same kind of gymnastics as for the complete constructive proof of the solution of the 17th Hilbert problem on  $\mathbb{R}$ , given in [26]. The bonus is that the solution is then completely explicit, i.e. it does not use any sign test (or dependent choice axiom) on  $\mathbb{R}$ .  $\square$

## D.6. The real lattice and spectrum of a commutative ring

A prime cone of the commutative ring  $\mathbf{A}$ , i.e. an element of the real spectrum  $\text{Sper } \mathbf{A}$ , can be given as a non-trivial integral quotient ring  $\mathbf{A}/\mathfrak{P}$  with a linearly ordered ring structure, in other words as a minimal model of the  $\mathcal{A}ito(\mathbf{A})$  theory of non-trivial integral linearly ordered rings based on  $\mathbf{A}$  (see Definition A.2.6).

As the theory of nontrivial linearly ordered integral rings is a dynamical theory without existential axioms, the real spectrum is identified with the spectrum of the distributive lattice  $\text{Reel}(\mathbf{A})$  obtained by “recopying”<sup>13</sup> the axioms of the dynamical theory  $\mathcal{A}ito(\mathbf{A})$ .

To find the usual topology on the set  $\text{Spec}(\text{Reel } \mathbf{A})$ <sup>14</sup> underlying the real spectrum  $\text{Sper } \mathbf{A}$ , we must consider the lattice based on the only predicate  $x > 0$ . This gives Definition D.6.2, which corresponds to the following valid dynamical rules in  $\mathcal{C}od$

$$\begin{array}{ll}
 \mathbf{col}_{\#} & 0 > 0 \vdash \perp & \mathbf{aso1} & \vdash 1 > 0 \\
 \mathbf{aso3} & x > 0, y > 0 \vdash x + y > 0 & \mathbf{OTF} & x + y > 0 \vdash x > 0 \quad \mathbf{op} \quad y > 0 \\
 \mathbf{aso4} & x > 0, y > 0 \vdash xy > 0 & \mathbf{OTF}^{\times} & xy < 0 \vdash x < 0 \quad \mathbf{op} \quad y < 0
 \end{array}$$

<sup>13</sup>As we do below, in Definition D.6.2.

<sup>14</sup>According to the tradition established when the real spectrum was invented.

*Remark D.6.1.* If we base ourselves solely on the predicate  $x > 0$  and if we introduce the predicate  $x \geq 0$  as the opposite of the predicate  $-x > 0$ , and the predicate  $x = 0$  as the conjunction  $x \geq 0 \wedge -x \geq 0$ , we obtain on the basis of the previous axioms alone a conservative extension which satisfies all the axioms of *Aito*. The minimal models of the dynamical theory described by the 6 previous axioms are therefore (in classical mathematics) the integral quotients of  $\mathbf{A}$  with a relation of total order. This justifies the following definition: the spectrum of the lattice  $\text{Reel } \mathbf{A}$  is indeed identified with the real spectrum of  $\mathbf{A}$  (in classical mathematics). ■

**Definition D.6.2.** The *real lattice* of a commutative ring  $\mathbf{A}$ , denoted  $\text{Reel } \mathbf{A}$ , is the distributive lattice generated by  $(\mathbf{A}, \vdash)$  where  $\vdash$  is the smallest entailment relation satisfying

$$\left. \begin{array}{l} 0 \vdash \\ x, y \vdash x + y \\ x, y \vdash xy \end{array} \quad \begin{array}{l} \vdash 1 \\ x + y \vdash x, y \\ -xy \vdash x, y \end{array} \right\} \quad (\text{D.5})$$

This simple and constructive way of defining the real lattice goes back to [10], which was inspired by [Johnstone, Section V-4.11].

# E. *Non* discrete real closed fields

## Sommaire

---

<b>Introduction</b> . . . . .	<b>86</b>
<b>E.1 2-closed ordered field (or euclidean field)</b> . . . . .	<b>86</b>
<b>E.2 Virtual roots</b> . . . . .	<b>87</b>
Definition and first properties . . . . .	87
A result à la Pierce-Birkhoff . . . . .	91
<i>f</i> -rings with virtual roots . . . . .	91
Domain variant . . . . .	92
Rings of integral continuous semialgebraic maps . . . . .	93
Pierce-Birkhoff rings . . . . .	93
<b>E.3 Real closed rings</b> . . . . .	<b>93</b>
Constructive definition and variants . . . . .	93
Continuous semialgebraic maps . . . . .	94
An example . . . . .	94
Ordered fields with virtual roots . . . . .	94
Formal Positivstellensatz . . . . .	94
Quotient, localisation and gluing of real closed rings . . . . .	95
Comparison with the definition in classical mathematics . . . . .	96
An axiomatic of Niels Schwartz . . . . .	96
The axiomatics of Prestel-Schwartz . . . . .	97
The axiomatics of Marcus Tressl . . . . .	98
<b>E.4 Non discrete real closed fields</b> . . . . .	<b>99</b>
A reasonable definition . . . . .	99
Real closure of a reduced <i>f</i> -ring . . . . .	99
Real closure of a <i>non</i> discrete ordered field . . . . .	100
<b>E.5 A non-archimedean <i>non</i> discrete real closed field</b> . . . . .	<b>100</b>
<b>E.6 Use of virtual roots in constructive real algebra</b> . . . . .	<b>104</b>
Basic semialgebraic subsets of the real line . . . . .	104
Sign and variation tables . . . . .	104
An approximate cylindrical algebraic decomposition (CAD)? . . . . .	105
Stratifications . . . . .	105
The Fundamental Theorem of Algebra ( <b>FTA</b> ) . . . . .	106
1. The square roots of a complex number $c = a + ib$ . . . . .	106
2. The general case . . . . .	106
3. The general case in terms of multisets. . . . .	107
<b>E.7 Some questions</b> . . . . .	<b>107</b>
Continuous semialgebraic maps . . . . .	107
Real closure . . . . .	108
Pierce-Birkhoff . . . . .	108
The 17th Hilbert problem . . . . .	108
The Grail? . . . . .	109

---



## Introduction

Section E.1 explains how to introduce square roots of the elements  $\geq 0$  into an  $f$ -ring and in particular into a *non* discrete ordered field. This is intended as an introduction to the more general notion of virtual roots. The case of discrete ordered fields was treated in [42, section 3.2]. The moral of this case is that we don't need to know whether a square root is already present in the ordered field in order to introduce it formally without any risk of contradiction. Here we see the superiority of the constructive point of view over the classical point of view (which usually uses **LEM** to decide whether the coveted square root is already present or not).

Section E.2 explains how to add virtual root maps in *non* discrete ordered fields. Virtual roots were introduced in [27] for discrete ordered fields. The aim was to have, for a real monic polynomial, continuous maps of the coefficients which cover the real roots. In particular, this made it possible to have a constructive version of the intermediate value theorem in which no sign test was used. In fact, similar work can be done on any  $f$ -ring.

Section E.3 deals with real closed rings and Section E.4 proposes a definition for *non* discrete real closed fields as local real closed rings. The theory of real closed rings is presented here in an elementary, purely equational form, in the style of [69].

### E.1. 2-closed ordered field (or euclidean field)

As a starting point, let's look at the question of introducing the square roots of the elements  $\geq 0$ . For the case of a discrete ordered field we refer to [42, section 3.2].

We are interested in the following rule which says that the elements  $\geq 0$  are squares.

$$\mathbf{sqr} \vdash \exists z \geq 0 \ x^+ = z^2$$

*Remark* E.1.1. In an  $f$ -ring, in the presence of nilpotents, two elements  $z$  and  $y \geq 0$  which have the same square are not necessarily equal, but if the ring is reduced, they are equal, by virtue of the simplification rule **Afrnz3**. So the rule **sqr** is a simple existential rule with unique existence and if we slolemise this rule in the theory **Afrnz** we get an essentially identical theory. ■

We now present a version in which a nonnegative square root of a nonnegative element is given as a unary law in the dynamical theory which extends **Afr**

$$\mathbf{Sqr}: \mathbf{R} \rightarrow \mathbf{R}, \ x \mapsto \sqrt{x^+} \quad \text{in case of a real closed field.}$$

This function symbol must obey the following natural direct rules.

$$\mathbf{sqr}_= \quad y = 0 \vdash \mathbf{Sqr}(x + y) = \mathbf{Sqr}(x)$$

$$\mathbf{sqr2} \vdash \mathbf{Sqr}(x) = \mathbf{Sqr}(x^+)$$

$$\mathbf{sqr0} \vdash \mathbf{Sqr}(0) = 0$$

$$\mathbf{sqr3} \vdash \mathbf{Sqr}(x)^2 = x^+$$

$$\mathbf{sqr1} \vdash \mathbf{Sqr}(x) \geq 0$$

$$\mathbf{sqr4} \vdash \mathbf{Sqr}(x^+y^+) = \mathbf{Sqr}(x)\mathbf{Sqr}(y)$$

#### Definition E.1.2.

- We denote **Afr2c** the purely equational theory of 2-closed  $f$ -rings: it is obtained from **Afr** by adding the unary function symbol **Sqr** with the six preceding axioms.
- We denote **Asr2c** the dynamical theory of 2-closed *strict*  $f$ -rings obtained from **Asr** in the same way that **Afr2c** was obtained from **Afr**.
- We denote **Co2c** the dynamical theory of 2-closed *non* discrete ordered fields obtained from **Co** in the same way.

Nota that  $\mathbf{Sqr}(x) = 0$  when  $x \leq 0$  and  $\mathbf{Sqr}(x) = \sqrt{x}$  when  $x \geq 0$ .

**Lemma E.1.3.** *A 2-closed  $f$ -ring is reduced.*

*Proof.* On the one hand  $|a|^2 = |a^2|$ , and on the other hand for a  $x \geq 0$  such that  $x^2 = 0$ , we have the equalities  $0 = \text{Sqr}(x^2) = \text{Sqr}(x)^2 = x^+ = x$ .  $\square$

**Lemma E.1.4.** *The following two extensions of the  $\mathcal{Afr}$  theory are essentially identical.*

1.  $\mathcal{Afr}2c$ : we have added the function symbol  $\text{Sqr}$  but the theory remains purely equational since **sqr1** can be written as  $\text{Sqr}(x) = \text{Sqr}(x)^+$ .
2. Dynamic rules **Anz** and **sqr** are added as axioms (the language is not changed).

*Proof.* First of all, in the theory  $\mathcal{Afrnz}$  the simple existential rule **sqr** has unique existence by virtue of Remark E.1.1. Next, we check that the symbol  $\text{Sqr}$  obtained by skolemising the existential axiom **sqr** satisfies the 6 desired axioms.  $\square$

The following lemma can be seen as a generalisation to the *non* discrete case of the fact that on a 2-closed discrete ordered field, the commutative ring structure completely determines the order structure.

**Lemma E.1.5.** *On a commutative ring, if there is a 2-closed  $f$ -ring structure, it is unique. More generally, a ring morphism between two 2-closed  $f$ -rings is a 2-closed  $f$ -ring morphism.*

*Proof.* Let  $\varphi: \mathbf{A} \rightarrow \mathbf{B}$  be a ring morphism where  $\mathbf{A}$  and  $\mathbf{B}$  are 2-closed  $f$ -rings. Since  $x \geq 0$  are squares, the order relation is respected. Now in a 2-closed  $f$ -ring (or more generally in a reduced  $f$ -ring) the element  $c = a \vee b$  is characterised by the equalities and inequalities  $c \geq a$ ,  $c \geq b$  and  $(c - a)(c - b) = 0$  (Lemma D.4.6). We deduce that the ring morphism is also a morphism for  $\vee$  laws. Finally, since in a reduced  $f$ -ring, two elements  $\geq 0$  which have the same square are equal (Remark E.1.1), the law  $\text{Sqr}$  is also respected by the ring morphism.  $\square$

Since the theory  $\mathcal{Afr}2c$  is purely equational, any  $f$ -ring  $\mathbf{A}$  freely generates a 2-closed  $f$ -ring: its 2-closure  $\text{AFR}2C(\mathbf{A})$ . The question then arises: what does the 2-closure of an  $f$ -ring look like? Here's the first clue.

**Lemma E.1.6.** *Any reduced  $f$ -ring injects into its 2-closure.*

*Proof.* The theory  $\mathcal{Afr}2c$  proves the same Horn rules as  $\mathcal{Afrnz}$ : this follows from Item 3 of Formal Positivstellensatz D.5.6, because the map  $\text{Sqr}$  added to the theory  $\mathcal{Crcd}$  gives an essentially identical theory. We therefore do not obtain any new equality between elements of the original  $f$ -ring after formally adding the square roots of the elements  $\geq 0$ .  $\square$

This generalises the fact that a discrete ordered field is injected into its 2-closure ([42, 43]), which is a discrete ordered field. For the *non* discrete case arises the natural question E.7.6.

**Lemma E.1.7.** *The  $\text{Co}2c$  theory is essentially identical to the following two theories.*

1. On the signature  $(\cdot = 0; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, - \cdot, \text{Fr}(\cdot), \text{Sqr}(\cdot), 0, 1)$  the theory obtained from  $\mathcal{Afr}2c$  by adding the function symbol  $\text{Fr}$  with axioms **fr1**, **fr2**, and the axiom **AFRL**.
2. On the signature  $(\cdot = 0, \cdot > 0; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, - \cdot, 0, 1)$  the theory obtained by adding as axioms to  $\mathcal{Afr}$  the rules **IV**, **OTF**, **FRAC**, **Anz** and **sqr**.

A 2-closed ordered field is also called a 2-closed real field or an euclidean field..

## E.2. Virtual roots

### Definition and first properties

References: [27, 16, 2, 5, 25].

The idea which guided the introduction of virtual roots was to have, for a real monic polynomial, continuous maps of the coefficients which cover the real roots. When a real root disappears in the

complex plane, it can be replaced by the root of the derivative that coincides with the double real root when it disappears.

For example, the virtual square roots of an arbitrary real  $a$  (i.e.  $-\text{Sqr}(a)$  and  $+\text{Sqr}(a)$ ) are equal to  $-\sqrt{a}$  and  $\sqrt{a}$  when  $a \geq 0$ , otherwise they are zero: this is the value they had when they disappeared (imagine the polynomial  $X^2 - a$  varying continuously with  $a \in \mathbf{R}$ ).

First, let's recall a purely algebraic version of the mean value theorem in case of polynomials.

**Lemma E.2.1** (algebraic mean value theorem). [43, 42]

We can construct two families  $(\lambda_{i,j})_{1 \leq i \leq j \leq n}$  and  $(r_{i,j})_{1 \leq i \leq j \leq n}$  in  $\mathbb{Q} \cap (0, 1)$ , with  $\sum_{i=1}^n r_{i,n} = 1$  for all  $n \geq 1$  and such that, for any polynomial  $f \in \mathbb{Q}[X]$  of degree  $\leq n$ , we have in  $\mathbb{Q}[a, b]$ :

$$f(b) - f(a) = (b - a) \times \sum_{i=1}^n r_{i,n} \cdot f'(a + \lambda_{i,n}(b - a)).$$

The result applies to any  $\mathbb{Q}$ -algebra  $\mathbf{A}$  (in particular to non-discrete ordered fields). If  $\mathbf{A}$  is a strictly ordered  $\mathbb{Q}$ -algebra, this shows that a polynomial whose derivative is  $> 0$  on an open interval  $(a, b)$  is a strictly increasing map on the closed interval  $[a, b]$ .

**Example E.2.2.** For example, for polynomials of degree  $\leq 4$  we have

$$\frac{f(1)-f(-1)}{2} = \frac{1}{3} f'(-\frac{2}{3}) + \frac{1}{6} f'(-\frac{1}{3}) + \frac{1}{6} f'(\frac{1}{3}) + \frac{1}{3} f'(\frac{2}{3}),$$

and more generally, with  $\Delta = b - a$

$$f(b) - f(a) = \Delta \cdot \left( \frac{1}{3} f'(a + \frac{1}{6}\Delta) + \frac{1}{6} f'(a + \frac{1}{3}\Delta) + \frac{1}{6} f'(a + \frac{2}{3}\Delta) + \frac{1}{3} f'(a + \frac{5}{6}\Delta) \right).$$

■

**Lemma E.2.3** (slight variation on [27, Proposition 1.2]).

1. Let  $\sigma = \pm 1$  and  $f: [a, b] \rightarrow \mathbb{R}$  ( $a \leq b \in \mathbb{R}$ ) be a continuously differentiable map such that  $\sigma f'(x) > 0$  on  $[a, b]$ . Then  $|f|$  reaches its minimum at a unique  $x \in [a, b]$ . We call this real  $\mathbf{R}(a, b, f)$ .

We have  $(x - a)(x - b)f(x) = 0$  and  $x$  is the only real number satisfying the following system of inequalities.

- $a \leq x \leq b$
- $\sigma(x - a)f(x) \leq 0$
- $\sigma(x - a)f(a) \leq 0$
- $\sigma(b - x)f(x) \geq 0$
- $\sigma(b - x)f(b) \geq 0$

2. Let  $\sigma = \pm 1$  and  $f: [a, +\infty) \rightarrow \mathbb{R}$  be a continuously differentiable map such that  $\sigma f'(x) > 0$  on  $(a, +\infty)$ . It is assumed that there is a  $b > a$  such that  $\sigma f(b) > 0$ .

Then  $|f|$  reaches its minimum at a single  $x \in [a, +\infty)$ . We denote  $\mathbf{R}(a, +\infty, f)$  this real. We have  $(x - a)f(x) = 0$  and  $x$  is the only real verifying the following system of inequalities:

- $a \leq x$
- $(x - a)f(x) \leq 0$
- $\sigma(x - a)f(a) \leq 0$
- $\sigma f(x) \geq 0$

3. A statement similar to the previous one, left to the reader, for the interval  $(-\infty, a]$ .

4. This lemma is also valid for a discrete real closed field  $\mathbf{R}$  if  $f$  is a continuous semialgebraic map continuously derivable on an interval  $[a, b]$ .

**Remark E.2.4.** 1) In the article [27], when  $f$  is a monic polynomial of degree  $d$ , the hypothesis is formulated in the form  $f'(x) \geq 0$  on  $[a, b]$ , which means that the set of parameters ( $a, b$  and the coefficients of  $f$ ) satisfying the hypothesis is a semialgebraic closure of  $\mathbb{R}^{d+2}$ . We then show that the map  $\mathbf{R}(a, b, f)$  is semialgebraically continuous on this closed set.

2) Note that Items 2 and 3 are offset from Item 1. 3) It seems that we can explain a uniform continuity modulus for  $\mathbf{R}$  if we give certain details about the continuous semialgebraic map  $f'$  (details available when  $f$  is a monic polynomial). ■

From this lemma we obtain the construction of *virtual roots* for a monic polynomial of degree  $d$ : firstly they “cover” all the real roots, and secondly they vary continuously as a function of the coefficients of the polynomial.

For a monic polynomial  $f$  of degree  $d$ ,  $f^{[k]}$  is the  $k$ -th derivative of  $f$  divided by its leading coefficient ( $0 \leq k < d$ ): it is a monic polynomial of degree  $d - k$ .

**Proposition and definition E.2.5.** *Let  $\mathbf{R}$  be a discrete real closed field or the field  $\mathbb{R}$ . For any monic polynomial*

$$f(X) = X^d - (a_{d-1}X^{d-1} + \cdots + a_1X + a_0) \quad (d \geq 1)$$

we define the maps virtual roots of  $f$

$$\rho_{d,j}(f) = \rho_{d,j}(a_{d-1}, \dots, a_0)$$

for  $1 \leq j \leq d$  by induction on  $d$ : (we abbreviate below  $\rho_{k,j}(f^{[d-k]})$  to  $\rho_{k,j}$ )

- $\rho_{1,1}(X - a) = \rho_{1,1}(a) := a$ ;
- $\rho_{d,j} := \mathbf{R}(\rho_{d-1,j-1}, \rho_{d-1,j}, f)$  for  $1 \leq j \leq d$  ( $d \geq 2$ );

By convention we have set  $\rho_{d,0} = (-1)^d \infty$  and  $\rho_{d,d+1} = +\infty$  for all  $d \geq 1$ , and the map  $\mathbf{R}$  is the one defined in Lemma E.2.3.

This proposition can be proved simultaneously with the Items 3d and 3e of the following theorem, using Lemma E.2.1.

**Theorem E.2.6** (some properties of virtual roots). [27, 16]

Let  $\mathbf{R}$  be a discrete real closed field or the field  $\mathbb{R}$ . Let  $\xi$  be an arbitrary element of the field.

1. By Lemma E.2.3, for a given monic polynomial  $f$  of degree  $d$ , the  $\frac{d(d+1)}{2}$  elements  $\rho_{k,j}(f^{[d-k]})$ ,  $k \in \llbracket 1..d \rrbracket$ ,  $j \in \llbracket 1..k \rrbracket$ , are defined by a system of large inequalities.
2. Each map  $\rho_{d,j} : \mathbf{R}^d \rightarrow \mathbf{R}$  is uniformly continuous on any ball

$$B_{d,M} := \{(a_{d-1}, \dots, a_0) \mid \sum_i a_i^2 \leq M\}, (M > 0).$$

Uniform continuity can be given in fully explicit form on  $B_{d,M}$ .

3. For a monic polynomial  $f$  of degree  $d$ , note  $\tilde{f} = \prod_{j=1}^d (X - \rho_{d,j}(f))$  and  $f^* = \prod_{j=0}^{d-1} f^{[j]}$ .

We use the conventions  $\rho_{d,0}(f) = (-1)^d \infty$  and  $\rho_{d,d+1}(f) = +\infty$ .

In the following, we fix  $f$  and note  $\rho_{\delta,j} = \rho_{\delta,j}(f^{[d-\delta]})$  for  $1 \leq j \leq \delta \leq d$ .

- (a) We have  $\rho_{d,1} \leq \rho_{d-1,1} \leq \cdots \leq \rho_{d-1,j} \leq \rho_{d,j+1} \leq \cdots \leq \rho_{d-1,d-1} \leq \rho_{d,d}$ .
- (b) If  $d \geq 2$  and  $f = X^d - a$ , then  $\rho_{d,d} = \sqrt[d]{a^+}$ ,  $\rho_{d,j} = 0$  for  $1 < j < d$ ,  $\rho_{d,1} + \rho_{d,d} = 0$  if  $d$  is even and  $\rho_{d,1} + \rho_{d,d} = \sqrt[d]{a}$  if  $d$  is odd.
- (c) If  $f = \prod_{i=1}^d (X - \xi_i)$  for  $\xi_i \in \mathbf{R}$ , then  $\tilde{f} = f$ . Consequently  $\rho_{d,1} = \bigwedge_i \xi_i$ ,  $\rho_{d,d} = \bigvee_i \xi_i$  and  $\rho_{d,k} = \bigwedge_{J \subseteq \llbracket 1..d \rrbracket, \#J=k} (\bigvee_{i \in J} \xi_i)$ .
- (d) • If  $\rho_{d-1,j} < \rho_{d-1,j+1}$ , ( $0 \leq j \leq d-1$ ), then  $f$  is strictly monotonic on the interval, increasing if  $d-j$  odd, decreasing otherwise.  
• For  $0 \leq j \leq d-1$ , we have  $(-1)^{d-j} (f(\rho_{d-1,j+1}) - f(\rho_{d-1,j})) \leq 0$ .<sup>1</sup>

<sup>1</sup>This implies that in the system of large inequalities which defines the  $\rho_{k,j}$  for  $k \leq d$  and  $1 \leq j \leq k$ , the signs (in the broad sense) of the  $\Delta$  of Item 1 of Lemma E.2.3 are known, and can be given directly, as in the example which follows the theorem, which simplifies things a little: the  $\Delta$  “disappear”.

- (e) If  $\rho_{d,j} < \xi < \rho_{d,j+1}$ , ( $0 \leq j \leq d$ ), then  $(-1)^{d-j} f(\xi) > 0$ .
- (f) The zeros of  $f$  are zeros of  $\tilde{f}$ , with multiplicity greater than or equal to  $\tilde{f}$ . More precisely
- If  $f(\xi) = 0$ , then  $\tilde{f}(\xi) = 0$ ;
  - If  $|\tilde{f}(\xi)| > 0$ , then  $|f(\xi)| > 0$ ;
  - If  $f^{[j]}(\xi) = 0$  for  $j \in \llbracket 1..k \rrbracket$ , then  $\tilde{f}^{[j]}(\xi) = 0$  for  $j \in \llbracket 1..k \rrbracket$ ;
  - If  $f^{[j]}(\xi) = 0$  for  $j \in \llbracket 1..k \rrbracket$  and  $|\tilde{f}^{[k+1]}(\xi)| > 0$ , then  $|f^{[k+1]}(\xi)| > 0$ .

Furthermore, if the multiplicities are known, the difference in multiplicities for  $f$  and  $\tilde{f}$  is even (for example, a non-zero  $\rho_{d,j}$  of  $f$  is of even multiplicity in  $\tilde{f}$ ).

- (g) The real zeros of  $f^*$  are exactly the  $\rho_{d,j}$ . More precisely
- each  $\rho_{d,j}$  is a zero of  $f^*$ ,
  - if all  $|\xi - \rho_{d,j}|$  are  $> 0$ , then  $|f^*(\xi)| > 0$ ,
  - the polynomial  $\tilde{f}$  divides  $(f^*)^d$ .
- (h) Let  $a \in \mathbf{R}$  be such that the  $|f^{[k]}(a)| > 0$  for  $0 \leq k \leq d$ , and let  $r$  be the number of sign changes in the sequence of  $f^{[k]}(a)$ , ( $k = d, \dots, 0$ ), ( $0 \leq r \leq d$ ). Then  $\rho_{d,d-r} < a < \rho_{d,d-r+1}$ .

- (i) (Intermediate Value Theorem)

If  $a < b$  and  $f(a)f(b) < 0$ , we have  $\prod_{j=1}^d f(\mu_j) = 0$ , where  $\boxed{\mu_j = a \vee (b \wedge \rho_{d,j})}$ .  
Special cases.

