Théories géométriques pour l'algèbre des nombres réels

Henri Lombardi, Assia Mahboubi

Théories géométriques pour l'algèbre des nombres réels

Henri Lombardi, Assia Mahboubi

6 mars 2017

version courte de l'article
« Théories géométriques pour l'algèbre des nombres réels
sans test de signe ni axiome de choix dépendant »
la dernière version en cours peut être trouvée en
http://hlombardi.free.fr/Reels-geom-court.pdf

Résumé

On cherche à déterminer une théorie dynamique aussi complète que possible pour décrire les propriétés algébriques du corps des réels en mathématiques constructives sans axiome du choix dépendant. Un but essentiel pour l'avenir est d'obtenir une version constructive des structures O-minimales

On propose ici une théorie qui s'avère très proche de la théorie des anneaux locaux réels clos en mathématiques classiques. La théorie des anneaux réels clos est présentée ici sous forme constructive comme une théorie purement équationnelle naturelle, qui utilise les fonctions racines virtuelles introduites dans des travaux antérieurs.

Table des matières

Introduction

Définissons *l'algèbre réelle* comme l'étude les propriétés algébriques des nombres réels, i.e., les propriétés de $\mathbb{R}$ formulables au premier ordre sur le langage

$$\{\cdot = 0, \cdot > 0, \cdot \geqslant 0, \cdot + \cdot, \cdot \times \cdot, 0, 1, -1\},$$

avec éventuellement comme constantes tout ou partie des réels constructifs. On peut en outre envisager d'introduire de nouveaux symboles de fonctions pour des fonctions $\mathbb{R}^n \to \mathbb{R}$ bien définies (d'un point de vue constructif) et dont la description est purement algébrique, comme les fonctions semialgébriques continues définies sur $\mathbb{Q}$.

L'*algèbre réelle constructive* n'est pas bien comprise ! D'un point de vue constructif, l'algèbre réelle est *assez éloignée* de la théorie usuelle classique des corps réels clos à la Artin-Schreier-Tarski, dans laquelle on suppose que l'on a un *test de signe*. La plupart des algorithmes de l'algèbre réelle classique requièrent un test de signe et donc ils échouent avec les nombres réels.

L'algèbre réelle peut être vue comme la plus simple des structures o-minimales (cf. [6, 34]). La théorie classique (non algorithmique) des structures o-minimales donne en effet des pseudo-algorithmes qui fonctionneraient correctement si l'on avait un test de signe sur les réels. Et la théorie des structures o-minimales a *a priori* un champ d'application très important en analyse.

Nous proposons pour la théorie dynamique convoitée celle de la structure d'anneau réel clos local archimédien. La théorie des anneaux réels clos est ici présentée sous une forme élémentaire, purement équationnelle, dans le style de [32].

Dans la section 1 nous donnons quelques généralités sur les théories dynamiques. La section 2 questionne les théories dynamiques pour les corps ordonnés *non* discrets [1]. La section 3 aborde le cas des corps réels clos *non* discrets.

Remerciements Nous remercions Michel Coste et Marcus Tressl pour leurs patientes réponses à nos nombreuses questions.

1 Théories géométriques

Cette section fait l'objet d'un article plus développé en préparation, que l'on trouve en : http://hlombardi.free.fr/Theories-geometriques.pdf

Terminologie. Comme nous nous situons en mathématiques constructives il apparaît inévitablement des problèmes terminologiques, du simple fait par exemple qu'en général un même concept classique donne lieu à plusieurs concepts constructifs intéressants non équivalents, mais équivalents en mathématiques classiques.

Nous donnons ci-dessous un petit tableau comparatif entre notre terminologie (en mathématiques constructives) et la terminologie anglaise la plus usuelle (en mathématiques classiques) pour ce qui concerne les théories géométriques. Celle que l'on trouve dans [12, Chapitre D1] et dans [1].