- If  $d$  is odd, then  $\prod_{j=1}^d f(\rho_{d,j}) = 0$ .
- If  $0 \leq k < \ell \leq d$  and  $f(\rho_{d-1,k})f(\rho_{d-1,\ell}) < 0$ , then  $\prod_{j=k}^{\ell-1} f(\rho_{d,j}) = 0$ .
- If, according to Item 3h we have  $\rho_{d,k} < a < \rho_{d,k+1} < b < \rho_{d,k+2}$ , then  $f(\rho_{d,k+1}) = 0$ .

- (j) (Extrema values) The monic polynomial  $f$  “attains its upper bound and its lower bound on any closed bounded interval” in the following precise sense: if  $a < b$ , we have

$$\begin{aligned} \sup_{\xi \in [a,b]} f(\xi) &= f(a) \vee f(b) \vee \sup_{j=1}^{d-1} f(\nu_j) \quad \text{where } \boxed{\nu_j = a \vee (b \wedge \rho_{d-1,j})}, \\ \inf_{\xi \in [a,b]} f(\xi) &= f(a) \wedge f(b) \wedge \inf_{j=1}^{d-1} f(\nu_j). \end{aligned}$$

If  $f$  has a constant strict sign  $\sigma = \pm 1$  on  $[a, b]$ , we have  $\inf_{\xi \in [a,b]} (\sigma f(\xi)) > 0$ .

- (k) (Minimum in absolute value and non intermediate value)

If  $a < b$ , we have

$$\inf_{\xi \in [a,b]} |f(\xi)| = |f(a)| \wedge |f(b)| \wedge \inf_{j=1}^d |f(\mu_j)|.$$

Furthermore, if the second member is  $> 0$ , then  $f$  has a constant sign on  $[a, b]$ .

- (l) (A bound) If  $f(x) = x^d + \sum_{k=0}^{d-1} a_k x^k$  we have  $|\rho_{d,j}| \leq \sup_{k=0}^d (1 + |a_k|)$  ( $1 \leq j \leq d$ ).
- (m) (Change of variable) Let  $f(x) = x^d + \sum_{k=0}^{d-1} a_k x^k$  and  $g(x) = x^d + \sum_{k=0}^{d-1} c^{d-k} a_k x^k$  (formally  $g(x) = c^d f(x/c)$ ).
- If  $c \geq 0$ , we have  $\rho_{d,j}(g) = c\rho_{d,j}(f)$  ( $1 \leq j \leq d$ ).
  - If  $c \leq 0$ , we have  $\rho_{d,j}(g) = c\rho_{d,d+1-j}(f)$  ( $1 \leq j \leq d$ ).
  - In all cases,  $\prod_{1 \leq j \leq d} (x - c\rho_{d,j}(f)) = \prod_{1 \leq j \leq d} (x - \rho_{d,j}(g))$ .

**Example E.2.7.** We explain here the inequalities mentioned in Item 1 of the previous theorem leading to  $\rho_{4,3}(f)$  for a polynomial  $f(X) = X^4 - (a_3 X^3 + a_2 X^2 + a_1 X + a_0)$ , written here in the form of direct rules without hypotheses. We use the conventions of Item 3 of Theorem E.2.6. Thus, let  $\rho_{1,1} = \rho_{1,1}(\frac{a_3}{4})$ ,  $\rho_{2,j} = \rho_{2,j}(\frac{a_3}{2}, \frac{a_2}{6})$ ,  $\rho_{3,j} = \rho_{3,j}(\frac{3a_3}{4}, \frac{a_2}{2}, \frac{a_1}{4})$ ,  $\rho_{4,j} = \rho_{4,j}(a_3, a_2, a_1, a_0)$ . The inequalities characterising  $\rho_{1,1}$ ,  $\rho_{2,2}$ ,  $\rho_{3,2}$  and  $\rho_{4,3}$  are given. Note that in the definition of virtual roots, the sign  $\sigma = \pm 1$  before  $x - a$  or  $b - x$  in Item 1 of Lemma E.2.3 is known because of Item 3d of Theorem E.2.6, which explains why this sign does not appear in the inequalities below.

$$\begin{array}{ll}
\mathbf{vr}_{1,1} \vdash \rho_{1,1} = \frac{a_3}{4} & \\
\mathbf{vr}_{2,1,0} \vdash \rho_{2,1} \leq \rho_{1,1} & \mathbf{vr}_{2,1,2} \vdash (\rho_{2,1} - \rho_{1,1}) f^{[2]}(\rho_{2,1}) \geq 0 \\
\mathbf{vr}_{2,1,1} \vdash (\rho_{2,1} - \rho_{1,1}) f^{[2]}(\rho_{1,1}) \leq 0 & \mathbf{vr}_{2,1,3} \vdash f^{[2]}(\rho_{2,1}) \geq 0 \\
\mathbf{vr}_{2,2,0} \vdash \rho_{1,1} \leq \rho_{2,2} & \mathbf{vr}_{2,2,2} \vdash (\rho_{2,2} - \rho_{1,1}) f^{[2]}(\rho_{2,2}) \leq 0 \\
\mathbf{vr}_{2,2,1} \vdash (\rho_{2,2} - \rho_{1,1}) f^{[2]}(\rho_{1,1}) \geq 0 & \mathbf{vr}_{2,2,3} \vdash f^{[2]}(\rho_{2,2}) \geq 0 \\
\mathbf{vr}_{3,3,0} \vdash \rho_{2,2} \leq \rho_{3,3} & \mathbf{vr}_{3,3,2} \vdash (\rho_{3,3} - \rho_{2,2}) f^{[1]}(\rho_{3,3}) \leq 0 \\
\mathbf{vr}_{3,3,1} \vdash (\rho_{3,3} - \rho_{2,2}) f^{[1]}(\rho_{1,1}) \geq 0 & \mathbf{vr}_{3,3,3} \vdash f^{[1]}(\rho_{3,3}) \geq 0 \\
\mathbf{vr}_{3,2,0} \vdash \rho_{2,1} \leq \rho_{3,2} \leq \rho_{2,2} & \mathbf{vr}_{3,2,3} \vdash (\rho_{3,2} - \rho_{2,1}) f^{[1]}(\rho_{3,2}) \geq 0 \\
\mathbf{vr}_{3,2,1} \vdash (\rho_{3,2} - \rho_{2,1}) f^{[1]}(\rho_{2,1}) \geq 0 & \mathbf{vr}_{3,2,4} \vdash (\rho_{3,2} - \rho_{2,2}) f^{[1]}(\rho_{3,2}) \geq 0 \\
\mathbf{vr}_{3,2,2} \vdash (\rho_{3,2} - \rho_{2,2}) f^{[1]}(\rho_{2,2}) \geq 0 & \\
\mathbf{vr}_{4,3,0} \vdash \rho_{3,2} \leq \rho_{4,3} \leq \rho_{3,3} & \mathbf{vr}_{4,3,3} \vdash (\rho_{4,3} - \rho_{3,2}) f(\rho_{4,3}) \geq 0 \\
\mathbf{vr}_{4,3,1} \vdash (\rho_{4,3} - \rho_{3,2}) f(\rho_{3,2}) \geq 0 & \mathbf{vr}_{4,3,4} \vdash (\rho_{4,3} - \rho_{3,3}) f(\rho_{4,3}) \geq 0 \\
\mathbf{vr}_{4,3,2} \vdash (\rho_{4,3} - \rho_{3,3}) f(\rho_{3,3}) \geq 0 & 
\end{array}$$

■

## A result à la Pierce-Birkhoff

We call *polyroot map* a map  $\mathbf{R}^m \rightarrow \mathbf{R}$  which can be written in the form  $\rho_{d,j}(f_1, \dots, f_d)$  for integers  $1 \leq j \leq d$  and polynomials  $f_j \in \mathbf{R}[x_1, \dots, x_m]$ .

The following theorem à la Pierce-Birkhoff is worth noting. It looks like a Nullstellensatz: it expresses that there is a purely algebraic reason for a map being semialgebraic continuous and integral over the ring of polynomials.

**Theorem E.2.8.** ([27, Theorem 6.4]) *Let  $\mathbf{R}$  be a discrete real closed field and let  $g: \mathbf{R}^m \rightarrow \mathbf{R}$  be an continuous semialgebraic map integral on the ring  $\mathbf{R}[x_1, \dots, x_m]$  (seen as a ring of functions). Then  $g$  is a combination by  $\vee$ ,  $\wedge$  and  $+$  of polyroot maps  $\mathbf{R}^m \rightarrow \mathbf{R}$ . More precisely, if  $g(\underline{x})$  is a root of the  $Y$ -monic polynomial  $P(Y, \underline{x})$  of degree  $d$ , it is expressed as a sup-inf combination of maps of the form*

$$\rho_{d,j}(P) + \sqrt[r]{R_\ell^+ \cdot \left(1 + \sum_{i=1}^n x_i^2\right)^s} \quad (\text{E.1})$$

for  $R_\ell \in \mathbf{R}[x_1, \dots, x_m]$  (the second term in the sum (E.1) is also a polyroot map, see Item 3b of Theorem E.2.6).

*Remark.* When the map  $g$  is piecewise polynomial, it cancels a monic polynomial  $P(Y) = \prod_{i=1}^d (Y - f_i)$  for  $f_i \in \mathbf{R}[x_1, \dots, x_m]$ . In the expression obtained by E.1 for  $g$ , it is the Łojasiewicz inequality which is responsible for the extraction of the  $r$ -th root in the formula. As for the  $\rho_{d,j}(P)$  they are sup-inf combinations of the  $f_i$  (Item 3c of Theorem E.2.6). ■

### $f$ -rings with virtual roots

**Example E.2.9.** We take again Example C.1.7 of the  $\mathbb{Q}$ -linearly ordered algebra  $\mathbb{Q}[\alpha]$ , with  $\alpha > 0$  and  $\alpha^6 = 0$ . We will see that the constraints imposed on  $\rho_{2,2}(f)$ , when  $f = X^2 - a^2$  and  $a \geq 0$ , do not necessarily imply that  $\rho_{2,2} = a$ . The constraints are as follows for  $x = \rho_{2,2}$  (note that  $\rho_{1,1} = 0$ ):

$$\mathbf{vr}_{2,2,0} \vdash 0 \leq x$$

$$\mathbf{vr}_{2,2,2} \vdash x(x^2 - a^2) \leq 0$$

$$\mathbf{vr}_{2,2,1} \vdash -x a^2 \leq 0$$

$$\mathbf{vr}_{2,2,3} \vdash (x^2 - a^2) \geq 0$$

If we take  $a = \alpha$ , all  $x \geq 0$  such that  $x^2 = a^2$  fit, and therefore all  $\alpha + y\alpha^5$  for  $y \in \mathbb{Q}[\alpha]$  are solutions. If we take  $a^2 = 0$  the constraints are equivalent to “ $x \geq 0$  and  $x^3 \leq 0$ ” and any element of the interval  $[0, \alpha^2]$  is a solution, including  $\zeta = \alpha^2$  whereas  $\zeta^2 > 0$ . ■

**Lemma E.2.10.** *On an  $f$ -ring, the system of inequalities satisfied by the virtual roots  $\rho_{k,j}$  ( $1 \leq j \leq k \leq d$ ) for a given monic polynomial of degree  $d$ , if they exist, defines these elements unambiguously.*

*Proof.* The uniqueness in question is expressed by means of Horn rules. The theory  $\mathcal{Afrnz}$  proves the same Horn rules as the theory of discrete real closed fields with sup (formal Positivstellensatz D.5.6). In the latter theory, uniqueness is guaranteed (Item 1 of Theorem E.2.6). □

Example E.2.9 and Lemmas E.2.10 and E.2.12 justify the following definition.

#### Definition E.2.11.

1. The purely equational theory  $\mathcal{Afrv}$  of  $f$ -rings with virtual roots is obtained as follows from the purely equational theory  $\mathcal{Afr}$ .
  - For  $1 \leq j \leq d$  in  $\mathbb{N}$ , we add a function symbol  $\rho_{d,j}$  of arity  $d$ ;
  - as axioms we add the inequalities described in Item 1 of Theorem E.2.6;
  - we add the following rule **vrsup**

$$\mathbf{vrsup} \vdash \rho_{2,2}(a + b, -ab) = a \vee b.$$

The signature is therefore as follows:  $(\cdot = 0 \cdot ; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, -, \cdot, (\rho_{d,j})_{1 \leq j \leq d}, 0, 1)$ .

2. In the same way, we define the Horn theory  $\mathcal{Asrv}$  of strict  $f$ -rings with virtual roots from the Horn theory  $\mathcal{Asr}$ .

**Lemma E.2.12.** *An  $f$ -ring with virtual roots is reduced.*

*Proof.* Given the rule **vrsup**, if  $a^2 = 0$ , we have with  $b = -a$ :

$$0 = \rho_{2,2}(0, 0) = \rho_{2,2}(a + b, -ab) = |a|.$$

□

#### • Domain variant

**Definition E.2.13** ( $f$ -ring with virtual roots, domain variant).

The Horn theory  $\mathcal{Aitorv}$  of linearly ordered domains with virtual roots is obtained from the Horn theory  $\mathcal{Aito}$  of linearly ordered domains by adding the virtual roots in the same way as the theory  $\mathcal{Afrv}$  is obtained from the theory  $\mathcal{Afr}$  in Definition E.2.11.

Note that we don't need to put the rule **vrsup** in the axioms.

**Lemma E.2.14.** *A linearly ordered domain with virtual roots is integrally closed and its field of fractions is discrete real closed. Reciprocally, an integrally closed domain whose fraction field is discrete real closed is an integrally closed domain with virtual roots.*

*Proof.* Let  $\mathbf{A}$  be the domain and  $\mathbf{K}$  its field of fractions, which is discrete.

*Direct implication.* A monic polynomial  $f \in \mathbf{A}[X]$  satisfies  $\mathbf{RCF}_n$  because of Item 3i of E.2.6 and the fact that  $\mathbf{K}$  is discrete. For an arbitrary polynomial of  $\mathbf{K}[X]$  we use the change of variables in Item 3m to reduce to a monic polynomial of  $\mathbf{A}[X]$ . So  $\mathbf{K}$  is discrete real closed. Finally  $\mathbf{A}$  is integrally closed due to Item 3f.

*Reciprocal implication.* The order on  $\mathbf{K}$  induces a total order on  $\mathbf{A}$ . It must be shown that for a monic polynomial  $f \in \mathbf{A}[X]$  the  $\rho_{d,j}(f)$  are in  $\mathbf{A}$ . Now they are zeros of  $f^*$ , a monic polynomial of  $\mathbf{A}[X]$ , so they are in  $\mathbf{K}$ , and  $\mathbf{A}$  is integrally closed, so they are in  $\mathbf{A}$ . Thus the maps  $\rho_{d,j}(a_0, \dots, a_n)$  defined from  $\mathbf{K}^n$  to  $\mathbf{K}$  are restricted to maps  $\mathbf{A}^n \rightarrow \mathbf{A}$ .  $\square$

#### • Rings of integral continuous semialgebraic maps

Theorem E.2.8 (for discrete real closed fields) legitimates the following definition.

**Definition and notation E.2.15.** Let  $\mathbf{R}$  be an  $f$ -ring with virtual roots (special cases: an ordered field with virtual roots or a real closed ring). The families  $\mathbf{Fsace}_m(\mathbf{R})$  ( $m \in \mathbb{N}$ ) of *integral continuous semialgebraic maps* are defined as the families of maps  $\mathbf{R}^m \rightarrow \mathbf{R}$  stable by composition, containing the polynomial maps (with coefficients in  $\mathbf{R}$ ) and the virtual root maps. In other words, an element of  $\mathbf{Fsace}_m(\mathbf{R})$  is a map  $\mathbf{R}^m \rightarrow \mathbf{R}$  defined by a term of the language of  $\mathcal{A}frrv(\mathbf{R})$  with the  $m$  variables  $x_1, \dots, x_m$  (some of which may be absent).

#### • Pierce-Birkhoff rings

**Definitions and notations E.2.16.** Let  $\mathbf{A}$  be a ring, or more generally a dynamic algebraic structure of an  $f$ -ring.

1. The ring  $\mathbf{AFRNZ}(\mathbf{A})$  is the *reduced  $f$ -ring generated by  $\mathbf{A}$* .
2. The ring  $\mathbf{AFRRV}(\mathbf{A})$  is the  *$f$ -ring with virtual roots generated by  $\mathbf{A}$* .
3. The ring  $\mathbf{Ppm}(\mathbf{A})$  is defined as the  *$f$ -subring of  $\mathbf{AFRRV}(\mathbf{A})$  formed by the elements  $x$  which cancel a polynomial  $\prod_{i=1}^k (X - a_i)$  for  $a_i \in \mathbf{A}$* .
4. A ring  $\mathbf{A}$  is called a *Pierce-Birkhoff ring* when the natural morphism  $\mathbf{AFRNZ}(\mathbf{A}) \rightarrow \mathbf{Ppm}(\mathbf{A})$  is an isomorphism.

See Question E.7.11.

## E.3. Real closed rings

### Constructive definition and variants

**Definition E.3.1** (real closed rings). The purely equational theory  $\mathcal{A}rc$  of *real closed rings* is obtained by adding to the theory  $\mathcal{A}frrv$  the function symbol  $\text{Fr}$  and the axioms **fr1** and **fr2**.

The signature is therefore as follows:  $(\cdot = 0 \cdot ; \cdot + \cdot, \cdot \times \cdot, \cdot \vee \cdot, -, \cdot, (\rho_{d,j})_{1 \leq j \leq d}, \text{Fr}(\cdot, \cdot), 0, 1)$

**Lemma E.3.2.** *On a commutative ring, if there is a real closed ring structure, it is unique. More generally, a ring morphism between two real closed rings is a real closed ring morphism.*

*Proof.* Results from the lemmas E.1.5 and E.2.10.  $\square$

In the following, when we do not specify otherwise, a *real closed ring* always designates a ring defined in E.3.1.

**Lemma E.3.3** (variants for  $\mathcal{A}rc$ ).



1. The theory  $\mathcal{A}rc$  can also be obtained from the Horn theory  $\mathcal{A}ftr$  by adding the virtual roots in the same way that the theory  $\mathcal{A}frrv$  is obtained from the theory  $\mathcal{A}fr$  in Definition E.2.11. Moreover, given Lemma E.2.12, the axiom **Anz** of the theory  $\mathcal{A}ftr$  can be omitted. A real closed ring can therefore be seen as a strongly real ring with virtual roots.
2. The theory  $\mathcal{A}rc$  is essentially identical to the theory  $\mathcal{A}strrv$  of strict  $f$ -rings with virtual roots to which we add the function symbol  $Fr$  and the axioms **fr1** and **fr2**. NB. The predicate  $x > 0$  must be added to  $\mathcal{A}rc$  as an abbreviation of “ $x$  is  $\geq 0$  and invertible”.

*Proof.* Item 1 is clear. We deduce Item 2 by recalling Lemma D.5.1.  $\square$

### • Continuous semialgebraic maps

We now take Definition C.5.5 (legitimised by Theorem C.5.4) and extend it to real closed rings. Note that every real closed ring contains a conformal copy of  $\mathbb{R}_{alg}$ .

We also assume that we have proved Theorem E.3.16 and its corollaries.

**Definition and notation E.3.4.** Let  $\mathbf{R}$  be a real closed ring and a map  $f: \mathbf{R}^n \rightarrow \mathbf{R}$ .

1. (Elementary case) The map  $f$  is said to be *semialgebraic continuous* (in an elementary way) if there exists a semialgebraic continuous map  $g: \mathbb{R}_{alg}^n \rightarrow \mathbb{R}_{alg}$  expressed by a term  $t(x_1, \dots, x_n)$  of  $\mathcal{A}rc$  and if  $f$  coincides with the map defined by this term.
2. (General case) The map  $f$  is *semialgebraic continuous* if there exists an integer  $r \geq 0$ , elements  $y_1, \dots, y_r \in \mathbf{R}$  and a map  $h: \mathbf{R}^{r+n} \rightarrow \mathbf{R}$  which belongs to the previous elementary case such that

$$\forall x_1, \dots, x_n \in \mathbf{R} \quad f(x_1, \dots, x_n) = h(y_1, \dots, y_r, x_1, \dots, x_n).$$

We denote  $\mathbf{F}fac_n(\mathbf{R})$  the ring of these maps (it is a real closed ring for the natural order relation). Theorem C.5.4 shows that for a discrete real closed field  $\mathbf{R}$  we find the usual definition of continuous semialgebraic maps.

For a comparison of  $\mathbf{F}fac_n(\mathbf{R})$  with  $\mathbf{F}face_n(\mathbf{R})$  see the question E.7.3.

### • An example

**Proposition E.3.5.** Let  $\mathbf{R}$  be an  $f$ -ring with virtual roots and let  $f: \mathbf{R}^n \times \mathbf{R}^p \rightarrow \mathbf{R}$  be a continuous semialgebraic map. The map

$$g: \mathbf{R}^p \rightarrow \mathbf{R}, \underline{x} \mapsto \sup_{\underline{z} \in [0,1]^n} f(\underline{z}, \underline{x})$$

is well-defined and continuous semialgebraic.

*Proof.* Given the ad hoc definition of the rings  $\mathbf{F}fac_m(\mathbf{R})$  we are immediately reduced to the case where  $\mathbf{R} = \mathbb{R}_{alg}$ .  $\square$

See also the questions E.7.5.

## Ordered fields with virtual roots

**Definition E.3.6.** (Compare with Definition E.2.11, see Lemma E.2.10).

1. The dynamical theory  $\mathcal{C}orv$  of *ordered fields with virtual roots* is obtained as follows from the dynamical theory  $\mathcal{C}o$ .
  - For  $1 \leq j \leq d$  in  $\mathbb{N}$ , we add a function symbol  $\rho_{d,j}$  of arity  $d$ ;
  - As axioms, we add the inequalities described in Item 1 of Theorem E.2.6;
2. The dynamical theory  $\mathcal{C}o0rv$  is obtained in the same way from the theory  $\mathcal{C}o0$ .
3. The dynamical theory  $\mathcal{C}odrv$  is obtained in the same way from the theory  $\mathcal{C}od$ .

*Remark.* The theory  $\mathcal{C}odrv$  is essentially identical to the theory obtained by adding to  $\mathcal{C}o0rv$  the axiom “of third excluded” **ED<sub>#</sub>** (see remark C.3.3).

## Formal Positivstellensatz

**Formal Positivstellensatz E.3.7** (formal Positivstellensatz, 3).

1. The theories *Codrv*, *Crcd* and *Crcdsup* are essentially identical.
2. The following dynamical theories prove the same Horn rules (written in the language of *Afrrv*).
  - (a) The theory *Afrrv* of  $f$ -rings with virtual roots.
  - (b) The theory *Arc* of real closed rings.
  - (c) The theory *Codrv* of discrete ordered fields with virtual roots.
3. The following dynamical theories prove the same Horn rules (written in the language of *Asrrv*).
  - (a) The theory *Asrrv* of strict  $f$ -rings with virtual roots.
  - (b) The theory *Corv* of ordered fields with virtual roots.
  - (c) The theory *Codrv* of discrete ordered fields with virtual roots.
4. Theorem E.2.6 is entirely valid for the theory *Asrrv* (thus also for *Corv*). The same is true for the purely equational theory *Afrrv* (so also for *Arc*) if the points which use the predicate  $\cdot > 0$  are deleted or suitably reformulated with  $\cdot \geq 0$ .

*Proof.* The first point is clear. Items 2 and 3 are therefore variants of formal Positivstellensatz D.5.6 taking into account Theorem A.5.5.

Finally, for Item 4, it follows from previous Items that the assertions of Items 2 and 3 of Theorem E.2.6 can be written in the form of Horn rules.  $\square$

In classical mathematics given the general representation theorem A.5.4, the formal Positivstellensätze stated so far give the following results, which can be seen in classical mathematics as characterising the dynamical theories under consideration.

**Corollary\* E.3.8.** *On their respective signatures, the following objects are all isomorphic to sub $\mathcal{T}$ -structures of products of discrete real closed fields (considered with the predicate  $x > 0$  and the maps  $\text{sup}$ ,  $\text{Fr}$  and  $\rho_{d,j}$ ).*

- A reduced  $f$ -ring (theory *Afrnz*).
- A reduced strict  $f$ -ring (theory *Asrnz*).
- A strongly real ring (theory *Aftr*).
- A local  $f$ -ring (theory *Co*).
- An  $f$ -ring with virtual roots (theory *Afrrv*).
- A real closed ring (theory *Arc*).
- A strict  $f$ -ring with virtual roots (theory *Asrrv*).
- An ordered field with virtual roots (theory *Corv*).

## Quotient, localisation and gluing of real closed rings

**Lemma E.3.9** (quotient structure). *Let  $\mathbf{A}$  be a real closed ring and  $I$  a radical ideal. Then  $\mathbf{A}/I$  is a real closed ring.*

*Proof.* Let us first show that the radical ideal  $I$  is solid. We must first show that if  $x \in I$ , then  $|x| \in I$ : indeed  $|x|^2 = x^2 \in I$ . Then if  $0 \leq |x| \leq y$  with  $y \in I$ , we must show that  $x \in I$ . Now, by **FRAC**,  $y$  divides  $|x|^2 = x^2$ , so  $x^2 \in I$ , then  $x \in I$ . The quotient  $\mathbf{A}/I$  is therefore an  $f$ -ring. Next we need to see that the virtual root maps  $\rho_{d,j}$  and the map “fraction”  $\text{Fr}$  “pass to the quotient”. Now these maps, when they exist in a reduced  $f$ -ring, are well-defined by the systems of inequalities they satisfy (Lemma E.2.10). As these inequalities pass to the quotient, everything is in order.  $\square$

**Lemma E.3.10** (localisation). *Let  $\mathbf{A}$  be a real closed ring and  $S$  be a monoid. Then  $S^{-1}\mathbf{A}$  is a real closed ring.*

*Proof.* We already know that  $S^{-1}\mathbf{A}$  has a  $\vee$  law which makes it an  $f$ -ring. Let’s see what happens to the virtual roots. Let’s take Example E.2.7 with a polynomial  $f(X) = X^4 - (\frac{a_3}{s}X^3 + \frac{a_2}{s}X^2 + \frac{a_1}{s}X + \frac{a_0}{s})$  with  $a_i \in \mathbf{A}$  and  $s \in S^+$ . In  $S^{-1}\mathbf{A}$  with  $Y = sX$  we have

$$s^4 f(X) = Y^4 - (a_3 Y^3 + sa_2 Y^2 + s^2 a_1 Y + s^3 a_0) = Y^4 - (b_3 Y^3 + b_2 Y^2 + b_1 Y + b_0) = g(Y)$$

and therefore also  $s^4 g(\frac{Y}{s}) = f(X)$ . Consider the virtual roots  $\rho_{i,j}$  for the monic polynomial  $g$  of  $\mathbf{A}[Y]$  with  $(i, j)$  equal to  $(1, 1)$ ,  $(2, 1)$ ,  $(2, 2)$ ,  $(3, 3)$ ,  $(3, 2)$ ,  $(4, 3)$ , and finally the  $\rho'_{i,j} = \frac{\rho_{i,j}}{s}$ . We see that the inequalities in Example E.2.7, just as they are satisfied for the  $\rho_{i,j}$  with respect to the polynomial  $g$  in  $\mathbf{A}[Y]$ , are ipso facto satisfied for the  $\rho'_{i,j}$  with respect to the polynomial  $f$  in  $S^{-1}\mathbf{A}[X]$ . These inequalities completely characterise the virtual roots when they exist (Lemma E.2.10).

A similar reasoning works for the map  $\text{Fr}(\cdot, \cdot)$ .  $\square$

**Concrete local-global principle E.3.11** (concrete gluing of real closed rings).

*Let  $S_1, \dots, S_n$  be comaximal monoids of a ring  $\mathbf{A}$ . Let  $\mathbf{A}_i$  denote  $\mathbf{A}_{S_i}$ ,  $\mathbf{A}_{ij}$  denote  $\mathbf{A}_{S_i S_j}$ , and assume that a structure of type **Arc** is given on each  $\mathbf{A}_i$ . It is further assumed that the images in  $\mathbf{A}_{ij}$  of the laws of  $\mathbf{A}_i$  and  $\mathbf{A}_j$  coincide. Then there exists a unique structure of real closed ring on  $\mathbf{A}$  which induces by localisation in each  $S_i$  the structure defined on  $\mathbf{A}_i$ . This real closed ring is identified with the projective limit of the diagram*

$$((\mathbf{A}_i)_{i < j \in \llbracket 1..n \rrbracket}, (\mathbf{A}_{ij})_{i < j \in \llbracket 1..n \rrbracket}; (\alpha_{ij})_{i < j \in \llbracket 1..n \rrbracket}),$$

where  $\alpha_{ij}$  are localisation morphisms, in the category of real closed rings.

*Proof.* We copy, mutatis mutandis, the proof of the concrete local-global principle D.3.5 for  $f$ -rings.  $\square$

*Remarks.* 1) This implies that the notion of a real closed scheme is well-defined.

2) The analogous concrete local-global principles, with the same proof, are valid for reduced  $f$ -rings, for strongly real rings, and for  $f$ -rings with virtual roots.  $\blacksquare$

## Comparison with the definition in classical mathematics

References: [63, 56, 69].

The structure of *real closed ring* is defined by N. Schwartz in a very abstract way in his Phd [62, Schwartz, 1984]. An axiomatisation as a coherent theory was proposed in [56, Prestel & Schwartz, 2002] (see Definition E.3.14 and Proposition E.3.15).

The aim of N. Schwartz was to give an abstract description of the rings of continuous semialgebraic maps on semialgebraic closures for a fixed real closed field  $\mathbf{R}$ , and to define abstract “real closed spaces”.

### • An axiomatic of Niels Schwartz

Here is the definition of real closed rings in classical mathematics given in [63, Schwartz, 1986].

**Definition\* E.3.12.** A ring *real closed* is a reduced ring  $\mathbf{A}$  satisfying the following properties.

1. The set of squares of  $\mathbf{A}$  is the set of  $\geq 0$  elements of a partial order which makes  $\mathbf{A}$  an  $f$ -ring.
2. If  $0 \leq a \leq b$ , there exists  $z$  such that  $zb = a^2$  (*convexity axiom*).
3. For any prime ideal  $\mathfrak{p}$ , the residual ring  $\mathbf{A}/\mathfrak{p}$  is integrally closed and its field of fractions is a real closed field.

**Proposition\* E.3.13.** *In classical mathematics, Definitions E.3.1 and E.3.12 are equivalent.*

*Proof. Direct.* For a real closed ring  $\mathbf{A}$  of Definition E.3.12, the virtual root maps are well-defined, as we know that all continuous semialgebraic maps defined on  $\mathbb{R}_{\text{alg}}$  are defined on  $\mathbf{A}$ . The same applies to the map “fraction” Fr.

*Reciprocal.* For a real closed ring  $\mathbf{A}$  of Definition E.3.1, we must show that Item 3 of Definition E.3.12 is satisfied. Given a prime ideal  $\mathfrak{p}$ , the residual ring  $\mathbf{A}/\mathfrak{p}$  has no zerodivisors and is therefore linearly ordered (Lemma D.4.1). It is also a real closed ring by Lemma E.3.9. Lemma E.2.14 tells us that  $\mathbf{A}/\mathfrak{p}$  is integrally closed and that its field of fractions is a real closed field.  $\square$

#### • The axiomatics of Prestel-Schwartz

The article [56, Prestel & Schwartz, 2002] shows in classical mathematics that the real closed ring structure of Definition E.3.12 is described by a coherent theory. The existential axioms proposed by the authors to replace Item 3 of E.3.12 are very sophisticated and the proof is also an astonishing tour de force.

**Definition E.3.14.** (*Prestel-Schwartz real closed rings*) A commutative ring is said to be real closed if it satisfies the following axioms.

i-iv) The commutative ring  $\mathbf{A}$  is reduced, the elements  $\geq 0$  are exactly the squares and the order relation makes  $\mathbf{A}$  a convex  $f$ -ring (axiom **CVX**)

v) For each  $d \geq 1$ , let  $f(x) = x^{2d+1} + \sum_{k=0}^{2d} a_k x^k$ ,  $\delta = \text{discr}_x(P)$  its discriminant, and  $g(x) = x^{2d+1} + \sum_{k=0}^{2d} \delta^{2(2d+1-k)} a_k x^k$ , we pose the axiom

$$\vdash \exists z g(z) = 0$$

vi) For each  $d \geq 1$  we pose the axiom

$$x^d + \sum_{k=0}^{d-1} a_k x^k y^{d-k} = 0 \vdash \exists z_1, \dots, z_d y(x - z_1 y) \cdots (x - z_d y) = 0$$

**Proposition E.3.15.** *In the theory  $\mathcal{Arc}$  the axioms of Definition E.3.14 are valid dynamical rules.*

*Proof.* Recall that Theorem E.2.6 is fully valid in the theory  $\mathcal{Arc}$  (Item 4 of E.3.7).

Let's look at the axiom vi). Let  $f = x^d + \sum_{k=0}^{d-1} a_k x^k$  and  $g = x^d + \sum_{k=0}^{d-1} a_k x^k y^{d-k}$ .

We denote  $\tilde{f} = \prod_{1 \leq j \leq d} (x - \rho_{d,j}(f))$  and  $\tilde{g} = \prod_{1 \leq j \leq d} (x - \rho_{d,j}(g))$ . Item 3m of Theorem E.2.6 gives the equality

$$\prod_{1 \leq j \leq d} (x - y \rho_{d,j}(f)) = \prod_{1 \leq j \leq d} (x - \rho_{d,j}(g)).$$

Moreover, Item 3f of Theorem E.2.6 for the polynomial  $g$  gives

$$x^d + \sum_{k=0}^{d-1} a_k x^k y^{d-k} = 0 \vdash (x - \rho_{d,1}(g)) \cdots (x - \rho_{d,d}(g)) = 0.$$

We therefore obtain in the  $\mathcal{Arc}$  theory, by taking  $z_k = \rho_{d,k}(f)$ , the valid rule

$$x^d + \sum_{k=0}^{d-1} a_k x^k y^{d-k} = 0 \vdash (x - z_1 y) \cdots (x - z_d y) = 0.$$

Let's look at the axiom  $v$ ). We will show that the element  $z$  whose existence is asserted can be chosen as a continuous semialgebraic map of the parameters  $a_k$ . Since this map is cancelled by the monic polynomial  $Q$  we then conclude by the theorem “à la Pierce-Birkhoff” E.2.8. Given the formal Positivstellensatz E.3.7 (Item 2) we need only prove the validity of the rule in the theory *Codrv*. Let us therefore consider a discrete real closed field and, in the parameter space, a connected component of the open  $\{\delta \neq 0\}$ . On this connected component, the real zeros of  $f$  are simple (there is at least one because the degree is odd) and vary continuously as a function of the parameters. Those of  $g$  are simply multiplied by  $\delta^2$ . So on this connected component we have the element  $z$  sought as a continuous semialgebraic function of the parameters by choosing the largest of the real zeros. As we approach an edge of a related component, these zeros tend towards 0 (they are zeros of  $f$  multiplied by  $\delta^2$ ). So these continuous semialgebraic maps join together to form a global continuous semialgebraic map.  $\square$

In classical mathematics, the reciprocal implication is demonstrated: the Prestel-Schwartz axioms imply the existence of virtual roots (because they are continuous semialgebraic maps). This gives the equivalence in classical mathematics of our axiomatics and that of Prestel-Schwartz.

• **The axiomatics of Marcus Tressl**

A more elementary version, similar to the one we propose, for the theory of real closed rings can be found in [69, Tressl, 2007] (see also [63, 61, 65, 64]). In this paper, a real closed ring is an  $f$ -ring  $\mathbf{R}$  on which are given all continuous semialgebraic maps defined on  $\mathbb{R}_{\text{alg}}$ , and for which all algebraic identities linking these maps on  $\mathbb{R}_{\text{alg}}$  are satisfied in  $\mathbf{R}$ .

A good analysis of the classical mathematical articles on real closed rings should allow us to understand why it is enough to add the fractions allowed by the rule **FRAC** to an  $f$ -ring with virtual roots to be able to capture all the continuous semialgebraic maps  $\mathbb{R}_{\text{alg}}^m \rightarrow \mathbb{R}_{\text{alg}}$ . This is the subject of the following concrete results, which are valid in classical mathematics, but for which we would like a constructive proof. See in particular the question E.7.2.

Recall that according to the finiteness theorem ([Bochnak, Coste & Roy, Theorem 2.7. 1]) the graph  $G_f = \text{set}\{(\underline{x}, y) \mid \underline{x} \in \mathbf{R}^n, y = f(\underline{x})\}$  of a continuous semialgebraic map  $f: \mathbb{R}_{\text{alg}}^n \rightarrow \mathbb{R}_{\text{alg}}$  is a semialgebraic closure of  $\mathbb{R}_{\text{alg}}^{n+1}$  which can be described as the zero set of a *semipolynomial map*  $F: \mathbb{R}_{\text{alg}}^{n+1} \rightarrow \mathbb{R}_{\text{alg}}$ , i. e. a map written in the form

$$\sup_i (\inf_{1 \leq j \leq k_i} p_{ij}) \quad \text{where } p_{ij} \in \mathbb{R}_{\text{alg}}[x_1, \dots, x_n, y]$$

We can decide whether such a graph is that of a continuous semialgebraic map. The following theorem means that in such a case we can prove the existence of  $y$  depending on  $x_i$  directly in the purely equational theory *Arc*.

**Theorem E.3.16.** *Any continuous semialgebraic map  $\mathbb{R}_{\text{alg}}^n \rightarrow \mathbb{R}_{\text{alg}}$  can be defined by a term of the theory *Arc*.*

**Corollary E.3.17.** *The axiomatisation proposed in E.3.1 for real closed rings is equivalent to that proposed by Tressl [69].*

**Corollary E.3.18.** *Let  $\mathbf{R}$  be a real closed ring. Any continuous semialgebraic map  $\mathbf{R}^n \rightarrow \mathbf{R}$  (Definition E.3.4) is defined by a term of *Arc*( $\mathbf{R}$ ) with  $n$  free variables.*

The following corollary is more problematic, can we return to the case  $\mathbf{R} = \mathbb{R}_{\text{alg}}$  ?

**Corollary E.3.19.** *Consider a real closed ring  $\mathbf{R}$ , a continuous semialgebraic map  $g: \mathbf{R}^n \rightarrow \mathbf{R}$  (an element of  $\text{Fsc}_n(\mathbf{R})$ ) and a polynomial  $p \in \mathbf{R}[x_1, \dots, x_n]$  with at least one invertible coefficient. We assume that, on the set  $\{\xi \in \mathbf{R}^n \mid |p(\xi)| > 0\}$ , the fraction  $f = g/p$  satisfies a uniform continuity modulus on all bounded subsets à la Łojasiewicz (as in Lemma C.5.3). Then there exists a unique continuous semialgebraic map  $h: \mathbf{R}^n \rightarrow \mathbf{R}$  such that  $hp = g$ .*

When the axiom **OTF** is added, Theorem E.3.16 gives the following corollary.

**Corollary E.3.20.** *The theories *Crc1* and *Corv* are essentially identical.*

## E.4. Non discrete real closed fields

### A reasonable definition

**Lemma E.4.1.** *A real closed ring is local if, and only if, it satisfies the rule **AFRL**.*

*Proof.* See Lemma D.5.5. □

We now propose for the theory of *non* discrete real closed fields a formulation essentially identical to *Corv*, but almost purely equational. The rule **AFRL** is preferred to the rule **OTF** because we do not introduce the predicate  $\cdot > 0$  which would take us out of the purely equational theories for *Arc*.

**Definition E.4.2.** The *dynamical theory of non discrete real closed fields*, denoted *Crc2*, is the extension of the purely equational theory *Arc* obtained by adding the rule **AFRL**. In other words, a *non* discrete real closed field is nothing other than a local real closed ring.

**Proposition E.4.3.** *The theories *Corv*, *Crc1* and *Crc2* are essentially identical (we must define the predicate  $> 0$  which we add to *Crc2*).*

*Proof.* Corollary E.3.20 compares *Corv* and *Crc1*. Lemma D.5.4 tells us that a *non* discrete ordered field is none other than a local strongly real ring. In other words, the theory *Co* is essentially identical to the theory *Aftr* to which we add the axiom **AFRL**. Let's start with *Aftr*. If we add the virtual roots then **AFRL** we pass to *Arc* (Lemma E.3.3 Item 1) then to *Crc2*. If we add **AFRL** then the virtual roots we go to *Co* then to *Corv*. □

*Remarks E.4.4.*

- 1) The field  $\mathbb{R}$  is a constructive model of the theory *Crc2*.
- 2) The theory *Crcd* of discrete real closed fields is essentially identical to the theory obtained by adding to *Crc2* the axiom **ED<sub>#</sub>** which says that equality is decidable.
- 3) The theory *Crc2* is nothing other than the theory of local real closed rings. However, there are local real closed rings which are not fields in Heyting's sense. For example, consider the ring  $\mathbf{A}$  of continuous semialgebraic maps on  $\mathbb{R}_{\text{alg}}$ , and let  $\mathbf{B} = S^{-1}\mathbf{A}$  where  $S$  is the monoid of maps  $f$  such that  $f(0) \neq 0$ . It is the ring of germs at  $(0)$  of maps  $f \in \mathbf{A}$ . An element  $f \in \mathbf{A}$  is  $> 0$  in  $\mathbf{B}$  (resp.  $\leq 0$  in  $\mathbf{B}$ ) if, and only if,  $f(0) > 0$  in  $\mathbb{R}_{\text{alg}}$  (resp.  $f(x) \leq 0$  in the neighbourhood of  $0$ ). This shows that **HOF** is not satisfied in  $\mathbf{B}$ , because it is not enough for  $f(0) \leq 0$  for  $f$  to be  $\leq 0$  in the neighbourhood of  $0$ . Note that this locally real closed ring admits two minimal prime ideals, with the respective locals being the germs of maps to the right (or left) of  $0$ .
- 4) The theory *Crc2* can be used to prove the existence of a square root for a complex number of modulus 1. The unit circle  $\{x^2 + y^2 = 1\}$  is covered by the open areas  $\{x > -1\}$  and  $\{x < 1\}$ , on each of which the existence is guaranteed by a continuous map. However, this existence cannot be proved in *Arc*, because in this purely equational theory, every existence is certified by a term, and every term defines a continuous semialgebraic map. ■

### Real closure of a reduced $f$ -ring

Given a reduced  $f$ -ring  $\mathbf{A}$ , we know (Positivstellensatz D.5.6) that the theory *Crcdsup*( $\mathbf{A}$ ) proves the same Horn rules as *Afrnz*( $\mathbf{A}$ ). The same applies to all intermediate theories, in particular to the theories *Afrrv* and *Arc*.

As the latter are purely equational theories, the reduced  $f$ -ring  $\mathbf{A}$  gives rise to an  $f$ -ring with virtual roots *AFRRV*( $\mathbf{A}$ ) and a real closed ring *ARC*( $\mathbf{A}$ ).

Since the theories *Afrnz*, *Afrrv* and *Arc* prove the same Horn rules,  $\mathbf{A}$  is a substructure (of  $f$ -ring) of *AFRRV*( $\mathbf{A}$ ) which is itself a substructure (of  $f$ -ring with virtual roots) of *ARC*( $\mathbf{A}$ ). In other words, adding the symbols for virtual roots and fractions (with their axioms) does not change  $\mathbf{A}$  as an  $f$ -ring.

These two constructions of “real fences” are without mystery, and unique to within a single isomorphism.

We are in the same situation as for the construction of the real closure of a discrete ordered field ([43, 42]), but here the result seems completely obvious whereas it requires a non-negligible effort in the articles quoted. The main reason for this (very small) miracle is that we are relying here on a constructive proof of the Positivstellensatz. The secondary reason is that we are dealing here only with Horn theories (instead of dynamical theories).

*Remark E.4.5.* A construction of the real closure of a discrete ordered field  $\mathbf{K}$  can also be obtained according to the following argument. We begin by establishing the simultaneous collapse of the theory of discrete ordered fields and that of discrete real closed fields (as in [17, Theorem 3.6]). This is a variant of the formal Positivstellensatz. Then we dynamically evaluate  $\mathbf{K}$  as a discrete real closed field. This forces us to introduce the real zeros of any polynomial, with a Thom coding for each of them (for a polynomial which cancels this zero). Since no ambiguity is possible, the dynamic algebraic structure constructed is in fact a usual algebraic structure of a real closed field. This construction is admittedly less detailed than the one explained in [42], but it is essentially equivalent. In fact, in the other direction, we could probably deduce Theorem 3.6 of [17] from the construction given in [42]. What improves [34] and [17] on the previous result is, on the one hand, that the formal Positivstellensatz is more general (Theorem 3.8 in [17]), and on the other hand, and above all, that the concrete Positivstellensatz is demonstrated. ■

## Real closure of a *non* discrete ordered field

Let us consider a discrete ordered field, *i.e.* a model  $\mathbf{K}$  of the theory  $\mathit{Co}$ . We know that  $\mathit{Corv}$  proves the same Horn rules as  $\mathit{Co}$ .

Let us denote  $\mathbf{R}$  the dynamic algebraic structure  $\mathit{Corv}(\mathbf{K})$ .

All the closed terms of the dynamic algebraic structure  $\mathbf{R}$  are constructed on elements of  $\mathbf{K}$  by means of the function symbols given in the signature (polynomials, virtual roots, legitimate fractions).

The dynamic structure  $\mathbf{R}$  is a natural candidate to be the (usual) algebraic structure of type  $\mathit{Corv}$  generated by  $\mathbf{K}$ , if one exists. However, the problem is that  $\mathbf{R}$  is a dynamic algebraic structure of type  $\mathit{Corv}$ , but not necessarily a model of this theory, because this dynamical theory is defined with non-algebraic axioms.

We can first consider the usual real closed ring algebraic structure  $\mathit{ARC}(\mathbf{K})$  which is identified with the dynamic algebraic structure  $\mathit{Arc}(\mathbf{K})$ . The question is: is the axiom  $\mathit{TsbAFRL}$  a valid rule in  $\mathit{ARC}(\mathbf{K})$ ? In other words, is  $\mathit{ARC}(\mathbf{K})$  a model of  $\mathit{Corv}$ ? In which case we can identify  $\mathbf{R}$  (dynamic algebraic structure) and  $\mathit{ARC}(\mathbf{K})$  (usual algebraic structure).

The answer is not obvious (see Question E.7.7).

## E.5. A non-archimedean *non* discrete real closed field

In this section we describe an example of a non-archimedean *non* discrete real closed field.

Let  $\varepsilon$  be an indeterminate. In Section C.4 we introduced the ordered non-archimedean *non* discrete ordered field  $\mathbf{Q} = \mathbf{Z}[1/\varepsilon]$  where  $\mathbf{Z} = \mathbb{Q}[[\varepsilon]]$  is the ring of formal series in  $\varepsilon$  with rational coefficients where  $\varepsilon$  is a strictly positive infinity.

In fact, the coefficients of the series under consideration could have been taken from any discrete ordered field, in particular from the field  $\mathbb{R}_{\text{alg}}$  of algebraic real numbers. We will denote  $\mathbf{R}_0 = \mathbb{R}_{\text{alg}}[[\varepsilon]]$  the analogue of  $\mathbf{Z}$  and  $\mathbf{R} = \mathbf{R}_0[1/\varepsilon]$  the analogue of  $\mathbf{Q}$ .

We now extend these constructions to the field  $\mathbf{P}$  of Puiseux series with real algebraic coefficients.

First we have the rings of series  $\mathbf{P}_{0,d} = \mathbb{R}_{\text{alg}}[[\varepsilon^{1/d}]]$  for the integers  $d \geq 1$ , all isomorphic to  $\mathbf{R}_0$ , with the inclusion morphisms  $\mathbf{P}_{0,d} \rightarrow \mathbf{P}_{0,dd'}$ . This forms an inductive system whose limit  $\mathbf{P}_0$  (the Puiseux series of valuation  $\geq 0$ ) can be seen as the union of  $\mathbf{P}_{0,d}$ .

Finally, the Puiseux series themselves form the ring defined as  $\mathbf{P} := \mathbf{P}_0[1/\varepsilon]$ .

Note that  $\mathbf{P}_{j,d} = \{ \alpha \in \mathbf{P}_{0,d}[1/\varepsilon] \mid \alpha/\varepsilon^{j/d} \in \mathbf{P}_{0,d} \}$ . We have  $\mathbf{P} = \bigcup_{j,d} \mathbf{P}_{j,d}$ .

We introduce notations which generalise to  $\mathbf{P}_{j,d}$  those already given for  $\mathbf{R}$ . These notations are consistent with the inclusions  $\mathbf{P}_{j,d} \subseteq \mathbf{P}_{j'd',dd'}$ .

Let  $\alpha = \sum_{k=j}^{\infty} a_{k/d} \varepsilon^{k/d} \in \mathbf{P}_{j,d} \subseteq \mathbf{P}_{0,d}[1/\varepsilon]$  ( $j, d \in \mathbb{Z}, d \geq 1$ ). We define:

- $c_{\ell/d}(\alpha) = \begin{cases} 0 & \text{if } \ell < j, \\ a_{\ell/d} & \text{if } \ell \geq j. \end{cases}$
- $\kappa_{\ell/d}(\alpha) = s_{\ell/d} \in \{-1, 0, 1\}$  is defined by recurrence as follows:  

$$s_{\ell/d} = \begin{cases} \text{if } \ell < j, \text{ then } 0 \\ \text{if } \ell \geq j, \begin{cases} \text{if } s_{(\ell-1)/d} \neq 0, \text{ alors } s_{(\ell-1)/d}, \\ \text{if } s_{(\ell-1)/d} = 0, \text{ then sign of } a_{\ell/d}. \end{cases} \end{cases}$$
- $\alpha > 0$  means  $\exists \ell \geq j \ \kappa_{\ell/d}(\alpha) = 1$ .
- $\alpha \geq 0$  means  $\forall \ell \geq j \ \kappa_{\ell/d}(\alpha) \geq 0$ .
- $v(\alpha) > k/d$  means  $\kappa_{k/d}(\alpha) = 0$ .
- $v(\alpha) \leq k/d$  means  $\kappa_{k/d}(\alpha) = \pm 1$ .
- $v(\alpha) \geq k/d$  means  $\kappa_{(k-1)/d}(\alpha) = 0$ .
- $v(\alpha) = k/d$  means  $v(\alpha) \geq k/d$  and  $v(\alpha) \leq k/d$ .

From the previous study in Section C.4 which led to Proposition C.4.1 for the ring  $\mathbf{Z}$  and to Theorem C.4.2 for the ring  $\mathbf{Q}$ , we deduce analogous results for the rings  $\mathbf{P}_{0,d}$  then for  $\mathbf{P}_0$ , then for  $\mathbf{P}$ .

**Proposition E.5.1.**

1. The ring  $\mathbf{P}_0$  is a reduced strict  $f$ -ring which satisfies the following properties.
  - It satisfies the rules **OTF**, **OTF<sup>×</sup>**, **FRAC** and **Val2**. In particular (Lemma D.4.7) the continuous semialgebraic map  $\text{Fr}$  satisfying the rules **Fr1** and **Fr2** is well-defined and the corresponding function symbol can be considered as part of the signature.
  - This is a residually discrete henselian local ring.
  - Its residual field is isomorphic to  $\mathbb{R}_{\text{alg}}$ .  
We have  $\mathbf{P}_0^\times = \{ \xi \in \mathbf{P}_0 \mid \kappa_0(\xi) = \pm 1 \}$  and  $\text{Rad}(\mathbf{P}_0) = \{ \xi \in \mathbf{P}_0 \mid \kappa_0(\xi) = 0 \}$ .
  - The valuation group is isomorphic to  $(\mathbb{Q}, +, \geq)$  (the class of  $\varepsilon$  corresponds to the element 1 of  $\mathbb{Q}$ ).
  - The elements  $\geq 0$  are squares: the ring  $\mathbf{P}_0$  is a 2-closed  $f$ -ring (theory **Asr2c**).
  - More generally, the elements  $\geq 0$  are powers  $k$ -th of elements  $\geq 0$ . Since we are dealing with unique existence, we can introduce the corresponding function symbols in the signature.
  - Furthermore, the ordered Heyting axiom  $\neg(\xi > 0) \Rightarrow \xi \leq 0$  is satisfied.
2. The ring  $\mathbf{P}$  is a reduced strict  $f$ -ring which satisfies the following properties.
  - An element is  $> 0$  if, and only if, it is  $\geq 0$  and invertible.
  - The rules **OTF**, **OTF<sup>×</sup>**, **FRAC** and **IV** (a fortiori **Val2**) are satisfied. In particular (Lemma D.4.7) the continuous semialgebraic map  $\text{Fr}$  satisfying the rules **Fr1** and **Fr2** is well-defined.
  - It is a local ring with  $\text{Rad}(\mathbf{P}) = 0$  (a Heyting field in the terminology of [CACM] or [MRR]).
  - The elements  $\geq 0$  are squares of elements  $\geq 0$ : the ring  $\mathbf{P}$  is a 2-closed strict  $f$ -ring (theory **Asr2c**).