La comparaison est un peu biaisée par le fait que dans les théories dynamiques on n'utilise pas la logique à proprement parler. Ce sont de pures machines de calcul. Ainsi, bien qu'une théorie dynamique finitaire définisse une théorie (du premier ordre) cohérente et bien que toute théorie cohérente advienne de cette façon, il ne s'agit pas des mêmes objets formels. Témoin le fait qu'une théorie cohérente ne fonctionne pas de la même manière avec la logique classique et avec la logique intuitionniste, alors qu'une théorie dynamique est insensible à cette distinction, car structurellement les démonstrations dynamiques sont toujours constructives.

1. Dans ce texte, une négation est mise en italique lorsque l'affirmation correspondante, vraie en mathématiques classiques, implique en mathématiques constructives un principe non constructif bien répertorié, tel que **LPO** ou même **MP**.

Théorie	Theory
dynamique	
purement équationnelle	algebraic
algébrique	Horn
existentiellement rigide	cartesian
existentielle	regular
cohérente	coherent
géométrique	geometric

Théories géométriques	Geometric theories
identiques	equivalent
essentiellement équivalentes	
classiquement essentiellement équivalentes	Morita equivalent

1.1 Théories géométriques du premier ordre

Théories cohérentes

Une *théorie cohérente* $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ est une théorie formelle du premier ordre basée sur le langage $\mathcal{L}$ dans laquelle les axiomes (les éléments de $\mathcal{A}$) sont tous *géométriques*, c'est-à-dire de la forme suivante :

$$A \implies \exists \underline{y^1}\, B_1 \ \vee \ \cdots \ \vee \ \exists \underline{y^m}\, B_m \tag{1.1}$$

où A et les B_j sont des *conjonctions de formules atomiques* du langage $\mathcal{L}$ de la théorie formelle et les $\underline{y^j}$ sont des listes de variables, éventuellement vides.

On dit aussi *théorie géométrique du premier ordre* à la place de théorie cohérente.

Théories dynamiques

Référence prncipale [8]. Dans l'article en question sont introduites les notions de «dyanamical theory» et de «dynamical proof». Voir également l'article [3, Bezem,Coquand 2005] qui décrit un certain nombre d'avantages fournis par cette approche, et les articles précurseurs [22, Prawitz 1971, sections 1.5 et 4.2], [21, Matijasevič 1975] et [13, Lifschitz 1980].

Si $\mathcal{T}$ est une théorie cohérente, la *théorie dynamique* correspondante s'en différencie seulement par un usage extrêmement limité des méthodes de démonstration :

— Premièrement, on n'utilise jamais d'autres formules que les formules atomiques : on n'introduit jamais aucun nouveau prédicat utilisant des connecteurs logiques ou des quantificateurs. Seules sont manipulées des listes de formules atomiques du langage $\mathcal{L}$.

— Deuxièmement, et conformément au point précédent, les axiomes ne sont pas vus comme des formules vraies, mais comme des *règles de déduction* : un axiome tel que (1.1) est utilisé en tant que règle [2] (1.2) :

$$A \ \vdash \ \textsf{Introduire}\ \underline{y^1}\ B_1 \ \ \textsf{ou} \ \ \cdots \ \ \textsf{ou} \ \ \textsf{Introduire}\ \underline{y^m}\ B_m \tag{1.2}$$

(voir l'exemple qui suit, les définitions formelles précises sont données dans [8], on peut les étendre au cas où il y a plusieurs types d'objets comme dans la théorie des modules sur un anneau commutatif avec les objets du type «éléments de l'anneau» et les objets du type «éléments du module»).

2. Ici les conjonctions de formules atomiques A, B_1, …, B_m de (1.1) ont été remplacées par les listes correspondantes de formules atomiques.

— Troisièmement, on ne prouve que des *règles dynamiques*, c'est-à-dire des théorèmes qui sont de la forme des règles de déduction ci-dessus.
— Troisièmement, on ne prouve que des *règles dynamiques*, c'est-à-dire des théorèmes qui sont de la forme des règles de déduction ci-dessus.
— Quatrièmement, la seule manière de prouver une règle dynamique est un calcul arborescent «sans logique». À la racine de l'arbre se trouvent toutes les hypothèses du théorème que l'on veut prouver. L'arbre se développe en appliquant les axiomes selon une pure machinerie de calcul algébrique dans la structure.

Lorsque l'on applique un axiome tel que (1.2), on substitue aux variables libres (x_i) présentes dans la règle des termes arbitraires (t_i) du langage. Si les hypothèses, réécrites avec ces termes, sont déjà prouvées, alors on ouvre des branches de calcul dans chacune desquelles on introduit des variables fraiches correspondant aux variables muettes $\underline{y^k}$ (il faut éventuellement changer leurs noms pour éviter un conflit avec les variables libres présentes dans les termes t_i) et chaque conclusion B_k est valide dans sa branche. On déclare valide une conclusion prouvée à chaque feuille d'un arbre de preuve ainsi construit.

Dans les théories dynamiques avec un prédicat d'égalité, celui-ci doit satisfaire les règles usuelles (relation d'équivalence stable par rapport aux symboles de fonction et aux autres prédicats).

Exemple 1.1. La théorie dynamique $\mathcal{C}\!\mathit{d}$ des corps discrets est basée sur le langage des anneaux commutatifs et elle a pour règles dynamiques, outre celles des anneaux commutatifs, celle des corps discrets :

$$\textsf{CD} \quad \vdash \; x = 0 \quad \textsf{ou} \quad \textsf{Introduire}\; y \;\; xy = 1$$

Pour démontrer la règle dynamique

$$\textsf{ASDZ} \quad xy = 0 \;\vdash\; x = 0 \quad \textsf{ou} \quad y = 0$$

on ouvre deux branches conformément à l'axiome **CD**. Dans la première on a $x = 0$ et la conclusion est prouvée. Dans la deuxième on introduit un paramètre (une variable fraiche) z avec la relation $xz = 1$. Les axiomes des anneaux commutatifs permettent alors de démontrer les égalités $y = 1 \times y = (xz)y = (xy)z = 0 \times z = 0$, et la conclusion est également prouvée.
Ensuite par exemple, on déduit de la règle dynamique précédente la règle algébrique

$$\textsf{Anz} \;\; z^2 = 0 \;\vdash\; z = 0$$

car cette fois-ci aux deux feuilles de l'arbre on a la même conclusion $z = 0$.

La logique remplacée par le calcul

En pratique, démontrer une règle dynamique dans le cadre d'une théorie dynamique suit toujours un raisonnement naturel intuitif et l'on peut voir cette gymnastique comme une version simplifiée de la déduction naturelle de Gentzen. Le symbole **ou** doit être compris comme une abréviation pour «**ou**vrir (des branches dans le calcul)».

Les symboles **ou** et **Introduire** ont été préférés à $\vee$ et $\exists$, pour bien marquer que leur utilisation dans les règles de déduction n'est pas l'utilisation de nouvelles formules construites à partir des formules atomiques. Le symbole $\vdash$ a été préféré à $\vdash$ pour éviter la confusion avec le symbole utilisé pour les relations implicatives dans les treillis distributifs. Notons aussi qu'il n'a pas la même interprétation que le symbole analogue utilisé dans les calculs de séquents à la Gentzen.

Ainsi le langage d'une théorie dynamique ne comporte aucun symbole logique (connecteur ou quantificateur) permettant de construire des formules compliquées à partir des formules atomiques. La logique est remplacée par les symboles $\vdash$, **ou** et **Introduire** et par le séparateur «,», mais ces symboles sont utilisés pour décrire une machinerie de calculs arborescents et non pour former des formules. La partie non logique d'une théorie dynamique est constituée de symboles pour les variables, et de la *signature*, qui contient les symboles pour les sortes, les prédicats et les fonctions (ou lois) définies dans la structure.