- More generally, the elements  $\geq 0$  are powers  $k$ -th of elements  $\geq 0$ . Since we are dealing with unique existence, we can introduce the corresponding function symbols in the signature.
- The ordered Heyting axiom  $\neg(\xi > 0) \Rightarrow \xi \leq 0$  is satisfied.

*Proof.* Only the fact that the elements  $\geq 0$  are powers  $k$ -th of elements  $\geq 0$  is a really new point which requires a proof. This is left to the reader.  $\square$

We denote  $\mathbf{P}_{\text{alg}}$  the integral closure of  $\mathbb{R}_{\text{alg}}(\varepsilon)$  in  $\mathbf{P}$ : this is the ring of Puiseux series which are integral over the discrete ordered subfield  $\mathbb{Q}(\varepsilon)$ .

In the following we will use the notion of extension by continuity. To talk about extension by continuity, we need to define the notion of a convergent sequence, and check that the usual rules for boundary crossing work for this notion.

**Definition E.5.2** (convergent sequences in  $\mathbf{P}$ ). We will say that *the sequence*  $(\alpha_n)_{n \in \mathbb{N}}$  *converges towards*  $\alpha$  *in*  $\mathbf{P}$  if there exist  $j$  and  $d \in \mathbb{Z}$  with  $d \geq 1$  such that

- $\alpha$  and the  $\alpha_n$  are all in  $\mathbf{P}_{j,d}$ ,
- $\lim_n v(\alpha_n - \alpha) = +\infty$ ,  $\forall k \geq j, \forall N \exists n \geq N \forall \ell \in \llbracket j..k \rrbracket c_{\ell/d}(\alpha_n) = c_{\ell/d}(\alpha)$ .

We will then write  $\alpha = \lim_n \alpha_n$ .

We can easily establish the following properties.

**Proposition E.5.3.**

1.  $\lim_n \alpha_n = 0$  if, and only if,  $\lim_n v(\alpha_n) = +\infty$ .
2. If  $\lim_n \alpha_n = \alpha$  then  $\alpha$  is invertible if, and only if,  $\exists N \forall n > N v(\alpha_n) = v(\alpha_n) < \text{inf ty}$ . In this case  $\alpha^{-1} = \lim_{n \geq N} \alpha_n^{-1}$ .
3. If  $\alpha = \lim_n \alpha_n$ ,  $\beta = \lim_n \beta_n$  and  $a \in \mathbb{R}_{\text{alg}}$ , then
  - $a\alpha = \lim_n a\alpha_n$ ,
  - $\alpha + \beta = \lim_n(\alpha_n + \beta_n)$ ,
  - $\alpha\beta = \lim_n(\alpha_n\beta_n)$ ,
  - $\alpha \vee \beta = \lim_n(\alpha_n \vee \beta_n)$ ,
  - $\text{Fr}(\alpha, \beta) = \lim_n \text{Fr}(\alpha_n, \beta_n)$  and
  - $(\alpha^+)^q = \lim_n(\alpha_n^+)^q$  ( $q \in \mathbb{Q}, q > 0$ ).
4. All  $\alpha \in \mathbf{P}_{j,d}$  is the limit of the sequence of Laurent polynomials  $\pi_m(\varepsilon^{1/d})$  for  $m \geq j$  obtained by truncation of the series  $\alpha$ , defined precisely by

$$\pi_m \in \mathbb{R}_{\text{alg}}[\varepsilon^{1/d}][1/\varepsilon], \quad \pi_m = \sum_{k: j \leq k < m} c_{k/d}(\alpha) \varepsilon^{k/d}$$

We also note that  $\mathbb{R}_{\text{alg}}[\varepsilon^{1/d}][1/\varepsilon] \subseteq \mathbf{P}_{\text{alg}}$ .

We will now prove the following theorem.

**Theorem E.5.4.** *The ring  $\mathbf{P} = \mathbf{P}_0[1/\varepsilon]$  satisfies all the axioms of the theory [Crc2](#). It is therefore a discrete Heyting non-archimedean real closed field.*

*First proof.* We are going to generalise the passage to the limit properties described in Proposition [E.5.3](#) to all continuous semialgebraic maps defined on  $\mathbb{R}_{\text{alg}}$ .

The paper [\[52\]](#) shows that  $\mathbf{P}_{\text{alg}}$  is a discrete real closed field. It is therefore a real closure of  $\mathbb{R}_{\text{alg}}(\varepsilon)$ , constructed in a very different way from that proposed in [\[42\]](#). Now consider a cube  $[-a, a]^r = K \subseteq \mathbb{R}_{\text{alg}}^r$  and a continuous semialgebraic map  $f: K \rightarrow \mathbb{R}_{\text{alg}}$ . Since  $\mathbf{P}_{\text{alg}}$  is a discrete

real closed field,  $f$  extends uniquely into a continuous semialgebraic map  $f_1: K_1 \rightarrow \mathbf{P}_{\text{alg}}$ , where  $K_1 \subseteq \mathbf{P}_{\text{alg}}^r$  is defined by the same system of inequalities as  $K$ . We will show that  $f_1$  extends by continuity into a map  $f_2: K_2 \rightarrow \mathbf{P}$ , where  $K_2 \subseteq \mathbf{P}^r$  is defined by the same system of inequalities as  $K$ . This will suffice to show that  $\mathbf{P}$  is a model of *Crc1*.<sup>2</sup>

**Proposition and definition E.5.5.** *We apply the previous notations for  $K \subseteq K_1 \subseteq K_2$ . Let  $f: K \rightarrow \mathbb{R}_{\text{alg}}$  be a continuous semialgebraic map and  $f_1: K_1 \rightarrow \mathbf{P}_{\text{alg}}$  be its extension to  $\mathbf{P}_{\text{alg}}$ . Then for any sequence  $(\alpha_n)$  in  $\mathbb{R}_{\text{alg}}[\varepsilon, \varepsilon^{-1}]^r \cap K_2$  which converges to a  $\alpha \in \mathbf{P}$ , the sequence  $f_1(\alpha_n)$  converges in  $\mathbf{P}$ . The limit depends only on  $\alpha$  and is denoted  $f_2(\alpha)$ .*

*Proof.* Not so simple! First we have to see that the  $f_1(\alpha_n)$ 's belong to a given  $\mathbf{P}_{j,D}$ ; next a Łojasiewicz inequality could be used for the convergence. □

□

*Second proof.* Given Proposition E.5.1 it suffices to prove the existence property of virtual roots for the ring  $\mathbf{P}$ . To do this we need only prove an analogue of Lemma E.2.3 for  $\mathbf{P}_0$ . In the recursive definition of virtual roots, not only is the polynomial assumed to be strictly monotone over the interval, but its derivative has a known strict sign over the entire open interval. We state the desired property in the following form (we restrict ourselves to the Item 1 of Lemma E.2.3 without loss of generality).

**Lemma E.5.6.** *Let  $s = \pm 1$ . Consider a monic polynomial  $f \in \mathbf{P}_0[X]$  and  $\alpha \leq \beta$  elements of  $\mathbf{P}_0$ . The following property is assumed to be satisfied: if  $\alpha < \zeta < \beta$ , then  $sf'(\zeta) > 0$ . Then the polynomial  $f$  reaches its absolute minimum on  $[\alpha, \beta]$  in a single  $\xi \in \mathbf{P}_0$ . We have  $(\xi - \alpha)(\xi - \beta)f(\xi) = 0$ , and  $\xi$  is the only element of  $\mathbf{P}_0$  satisfying the following system of inequalities:*

- |  |  |
|--|--|
| <p>(1) <math>\alpha \leq \xi \leq \beta</math></p> <p>(2) <math>s(\xi - \alpha)f(\alpha) \leq 0</math></p> <p>(3) <math>s(\beta - \xi)f(\beta) \geq 0</math></p> | <p>(4) <math>s(\xi - \alpha)f(\xi) \leq 0</math></p> <p>(5) <math>s(\beta - \xi)f(\xi) \geq 0</math></p> |
|--|--|

We note  $R(\alpha, \beta, f)$  this element  $\xi$ .

A monic polynomial  $f$  of degree  $n$  is given by its  $n$  coefficients in degrees  $< n$ , and the map

$$\mathbb{R}_{\text{alg}}^{n+2} \text{ to } \mathbb{R}_{\text{alg}}, (\alpha, \beta, f) \mapsto R(\alpha, \sup(\alpha, \beta), f)$$

is a continuous semialgebraic map defined on  $\mathbb{R}_{\text{alg}}$ . The aim here is to see that it extends to  $\mathbf{P}_0$ . We already know that such an extension is unique when it exists (Lemma E.2.10).

*Proof.* We need only deal with the case where  $\alpha, \beta$  and the coefficients of  $f$  are in  $\mathbb{R}_{\text{alg}}[[\varepsilon]]$ . It is also assumed without loss of generality that  $\alpha = 0$  and  $s = 1$ . The desired inequalities then become

- |  |  |
|--|--|
| <p>(1) <math>0 \leq \xi \leq \beta</math></p> <p>(2) <math>\xi f(0) \leq 0</math></p> <p>(3) <math>(\beta - \xi)f(\beta) \geq 0</math></p> | <p>(4) <math>\xi f(\xi) \leq 0</math></p> <p>(5) <math>(\beta - \xi)f(\xi) \geq 0</math></p> |
|--|--|

If  $0 < \xi < \beta$  the inequalities (4) and (5) force  $f(\xi) = 0$ . Furthermore, since  $f' > 0$  on the open interval, we also have  $f(0) < f(\xi) < f(\beta)$ .

The difficult case to deal with is where  $f(0) < 0 < f(\beta)$ . □

□

---

<sup>2</sup>The details of this statement are left to the reader.

## E.6. Use of virtual roots in constructive real algebra

The results stated in this subsection for the real number field also seem valid in the dynamical theory *Corv*. Some may require only *Co0rv* or *Arc*.

### Basic semialgebraic subsets of the real line

Let us define a *basic semialgebraic closed subset* of the real line as a subset of the form  $F_f = \{x \in \mathbb{R} \mid f(x) \geq 0\}$  for an  $f \in \mathbb{R}[X]$ .

*First example.* Consider the polynomials  $f(X) = X^2 - b$  and  $g = -f$ .

- If  $b < 0$ , we have  $F_f = \mathbb{R}$  and  $F_g = \emptyset$ .
- If  $b > 0$ , we have  $F_f = ]-\infty, -\sqrt{b}] \cup [\sqrt{b}, +\infty[$  and  $F_g = [-\sqrt{b}, \sqrt{b}]$ .
- If  $b = 0$ , we have  $F_f = \mathbb{R}$  and  $F_g = \{0\}$ .

To obtain such a precise description of these semialgebraic closures it is absolutely necessary to know the sign of  $b = -f(0)$ .

If we denote  $\alpha$  and  $\beta$  the virtual roots of  $f$ , we have the following alternative description.

- If  $\alpha < \beta$ , i.e. if  $f(\frac{\alpha+\beta}{2}) > 0$  we have  $F_f = ]-\infty, \alpha] \cup [\beta, +\infty[$  and  $F_g = [\alpha, \beta]$ .
- If  $\alpha = \beta$  and  $f(\alpha) < 0$ , i.e. if  $f(\frac{\alpha+\beta}{2}) < 0$ , we have  $F_f = \mathbb{R}$  and  $F_g = \emptyset$ .
- If  $\alpha = \beta$  and  $f(\alpha) = 0$ , that is if  $f(\frac{\alpha+\beta}{2}) = 0$ , we have  $F_f = \mathbb{R}$  and  $F_g = \{\alpha\}$ .

*Second example.*

The case of a monic polynomial  $f$  of degree  $\delta > 2$ . Let us denote  $\text{Vr}_f$  the list of its virtual roots. Theorem E.2.6 allows us to describe the adherence of  $F_f \cup \text{Vr}_f$  exactly as the adherence of the union of the following intervals

- $(-\infty, \rho_{\delta,1}]$  if  $\delta \equiv 0 \pmod{2}$
- $[\rho_{\delta,k}, \rho_{\delta,k+1}]$  for  $k \in \llbracket 0..\delta - 2 \rrbracket$ ,  $k \equiv \delta \pmod{2}$
- $[\rho_{\delta,\delta}, +\infty)$

In imprecise imagery: “we know  $F_f$  to the nearest  $\text{Vr}_f$ ”.

Generally speaking, the problem with a polynomial of known degree arises from the fact that Theorem E.2.6 asserts something precise about the sign of the polynomial on an interval  $[\rho_{\delta,j}, \rho_{\delta,j+1}]$  only when  $\rho_{\delta,j} < \rho_{\delta,j+1}$ . The result is as follows.

**Lemma E.6.1.** *Let  $f \in \mathbb{R}[X]$  be a polynomial of degree  $\delta$  known and  $g = f/c_\delta$  the corresponding monic polynomial ( $c_\delta$  is the leading coefficient,  $> 0$  or  $< 0$ ). Let us note  $\rho_{\delta,k} = \rho_{\delta,k}(g)$ .*

1. *The adherence of  $F_f \cup \text{Vr}_f$  is equal to the adherence of an explicit finite union of closed intervals whose bounds are  $\rho_{\delta,k}$  or  $+\infty$ , or  $-\infty$ .*
2. *When we know the signs of  $(\rho_{\delta,k+1} - \rho_{\delta,k})$  and  $g(\rho_{\delta,k})$ , we have an exact description of the closed  $F_f$  in the form of a finite union of disjoint closed intervals. The information required is equivalent to giving the signs of  $g(\frac{\rho_{\delta,k} + \rho_{\delta,k+1}}{2})$ .*

When the degree of  $f$  is not known, we lose control of the situation in  $+\infty$  and  $-\infty$ . The fuzziest situation, in which we have no control at all, arises when we don't know whether the polynomial is identically zero or not.

Similar results hold for a basic open  $U_f = \{x \in \mathbb{R} \mid f(x) > 0\}$ .

## Sign and variation tables

Let  $\mathbf{R}$  be a constructive model of *Co0*. Two elements  $a$  and  $b$  are said to be “distinct” if  $a \neq b$ , i.e.  $a - b$  is invertible.

**Lemma E.6.2.** *Given a list  $L$  of  $k$  elements and a list  $L'$  of  $k + \ell$  distinct elements in  $\mathbf{R}$ , at least  $\ell$  elements of  $L'$  are distinct from all elements of  $L$ .*

Theorem E.2.6, Items 3d and 3e, almost gives a complete table of signs and variations for the monic polynomial  $f$ .

For the complete table of signs of  $f$ , any hesitations concern the signs of  $f$  in the virtual roots  $\xi_k$  of  $f'$ . The same applies to the table of variations of  $f$ , with the signs of  $f'$  at the virtual roots of  $f''$ .

This leads to the following result.

**Proposition E.6.3.** *Let  $\mathbf{R}$  be an ordered field with virtual roots.*

1. *Let  $f(x) \in \mathbf{R}[x]$  be a monic polynomial of degree  $k \geq 2$  and  $k + \ell - 1$  distinct elements  $a_i \in \mathbf{R}$ . For at least  $\ell$  of these elements, the polynomial  $f(x) + a_i$  has a known strict sign at each of the virtual roots of  $f'$ , and its complete sign table is known exactly. If  $k = 2$  then the complete table of signs and variations is known exactly.*
2. *Let  $f(x) \in \mathbf{R}[x]$  be a monic polynomial of degree  $k \geq 3$ ,  $k + \ell - 1$  distinct elements  $a_i \in \mathbf{R}$ , and  $k + \ell - 2$  distinct elements  $b_j \in \mathbf{R}$ . For at least  $\ell^2$  of the pairs  $(a_i, b_j)$ , we have a complete table of signs and variations known exactly for the polynomial  $f(x) + b_j x + a_i$ .*

Remarks E.6.4.

1) We probably have a perturbation result of the same style which says that for almost all perturbations of a finite number of monic polynomials  $f_i$ , we know with certainty the strict equalities and inequalities between all the virtual roots of  $f_i$  and all their derivatives, as well as the signs of  $f_i$  in each of these virtual roots, which gives a complete table of signs and variations for the family of  $f_i$  and their derivatives.

2) If we want a result analogous to Proposition E.6.3 for a continuous semialgebraic map, we will have to place ourselves in the theory *Corv* and restrict the table of signs and variations sought to a bounded closed interval. ■

## An approximate cylindrical algebraic decomposition (CAD)?

The problem arises of giving an approximate CAD for a finite family of polynomials of  $\mathbf{R}[X_1, \dots, X_n]$  where  $\mathbf{R}$  is a constructive model of *Co0rv* (or of *Corv*). This would be a result that cleverly generalises Lemma E.6.1 or Proposition E.6.3.

In piano-mover terms, instead of deciding whether “this passes” or “that doesn’t pass”, we’d get approximate results of the following kind: given the data of the problem and a desired precision  $\epsilon$ , we’d compute uniformly a  $\alpha \in \mathbf{R}$  such that:

- if  $\alpha > 0$ , there is a way of passing at a distance  $> \epsilon$  from the obstacles, and we’ll tell you how,
- si  $\alpha < 1$  il n’y a pas moyen de passer en respecter un distance  $> 2\epsilon$ .

Naturally, the piano must be a well-defined semialgebraic compact, as must the obstacles, and as must the space in which the piano is moved.

In general, since it is impossible to control, even in an approximate way, the behaviour at infinity of a polynomial whose coefficients are all close to 0, we must necessarily limit ourselves to calculating an approximate CAD for a finite family of polynomials on a well-defined compact of the style  $[0, 1]^n$ . If we try to reproduce a usual CAD (for a discrete real closed field) on  $\mathbb{R}$ , we can see that the coefficients of a sub-resultant polynomial may well all be very close to 0. But *a priori* virtual roots are only effective for monic polynomials.

On this kind of subject, we’re still in our infancy.

## Stratifications

It seems that stratifications, when assumed, are a restful framework in which many results valid for discrete real closed fields can be extended without too much difficulty to the *non* discrete case.

## The Fundamental Theorem of Algebra (FTA)

For a treatment of **FTA** without the axiom of dependent choice, see [58].

Since the virtual roots are continuous maps, and since it is impossible to follow by continuity the zeros of a complex polynomial (monic of fixed degree  $m$  and with variable coefficients), we certainly cannot obtain one of these zeros expressed as an element of  $\text{Fspace}_m(\mathbb{R})$ . Nevertheless, we can cover the zeros of a complex polynomial of degree  $\delta$  by a finite number of expressions in  $\text{Fspace}_{\delta^2}(\mathbb{R})$ .

What we'd like to do here is to do it in a fairly optimal way.

### • 1. The square roots of a complex number $c = a + ib$ .

The zeros of the polynomial  $f(Z) = Z^2 - c$  are given in the form  $x + iy$  by the real solutions of the system “ $x^2 - y^2 = a$ ,  $2xy = b$ ” and are calculated as follows:

- $(x^2 + y^2)^2 = a^2 + b^2$ , so  $x = \pm u$  with  $u = \sqrt{\frac{1}{2}(a + \sqrt{a^2 + b^2})} \in \text{Fspace}_4(\mathbb{R})$
- $y = \pm v$  with  $v = \sqrt{\frac{1}{2}(-a + \sqrt{a^2 + b^2})}$ , with the constraint  $xyb \geq 0$ .

If we denote  $z_1 = u + iv$ ,  $z_2 = -z_1$ ,  $f_1(Z) = (Z - z_1)(Z - \bar{z}_1)$ ,  $f_2(Z) = (Z - z_2)(Z - \bar{z}_2)$  and  $g(Z) = (Z - c)(Z - \bar{c})$  we obtain the equality

$$g(Z^2) = f(Z)\bar{f}(Z) = f_1(Z)f_2(Z) \quad (\text{E.2})$$

The polynomials  $f_1$ ,  $f_2$ ,  $g$  and  $f\bar{f}$  are real, everywhere  $\geq 0$ , each with a simple algebraic certificate for its character  $\geq 0$  when the variable is real. When  $c \neq 0$ , the zeros of  $f$  are divided between the zeros of  $f_1$  and those of  $f_2$ .

We can estimate that we have thus obtained the optimal solution for the square roots of a complex number in the context of the  $\mathbb{R}$ -algebra of maps generated by the maps “virtual square roots”  $\rho_{2,2}$ , and more generally the optimal solution in the context of the algebras  $\text{Fspace}_m(\mathbb{R})$ .

Note that  $x$  and  $y$  being roots of real polynomials of degree 4, there were 16 possible choices for  $x + iy$ .

### • 2. The general case.

We have the following non-optimal result.

**Proposition E.6.5 (FTA via the virtual roots).**

*Let  $f$  be a complex monic polynomial of degree  $\delta$ . There exist  $\delta^4$  polynomials  $q_\ell$  positive quadratic<sup>3</sup> having their coefficients constructed over  $\rho_{\delta^2,k}(\dots)$  (polyroots in the real and imaginary parts of the coefficients of  $f$ ) such that  $f\bar{f}$  divides the product of  $q_\ell$ .*

*If the real closed field under consideration is discrete, the polynomial  $f(z)$  decomposes into a product of  $(z - \zeta_j)$  factors explicit on  $\mathbf{C}$ , with the  $\zeta_j$  whose real and imaginary parts are roots of monic real polynomials of degree  $\delta^2$ , whose coefficients are  $\mathbb{Q}$ -polynomials in the real and imaginary parts of the coefficients of  $f$ .*

*Proof.* The real part of a zero  $\zeta_j$  of  $f$  is written  $(\zeta_j + \bar{\zeta}_j)/2$ . The  $(\zeta_j + \bar{\zeta}_k)/2$  are  $\delta^2$  and are the zeros of a real polynomial  $h_1$  of degree  $\delta^2$  whose coefficients are expressed as  $\mathbb{Q}$ -polynomials in the real and imaginary parts of the coefficients of  $f$ . Among the real zeros of  $h_1$  are the  $\frac{1}{2}(\zeta_j + \bar{\zeta}_j)$ . These are therefore virtual roots of  $h_1$ . Similar reasoning applies to the imaginary part, with a real polynomial  $h_2$  of degree  $\delta^2$ . If  $\alpha$  is a virtual root of  $h_1$  and  $\beta$  a virtual root of  $h_2$ , we associate the polynomial

$$q = (z - \alpha + i\beta)(z - \alpha + i\beta) = (z - \alpha)^2 + \beta^2$$

which is one of the  $q_\ell$  in the statement. □

<sup>3</sup>Precisely: monic polynomials of degree 2 everywhere  $\geq 0$ .

*Remark E.6.6.* In the paper [54] the authors prove that a discrete ordered field  $\delta^2$ -closed (i.e. satisfying the intermediate value theorem for polynomials of degree  $\leq \delta^2$ ) satisfies the fundamental theorem of algebra for polynomials of degree  $\leq \delta$ . We can deduce this result from Proposition E.6.5 using the formal Positivstellensatz as follows. Assume that the real closed field is discrete. Then the fact that  $f\bar{f}$  divides the product of  $q_\ell$  implies that  $f$  admits at least one complex zero, among the zeros of  $q_\ell$ .<sup>4</sup> Moreover, the virtual roots of  $h_1$  and  $h_2$  are characterised by systems of large inequalities. A Horn rule on the language of ordered fields states that, for a discrete real closed field, if we put these systems of large inequalities into hypotheses, we obtain as a valid consequence the fact that the product of  $f(\alpha \pm i\beta)$  suitable is zero. According to Item 2 of the formal Positivstellensatz C.2.1, this Horn rule is valid for any ordered field (discrete or not) as well as for real closed rings, since it is valid in the theory *Asonz*. And if the field satisfies the **TVI** for polynomials of degree  $\leq \delta^2$ , the hypotheses are satisfied by the virtual roots of  $h_1$  and  $h_2$ . In the same way, if the language of ordered fields has been enriched by introducing virtual root maps for polynomials of degree  $\leq \delta^2$ , with the corresponding axioms, we will also obtain for the corresponding dynamic algebraic structures the fact that the product of  $f(\alpha \pm i\beta)$  suitable is zero. ■

• **3. The general case in terms of multisets.** Reference: the **FTA** in [58, Richman].

*A priori*, the “**FTA** version multisets” seems difficult to formulate correctly without having the metric space of  $n$ -multisets of complex numbers.

To get around this, we can reduce the “**FTA** version multisets” to a set of dynamically valid rules giving an essentially equivalent formulation that uses counting the number of zeros inside rectangles in the style of [24, Eisermann]. The article [54] seems to us to give all the necessary details.

Since we do not assume that the ordered field is discrete, we must use only rectangles on whose edges we are certain that there are no complex zeros of the polynomial under consideration.

An explicit test shows that we must avoid at most  $\delta$  horizontal lines and at most  $\delta$  vertical lines for our rectangles. This is formulated by saying that if we consider  $\delta + m$  distinct horizontal lines, we are certain that at least  $m$  of them are good (the same goes for the verticals).

For these rectangles, counting the zeros inside works and always gives a well-defined integer.

We have a valid rule which ensures that no complex zero lies outside an explicitly large enough rectangle. For this sufficiently large rectangle the count gives the expected number  $\delta$ . And a valid rule says that when a rectangle is cut in half, the sum of the two counts equals the previous count.

If we also want to deal with the non-archimedean case, we need to establish Horn rules saying that we can enclose the  $\delta$  zeros in a union of rectangles of arbitrarily small size.

Further study of the paper [54] should lead to the desired results, which are more precise than the **FTA** considered in Item 2, results which can be considered to be the satisfactory constructive form of **FTA**, and which will be valid for *Corv* theory, formulable as valid Horn rules in that theory. But these Horn rules would not be valid in the theory of real closed rings.

## E.7. Some questions

### Continuous semialgebraic maps

**Question E.7.1.** Make more explicit the (constructive) result of continuity of virtual root maps: Item 2 of Theorem E.2.6. Each map  $\rho_{d,j} : \mathbf{R}^d \rightarrow \mathbf{R}$  is uniformly continuous on any ball  $B_{d,M} := \{(a_{d-1}, \dots, a_0) \mid \sum_i a_i^2 \leq M\}$ , ( $M > 0$ ). Continuity should be given in fully explicit form à la Łojasiewicz.

**Question E.7.2.** Give a constructive proof of Theorem E.3.16.

**Question E.7.3.** Let  $\mathbf{R}$  be a real closed ring. Is any element of  $\text{Fsac}_n(\mathbf{R})$  an integer on the ring of polynomials  $\mathbf{R}[x_1, \dots, x_n]$  an element of  $\text{Fspace}_n(\mathbf{R})$  ?

<sup>4</sup>We have a little better. The product of  $q_\ell$  decomposes into a product of linear, and therefore irreducible, factors in  $\mathbf{C}[Z]$ . Since  $f(Z)$  divides this product, and since  $\mathbf{C}[Z]$  is a gcd domain, it is in fact a by-product.

**Question E.7.4.** Is every continuous map  $\mathbb{R}^m \rightarrow \mathbb{R}$  which is integral on the ring of polynomials an element of  $\text{Fsace}_m(\mathbb{R})$ ? The answer in classical mathematics is yes, because we can apply Theorem E.2.8 to  $\mathbb{R}$ .

Questions E.7.5 have to do with the o-minimal character of the *non* discrete real closed field structure. The word “compact” below is used to mean “closed bounded subset”.

**Questions E.7.5.** (remember Proposition E.3.5)

Consider an ordered field with virtual roots  $\mathbf{R}$ .

1. Show that a continuous semialgebraic map which is everywhere  $> 0$  on the compact  $[0, 1]^n \subseteq \mathbf{R}^n$  is minorized (on this compact) by an element  $> 0$ . And that the lower bound is an element of  $\mathbf{R}$ .
2. Extend the result to an arbitrary “well-defined” semialgebraic compact: by this we mean a bounded semialgebraic closure  $K$  for which the function “distance to  $K$ ” is a continuous semialgebraic map (an element of  $\text{Fsac}_n(\mathbf{R})$ ).

## Real closure

**Question E.7.6.** If  $\mathbf{K}$  is a model of  $\mathcal{C}o$  (or of  $\mathcal{C}o0$ ), is its 2-closure  $\mathbf{L}$  as an  $f$ -ring still a model of  $\mathcal{C}o$  (or of  $\mathcal{C}o0$ )?

We repeat the previous question (adding some details) for the real closure.

**Question E.7.7.** Let  $\mathbf{K}$  be a model of the theory  $\mathcal{C}o$  and  $\mathbf{R}$  be the dynamic algebraic structure  $\text{Corv}(\mathbf{K})$  (as page ??). Is  $\mathbf{R}$  a constructive model of  $\text{Corv}$ ?

In particular, is the following metatheorem satisfied? Given two closed terms  $\alpha$  and  $\beta$  of  $\mathbf{R}$  such that the rule  $\vdash \alpha + \beta > 0$  is valid, is it true that one of the two rules  $\vdash \alpha > 0$ ,  $\vdash \beta > 0$  is valid?

We can ask the same question in the following form: if  $\mathbf{K}$  is a model of  $\mathcal{C}o$ , does the (usual) algebraic structure  $\text{ARC}(\mathbf{K})$  satisfy the rule **AFRL**?

**Question E.7.8.** Can the article [24, Eisermann] be reread for a *non* discrete real closed field, i.e. in the theory  $\text{Crc2}$ ? This question requires a detailed development of the ideas in Item 3, page 107 in the paragraph concerning **FTA**.

**Question E.7.9.** Show that the intermediate value theorem, stated in the form of the rule **RCF<sub>n</sub>** page 45, is not valid in the theory  $\text{Crc2}$ . Note that a slightly weakened form is valid: see Item 4 of the formal Positivtellsatz E.3.7 and Item 3i of Theorem E.2.6.

**Question E.7.10.** Show that the theorem which states that every complex number has a square root is not a valid rule in the theory  $\text{Crc2}$ . Compare with Proposition E.6.5 which might seem to assert the opposite.

## Pierce-Birkhoff

**Questions E.7.11.**

- 1) Does the definition of a Pierce-Birkhoff ring given in E.2.16 coincide in classical mathematics with the notion defined in [49, Madden, 1989]?
- 2) If this is indeed the case, the question arises of giving constructive proofs for sophisticated results, such as the fact that a regular Noetherian coherent ring of dimension  $\leq 2$  is a Pierce-Birkhoff ring [48].
- 3) Recall that the usual Pierce-Birkhoff conjecture is proved in [51] for  $\mathbf{R}[x, y]$  when  $\mathbf{R}$  is a discrete real closed field but it is not so clear that there is a constructive proof for  $\mathbb{R}[x, y]$ .

### The 17th Hilbert problem

**Question E.7.12.** To what extent does the constructive solution of the 17th Hilbert problem for  $\mathbb{R}$  (see [26, section 6.1]) apply to any strict  $f$ -ring with virtual roots? If not, what stronger theory would do: *Crc2*, *Arc*, *Crc*, *Icrc* (page ??)?

### The Grail?

The question arises of a theorem analogous to Theorem C.2.5, but now for the non-discrete case.

The formal Positivstellensatz E.3.7 implies that the theory *Arc* is the Horn theory generated by  $\mathbf{R}_{\text{alg}}$ , by  $\mathbb{R}$  or by  $\mathbb{R}_{\text{PR}}$  on the signature of *Arc*.

**Question E.7.13.** Is the theory *Arc* skolemised from the cartesian theory generated by  $\mathbf{R}_{\text{alg}}$ , by  $\mathbb{R}$  or by  $\mathbb{R}_{\text{PR}}$  on the signature of commutative rings?

**Question E.7.14.** In what sense could we say that the theory *Corv* is the dynamical theory generated by  $\mathbb{R}$  “without axiom of dependent choice” on the signature of *Arc*? Same question with  $\mathbb{R}_{\text{PR}}$ .

NB: this question seems impossible to formulate in classical mathematics, and in constructive mathematics, we would need to have a clear idea of  $\mathbb{R}$  “without an axiom of dependent choice”.





# F. The axiom of archimedeanity

## Sommaire

---

<b>F.1</b>	<b>Archimedean <i>non</i> discrete real closed fields</b>	111
<b>F.2</b>	<b>Some questions</b>	111
	Axiom of archimedeanity	111
	The principle of omniscience <b>LPO</b> is safe in real algebra?	112
	Convergent series in real algebra?	112
	Schmüdgen's Positivstellensatz	112

---

In this chapter, in order to better describe the algebraic properties of  $\mathbb{R}$ , we make an attempt which consists in not leaving the dynamical theories while preserving the essence of the non-dynamical rule **HOF**.

However, the language remains essentially that of ordered rings.

In the third part, we will make a much more ambitious attempt using a much richer language, which will essentially show us a geometric theory of the reals as a precursor of the theory of o-minimal structures.

## F.1. Archimedean *non* discrete real closed fields

The following rule, which means that the field is archimedean, is satisfied on  $\mathbb{R}$

$$\mathbf{AR1} \vdash \text{OP}_{n \in \mathbb{N}} |x| \leq n \quad (\text{Archimedes 1})$$

**Definition F.1.1.** We define the theory *Crca* of real closed archimedean fields as the geometric theory obtained by adding the axiom **AR1** to the theory *Crc2*.

The example given in Item 3 of Remark E.4.4 (a local real closed ring with zerodivisors, model of the theory *Crc2*) remains a model of *Crca*. Examples C.3.4 are also models of the theory *Crca*: in general the subrings of  $\mathbb{R}$  stable for virtual root maps, the fraction Fr and the inverses of invertible elements, are models of *Crca*.

## F.2. Some questions

### Axiom of archimedeanity

#### Questions F.2.1.

We know that we cannot express the fact that  $\mathbb{R}$  is archimedean in a finitary way. We express it with the infinite rule **AR1**.

- One question that arises is whether the theory *Crca* obtained by adding the rule **AR1** is a conservative extension of *Crc2*, this seems likely.

- We could start by showing that *Crca* proves the same Horn rules as *Crc2*.
- On the other hand, for the corresponding formal theory in which we allow the introduction of predicates for  $P \Rightarrow Q$  and  $\forall xP$  (with Gentzen's natural deduction rules) it could be that a statement like **HOF** becomes provable.

• **The principle of omniscience LPO is safe in real algebra?**

**Question F.2.2.**

The following rule is not satisfied on  $\mathbb{R}$ , because it implies the **ED<sub>#</sub>** rule.

$$\mathbf{AR2} \vdash x = 0 \quad \mathbf{op} \quad \mathbf{OP}_{n \in \mathbb{N}} |x| > 1/2^n \quad (\mathbf{Archimedes 2})$$

But no doubt it is “admissible”, in the sense that adding it to *Crca* would provide a conservative extension of *Crcd*.

This result would be a kind of realisation of Hilbert's programme for **LPO**, restricted to the theory *Crca*. Indeed, the theory *Crcd* is itself harmless compared to *Crc2* because it proves the same Horn rules.

• **Convergent series in real algebra?**

**Question F.2.3.** Let  $[x]^n = \frac{1}{2^n} \wedge (x \vee -\frac{1}{2^n})$ . The following rule is not a dynamical rule

$$\mathbf{Cauchy} \vdash \exists x \bigwedge_{n \in \mathbb{N}} |x - \text{som}_{p=0}^n [x_p]^p| \leq 1/2^n \quad (\mathbf{Cauchy})$$

A function symbol  $\sum_{n=0}^{\infty} [x_n]^n$  should be introduced for these infinite sums. This would replace the illegitimate rule **Cauchy** by an infinite number of legitimate Horn rules. But is such a function symbol legitimate?

## Schmüdgen's Positivstellensatz

References: [60, 66, 67]

**Question F.2.4.** Is geometric theory sufficient to develop theorems of the Schmüdgen type?

# Conclusion

The most important questions that remain to be resolved for this 2nd part seem to us to be the following.

1. Question [C.7.1](#). Give a constructive proof of Theorem [C.5.4](#).
2. Let  $\mathbf{R}$  be a discrete real closed field and  $f: \mathbf{R}^n \rightarrow \mathbf{R}$  be a continuous semialgebraic map. There exists an integer  $r \geq 0$ , a continuous semialgebraic map  $g: \mathbf{R}^{r+n} \rightarrow \mathbf{R}$  defined on  $\mathbb{R}_{\text{alg}}$ , and an element  $\underline{y} \in \mathbf{R}^r$  such that

$$\forall x_1, \dots, x_n \in \mathbf{R} \quad f(x_1, \dots, x_n) = g(y_1, \dots, y_r, x_1, \dots, x_n).$$

3. Question [E.7.1](#). Make explicit Item 2 of Theorem [E.2.6](#) asserting the uniform continuity of maps  $\rho_{d,j}: \mathbf{R}^d \rightarrow \mathbf{R}$  on any closed ball.
4. Question [E.7.2](#). Give a constructive proof of Theorem [E.3.16](#) *Any continuous semialgebraic map  $\mathbb{R}_{\text{alg}}^n \rightarrow \mathbb{R}_{\text{alg}}$  can be defined by a term of the theory  $\mathcal{Arc}$ .* This will make it possible to clarify definitively the constructive Definition [E.3.1](#) of real closed rings and its relationship in classical mathematics with various constructive characterisations of real closed rings.
5. Question [E.7.7](#) concerning the possibility of constructing a real closure of a non-discrete ordered field. Let  $\mathbf{K}$  be a model of the theory [Co](#) and  $\mathbf{R}$  the dynamical algebraic structure [Corv](#)( $\mathbf{K}$ ) (as page ??). Is  $\mathbf{R}$  a constructive model of [Corv](#)?



## Part III

An improved version of the theory  
of *non* discrete real closed fields  
and an attempt at a constructive  
version of o-minimal structures



# Introduction

In this third part we explore the possibility of better describing the algebraic properties of  $\mathbb{R}$  by extending the language through the introduction of sorts for continuous semialgebraic maps on compact cubes.

Indeed, we note that the general situation became clearer when we introduced the maps  $\vee$ ,  $\wedge$  and the virtual root maps. These natural extensions to the language used have gone a long way towards overcoming the obstacles that the notion of *non* discrete order seems to offer to a formalisation in finitary dynamical theory.

However, from a constructive point of view, it is not natural to be interested in the real zeros of polynomials whose degree is fixed. The good reason for this with  $\mathbb{R}$  is that we don't control the zeros in the neighbourhood of infinity when the degree is not clearly fixed. By replacing  $\mathbb{R}$  by the real interval  $\mathbb{I}_{\mathbb{R}} = [-1, 1] \subseteq \mathbb{R}$  this so-called good reason disappears by itself.

The idea is that you control things constructively only within the compact framework. We need to detox from  $\pm\infty$  and go back to Greek mathematics! Consequently, we must drop  $\mathbb{R}$  in favour of the interval  $\mathbb{I}_{\mathbb{R}}$ , for example by replacing  $+$  by the half-sum. This requires us to go back to the axiomatics, but the benefit will be that it will be easier to formulate certain properties linked to the fact that from the constructive point of view  $\mathbb{R}$  is *not* discrete.

Note that up to now, we have been rather dry concerning some of the desirable properties stated in C.5.6: indeed we have not been able to correctly state the principles of extension by continuity or the gluing principles with sufficient generality. We could only talk about uniform continuity from outside the dynamical theory. Indeed, uniform continuity requires an alternation of quantifiers of the type  $\forall n \exists m \forall x, y$  which requires a priori to leave the framework of geometric theories. This is also due to the fact that we had no sort of continuous semialgebraic maps.

In this section we try to make up for this lack. And we must remember that from a constructive point of view, a continuous map on a compact does not exist without a uniform continuity modulus. The gamble we take here is to internalise the question of uniform continuity. This means that, for the moment, we remain within a finitary dynamical theory framework.

Moreover, the extended framework that we propose with the introduction of these new sorts seems to be a correct framework for approaching a constructive treatment of o-minimal structures.

Here is a brief description of the contents of the third part.

Chapter G recalls the fascinating properties of o-minimal structures in classical mathematics. These are finiteness properties exactly similar to those of the algebraic geometry of discrete real closed fields, and yet devoid of algorithmic character by the use of the sign test on real numbers in classical theory. Constructing an algorithmic theory of o-minimal structures is a crucial challenge in the “constructive Hilbert programme”, which aims to uncover hidden constructions in contemporary classical mathematics and to reformulate purely ideal theorems into constructive statements. This programme avoids the use of the formal theory  $ZFC$ , which describes an hypothetical set universe that does not correspond to any proven mathematical construction.

Chapter H proposes a first finitary dynamical theory for sorts describing uniformly continuous real maps with values in  $\mathbb{I}_{\mathbb{R}}$ .

Chapter J gives a general framework to describe the properties of uniformly continuous maps defined on  $\mathbb{I}_{\mathbb{R}}^m$  with values in  $\mathbb{I}_{\mathbb{R}}^n$ . A decisive aspect is to take into account the fact that a uniform



continuity modulus of a map  $f$  can be seen as another uniformly continuous map  $g$  attached to the map  $f$ .

Chapter [K](#) proposes new axioms which are a priori satisfied for the algebraic geometry of real closed fields and which seem decisive for approaching an hypothetical and highly desirable constructive theory of o-minimal structures. We are nevertheless very far from having formalised in a dynamical theory what would be a constructive version of o-minimal structures.

# G. O-minimal structures

## Sommaire

---

Definition, definable parts . . . . .	119
Definable maps, outstanding results . . . . .	119
Variant . . . . .	120

---

## Definition, definable parts

References: [Coste], [van den Dries, 1998], [70, 21].

The definition of an o-minimal structure over a real closed field  $\mathbf{R}$  in classical mathematics is given by a collection  $(S_n)_{n \in \mathbb{N}}$ , where each  $S_n$  is a set of parts of  $\mathbf{R}^n$ , which verifies the following stability properties.

1. The semi-algebraic subsets of  $\mathbf{R}^n$  are in  $S_n$ .
2. Every  $S_n$  is a Boolean algebra of sets (stability by finite intersection and reunion, and complementary passage).
3. If  $A \in S_n$  and  $B \in S_m$  then  $A \times B \in S_{m+n}$ .
4. If  $A \in S_{n+1}$  and  $p_n : \mathbf{R}^{n+1} \rightarrow \mathbf{R}^n$  is the projection onto the first subspace  $\mathbf{R}^n$  of coordinates (forgetting the last coordinate), then  $p_n(A) \in S_n$ .
5. The elements of  $S_1$  are precisely the finite unions of open intervals and points.

The elements of  $S_n$  are called the *definable parts* of the o-minimal structure under consideration.

## Definable maps, outstanding results

A map  $A \rightarrow B$  between definable sets is said to be *definable* if its graph is definable.

Let's recall some key results.

- The domain of definition and the image set of a definable map are definable.
- The composite of two definable maps is definable.
- Any definable part is a Boolean combination of definable closed parts. More precisely, we have a definable cylindrical decomposition of  $\mathbf{R}^n$  adapted to any finite family of definable parts (analogously to the CAD in the case of semi-algebraic parts for a discrete real closed field). The cells of the decomposition are homeomorphic to open simplexes, with definable homeomorphisms.

- If  $A \in S_n$  is closed (for the Euclidean distance of  $\mathbf{R}^n$ ) and non-empty, then the function “distance to  $A$ ”

$$d_A : \mathbf{R}^n \rightarrow \mathbf{R}, x \mapsto \inf_{y \in A} \|x - y\|$$

is (continuous and) definable.

- If  $f: \mathbf{R}^n \rightarrow \mathbf{R}$  is continuous and definable, the zeros of  $f$  form a definable closed part. Conversely, according to the previous item, any definable closed part of  $\mathbf{R}^n$  is the zero set of a definable continuous map.
- If  $I = (a, b) \subseteq \mathbf{R}$  (with  $a, b \in \mathbf{R}_\infty := \mathbf{R} \cup \{-\infty, +\infty\}$ ) and if  $f: I \rightarrow \mathbf{R}$  is a definable map, then

– there is a subdivision of  $I$

$$a = a_0 < a_1 < \dots < a_k = b$$

such that on each open interval of the subdivision,  $f$  is either constant, or strictly monotone and continuous,

– we also have a subdivision such that on each open interval of the subdivision,  $f$  is derivable with definable derivative, continuous and of constant sign ( $= 0$  or  $> 0$  or  $< 0$ ).

- If  $A \in S_n$  is a definable closed subset and  $f: A \rightarrow \mathbf{R}$  is definable continuous, it can be extended into a definable continuous map on  $\mathbf{R}^n$ .
- Any definable continuous map  $(-1, 1) \rightarrow (-1, 1)$  extends by continuity into a definable continuous map  $[-1, 1] \rightarrow [-1, 1]$ .
- Any continuous map  $[-1, 1] \rightarrow [-1, 1]$  is bounded.
- If  $f: [-1, 1]^{n+1} \rightarrow \mathbf{R}$  is continuous and definable, the map  $g: [-1, 1]^n \rightarrow \mathbf{R}$  defined by

$$g(x_1, \dots, x_n) := \sup_{y \in [-1, 1]} f(x_1, \dots, x_n, y)$$

is continuous and definable. Note that in particular if  $f$  is everywhere  $\leq 0$  and if  $A$  is the zero set  $f$ , then  $p_n(A)$  is the zero set  $g$ . If  $A$  is a definable closed set  $\subseteq [-1, 1]^{n+1}$ , we can take for  $f$  the map  $-d_A: [-1, 1]^{n+1} \rightarrow \mathbf{R}$ .

## Variant

All this implies that we could just as easily define the considered o-minimal structure on  $\mathbf{R}$  by giving the following objects.

1. Definable continuous maps  $[-1, 1]^n \rightarrow [-1, 1]$ .
2. The bicontinuous increasing bijection (definable in any o-minimal structure)

$$(-1, 1) \rightarrow \mathbf{R}, x \mapsto x/(1 - x^2)$$

and the reciprocal bijection

$$\mathbf{R} \rightarrow (-1, 1), x \mapsto (\sqrt{4x^2 + 1} - 1)/2x$$

In fact, using the coding given in Item 2, to get the definable continuous maps  $\mathbf{R}^n \rightarrow \mathbf{R}$  we just need to know how to describe the definable continuous maps  $f: (-1, 1)^n \rightarrow (-1, 1)$ . To do this, all we need to know is how to describe the continuous definable maps  $g: [-1, 1]^n \rightarrow [-1, 1]$ .

Let us note  $\|x\| = \sup_{i \in [1..n]} |x_i|$  for  $x = (x_1, \dots, x_n) \in \mathbf{R}^n$ .

In the case where the growth to infinity of any definable map  $f$  from  $\mathbf{R}^n$  to  $\mathbf{R}$  is bounded by a polynomial, for such a map  $f$ , we have a continuous definable map  $g: [-1, 1]^n \rightarrow [-1, 1]$  written in the form  $g(x) = (1 - \|x\|^2)^k f(x)$ , and the map  $f$  can be encoded by the pair  $(g, k)$ . The map  $g$  tends uniformly towards 0 when  $x$  tends towards the edge of  $[-1, 1]^n$ .

In the general case, we can replace  $h(x) := 1 - \|x\|^2$  in  $g(x)$  by a map  $\varphi \circ h$  where  $\varphi: [0, 1] \rightarrow [0, 1]$  is continuous definable and strictly positive on  $[0, 1]$ .

# H. Rings of bounded real maps

## Sommaire

---

<b>H.1</b> Some reminders of the second part . . . . .	121
<b>H.2</b> Dynamical theory of rings of bounded real maps . . . . .	121
<b>H.3</b> Dynamical theory of compact real intervals . . . . .	122

---

## H.1. Some reminders of the second part

The Horn theory  $\mathcal{A}fr$  of strongly real rings is the theory of reduced  $f$ -rings to which we add the relation symbol  $\cdot > 0$  as an abbreviation of “ $x \geq 0 \wedge \exists z \, xz = 1$ ” and the function symbol  $\text{Fr}$  with the axioms **fr1** and **fr2** (Definition D.5.2).

A strongly real ring is therefore a reduced  $\mathbb{Q}$ - $f$ -algebra in which any element greater than an invertible positive element is itself invertible, and in which the rule **FRAC** is valid.

Finally, the dynamical theory  $\mathcal{C}o$  of *non* discrete ordered fields can be described as the theory of local strongly real rings, which amounts to adding the axiom **OTF** (Lemma D.5.4, Item 3) to the theory  $\mathcal{A}tfr$ .

**Lemma H.1.1.** *Let  $\mathbf{A}$  be a strongly real ring. Let  $\mathbf{I} = \{x \in \mathbf{A} \mid -1 \leq x \leq 1\}$ . We define on  $\mathbf{I}$  the law  $x \uplus y = \frac{1}{2}(x + y)$ . The structure obtained on  $\mathbf{I}$  for the signature*

$$\text{Signature : } \boxed{\Sigma_{Icr} = (\cdot = \cdot, \cdot \geq \cdot, \cdot > \cdot; \cdot \uplus \cdot, \cdot \times \cdot, \cdot \vee \cdot, \text{Fr}(\cdot, \cdot), -\cdot, 0)}$$

*allows us to reconstruct, in a unique way, the structure of  $\mathbf{A}$  as a strongly real ring.*

*Proof.* This is essentially because any element  $z \in \mathbf{A}$  can be written in the form  $x/y$  with  $-1 < x < 1$  and  $0 < y < 1$  (for example  $x = \frac{z}{2+|z|}$  and  $y = \frac{1}{2+|z|}$ ).  $\square$

## H.2. Dynamical theory of rings of bounded real maps

We are going to use a more complete signature which corresponds better to the intuition of an interval as a convex subset.

We denote  $x \oplus y$  the following composition law in an  $f$ -ring:  $(x, y) \mapsto -1 \vee (1 \wedge (x + y))$ .<sup>1</sup>

We denote  $\text{Cb}$  the set of *systems of barycentric coefficients*, defined precisely as follows:

$$\text{Cb} = \left\{ (r_k)_{k \in [1..n]} \mid n \geq 2, r_1, \dots, r_n \in \mathbb{Q}, r_1, \dots, r_n \geq 0, \sum_{k=1}^n r_k = 1 \right\}.$$

We note  $\mathbb{I}_{\mathbb{Q}} = \{r \in \mathbb{Q} \mid -1 \leq r \leq 1\}$ .

---

<sup>1</sup>This is the addition, put back into the interval  $\mathbf{I}$  if it comes out of it.

For each  $\rho = (r_k)_{k \in \llbracket 1..n \rrbracket}$  in  $\text{Cb}$ ,  $\text{Brc}_\rho$  is a function symbol of arity  $n$  corresponding to the map:  $\mathbf{I}^n \rightarrow \mathbf{I}$ ,  $(x_k)_{k \in \llbracket 1..n \rrbracket} \mapsto \sum_{k=1}^n r_k x_k$ . The language of the dynamical theory of *rings of bounded real maps*  $\mathcal{Afrb}$  is defined by the following signature. There is only one sort, denoted  $\mathcal{Afrb}$

**Signature :**  $\Sigma_{\mathcal{Afrb}} = (\cdot = 0, \cdot > 0, \cdot \geq 0 ; (\text{Brc}_\rho)_{\rho \in \text{Cb}}, \cdot \oplus \cdot, \cdot \times \cdot, -\cdot, \cdot \vee \cdot, \text{Fr}(\cdot, \cdot), (r)_{r \in \mathbb{I}\mathbb{Q}})$

### Abbreviations

Function symbols

- $x \wedge y$  means  $-(x \vee -y)$
- $|x|$  means  $x \vee -x$
- $x^+$  means  $x \vee 0$
- $x^-$  means  $-x \vee 0$

Predicates

- $x = y$  means  $x - y = 0$
- $x \geq y$  means  $x - y \geq 0$
- $x > y$  means  $x - y > 0$
- $x \perp y$  means  $|x| \wedge |y| = 0$
- $x \leq y$  means  $y \geq x$
- $x < y$  means  $y > x$

### Axioms

The axioms are all the dynamical rules stated in the language of  $\mathcal{Afrb}$  which are valid for the interval  $\mathbf{I} = [-1, 1]$  in the theory  $\mathcal{Afr}(\mathbb{Q})$  of strongly real  $\mathbb{Q}$ -algebras.