Dans la suite, nous remplaçons «**Introduire**» par le symbole moins encombrant «**∃**», plus proche et néanmoins différent du traditionnel «$\exists$».

Collapsus

Une règle dynamique s'appelle une *règle de collapsus* ou *d'effondrement* lorsque le second membre est « le Faux », que l'on note $\bot$. Le symbole $\bot$ doit être rangé avec les formules atomiques et peut être considéré comme (le seul) symbole logique dans les théories dynamiques. On peut aussi voir $\bot$ comme désignant la disjonction vide. Lorsque l'on a prouvé $\bot$, l'univers du discours s'effondre, et toute formule atomique du langage est alors réputée vraie, ou du moins valide. C'est l'application de la règle *ex falso quod libet*, qui est la signification intuitive pertinente du Faux en mathématiques constructives. Ainsi dans les théories dynamiques les règles

$\textsf{Faux}_P \quad \bot \vdash P$

sont valides pour toutes les formules atomiques.

Même si une théorie dynamique ne comporte pas de règle de collapsus, elle admet toujours le modèle réduit à un point [3] où toutes les formules atomiques sont évaluées vraies. Et l'on dit qu'une théorie dynamique s'effondre si toutes les formules atomiques sont valides.

Considérer l'effondrement dans le sens qui vient d'être expliqué, plutôt que dans le sens du pur néant, est seulement une affaire de goût qui ne change rien au fond des choses.

Théories algébriques

Une règle dynamique qui ne contient à droite du $\vdash$ ni **ou**, ni $\exists$ est appelée une *règle algébrique*.

Une théorie dynamique est dite *algébrique* lorsqu'elle ne comporte comme axiomes que des règles algébriques.

L'*algèbre universelle* correspond aux théories algébriques *purement équationnelles*, celles où les seules règles sont des égalités entre termes.

Théories existentielles

Un règle dynamique est dite *existentielle simple* si le second membre (la conclusion) est de la forme $\exists \underline{x}\ A$ où A est une liste finie de formules atomiques.

Structures algébriques dynamiques

Références [8], [14].

Si $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ est une théorie dynamique, une *structure algébrique dynamique de type* $\mathcal{T}$ est donnée par un ensemble G de générateurs et un ensemble R de *relations*. Une relation est par définition une formule atomique $P(\underline{t})$ construite sur le langage $\mathcal{L} \cup G$ avec des termes t_i clos dans ce langage. À une telle relation est associé l'axiome « $\vdash P(\underline{t})$ » de la structure algébrique dynamique.

Exemple 1.2. Par exemple on obtient une structure algébrique dynamique de corps discret

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

en prenant $G = \{\, a, b \,\}$ et $R = \big\{\, 105 = 0,\ a^2 + b^2 - 1 = 0 \,\big\}$. Ce corps discret dynamique correspond à n'importe quel corps de caractéristique 3 ou 5 ou 7 engendré par deux éléments α et β vérifiant $\alpha^2 + \beta^2 = 1$. Outre les règles dynamiques valables dans tous les corps discrets, il y a maintenant celles que l'on obtient en élargissant le langage avec les constantes prises dans G et en ajoutant aux axiomes les relations prises dans R.

Définition 1.3. Soit $\mathbf{A}$ une structure algébrique dynamique. Une règle directe sans hypothèse et sans variable s'appelle un *fait* (dans $\mathbf{A}$). Un fait concerne uniquement des objets définissables syntaxiquement dans la structure.

Dans une structure algébrique dynamique un fait $P(\underline{t})$ est *absolument vrai* s'il est prouvable (c'est-à-dire si la règle « $\vdash P(\underline{t})$ » est valide). Il est *absolument faux*, ou plus justement *catastrophique* si « $P(\underline{t}) \vdash \bot$ » est valide. Intermédiaires entre ces deux cas existent de nombreuses possibilités :

3. S'il y a plusieurs sortes, chaque sorte est réduite à un point.

une structure algébrique dynamique n'a pas un modèle figé unique, mais représente à l'état potentiel toutes les réalisations éventuelles idéales de la structure (cette notion reste volontairement floue). Ajouter un fait catastrophique comme axiome revient à supprimer tous les modèles [4].