**Lemma H.2.1.** *Valid Horn rules in  $\mathcal{Afrb}$  are decidable.*

*Proof.* Consequence of Item 3 of Corollary D.5.8. □

Note that it is not known whether valid dynamical rules are decidable. The same question arises in the local case for the dynamical theory  $\mathcal{Co}$ . This question does not seem very important insofar as we are essentially interested in the case of the theories  $\mathcal{Crc1}$  and  $\mathcal{Crc2}$ , where the problem remains mysterious and is added to that of knowing whether we have captured all the algebraic properties of the field  $\mathbb{R}$ .

## H.3. Dynamical theory of compact real intervals

The dynamical theory  $\mathcal{Icr}$  of *compact real intervals* has a single sort, denoted  $\mathcal{Icr}$ . Its language is defined by the following signature.

**Signature :**  $\Sigma_{\mathcal{Icr}} = (\cdot = 0, \cdot > 0, \cdot \geq 0 ; (\text{Brc}_\rho)_{\rho \in \text{Cb}}, \cdot \oplus \cdot, \cdot \times \cdot, -\cdot, \cdot \vee \cdot, (\text{T}_n)_{n \in \mathbb{N}}, \text{Fr}(\cdot, \cdot), (r)_{r \in \mathbb{I}\mathbb{Q}})$

The dynamical theory  $\mathcal{Icr}$  is obtained from the theory  $\mathcal{Afrb}$  described in Section H.2 by adding

- The function symbols  $\text{T}_n$  for Chebyshev polynomials, with the axioms  $\vdash \text{T}_0(x) = 1$ ,  $\vdash \text{T}_1(x) = x$ ,  $\vdash \text{T}_n(x) = 2x\text{T}_{n-1}(x) - \text{T}_{n-2}(x)$  ( $n \geq 2$ ). For the main properties of Chebyshev polynomials we refer to the book [Mason & Handscomb, Chebyshev Polynomials]
- The axiom **OTF** (valid for the *non* discrete ordered field structure) reformulated as follows:

$$\mathbf{OTF}' \quad x \oplus y > 0 \vdash_{x,y:\mathcal{Icr}} x > 0 \quad \mathbf{op} \quad y > 0$$

*Remark H.3.1.* Theories  $\mathcal{Icr}$  and  $\mathcal{Co}$  are probably essentially identical. Otherwise it would be necessary to add axioms to  $\mathcal{Icr}$  to make it true. ■

# J. A reinforced language and the first corresponding axioms

## Sommaire

---

<b>Introduction</b> . . . . .	<b>123</b>
<b>J.1 The sorts of reinforced language</b> . . . . .	<b>123</b>
<b>J.2 An abstraction principle</b> . . . . .	<b>124</b>
<b>J.3 First structures on sorts <math>Df_{m,n}</math></b> . . . . .	<b>124</b>
Sorts $Df_{m,n}$ . . . . .	124
Identification of $Df_{m,n}$ and $(Df_m)^n$ . . . . .	124
Composition of maps . . . . .	124
Evaluation of maps . . . . .	125
Constant maps . . . . .	125
Rearrangement of variables . . . . .	125
Gluing of elements of $Df_1$ on consecutive intervals . . . . .	125
Restrict an element of $Df_1$ to an interval . . . . .	125
Gluing . . . . .	126
Axioms of weak extensionality . . . . .	126

---

## Introduction

We now introduce the sorts of continuous semialgebraic maps in order to obtain a more expressive dynamical theory than *Crc2* for *non* discrete real closed fields.

This new dynamical theory, which we shall call *Crc3*, attempts here to summarise what we are entitled to expect from an o-minimal structure for uniformly continuous definable maps on  $\mathbb{I}_{\mathbb{R}}$ .

As we have already indicated, we restrict ourselves to uniformly continuous bounded maps, in much the same spirit as Bishop.

### J.1. The sorts of reinforced language

1. The sort *Icr*, for the compact interval  $\mathbf{I} = [-1, 1]$ .
2. For each  $m \geq 0, n \geq 1$ , a sort  $Df_{m,n}$  for uniformly continuous definable maps<sup>1</sup>  $\mathbf{I}^m \rightarrow \mathbf{I}^n$ , the sort  $Df_{m,1}$  is noted  $Df_m$ . In particular  $Icr = Df_0 = Df_{0,1}$ .
3. A sort  $Li_n$  seen as a subset of  $Df_n$ , for certain smooth maps given at the start (at least Chebyshev polynomials).
4. A sort *Mc* for uniform continuity moduli. They are seen as particular objects of sort  $Df_1$ .

---

<sup>1</sup>Continuous semialgebraic maps for the theory of real closed fields.

5. A sort  $Dfmc_n$  for pairs formed by an object of sort  $Df_n$  and by a uniform continuity modulus that fits it.

## J.2. An abstraction principle

For any term  $t(x_1, \dots, x_n)$  of type  $Icr^n \rightarrow Icr$  from the theory (where the  $x_i$  cover all the free variables present in the term), a term which provides a map  $\mathbf{I}^n \rightarrow \mathbf{I}$  in a model, we must do what is necessary so that there exists a term  $\dot{t}$  in  $Df_n$  which “evaluates as  $t$ ”. In other words, we need to put in place what we need to mimic, within our geometric theory, the  $\lambda$ -abstraction of the  $\lambda$ -calcul.

To do this, the signature

- symbols of type  $Df_n \times Icr^n \rightarrow Icr$  for the evaluation of a  $u : Df^n$  into  $x_i : Icr$ ;
- symbols for the composition of maps (with suitable axioms);
- symbols which give a name to the maps given in the signature (for example  $\cdot \times \cdot$  must have a name as an object so  $Df_2$ );
- ...

This approach is essential if we are to be able to talk uniformly, and not just occasionally, about the properties of continuous definable maps.<sup>2</sup>

*Remark J.2.1.* One might think that some function symbols introduced *a priori* to mimic  $\lambda$ -abstraction could have been added *a posteriori* by virtue of the possibility of adding a function symbol in the case of unique existence, thus providing a dynamical theory essentially identical to the previous one. But the existence (in the unique existence in question) of a well-defined map from the sort  $Icr \times Icr$  to the sort  $Icr$  does not mean the existence of a corresponding object in  $Df_2$ , or even its uniqueness (because the extensionality axioms introduced later are too weak). What we mean by introducing *a priori* these maps as objects of sort  $Df_{m,n}$ , is that all sufficiently simple maps, in particular those described in the signatures, are indeed continuous and definable. ■

## J.3. First structures on sorts $Df_{m,n}$

### Sorts $Df_{m,n}$

The sort  $Icr$  of compact real intervals ( $f$ -rings) has the structure described in Section H.3.

Each sort  $Df_m$  ( $m \geq 0, n \geq 1$ ) is accompanied by function symbols and predicates as well as axioms of rings of bounded real maps (dynamical theory *Afrb*).

*Remark.* The axiom **OTF'** page 122 is not valid for the sorts  $Df_m = Df_{m,1}$  for  $m \geq 1$ . ■

#### • Identification of $Df_{m,n}$ and $(Df_m)^n$

For each  $i \in \llbracket 1..n \rrbracket$  we have a function symbol  $\pi_{m,n,i}$  of type  $Df_{m,n} \rightarrow Df_m$  corresponding to the  $i$ -th coordinate. We also give a function symbol of type  $(Df_m)^n \rightarrow Df_{m,n}$  for the bijection; we will note it  $(\varphi_1, \dots, \varphi_n)$  in an admittedly somewhat ambiguous way. With the appropriate axioms, this allows us to identify  $Df_{m,n}$  and  $(Df_m)^n$ .

$$\vdash_{\varphi_1, \dots, \varphi_n : Df_m} \varphi_i = \pi_{m,n,i}((\varphi_1, \dots, \varphi_n)) \quad (i \in \llbracket 1..n \rrbracket)$$

$$\vdash_{\varphi : Df_{m,n}} \varphi = (\pi_{m,n,1}(\varphi), \dots, \pi_{m,n,n}(\varphi))$$

We give the axioms that  $\pi_{m,n,i}$  is a morphism for the ring structures of bounded real maps of  $Df_{m,n}$  and  $Df_m$ .

<sup>2</sup>This is reminiscent of what Kleene does when he defines (uniformly) primitive recursive maps.

- **Composition of maps**

We have function symbols  $C_{m,n,p}$  of type  $Df_{n,p} \times Df_{m,n} \rightarrow Df_{m,p}$  corresponding to the composition of maps. For  $\varphi: Df_{m,n}$  and  $\psi: Df_{n,p}$ , we write  $\psi \circ \varphi := C_{m,n,p}(\psi, \varphi)$ . We have constants of sort  $Df_{n,n}$  for the “identity maps”  $\text{Id}_n: \mathbf{I}^n \rightarrow \mathbf{I}^n$ .

The axioms for the associativity of composition are given.

We give the axioms which say that for  $\varphi$  fixed of sort  $Df_{m,n}$ , the map  $\psi \mapsto \psi \circ \varphi$  is a morphism for the ring structures of bounded real maps of  $Df_{n,p}$  and  $Df_{m,p}$ .

We abbreviate  $C_{n,m}$  to the term of type  $Df_n \times (Df_m)^n \rightarrow Df_m$ , defined by

$$C_{n,m}(\varphi, \eta_1, \dots, \eta_n) \stackrel{\text{d\u00e9f}}{=} \varphi \circ (\eta_1, \dots, \eta_n).$$

- **Evaluation of maps**

For  $Icr = Df_0$ , the function symbol  $C_{n,0}$  of type  $Df_n \times Icr^n \rightarrow Icr$  defines the evaluation of a map in variables taken from  $\mathbf{I}$ . The associativity of composition is then naturally related as follows with  $x_i$  of sort  $Icr$ ,  $\varphi$  of sort  $Df_n$  and  $\psi$  of sort  $Df_1$

$$(\psi \circ \varphi)(x_1, \dots, x_n) = (\psi \circ \varphi) \circ (x_1, \dots, x_n) = \psi \circ (\varphi \circ (x_1, \dots, x_n)) = \psi(\varphi(x_1, \dots, x_n)).$$

- **Constant maps**

We have a function symbol  $J_n = J_{0,n}$  of type  $Icr \rightarrow Df_n$  for constant maps.

Axioms are given which say that these are morphisms for ring structures of bounded real maps<sup>3</sup> and that the evaluation of a constant map in any arguments is indeed the desired constant.

More generally, if  $0 \leq m < n$  we have a function symbol  $J_{m,n}$  of type  $Df_m \rightarrow Df_n$  for objects of sort  $Df_n$  corresponding to maps which depend only on the  $m$  first variables and which can therefore be expressed from objects of sort  $Df_m$ . The axioms are analogous to those given for the case  $m = 0$ .

- **Rearrangement of variables**

For  $m, n > 0$  and a map  $\kappa: \llbracket 1..m \rrbracket \rightarrow \llbracket 1..n \rrbracket$  we have an object  $\tilde{\kappa}$  of sort  $Df_{n,m}$  with the axiom

$$\mathbf{c}_\kappa \vdash_{x_1, \dots, x_n: Icr} \tilde{\kappa}(x_1, \dots, x_n) = (x_{\kappa_1}, \dots, x_{\kappa_m})$$

We also give the associated natural axioms:  $\widetilde{\kappa \circ \tau} = \tilde{\kappa} \circ \tilde{\tau}$ .

So for  $m < n$  we have the equality  $J_{m,n}(\varphi) = \varphi \circ \tilde{\kappa}$ , where  $\kappa: \llbracket 1..m \rrbracket \rightarrow \llbracket 1..n \rrbracket$  verifies  $\kappa(i) = i$  for  $i \in \llbracket 1..m \rrbracket$ . This equality means that we do not need to introduce the symbol  $J_{m,n}$ .

We also have, for  $\tau_{n,i}: [1] \rightarrow \llbracket 1..n \rrbracket$  defined by  $\tau_{n,i}(1) = i$  and  $\psi$  so that  $Df_{m,n}$ , the equality  $\pi_{m,n,i}(\psi) = \widetilde{\tau_{n,i}} \circ \psi$ .

## Gluing of elements of $Df_1$ on consecutive intervals

- **Restrict an element of  $Df_1$  to an interval**

If  $f$  is of sort  $Df_1$ , we want to have a name for the map  $g$  obtained from the restriction of  $f$  to an interval  $[a, b] \subseteq \mathbf{I}$ .

This is done using a function symbol  $\text{Rs}: Df_1 \times Icr \times Icr \rightarrow Df_1$ .

When  $a \leq b$ , we extend  $g$  with  $g(x) = f(b)$  if  $x \geq b$  and  $g(x) = f(a)$  if  $x \leq a$ . When  $a \geq b$ , we permute  $a$  and  $b$ . We therefore have the following axioms

<sup>3</sup>For example for  $r \in \mathbb{I}_{\mathbb{Q}}$ , an axiom says that  $J_n(r)$  is equal, as an object of sort  $Df_n$ , to the  $r$  given in the ring structure of bounded real maps.



- $\vdash_{a,b:Icr,f:Df_1} \text{Rs}(f, a, b) = \text{Rs}(f, a \wedge b, a \vee b)$
- $x \leq a \wedge b \vdash_{a,b,x:Icr,f:Df_1} \text{Rs}(f, a, b)(x) = f(a \wedge b)$
- $x \geq a \vee b \vdash_{a,b,x:Icr,f:Df_1} \text{Rs}(f, a, b)(x) = f(a \vee b)$
- $a \wedge b \leq x \leq a \vee b \vdash_{a,b,x:Icr,f:Df_1} \text{Rs}(f, a, b)(x) = f(x)$

- **Gluing**

If  $f_0, \dots, f_n$  are of sort  $Df_1$ , and if  $0 \leq a_1 \leq \dots \leq a_n \leq 1$  we want to have a name for the map which glues the  $f_i$  restricted to  $[a_i, a_{i+1}]$ , possibly shifted vertically to ensure continuity.

This is done using a function symbol  $\text{Rc}_n : (Df_1)^{n+1} \times (Icr)^n \rightarrow Df_1$ .

We have the following basic axioms (let  $a_0 = 0$  and  $a_{n+1} = 1$ )

$$\mathbf{Rc}_{n,j} \bigwedge_i (a_i \leq a_{i+1}, f_i(a_{i+1}) = f_{i+1}(a_{i+1})) \vdash_{a_i:Icr,f_i:Df_1} \text{Rs}(\text{Rc}(\underline{f}, \underline{a}), a_j, a_{j+1}) = \text{Rs}(f_j, a_j, a_{j+1})$$

We add the appropriate axioms to force the assumptions of  $\mathbf{Rc}_{n,j}$ .

### Axioms of weak extensionality

For each sort  $Df_n$  with  $n \geq 1$  we have the following axiom of weak extensionality.

$$\mathbf{EXT}_n \quad a > 0 \vdash_{a:Icr,\varphi:Df_n} |\varphi| < J_n(a) \quad \mathbf{op} \quad \exists x |\varphi(x)| > \frac{a}{2}$$

As a consequence, a map which is everywhere null is “almost” null: it is increased in absolute value by any constant  $> 0$ . To conclude that it is null, we would have to invoke **HOF**, a non-geometric axiom which we do not want, or a dubious axiom of archimedeanity such as **AR2** in an infinitary geometric theory.<sup>4</sup>

Note that the axiom  $\mathbf{EXT}_0$  simply says that for  $x, a : Icr$  and  $a > 0$ , we have  $|x| < a$  or  $|x| > \frac{a}{2}$ , which is a variant of **OTF**.

Finally, note that the rule  $\mathbf{EXT}_n$  follows from **OTF** and the upper bound axioms in Section K.1 (with  $m = 0$ ).

---

<sup>4</sup>A very unsound solution to this weakness of dynamical theory would be to consider as models only those where objects of sort  $Df_n$  are  $\geq 0$  (resp.  $> 0$ ) exactly when they are evaluated  $\geq 0$  (resp.  $> 0$ ) at any point of  $\mathbf{I}$ .

# K. Decisive axioms

## Sommaire

---

<b>K.1 Upper bound axioms</b> . . . . .	<b>127</b>
Axioms of uniform continuity . . . . .	127
<b>K.2 Axioms for smooth maps</b> . . . . .	<b>129</b>
Density axiom . . . . .	129
The derivation . . . . .	129
What other axioms for derivation? . . . . .	130
Axioms of virtual roots . . . . .	130
<b>K.3 Axioms of real closure or o-minimal closure</b> . . . . .	<b>130</b>
Finiteness axioms . . . . .	130
Gluing of maps defined on an open covering . . . . .	130
Gluing of maps defined on a closed covering . . . . .	131
Axioms of extension by continuity . . . . .	131
Conclusion: the improved real closed field structure . . . . .	132
<b>K.4 O-minimal structures</b> . . . . .	<b>132</b>
<b>K.5 Some questions</b> . . . . .	<b>133</b>

---

## K.1. Upper bound axioms

The upper bound axioms replace *a priori* the projection axiom for definable parts in o-minimal structures.

For  $m > 0$  we have a function symbol  $\text{sup}_m$  of type  $Df_m \rightarrow Icr$  for the lub. It satisfies the axioms describing the lub, namely

$$\begin{aligned} \text{sup}_m^{Df} \quad & \vdash_{\varphi:Df_m} \varphi \leq J_m(\text{sup}_m(\varphi)) \\ \text{SUP}_m^{Df} \quad & \epsilon > 0 \vdash_{\epsilon:Icr;\varphi:Df_m} \exists \underline{y} \varphi(\underline{y}) + \epsilon > \text{sup}_m(\varphi) \end{aligned}$$

More generally for  $n \geq 0$  and  $m > 0$  we have a function symbol  $\text{sup}_{m+n,n}$  of type  $Df_{m+n} \rightarrow Df_n$  for the upper bound on the  $m$  last variables (in  $\mathbf{I}^m$ ) with the following axioms (so  $\text{sup}_{m,0}$  is none other than  $\text{sup}_m$ ).

$$\begin{aligned} \text{sup}_{m+n,n}^{Df} \quad & \vdash_{\varphi:Df_{n+m}} J_{n,m+n}(\text{sup}_{m+n,n}(\varphi)) \\ \text{SUP}_{m+n,n}^{Df} \quad & \epsilon > 0 \vdash_{\epsilon,x_1,\dots,x_n:Icr;\varphi:Df_{n+m}} \text{sup}_{m+n,n}(\varphi(\underline{x}, \underline{y})) + \epsilon > \text{sup}_{m+n,n}(\varphi)(\underline{x}) \end{aligned}$$

■

## Axioms of uniform continuity

We now explain how a suitable system of axioms can translate the fact that any definable continuous map admits a uniform continuity modulus, while remaining within the framework of a geometric theory. This is possible because definable continuous maps admit uniform continuity moduli that are themselves particular continuous definable maps. The sorts  $Mc$  and  $Dfmc_n$  with their axioms are crucial here.

We start by giving a function symbol  $j_{Mc}$  for an injection of type  $Mc \rightarrow Df_1$ . An axiom specifies that  $j_{Mc}$  is injective.

We have a predicate  $Mcu_n$  on  $Df_n \times Mc$  which expresses that  $\mu$  is a modulus for  $\varphi$  by means of the following abbreviation.

- $Mcu_n(\varphi, \mu)$  is an abbreviation for:  $\mu(|\varphi(\underline{x}) - \varphi(\underline{x}')|) \leq \|(\underline{x}) - (\underline{x}')\|$

where  $\|(\underline{z})\| = \sup_i |z_i|$ . Here the inequality seems to be written, in the form of evaluated maps, with  $x_i$  and  $x'_i$  of sort  $Icr$ . But in fact, this inequality should be read as linking two objects of sort  $Df_{2n}$ . This avoids the use of the universal quantifier on  $x_i$  and  $x'_j$  in the definition of uniform continuity! Dynamic theories do not allow the creation of new formulas using universal quantifiers, so we get round the difficulty by mimicking  $\lambda$ -abstraction!

The following axioms specify constraints on objects  $\mu$  of sort  $Mc$ .

$$\mathbf{Mc}_1 \quad 0 < b < c \vdash_{\mu:Mc;b,c:Icr} 0 < \mu(b) < \mu(c) \quad \mathbf{Mc}_2 \quad a \leq 0 \vdash_{\mu:Mc;a:Icr} \mu(a) = 0$$

$$\mathbf{mc}_1 \quad \vdash_{\mu:Mc} Mcu_1(j_{Mc}(\mu), \mu)$$

*Remark.* In the case where we consider only continuous semialgebraic maps, Łojasiewicz assures us that any uniform continuity modulus can be taken from the only maps  $\epsilon > 0 \mapsto c \epsilon^n$  (with some  $c > 0$ ) ■

The not very intuitive axiom  $\mathbf{mc}_1$  will be a valid rule if we require in another axiom that any object of sort  $Mc$  corresponds to a convex map. ■

The sort  $Dfmc_n$  is defined as a subsort of the product sort  $Df_n \times Mc$ . It is accompanied by two function symbols  $df_n$  and  $mc_n$ , with the appropriate axioms, which mean that an object of sort  $Dfmc_n$  can be considered as a pair of objects  $(\varphi, \mu)$  of respective sorts<sup>1</sup>  $Df_n$  and  $Mc$ . The axiom  $\mathbf{mcu}_n$  says how the subsort is defined: if  $(\varphi, \mu)$  is of sort  $Dfmc_n$ , then the predicate  $Mcu_n(\varphi, \mu)$  is satisfied.

$$\mathbf{mcu}_n \quad \vdash_{\psi:Dfmc_n} Mcu_n(df_n(\psi), mc_n(\psi))$$

Finally, we have the axiom  $\mathbf{DFMC}_n$  which says that any object  $\varphi$  of sort  $Df_n$  is the image by  $df_n$  of an object  $\theta$  of sort  $Dfmc_n$ .

$$\mathbf{DFMC}_n \quad \vdash_{\varphi:Df_n} \exists \theta; df_n(\theta) = \varphi$$

All this machinery explicitly guarantees the uniform continuity of maps represented by objects of sort  $Df_n$ .

*Remark K.1.1.* Each time we introduced a constant of sort  $Df_n$ , we actually had to introduce a constant “above it” of sort  $Dfmc_n$ . This is not difficult because in each case a uniform continuity modulus is obvious. ■

<sup>1</sup>It is not necessary to create the product type as such. The following axiom will suffice:  $df_n(\theta) = df_n(\theta'), mc_n(\theta) = mc_n(\theta') \vdash_{\theta,\theta':Dfmc_n} \theta = \theta'$ .

## K.2. Axioms for smooth maps

Objects of sort  $Li_n$  are seen as objects of sort  $Df_n$  which define certain smooth maps (i.e.  $C^\infty$ ). The signature includes a function symbol  $j_{Li_n}$  for the corresponding injection, with the axioms which say that it is an injective morphism for suitable laws (those which preserve the smooth maps).

Constant maps and coordinate maps are given as objects of sort  $Li_n$ .

The sort  $Li_1$  contains the Chebyshev polynomials.

It might be possible to introduce other Nash maps into  $Li_n$ ; this should not change the dynamical theory but could facilitate certain proofs.

In the case where we are aiming at a particular o-minimal structure (other than that provided by the continuous semialgebraic maps), other maps can be given which will serve as a basis for the definition of the structure.

### Density axiom

The zeros of a non-zero smooth map (in an o-minimal structure) form a closed  $F$  with an empty interior. We can express (at least partially) this density property (for the complementary of  $F$ ) by means of the following axiom

$$\mathbf{Dens}_n \quad |\varphi(a_1, \dots, a_n)| > 0, \varphi \times \psi = 0 \vdash_{a_1, \dots, a_n: Icr; \varphi: Li_n; \psi: Df_n} \psi = 0$$

### The derivation

We think it is convenient to introduce the derivative (or partial derivative) following the Bridger-Stolzenberg definition (see [1] and [9]). A map  $\varphi: \mathbb{I} \rightarrow \mathbb{R}$  is continuously derivable if the map “rate of increase” can be extended by continuity, i.e. if there exists a uniformly continuous map  $\psi: \mathbb{I}^2 \rightarrow \mathbb{R}$  satisfying the identity  $\varphi(x_1) - \varphi(x_2) = \psi(x_1, x_2) \times (x_1 - x_2)$ . The derivative of  $\varphi$  is then given by  $\varphi'(x) = \psi(x, x)$ .

As we only want maps  $\mathbf{I}^n \rightarrow \mathbf{I}$ , we must use an implicit coding  $(x, p)$  with  $x \in \mathbf{I}$  and  $p \in \mathbb{N}$  for the real  $px$ .

The map  $\psi$  is uniquely determined by  $\varphi$  (see below the valid rule **Der**) so in our dynamical theory we can introduce it by means of a function symbol  $\Delta = \Delta_{1,1}$  of type  $Li_1 \rightarrow Li_2$  which satisfies the axiom

$$\mathbf{der} \quad \vdash_{\varphi: Li_1} \varphi(x_1) - \varphi(x_2) = \Delta(\varphi)(x_1, x_2) \times (x_1 - x_2)$$

*Remark.* This equality appears to be written in the form of maps evaluated as linking two objects of sort  $\mathbf{R}$ , but in fact *it should be read as linking two objects of sort  $Li_2$* , which are evaluated in  $(x_1, x_2)$  in the form indicated in the axiom as it appears to be written.

In fact we have to use the implicit coding alluded to above and the rule **der** must in fact be written in the form

$$\mathbf{der} \quad \vdash_{\varphi: Li_1} \frac{1}{2^p}(\varphi(x_1) - \varphi(x_2)) = \Delta_p(\varphi)(x_1, x_2) \times (x_1 - x_2)$$

To avoid complicating the presentation, in the following we pretend that  $\Delta(\varphi)$  is the real map “rate of increase”.

The following uniqueness rule follows from the axiom **Dens<sub>2</sub>**: in the first member we must read an equality between objects of sort  $Df_2$  and the smooth map is  $x_1 - x_2$  seen as an element of  $Li_2$ .

$$\mathbf{Der} \quad \varphi(x_1) - \varphi(x_2) = \psi(x_1, x_2) \times (x_1 - x_2) \vdash_{\varphi: Li_1; \psi: Df_2} \Delta(\varphi) = \psi$$

In the same way, for several variables, analogous axioms are required for each partial derivative.

In particular, for  $n \geq 2$  and  $i \in \llbracket 1..n \rrbracket$  we have a function symbol  $\Delta_{n,i}$  of type  $Li_n \rightarrow Li_{n+1}$  which satisfies the axiom

$$\mathbf{der}_{n,i} \vdash_{\varphi:Li_n} \varphi(x_1, \dots, x_i, \dots, x_n) - \varphi(x_1, \dots, x'_i, \dots, x_n) = \Delta_{n,i}(\varphi)(x_1, \dots, x_i, x'_i, \dots, x_n) \times (x_i - x'_i)$$

This equality must be read as linking two objects of sort  $Li_{n+1}$ .

*Remark.* Using the upper bound axiom, we obtain that smooth maps are lipschitzian, which gives a particularly simple uniform continuity modulus. ■

## What other axioms for derivation?

Here we need to consider which axioms need to be introduced corresponding to the usual properties of derivation. Most of these properties should result from the definition (axioms  $\mathbf{der}_{n,i}$ ) and the axioms  $\mathbf{Dens}_n$ .

## Axioms of virtual roots

Virtual roots can be defined a priori for any smooth map whose derivative of order  $k$  is  $> 0$  (on  $\mathbb{I}$ ), by virtue of Lemma E.2.3 and the uniform constructive version of the mean value theorem. We then obtain most of the properties described in Definition E.2.5 and Theorem E.2.6. The polynomial  $f(X) = X^d - (a_{d-1}X^{d-1} + \dots + a_1X + a_0)$  which depends on  $d+1$  variables can be replaced by any smooth  $\varphi$  map of  $d+1$  variables  $X, a_1, \dots, a_d$  whose  $k$ -th partial derivative with respect to  $X$  is  $> 0$  as an object of sort  $Li_{d+1}$ .

If  $\inf(\varphi^{(k)}) = \phi(a_1, \dots, a_d)$ , we can treat the map  $\psi_k = \varphi + (c - \phi)^+ X^k / k!$ , for a constant  $c > 0$ . Its  $k$ -th derivative with respect to  $X$  is  $\geq c$ , and it is equal to  $\varphi$  if  $\phi \geq c$ . We can then introduce the  $k$  virtual roots of  $\varphi$  on  $\mathbf{I}$  as objects of sort  $Df_d$  as in Definition E.2.5 and Theorem E.2.6, but using our  $\lambda$ -abstraction. More precisely, we have “virtual roots” function symbols  $\text{Rv}_{d,k,j}$  of type  $Li_{d+1} \rightarrow Df_d$ . And we have the corresponding axioms, direct translations of Definition E.2.5 and of Theorem E.2.6 (by replacing  $-\infty$  and  $+\infty$  by  $-1$  and  $+1$ ).

## K.3. Axioms of real closure or o-minimal closure

From now on we deal with axioms that correspond to the general idea of real closure and o-minimal structure.

### Finiteness axioms

The virtual root axioms are already axioms of finiteness, but independent of any o-minimal structure.

We should have an analogue to Proposition E.6.3 (table of signs and variations) for continuous semialgebraic maps, and this should also work for o-minimal structures. In classical mathematics, tables of signs and variations exist for definable maps of an o-minimal structure, and Proposition E.6.3 shows how to transform the classical statement into a constructive one. Here again, the problem is to formulate dynamical axioms that capture this type of result. One solution would be to have an infinite dynamical theory with axioms that say roughly that a continuous definable map is “piecewise smooth monotone” in a statement to be specified, similar to Item 2 of Proposition E.6.3.

### Gluing of maps defined on an open covering

A finite cover of  $\mathbf{I}^n$  by definable opens is given here in the form

$$V_i = \{ \underline{x} \in \mathbf{I}^n \mid g_i(\underline{x}) > 0 \} \quad i \in \llbracket 1..p \rrbracket$$

where  $g_i$  are of sort  $Df_n$  and satisfy  $\boxed{\sum_i g_i^+ > 0} \text{ (1)}$ . Functions  $h_i$  of sort  $Df_n$  are considered, for which a priori only the restrictions  $h_i|_{V_i}$  are relevant. The fact that  $h_i$  and  $h_j$  coincide on  $V_i \cap V_j$  results in the equality  $\boxed{h_i g_i^+ g_j^+ = h_j g_j^+ g_i^+} \text{ (2)}$ . Under hypotheses (1) and (2) we ask for the existence and uniqueness of an  $f$  of sort  $Df_n$  verifying  $f g_i^+ = h_i g_i^+$  for each  $i$  (which means that  $f|_{V_i} = h_i|_{V_i}$ ). A priori we must have  $f = (\sum_i h_i g_i^+) (\sum_i g_i^+)^{-1}$  (hence the uniqueness). And we get

$$f g_k^+ = \frac{\sum_i h_i g_i^+ g_k^+}{\sum_i g_i^+} = \frac{\sum_i h_k g_i^+ g_k^+}{\sum_i g_i^+} = \frac{(h_k g_k^+) \sum_i g_i^+}{\sum_i g_i^+} = h_k g_k^+.$$

### Gluing of maps defined on a closed covering

A finite covering of  $\mathbf{I}^n$  by definable closed subsets is given here in the form

$$F_i = \{ \underline{x} \in \mathbf{I}^n \mid g_i(\underline{x}) \geq 0 \} \quad i \in \llbracket 1..p \rrbracket$$

where  $g_i$  are of sort  $Df_n$  and satisfy  $\boxed{\sup_i g_i \geq 0}$ . Functions  $h_i$  of sort  $Df_n$  are considered, for which a priori only the restrictions  $h_i|_{F_i}$  are relevant. The fact that  $h_i$  and  $h_j$  coincide on  $F_i \cap F_j$  results in the validity of the rules ( $i, j \in \llbracket 1..p \rrbracket$ )

$$g_i(\underline{x}) \geq 0, g_j(\underline{x}) \geq 0 \vdash_{x_1, \dots, x_n: Icr; g_i, h_i, g_j, h_j: Df_n} h_i(\underline{x}) = h_j(\underline{x})$$

A uniform algebraic version of this validity can be stated as follows

- $\vdash_{g_i, h_i, q_{ij}, q_{ji}: Df_n} (h_i - h_j)^2 + g_i q_{ij}^+ + g_j q_{ji}^+ = 0$

where the  $q_{k\ell}$  are of sort  $Df_n$ . Let's abbreviate the second member as  $E_{ij}$ . Under the hypothesis of the equalities  $E_{ij}$ , we want to have a map  $f$  (an object  $f$  of sort  $Df_n$ ) satisfying an identity which means that  $f|_{F_i} = h_i|_{F_i}$ . This can be expressed in the form of the following rule

$$\mathbf{RCVF} \quad \sup_i g_i \geq 0, E_{1,2}, \dots, E_{p-1,p} \vdash_{g_i, h_i, q_{ij}, q_{ji}: Df_n} \exists f, q_1, \dots, q_p \bigwedge_i (f - h_i)^2 + g_i q_i^+ = 0$$

All the (free or dummy) variables in this rule are of sort  $Df_n$ .

In classical mathematics, this type of rule is valid for o-minimal structures. However, from a constructive point of view, we may have to restrict ourselves to coverings by *located closed subsets*.<sup>2</sup> This will complicate the writing of the axioms.

Note that the object  $f$  whose existence is postulated is provably unique by virtue of a classical calculation for Positivstellensätze: we use the identity  $(a + b)^2 + (a - b)^2 = 2(a^2 + b^2)$ .

### Axioms of extension by continuity

Typically, the **FRAC** <sub>$n$</sub>  rules are special continuity extension axioms. The aim here is to state different rules that apply more generally (without the continuity extension giving 0 to the disputed values) but with a smooth denominator.

For example, a map that is definable outside the zeros of a smooth (non-zero) map and continuous on its domain of definition is uniquely extended by continuity if it is uniformly continuous.

The problem is to formulate this in the context of our dynamical theory.

It will be good enough to be able to formulate it for a quotient  $f/g$  (well-defined outside the zeros of  $g$ ) with  $g$  smooth.

The fact that  $f$  cancels at the zeros of  $g$  can be put as an hypothesis in the following strong form: there exists an  $\alpha$  of such a sort  $Mc$  that  $\boxed{\alpha \circ |f| \leq |g|}$ .

<sup>2</sup>A closed subset is said to be *located* when the distance to it is a well-defined map from a constructive point of view. It seems necessary to add an axiom saying that the distance map to the zero set of a continuous definable map is itself definable.

The uniform continuity of  $f/g$  outside the zeros of  $g$  seems to be stated using the reciprocal bijection of an object of sort  $Mc$  on the interval  $[0, 1]$ . In fact, we want to write something like

$$\mu \left( \left| \frac{f(\underline{x})g(\underline{x}') - f(\underline{x}')g(\underline{x})}{g(\underline{x})g(\underline{x}')} \right| \right) \leq \|(\underline{x}) - (\underline{x}')\|$$

for  $\|(\underline{x}) - (\underline{x}')\| > 0$ , which could be rewritten without the assumption  $\|(\underline{x}) - (\underline{x}')\| > 0$  in the framework of geometric theory as

$$|f(\underline{x})g(\underline{x}') - f(\underline{x}')g(\underline{x})| \leq |g(\underline{x})g(\underline{x}')|, \nu(\|(\underline{x}) - (\underline{x}')\|)$$

with the reciprocal bijection  $\nu$  (on  $[0, \mu(1)]$ ) of  $\mu|_{[0,1]}$ .

### Conclusion: the improved real closed field structure

The theory *Crc3* will be obtained once all the axioms have been worked out. We have seen that the theory *Icr* can be considered as a variant of the theory *Co*. The theory *Crc3*, which could also be called the theory of *compact real closed intervals*, is an improved variant of *Crc2*, in which o-minimal structures (which are enriched structures of real closed fields) could have a place as particular dynamic algebraic structures.

**Theorem K.3.1.** *In constructive mathematics, the real interval  $\mathbb{I} = \mathbb{I}_{\mathbb{R}}$  and the continuous semi-algebraic maps  $\mathbb{I}^n \rightarrow \mathbb{I}$ , provides a model of the dynamical theory *Crc3*.*

*Proof.* It seems that the ad hoc definition of continuous semialgebraic maps adopted in E.3.4 reduces this theorem to a theorem concerning essentially  $\mathbb{R}_{\text{alg}}$ . But we need to check all the details and this may lead us to change the formulation of some axioms. □

This theory *Crc3* should make it possible to demonstrate constructive results which escape the more elementary theory *Crc2* for the simple reason that they do not correspond to dynamical rules of *Crc2*. Moreover, the same question arises for the dynamical rules of *Crc2* themselves.

## K.4. O-minimal structures

It seems that the axioms proposed here for the structure of compact real closed intervals are almost correct for constructively describing certain o-minimal structures defined in classical mathematics: those generated by the restrictions to the compact cube  $\mathbb{I}^n$  of certain smooth maps in the neighbourhood of  $\mathbb{I}^n$ .

The weakest point seems to be stability by projection. A priori, the current system of axioms only guarantees this stability for definable closed bounded parts.

The resulting structure depends on the smooth maps given at the outset in the  $Li_n$  sorts.

We are primarily interested in the structure obtained by taking the real analytic maps in the vicinity of the cube as the starting smooth maps. In dimension 1, this probably works well with Chebyshev series.

It is a real challenge to give a constructive version of the classical theory, for example starting from the presentations given in [70] and [21]. It would at least be necessary to demonstrate constructively that real analytic maps in the neighbourhood of the cube give rise to a structure which is a model of the dynamical theory *Crc3*.

Note also that from a strictly computational point of view, we are a priori more interested in the enumerable field  $\mathbb{R}_{\text{PR}}$  of real numbers computable in primitive recursive time, or in the enumerable field  $\mathbb{R}_{\text{Ptime}}$  of real numbers computable in polynomial time (see Example C.3.4). As for the definable continuous maps corresponding to these fields (for a fixed o-minimal structure), they too can no doubt be enumerated using Chebyshev series.

Finally, it should be pointed out that, as things stand, the system of axioms envisaged does not seem sufficient to really describe o-minimal structures, since it only guarantees stability by projection for bounded closed definable parts.

## K.5. Some questions

### Question K.5.1.

Does the theory [Crc3](#) prove more dynamical rules than the theory of the interval  $[-1, 1]$  for a real closed field described by [Crc1](#), or by [Crc2](#)?

### Questions K.5.2.

- 1) Does  $\mathbb{R}$  (for the sort  $R$ ), with  $\mathbb{I} = \mathbb{I}_{\mathbb{R}}$  (for the sort  $Icr$ ) and for  $Li_n$  the maps  $\mathbb{I}^n \rightarrow \mathbb{I}$  which are analytic in a neighbourhood of  $\mathbb{I}^n$ , support a model of the dynamical theory [Crc3](#)?
- 2) If so, do the objects of sort  $Df_n$  correspond exactly to the elements of the strongly real ring generated by the maps associated with the objects of sort  $Li_n$ ?





# General conclusion

This dissertation, and the unanswered questions it contains, is a measure of our ignorance of real algebra.



# Références et index



# References. Livres

- [Balbes & Dwinger] Raymond Balbes and Philip Dwinger. *Distributive lattices*. University of Missouri Press, Columbia, Mo., 1974, pp. xiii+294 (cit. on p. 31).
- [Bigard, Keimel & Wolfenstein] Alain Bigard, Klaus Keimel and Samuel Wolfenstein. *Groupes et anneaux réticulés*. Lecture Notes in Mathematics, Vol. 608. Springer-Verlag, Berlin-New York, 1977 (cit. on pp. 69, 70, 72, 73).
- [Bishop] Errett Bishop. *Foundations of constructive analysis*. McGraw-Hill, New York, 1967 (cit. on p. 3).
- [Bishop & Bridges] Errett Bishop and Douglas Bridges. *Constructive analysis*. Vol. 279. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1985. DOI: [10.1007/978-3-642-61667-9](https://doi.org/10.1007/978-3-642-61667-9) (cit. on p. 3).
- [Bochnak, Coste & Roy] Jacek Bochnak, Michel Coste and Marie-Françoise Roy. *Real algebraic geometry*. Vol. 36. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Translated from the 1987 French original, Revised by the authors. Berlin: Springer-Verlag, 1998 (cit. on pp. 48, 50, 58–60, 98).
- [Bridges & Richman] Douglas Bridges and Fred Richman. *Varieties of constructive mathematics*. Vol. 97. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1987. DOI: [10.1017/CB09780511565663](https://doi.org/10.1017/CB09780511565663) (cit. on p. 3).
- [Caramello] Olivia Caramello. *Theories, Sites, Toposes*. Oxford University Press, 2017 (cit. on p. 8).
- [Coste] Michel Coste. *An introduction to O-minimal Geometry*. Vol. 1. 1. Dip. Mat. Univ. Pisa, Dottorato di Ricerca in Matematica, Istituti Editoriali e Poligrafici Internazionali, Pisa, 2000, p. 1. URL: <https://perso.univ-rennes1.fr/michel.coste/polyens/OMIN.pdf> (cit. on pp. 3, 119).
- [van den Dries] Lou van den Dries. *Tame topology and o-minimal structures*. Vol. 248. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1998. DOI: [10.1017/CB09780511525919](https://doi.org/10.1017/CB09780511525919) (cit. on pp. 3, 119).
- [Goodstein, 1957] R.L. Goodstein. *Recursive number theory. A development of recursive arithmetic in a logic-free equation calculus*. Studies in Logic and the Foundations of Mathematics. Amsterdam: North-Holland Publishing Company XII, 190 p. (1957)., 1957 (cit. on p. 23).
- [Goodstein, 1961] R.L. Goodstein. *Recursive analysis*. Studies in Logic and the Foundations of Mathematics. Amsterdam: North- Holland Publishing Company. VIII, 138 p. (1961)., 1961 (cit. on p. 23).
- [Goodstein, 1979] R.L. Goodstein. *Fundamental concepts of mathematics. 2nd ed.* 1979 (cit. on p. 23).
- [Johnstone] Peter T. Johnstone. *Stone spaces*. Vol. 3. Cambridge studies in advanced mathematics. Reprint of the 1982 edition. Cambridge university press, Cambridge, 1986 (cit. on pp. 31, 72, 84).

- [Johnstone, Sketches 2] Peter T. Johnstone. *Sketches of an elephant: a topos theory compendium. Vol. 2.* Vol. 44. Oxford Logic Guides. The Clarendon Press, Oxford University Press, Oxford, 2002 (cit. on p. 8).
- [LPR] Henri Lombardi, Daniel Perrucci and Marie-Françoise Roy. *An elementary recursive bound for effective positivstellensatz and Hilbert's 17th problem.* Vol. 1277. Providence, RI: American Mathematical Society (AMS), 2020. URL: <http://arxiv.org/abs/1404.2338> (cit. on p. 50).
- [CACM] Henri Lombardi and Claude Quitté. *Commutative algebra: constructive methods. Finite projective modules.* Algebra and applications, 20. Translated from [ACMC] (Calvage & Mounet, Paris, 2011, revised and extended by the authors) by Tania K. Roblot. Springer, Dordrecht, 2015 (cit. on pp. 3, 30, 37, 50, 57, 68–71, 101).
- [ACMC] Henri Lombardi and Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini. Cours et exercices.* French. Second edition, revised and extended, of the 2011 book. Paris: Calvage & Mounet, 2021 (cit. on pp. 22, 30, 140).
- [Mason & Handscomb] J. C. Mason and D. C. Handscomb. *Chebyshev polynomials.* Chapman & Hall/CRC, Boca Raton, FL, 2003 (cit. on p. 122).
- [MRR] Ray Mines, Fred Richman and Wim Ruitenburg. *A course in constructive algebra.* Universitext. Traduction française par Henri Lombardi, révisée par Stefan Neuwirth. Un cours d'algèbre constructive. Presses Universitaires de Franche-Comté. 2020. Springer-Verlag, New York, 1988. DOI: [10.1007/978-1-4419-8640-5](https://doi.org/10.1007/978-1-4419-8640-5). URL: [http://dx.doi/10.1007/978-1-4419-8640-5](http://dx.doi.org/10.1007/978-1-4419-8640-5) (cit. on pp. 3, 19, 57, 101).
- [Proofs, 2013] Dieter Probst and Peter Schuster, eds. *Concepts of proof in mathematics, philosophy, and computer science. Based on the Humboldt-Kolleg, Bern, Switzerland, September 9–13, 2013.* English. Berlin: De Gruyter, 2016. DOI: [10.1515/9781501502620](https://doi.org/10.1515/9781501502620) (cit. on pp. 37, 144).
- [CCAPM] Ihsen Yengui. *Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases.* Lecture Notes in Mathematics, 2138. Springer, Cham, 2015, pp. vii+271. DOI: [10.1007/978-3-319-19494-3](https://doi.org/10.1007/978-3-319-19494-3) (cit. on p. 3).
- [Zaanen] Adriaan C. Zaanen. *Introduction to operator theory in Riesz spaces.* Springer-Verlag, Berlin, 1997. DOI: [10.1007/978-3-642-60637-3](https://doi.org/10.1007/978-3-642-60637-3) (cit. on p. 69).

# References. Articles

- [1] Ernesto Acosta and Cesar Delgado. ‘Uniform calculus and the law of bounded change’. In: *Amer. Math. Monthly* 101.4 (1994), pp. 332–338 (cit. on p. 129).
- [2] María Emilia Alonso Garcia and André Galligo. ‘A root isolation algorithm for sparse univariate polynomials’. In: *ISSAC 2012—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 2012, pp. 35–42. DOI: [10.1145/2442829.2442839](https://doi.org/10.1145/2442829.2442839) (cit. on p. 87).
- [3] María Emilia Alonso Garcia, Henri Lombardi and Hervé Perdry. ‘Elementary constructive theory of Henselian local rings’. In: *MLQ Math. Log. Q.* 54.3 (2008), pp. 253–271. DOI: [10.1002/malq.200710057](https://doi.org/10.1002/malq.200710057). URL: <https://arxiv.org/abs/2202.06595> (cit. on pp. 55, 57).
- [4] Thomas William Barrett and Hans Halvorson. ‘Quine’s conjecture on many-sorted logic’. In: *Synthese* 194.9 (2017), pp. 3563–3582. DOI: [10.1007/s11229-016-1107-z](https://doi.org/10.1007/s11229-016-1107-z) (cit. on p. 8).
- [5] Daniel Bembé and André Galligo. ‘Virtual roots of a real polynomial and fractional derivatives’. In: *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 2011, pp. 27–34. DOI: [10.1145/1993886.1993897](https://doi.org/10.1145/1993886.1993897) (cit. on p. 87).
- [6] Marc Bezem and Thierry Coquand. ‘Automating coherent logic.’ In: *Logic for programming, artificial intelligence, and reasoning. 12th international conference, LPAR 2005, Montego Bay, Jamaica, December 2–6, 2005. Proceedings*. Berlin: Springer, 2005, pp. 246–260. DOI: [10.1007/11591191\\_18](https://doi.org/10.1007/11591191_18) (cit. on p. 12).
- [7] Marc Bezem and Thierry Coquand. ‘Skolem’s Theorem in Coherent Logic.’ In: *Fundam. Inform.* (2019) (cit. on p. 29).
- [8] Garrett Birkhoff and R. S. Pierce. ‘Lattice-ordered rings’. In: *An. Acad. Brasil. Ci.* 28 (1956), pp. 41–69 (cit. on p. 72).
- [9] Mark Bridger and Gabriel Stolzenberg. ‘Uniform calculus and the law of bounded change’. In: *Amer. Math. Monthly* 106.7 (1999), pp. 628–635. DOI: [10.2307/2589492](https://doi.org/10.2307/2589492) (cit. on p. 129).
- [10] Jan Cederquist and Thierry Coquand. ‘Entailment relations and distributive lattices’. In: *Logic Colloquium ’98 (Prague)*. Vol. 13. Lect. Notes Log. Assoc. Symbol. Logic, Urbana, IL, 2000, pp. 127–139 (cit. on pp. 30, 66, 84).
- [11] Thierry Coquand. ‘A completeness proof for geometrical logic.’ In: *Logic, methodology and philosophy of science. Proceedings of the 12th international congress, Oviedo, Spain, August 2003*. London: King’s College Publications, 2005, pp. 79–89 (cit. on p. 28).
- [12] Thierry Coquand and Henri Lombardi. ‘A logical approach to abstract algebra’. In: *Math. Structures Comput. Sci.* 16.5 (2006), pp. 885–900. DOI: [10.1017/S0960129506005627](https://doi.org/10.1017/S0960129506005627) (cit. on pp. 37, 66).
- [13] Thierry Coquand and Henri Lombardi. ‘A note on the axiomatisation of real numbers’. In: *Math. Log. Q.* 54.3 (2008), pp. 224–228. DOI: [10.1002/malq.200710039](https://doi.org/10.1002/malq.200710039) (cit. on p. 51).



- [14] Thierry Coquand, Henri Lombardi and Stefan Neuwirth. ‘Lattice-ordered groups generated by an ordered group and regular systems of ideals.’ In: *Rocky Mt. J. Math.* 49.5 (2019), pp. 1449–1489. URL: <https://arxiv.org/abs/1701.05115> (cit. on p. 71).
- [15] Thierry Coquand, Henri Lombardi and Claude Quitté. ‘Dimension de Heitmann des treillis distributifs et des anneaux commutatifs’. In: *Publications Mathématiques de l’Université de Franche-Comté Besançon. Algèbre et théorie des nombres. Années 2003–2006*. Besançon: Laboratoire de Mathématiques de Besançon, 2006, p. 57–100, version corrigée, 2020. URL: <http://arxiv.org/abs/1712.01958> (cit. on p. 66).
- [16] Michel Coste, Tomás Lajous-Loaeza, Henri Lombardi and Marie-Françoise Roy. ‘Generalized Budan-Fourier theorem and virtual roots’. In: *J. Complexity* 21.4 (2005), pp. 479–486. DOI: [10.1016/j.jco.2004.11.003](https://doi.org/10.1016/j.jco.2004.11.003) (cit. on pp. 87, 89).
- [17] Michel Coste, Henri Lombardi and Marie-Françoise Roy. ‘Dynamical method in algebra: effective Nullstellensätze’. In: *Ann. Pure Appl. Logic* 111.3 (2001), pp. 203–256. DOI: [10.1016/S0168-0072\(01\)00026-4](https://doi.org/10.1016/S0168-0072(01)00026-4) (cit. on pp. 12, 17, 18, 20, 28, 29, 44, 46–50, 100).
- [18] Jean Della Dora, Claire Dicrescenzo and Dominique Duval. ‘About a new method for computing in algebraic number fields’. In: *EUROCAL ’85. Lecture Notes in Computer Science no. 204, (Ed. Caviness B.F.)* Springer, Berlin, 1985, pp. 289–290 (cit. on p. 18).
- [19] Charles N. Delzell. ‘On the Pierce-Birkhoff conjecture over ordered fields’. In: *Rocky Mountain J. Math.* 19.3 (1989). Quadratic forms and real algebraic geometry (Corvallis, OR, 1986), pp. 651–668. DOI: [10.1216/RMJ-1989-19-3-651](https://doi.org/10.1216/RMJ-1989-19-3-651) (cit. on p. 76).
- [20] Charles N. Delzell and James J. Madden. ‘Lattice-ordered rings and semialgebraic geometry. I’. In: *Real analytic and algebraic geometry (Trento, 1992)*. de Gruyter, Berlin, 1995, pp. 103–129 (cit. on p. 72).
- [21] J. Denef and Lou van den Dries. ‘ $p$ -adic and real subanalytic sets.’ In: *Ann. Math. (2)* 128.1 (1988), pp. 79–138. DOI: [10.2307/1971463](https://doi.org/10.2307/1971463) (cit. on pp. 119, 132).
- [22] Roy Dyckhoff. ‘Invited talk: coherentisation of first-order logic.’ In: *Automated reasoning with analytic tableaux and related methods. 24th international conference, TABLEAUX 2015, Wrocław, Poland, September 21–24, 2015. Proceedings*. Cham: Springer, 2015, pp. 3–5. DOI: [10.1007/978-3-319-24312-2\\_1](https://doi.org/10.1007/978-3-319-24312-2_1) (cit. on p. 28).
- [23] Roy Dyckhoff and Sara Negri. ‘Geometrisation of first-order logic.’ In: *Bull. Symb. Log.* 21.2 (2015), pp. 123–163. DOI: [10.1017/bsl.2015.7](https://doi.org/10.1017/bsl.2015.7) (cit. on p. 28).
- [24] Michael Eisermann. ‘The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains’. In: *Amer. Math. Monthly* 119.9 (2012), pp. 715–752. DOI: [10.4169/amer.math.monthly.119.09.715](https://doi.org/10.4169/amer.math.monthly.119.09.715) (cit. on pp. 107, 108).
- [25] André Galligo. ‘Budan tables of real univariate polynomials’. In: *J. Symbolic Comput.* 53 (2013), pp. 64–80. DOI: [10.1016/j.jsc.2012.11.004](https://doi.org/10.1016/j.jsc.2012.11.004) (cit. on p. 87).
- [26] Laureano González-Vega and Henri Lombardi. ‘A real Nullstellensatz and Positivstellensatz for the semipolynomials over an ordered field’. In: *J. Pure Appl. Algebra* 90.2 (1993), pp. 167–188. DOI: [10.1016/0022-4049\(93\)90128-G](https://doi.org/10.1016/0022-4049(93)90128-G). URL: <http://hlombardi.free.fr/publis/PstSemiPols.pdf> (cit. on pp. 51, 62, 83, 109).
- [27] Laureano González-Vega, Henri Lombardi and Louis Mahé. ‘Virtual roots of real polynomials’. In: *J. Pure Appl. Algebra* 124.1-3 (1998), pp. 147–166. DOI: [10.1016/S0022-4049\(96\)00102-8](https://doi.org/10.1016/S0022-4049(96)00102-8). URL: <http://arxiv.org/abs/1712.01952> (cit. on pp. 86–89, 91).
- [28] M. Hochster. ‘Prime ideal structure in commutative rings.’ In: *Trans. Am. Math. Soc.* 142 (1969), pp. 43–60. DOI: [10.2307/1995344](https://doi.org/10.2307/1995344) (cit. on p. 31).
- [29] P. T. Johnstone. *A syntactic approach to Diers’ localizable categories*. Applications of sheaves, Proc. Res. Symp., Durham 1977, Lect. Notes Math. 753, 466–478 (1979). 1979 (cit. on pp. 9, 17).