Modèles d'une structure algébrique dynamique

On considère une structure algébrique dynamique $\mathbf{A} = \big((G, R), \mathcal{T}\big)$ de type $\mathcal{T}$ (avec une ou plusieurs sortes). Un *modèle de* $\mathbf{A}$ est une structure algébrique usuelle (statique) décrite dans le langage associé à $\mathbf{A}$ et vérifiant les axiomes de $\mathbf{A}$ (ceux de $\mathcal{T}$ et ceux donnés par la présentation de $\mathbf{A}$). Lorsque $\mathbf{A}$ est défini par la présentation vide, on parle de *modèles de* $\mathcal{T}$.

La notion de modèle est donc basée *a priori* sur une notion intuitive de *structure algébrique* à la Bourbaki. Mais ici il s'agit d'un ensemble « naïf » structuré par la donnée de prédicats et de fonctions (au sens naïf) soumis à certains axiomes. La théorie constructive des ensembles à laquelle nous nous référons est *a priori* celle, informelle, de Bishop. S'il s'agit d'une théorie formelle, à la Aczel, à la Martin-Löf, ou à la Voevodsky, il se pourrait que cela ait des conséquences en termes de métathéorèmes (les théorèmes de la théorie des modèles constructive).

Une théorie dynamique $\mathcal{T}' = (\mathcal{L}', \mathcal{A}')$ est dite *extension simple* de $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ si $\mathcal{L} \subseteq \mathcal{L}'$ et $\mathcal{A} \subseteq \mathcal{A}'$.

Définition 1.4. Soit $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ une théorie dynamique et M un modèle de $\mathcal{T}$. On appelle *diagramme positif de M pour $\mathcal{T}$*, une présentation (G, R) de M comme structure algébrique dynamique de type $\mathcal{T}$. En pratique, on peut prendre pour générateurs une constante x_a pour chaque élément a de M et pour relations toutes les formules atomiques closes satisfaites dans M. Un tel diagramme est noté $\mathrm{Diag}(M, \mathcal{T})$. Si $\mathcal{T}'$ est une extension simple de $\mathcal{T}$, on note $\mathcal{T}'(M)$ la structure algébrique dynamique de type $\mathcal{T}'$ et de présentation $\mathrm{Diag}(M, \mathcal{T})$.

1.2 Théories dynamiques essentiellemement équivalentes

Position du problème

Définition 1.5. Deux théories dynamiques sur le même langage sont dites *identiques* si elles prouvent les mêmes règles dynamiques, c'est-à-dire si les axiomes de chacune sont des règles valides dans l'autre. Dans ce cas les modèles sont les mêmes aussi bien en mathématiques constructives qu'en mathématiques classiques.

Définition informelle 1.6. On considère une théorie dynamique $\mathcal{T}$ et une extension simple $\mathcal{T}'$ de $\mathcal{T}$. On dit que $\mathcal{T}'$ est un extension *intuitivement équivalente* à $\mathcal{T}$ si sont vérifiées les deux propriétés suivantes.

1. Si une règle dynamique formulée dans le langage de $\mathcal{T}$ est valide dans $\mathcal{T}'$, alors elle est valide dans $\mathcal{T}$ [5].
2. Pour toute présentation (G, R) dans le langage de $\mathcal{T}$, les structures algébriques dynamiques $\mathbf{A} = \big((G, R), \mathcal{T}\big)$ et $\mathcal{T}'(\mathbf{A}) := \big((G, R), \mathcal{T}'\big)$ ont les mêmes modèles (en mathématiques constructives comme en mathématiques classiques).

Nous donnons maintenant la liste de constructions d'extensions que nous considérons comme fournissant chaque fois une extension intuitivement équivalente d'un point de vue constructif.