- [30] F.-V. Kuhlmann and Henri Lombardi. ‘Construction of the Henselization of a valued field. (Construction du hensélisé d’un corps valué.)’ In: *J. Algebra* 228.2 (2000), pp. 624–632. URL: <http://arxiv.org/abs/2202.05503> (cit. on p. 57).
- [31] Franz-Viktor Kuhlmann, Henri Lombardi and Hervé Perdry. ‘Dynamic computations inside the algebraic closure of a valued field’. In: *Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999)*. Vol. 33. Fields Inst. Commun. Amer. Math. Soc., Providence, RI, 2003, pp. 133–156. URL: <http://arxiv.org/abs/2202.05512> (cit. on p. 57).
- [32] S. Labhalla, H. Lombardi and E. Moutai. ‘Espaces métriques rationnellement présentés et complexité: le cas de l’espace des fonctions réelles uniformément continues sur un intervalle compact’. In: *Theoret. Comput. Sci.* 250.1-2 (2001), pp. 265–332. DOI: [10.1016/S0304-3975\(99\)00139-5](https://doi.org/10.1016/S0304-3975(99)00139-5) (cit. on p. 71).
- [33] Vladimir Lifschitz. ‘Semantical completeness theorems in logic and algebra’. In: *Proc. Amer. Math. Soc.* 79.1 (1980), pp. 89–96. DOI: [10.2307/2042394](https://doi.org/10.2307/2042394) (cit. on p. 12).
- [34] Henri Lombardi. ‘Effective real Nullstellensatz and variants’. In: *Effective methods in algebraic geometry (Castiglione, 1990)*. Vol. 94. Progr. Math. Birkhäuser Boston, Boston, MA, 1991, pp. 263–288 (cit. on pp. 50, 100).
- [35] Henri Lombardi. ‘Relecture constructive de la théorie d’Artin-Schreier’. In: *Ann. Pure Appl. Logic* 91.1 (1998), pp. 59–92. DOI: [10.1016/S0168-0072\(97\)80700-2](https://doi.org/10.1016/S0168-0072(97)80700-2) (cit. on p. 34).
- [36] Henri Lombardi. ‘Dimension de Krull, Nullstellensätze et évaluation dynamique’. In: *Math. Z.* 242.1 (2002), pp. 23–46. DOI: [10.1007/s002090100305](https://doi.org/10.1007/s002090100305) (cit. on p. 18).
- [37] Henri Lombardi. ‘Structures algébriques dynamiques, espaces topologiques sans points et programme de Hilbert’. In: *Ann. Pure Appl. Logic* 137.1-3 (2006), pp. 256–290. DOI: [10.1016/j.apal.2005.05.023](https://doi.org/10.1016/j.apal.2005.05.023) (cit. on p. 18).
- [38] Henri Lombardi. ‘Le mystère de la structure du continu’. In: *Des Nombres et des Mondes. Actes du colloque en l’honneur de Guy Wallet (2011 à La Rochelle)*. Hermann, Paris, 2013, pp. 53–67 (cit. on p. 4).
- [39] Henri Lombardi. ‘Théories géométriques pour l’algèbre constructive’. <http://hlombardi.free.fr/Theories-geometriques.pdf>. 2022 (cit. on pp. 7, 34).
- [40] Henri Lombardi and Assia Mahboubi. ‘Théories géométriques pour l’algèbre des nombres réels’. French. In: *Ordered algebraic structures and related topics. International conference at CIRM, Luminy, France, October 12–16, 2015. Proceedings*. Vol. 697. Providence, RI: American Mathematical Society (AMS), 2017, pp. 239–264. URL: <https://hal.inria.fr/hal-01426164> (cit. on pp. 1, 3, 4, 41, 53, 54, 62, 78, 81).
- [41] Henri Lombardi and Assia Mahboubi. ‘Valuative lattices and spectra’. In: *Algebraic, number theoretic, and topological aspects of ring theory*. Ed. by Jean-Luc Chabert et al. Cham: Springer, 2023, pp. 275–341. DOI: [10.1007/978-3-031-28847-0\\_17](https://doi.org/10.1007/978-3-031-28847-0_17). URL: <http://arxiv.org/abs/2210.16558> (cit. on pp. 4, 7, 18, 27, 30).
- [42] Henri Lombardi and Marie-Françoise Roy. ‘Elementary constructive theory of ordered fields’. In: *Effective methods in algebraic geometry (Castiglione, 1990)*. Vol. 94. Progr. Math. Birkhäuser Boston, Boston, MA, 1991, pp. 249–262 (cit. on pp. 50, 86–88, 100, 102).
- [43] Henri Lombardi and Marie-Françoise Roy. ‘Théorie constructive élémentaire des corps ordonnés’. In: *Théorie des nombres, Années 1989/90–1990/91*. Publ. Math. Fac. Sci. Besançon. Univ. Franche-Comté, Besançon, 1991, pp. x–x+21 (cit. on pp. 50, 87, 88, 100).
- [44] Paul Lorenzen. ‘Abstrakte Begründung der multiplikativen Idealtheorie’. In: *Math. Z.* 45 (1939), pp. 533–553 (cit. on p. 71).
- [45] Paul Lorenzen. ‘Über halbgeordnete Gruppen’. In: *Math. Z.* 52 (1950), pp. 483–526. URL: <http://eudml.org/doc/169131> (cit. on p. 71).

- [46] Paul Lorenzen. ‘Algebraische und logistische Untersuchungen über freie Verbände’. In: *J. Symbolic Logic* 16 (1951). Translation by Stefan Neuwirth: *Algebraic and logistic investigations on free lattices*, <http://arxiv.org/abs/1710.08138>, pp. 81–106. URL: <http://www.jstor.org/stable/2266681> (cit. on pp. 30, 66).
- [47] Paul Lorenzen. ‘Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen’. German. In: *Math. Z.* 58 (1953), pp. 15–24. URL: <http://eudml.org/doc/169331> (cit. on p. 71).
- [48] F. Lucas, J. Madden, D. Schaub and M. Spivakovsky. ‘Approximate roots of a valuation and the Pierce-Birkhoff conjecture’. In: *Ann. Fac. Sci. Toulouse Math. (6)* 21.2 (2012), pp. 259–342. URL: [http://afst.cedram.org/item?id=AFST\\_2012\\_6\\_21\\_2\\_259\\_0](http://afst.cedram.org/item?id=AFST_2012_6_21_2_259_0) (cit. on p. 108).
- [49] James J. Madden. ‘Pierce-Birkhoff rings’. In: *Arch. Math. (Basel)* 53.6 (1989), pp. 565–570. DOI: [10.1007/BF01199816](https://doi.org/10.1007/BF01199816) (cit. on p. 108).
- [50] James J. Madden. ‘On  $f$ -rings that are not formally real’. In: *Ann. Fac. Sci. Toulouse Math. (6)* 19.Fascicule Special (2010), pp. 143–157. URL: [http://afst.cedram.org/item?id=AFST\\_2010\\_6\\_19\\_\\_143\\_0](http://afst.cedram.org/item?id=AFST_2010_6_19__143_0) (cit. on p. 72).
- [51] Louis Mahé. ‘On the Pierce-Birkhoff conjecture’. In: *Rocky Mountain J. Math.* 14.4 (1984). Ordered fields and real algebraic geometry (Boulder, Colo., 1983), pp. 983–985. DOI: [10.1216/RMJ-1984-14-4-983](https://doi.org/10.1216/RMJ-1984-14-4-983) (cit. on p. 108).
- [52] Bassel Mannaa and Thierry Coquand. ‘Dynamic Newton-Puiseux theorem’. In: *J. Log. Anal.* 5 (2013), Paper 5. DOI: [10.4115/jla.2013.5.5](https://doi.org/10.4115/jla.2013.5.5) (cit. on p. 102).
- [53] Ju. V. Matijasevič. ‘A metamathematical approach to proving theorems in discrete mathematics’. In: *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* 49 (1975). Theoretical applications of the methods of mathematical logic, I, pp. 31–50, 177 (cit. on p. 12).
- [54] Daniel Perrucci and Marie-Françoise Roy. ‘Quantitative Fundamental Theorem of Algebra. Preprint.’ 2019. URL: <http://arxiv.org/abs/1803.04358> (cit. on p. 107).
- [55] Dag Prawitz. ‘Ideas and results in proof theory’. In: *Proceedings of the Second Scandinavian Logic Symposium (Univ. Oslo, Oslo, 1970)*. North-Holland, Amsterdam, 1971, 235–307. *Studies in Logic and the Foundations of Mathematics*, Vol. 63 (cit. on pp. 12, 28).
- [56] Alexander Prestel and Niels Schwartz. ‘Model theory of real closed rings’. In: *Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999)*. Vol. 32. Fields Inst. Commun. Amer. Math. Soc., Providence, RI, 2002, pp. 261–290 (cit. on pp. 52, 96, 97).
- [57] Michael Rathjen. ‘Remarks on Barr’s theorem proofs in geometric theories’. In: *Concepts of proof in mathematics, philosophy, and computer science. Based on the Humboldt-Kolleg, Bern, Switzerland, September 9–13, 2013. [Proofs, 2013]*. Berlin: De Gruyter, 2016, pp. 347–374 (cit. on p. 37).
- [58] Fred Richman. ‘The fundamental theorem of algebra: a constructive development without choice’. In: *Pacific J. Math.* 196.1 (2000), pp. 213–230. DOI: [10.2140/pjm.2000.196.213](https://doi.org/10.2140/pjm.2000.196.213) (cit. on pp. 106, 107).
- [59] Fred Richman. ‘Constructive mathematics without choice’. In: *Reuniting the antipodes – constructive and nonstandard views of the continuum (Venice, 1999)*. Vol. 306. Synthese Lib. Kluwer Acad. Publ., Dordrecht, 2001, pp. 199–205 (cit. on p. 3).
- [60] Konrad Schmüdgen. ‘The  $K$ -moment problem for compact semi-algebraic sets’. In: *Math. Ann.* 289.2 (1991), pp. 203–206. DOI: [10.1007/BF01446568](https://doi.org/10.1007/BF01446568) (cit. on p. 112).
- [61] Niels Schwartz. ‘Real closed spaces’. In: *Rocky Mountain J. Math.* 14.4 (1984). Ordered fields and real algebraic geometry (Boulder, Colo., 1983), pp. 971–972. DOI: [10.1216/RMJ-1984-14-4-971](https://doi.org/10.1216/RMJ-1984-14-4-971) (cit. on p. 98).
- [62] Niels Schwartz. ‘Real closed spaces. Habilitationsschrift. München’. Habilitationsschrift. München, 1984 (cit. on p. 96).

- [63] Niels Schwartz. ‘Real closed rings’. In: *Algebra and order (Luminy-Marseille, 1984)*. Vol. 14. Res. Exp. Math. Heldermann, Berlin, 1986, pp. 175–194 (cit. on pp. [52](#), [96](#), [98](#)).
- [64] Niels Schwartz. ‘The basic theory of real closed spaces’. In: *Mem. Amer. Math. Soc.* 77.397 (1989), pp. viii+122. DOI: [10.1090/memo/0397](#) (cit. on p. [98](#)).
- [65] Niels Schwartz. ‘Rings of continuous functions as real closed rings’. In: *Ordered algebraic structures (Curaçao, 1995)*. Kluwer Acad. Publ., Dordrecht, 1997, pp. 277–313 (cit. on p. [98](#)).
- [66] Markus Schweighofer. ‘An algorithmic approach to Schmüdgen’s Positivstellensatz’. In: *J. Pure Appl. Algebra* 166.3 (2002), pp. 307–319. DOI: [10.1016/S0022-4049\(01\)00041-X](#) (cit. on p. [112](#)).
- [67] Markus Schweighofer. ‘Iterated rings of bounded elements and generalizations of Schmüdgen’s Positivstellensatz’. In: *J. Reine Angew. Math.* 554 (2003), pp. 19–45. DOI: [10.1515/cr11.2003.004](#) (cit. on p. [112](#)).
- [68] M. H. Stone. ‘Topological representations of distributive lattices and Brouwerian logics.’ In: *Cas. Mat. Fys.* 67 (1937), pp. 1–25 (cit. on p. [31](#)).
- [69] Marcus Tressl. ‘Super real closed rings’. In: *Fund. Math.* 194.2 (2007), pp. 121–177. DOI: [10.4064/fm194-2-2](#) (cit. on pp. [4](#), [41](#), [61](#), [86](#), [96](#), [98](#)).
- [70] Lou van den Dries. ‘A generalization of the Tarski-Seidenberg theorem, and some nondefinability results.’ In: *Bull. Am. Math. Soc., New Ser.* 15 (1986), pp. 189–193. DOI: [10.1090/S0273-0979-1986-15468-6](#) (cit. on pp. [119](#), [132](#)).



# Notations index

## Logic

$\vdash$	deduction rule	12
<b>op</b>	open branches of computation	12
$\exists u$	introduce a fresh variable $u$	14
$\perp$	collapse symbol	16
$\wedge$	logical “and”	27
$\vee$	logical “or”	27
$\exists$	logical “there exists”	27

## Function symbols

$a \vee b$	$\sup(a, b)$	48
$\text{Fr}(a, b)$	$a/b$ (supposed well-defined)	53
$\text{fsa}_F$	continuous semialgebraic map of graph $F$	61
$a \wedge b$	$\inf(a, b)$	68
$\text{Sqr}$	$\text{Sqr}(x) = \sqrt{x^+}$	86
$\rho_{d,j}$	virtual root	89
$\uplus$	$\frac{1}{2}(x+y)$ on interval $[-1, +1]$	121
$\oplus$	forced addition on $[-1, +1]$	121
$\text{Cb}$	barycentric coefficients	122
$\text{Brc}$	barycenters	122
$\text{T}_n$	Chebyshev polynomial	122

## Theories

$\mathcal{Cd}$	discrete fields	13
$\mathcal{Ac}$	commutative rings	18
$\mathcal{Cod}$	discrete ordered fields	44
$\mathcal{Apo}$	preordered rings	46
$\mathcal{Ao}$	ordered rings	46
$\mathcal{Aonz}$	strictly reduced ordered rings	46
$\mathcal{Ato}$	linearly ordered rings	46
$\mathcal{Atonz}$	reduced linearly ordered rings	46
$\mathcal{Apro}$	proto-ordered rings	46
$\mathcal{Aso}$	strictly ordered rings	46

$\mathcal{A}sto$	linearly, strictly ordered rings.....	47
$\mathcal{A}sonz$	reduced strictly ordered rings.....	47
$\mathcal{A}ito$	linearly ordered domains.....	47
$\mathcal{C}rcd$	discrete real closed fields.....	45
$\mathcal{C}odsup$	discrete ordered fields with sup.....	48
$\mathcal{A}tosup$	linearly ordered rings with sup.....	48
$\mathcal{A}stosup$	strict $f$ -rings with sup.....	48
$\mathcal{C}rcdsup$	real closed fields with sup.....	48
$\mathcal{C}o0$	minimal theory of <i>non</i> discrete ordered fields.....	51
$\mathcal{C}o$	<i>non</i> discrete ordered fields.....	53
$\mathcal{C}rc1$	<i>non</i> discrete real closed fields.....	60
$\mathcal{T}r0$	(bounded) lattices.....	66
$\mathcal{T}r$	nontrivial lattices.....	66
$\mathcal{T}rdi$	distributive lattices.....	66
$\mathcal{G}rl$	$\ell$ -groups.....	68
$\mathcal{G}tosup$	linearly ordered groups with sup.....	70
$\mathcal{A}fr$	$f$ -rings.....	72
$\mathcal{A}frnz$	reduced $f$ -rings.....	78
$\mathcal{A}frsdz$	$f$ -rings without zerodivisor.....	77
$\mathcal{A}sr$	strict $f$ -rings.....	78
$\mathcal{A}srnz$	reduced strict $f$ -rings.....	78
$\mathcal{A}fr$	strongly real $f$ -rings.....	80
$\mathcal{A}fr2c$	2-closed $f$ -rings.....	86
$\mathcal{A}sr2c$	2-closed strict $f$ -rings.....	86
$\mathcal{C}o2c$	2-closed <i>non</i> discrete ordered fields.....	86
$\mathcal{C}orv$	<i>non</i> discrete ordered fields with virtual roots.....	94
$\mathcal{C}o0rv$	.....	94
$\mathcal{A}frv$	$f$ -rings with virtual roots.....	92
$\mathcal{A}rc$	real closed rings.....	93
$\mathcal{A}srv$	strict $f$ -rings with virtual roots.....	92
$\mathcal{A}itorv$	linearly ordered domains with virtual roots.....	92
$\mathcal{C}rc2$	<i>non</i> discrete real closed fields, 2; essentially identical to $\mathcal{C}orv$ and to $\mathcal{C}rc1$ ..	99
$\mathcal{C}rca$	archimedean <i>non</i> discrete real closed fields.....	111
$\mathcal{I}cr$	compact real intervals.....	122
$\mathcal{I}crc$	compact real closed intervals.....	??

### Some axioms and dynamical rules

<b>AL</b>	$(x + y)z = 1 \vdash \exists u \, xu = 1 \quad \text{op} \quad \exists v \, yv = 1$ local rings axiom.....	13
<b>AL1</b>	$U(x + y) \vdash U(x) \quad \text{op} \quad U(y)$ .....	31
<b>Anz</b>	$x^2 = 0 \vdash x = 0$ .....	13
<b>ASDZ</b>	$xy = 0 \vdash x = 0 \quad \text{op} \quad y = 0$ .....	13
<b>CD</b>	$\vdash x = 0 \quad \text{op} \quad \exists y \, xy = 1$ .....	13
<b>NIL</b>	$Z(x) \vdash \text{OP}_{n \in \mathbb{N}^+} x^n = 0$ .....	36
<b>Gao</b>	$x \geq 0, x \leq 0 \vdash x = 0$ .....	45

<b>aso1</b> à <b>aso4</b>	.....	45
<b>lv</b>	$xy = 1 \vdash x^2 > 0$ .....	45
<b>IV</b>	$x > 0 \vdash \exists y xy = 1$ .....	45
<b>ED<sub>#</sub></b>	$\vdash x = 0 \quad \text{op} \quad x \# 0$ .....	45
<b>OT</b>	$\vdash x \geq 0 \quad \text{op} \quad x \leq 0$ .....	45
<b>Aonz</b>	$c \geq 0, x(x^2 + c) \geq 0 \vdash x \geq 0$ strictly reduced ordered rings.....	45
<b>Aso1</b>	$x > 0, xy \geq 0 \vdash y \geq 0$ .....	45
<b>Aso2</b>	$x \geq 0, xy > 0 \vdash y > 0$ .....	45
<b>OTF</b>	$x + y > 0 \vdash x > 0 \quad \text{op} \quad y > 0$ .....	45
<b>OTF<sup>×</sup></b>	$xy < 0 \vdash x < 0 \quad \text{op} \quad y < 0$ .....	45
<b>Afr4</b>	$y \geq 0, xy = 1 \vdash x \geq 0$ .....	47
<b>Afr5</b>	$c \geq 0, x(x^2 + c) \geq 0 \vdash x^3 \geq 0$ .....	47
<b>RCF<sub>n</sub></b>	$a < b, P(a)P(b) < 0 \vdash \exists x (P(x) = 0, a < x < b) \quad (P(x) = \sum_{k=0}^n a_k x^k)$ .....	45
<b>sup1</b>	$\vdash x \vee y \geq x$ .....	48
<b>sup2</b>	$\vdash x \vee y \geq y$ .....	48
<b>Sup</b>	$z \geq x, z \geq y \vdash z \geq x \vee y$ .....	48
<b>sup</b>	$\vdash ((x \vee y) - x)((x \vee y) - y) = 0$ .....	48
<b>grl</b>	$\vdash x + (y \vee z) = (x + y) \vee (x + z)$ .....	52
<b>afr</b>	$\vdash x^+ (y \vee z) = (x^+ y) \vee (x^+ z)$ .....	52
<b>CVX</b>	$0 \leq a \leq b \vdash \exists z zb = a^2$ .....	53
<b>FRAC</b>	$0 \leq a \leq b \vdash \exists z (zb = a^2, 0 \leq z \leq a)$ .....	53
<b>fr1</b>	$\vdash \text{Fr}(a, b)  b  = ( a  \wedge  b )^2$ .....	53
<b>fr2</b>	$\vdash 0 \leq \text{Fr}(a, b) \leq  a  \wedge  b $ .....	53
<b>FRAC<sub>n</sub></b>	$ u ^n \leq  v ^{n+1} \vdash \exists z (zv = u,  z ^n \leq  v ) \quad (n \geq 1)$ .....	54
<b>afr1 - afr7</b>	.....	73
<b>Afr1 - Afr5</b>	.....	73
<b>Afrnz1 - Afrnz3</b>	.....	79
<b>AFRL</b>	$z(x + y) = 1, x + y \geq 0 \vdash \exists u (ux = 1, x \geq 0) \quad \text{op} \quad \exists v (vy = 1, y \geq 0)$ .....	81
<b>sqr0</b>	$\vdash \text{Sqr}(0) = 0$ .....	86
<b>sqr1</b>	$\vdash \text{Sqr}(x) \geq 0$ .....	86
<b>sqr2</b>	$\vdash \text{Sqr}(x) = \text{Sqr}(x^+)$ .....	86
<b>sqr3</b>	$\vdash \text{Sqr}(x)^2 = x^+$ .....	86
<b>sqr4</b>	$\vdash \text{Sqr}(x^+ y^+) = \text{Sqr}(x) \text{Sqr}(y)$ .....	86
<b>vr<sub>i,j,k</sub></b>	axioms for virtual roots, examples.....	90

**Algebraic structures, generic models**

$\mathbb{R}_{\text{alg}}$	the field of real algebraic numbers.....	50
$\mathbb{R}_{\text{PR}}$	the field of primitive recursive real numbers.....	52
$\mathbb{R}_{\text{Ptime}}$	the field of real numbers computable in polynomial time.....	52
$\mathbb{R}_{\text{Rec}}$	the field of recursive real numbers.....	52
$\text{Fsac}_n(\mathbb{R})$	<b>C.5.5</b> : semialgebraic continuous functions in $n$ variables, see also <b>E.3.4</b> .....	59

In the following **A** is a commutative ring with a suitable algebraic structure over a suitable dynamical theory in some context, **R** is an  $f$ -ring with virtual roots.

<b>AFR(A)</b>	$f$ -ring freely generated by <b>A</b> .....	77
---------------	--	----



$\text{Sipd}_n(\mathbf{A})$	ring of semipolynomials (or sipd maps) in $n$ variables over $\mathbf{A}$ .....	77
$\text{Sipd}_n(\mathbf{A}, \mathbf{B})$	ring of $\mathbf{A}$ -semipolynomials in $n$ variables over $\mathbf{B}$ .....	77
$\text{AFR2C}(\mathbf{A})$	2-closure of an $f$ -ring .....	87
$\text{Fsace}_n(\mathbf{R})$	ring of integral continuous semialgebraic maps in $n$ variables .....	93
$\text{Fsac}_n(\mathbf{R})$	ring of continuous semialgebraic maps in $n$ variables .....	94
$\text{AFRNZ}(\mathbf{A})$	reduced $f$ -ring generated by $\mathbf{A}$ .....	93
$\text{AFRRV}(\mathbf{A})$	$f$ -ring with virtual roots generated by $\mathbf{A}$ .....	93
$\text{Ppm}(\mathbf{A})$	ring of piecewise polynomial elements of $\text{AFRRV}(\mathbf{A})$ .....	93
$\text{ARC}(\mathbf{A})$	real closed ring generated by $\mathbf{A}$ .....	99