1. Ajout de simples abréviations dans le langage.
2. Ajout d'un nouveau prédicat pour la conjonction de prédicats déjà définis (avec les axiomes afférents).
3. Ajout d'un nouveau prédicat pour la disjonction de prédicats déjà définis.
4. Ajout d'un nouveau prédicat Q pour $\exists x P$ (P déjà défini)

4. Dans la variante où le collapsus réduit tout modèle à un singleton : ... revient à n'autoriser que le modèle trivial.

5. La réciproque est claire.

5. Ajout d'un symbole de fonction f dans le cas où une existence unique est valide dans la théorie.
6. Ajout d'une sous-sorte correspondant à $\{\ x \in A \,|\, P\ \}$ pour une sorte A et une formule atomique P dans lequel la variable x est de sorte A.
7. Ajout d'une sorte quotient pour une relation d'équivalence (prouvée dans la théorie dynamique).
8. Ajout d'une sorte produit fini de sortes déjà définies.
9. Ajout d'une sorte somme disjointe finie de sortes déjà définies.

L'idée directrice est celle de la «liberté des définitions» en mathématiques : *rien ne change d'essentiel lorsque l'on rajoute des symboles formels correspondant à des objets bien définis.*

Définition 1.7. On considère une théorie dynamique $\mathcal{T}$ avec égalité.

1. Une extension simple $\mathcal{T}'$ de $\mathcal{T}$ est dite *extension essentiellement équivalente simple de* $\mathcal{T}$ si elle est identique à $\mathcal{T}$ ou si elle est une extension intuitivement équivalente obtenue en application répétée d'ajouts autorisés dans la liste précédente.
2. On dit que $\mathcal{T}$ et $\mathcal{T}'$ sont des théories essentiellement équivalentes si l'on peut trouver une théorie dynamique $\mathcal{T}''$ qui est une extension essentiellement équivalente simple à la fois de $\mathcal{T}$ et de $\mathcal{T}'$, à un renommage éventuel près de certains symboles de sortes, de fonctions et de prédicats dans $\mathcal{T}$ et/ou $\mathcal{T}'$.
3. On dit que *la théorie dynamique* $\mathcal{T}'$ *est une extension de la théorie dynamique* $\mathcal{T}$ si elle est une extension simple d'une théorie essentiellement équivalente à $\mathcal{T}$.

1.3 Extensions conservatives d'une théorie dynamique

Définition 1.8. Dans cette définition on sous-entend que les sortes, prédicats ou symboles de fonctions d'une des deux théories peuvent éventuellement être renommés, le renommage étant bien entendu explicité. On dit que $\mathcal{T}'$ est une *extension conservative de* $\mathcal{T}$ si c'est un extension de $\mathcal{T}$ et si en outre les règles dynamiques formulables dans $\mathcal{T}$ et valides dans $\mathcal{T}'$ sont valides dans $\mathcal{T}$.

Le cas le plus simple est celui des extensions qui sont essentiellement équivalentes.

On a le théorème fondamental 1.9 ci-après (cf. par exemple le théorème 1 dans [8]). Ce théorème est déjà donné pour les théories purement équationnelles dans [22, Prawitz], et ce genre de résultat est omniprésent dans la littérature contemporaine, sous des formes plus ou moins variées. Du moins la démonstration dans [8] est-elle simple et constructive.

Théorème 1.9. (Élimination des coupures, théorème fondamental des théories dynamiques) *Pour ce qui concerne les théories dynamiques du premier ordre, la logique, y compris classique (et en particulier le principe du tiers exclu) ne sert à rien, si ce n'est à raccourcir les preuves. Plus précisément : une règle dynamique est valide dans une théorie dynamique* $\mathcal{T}$ *si, et seulement si, elle est valide dans la théorie cohérente correspondante (celle qui a la même signature et les mêmes axiomes que* $\mathcal{T}$*) : on utilise dans la théorie cohérente les connecteurs, les quantificateurs et la logique classique du premier ordre.*

Théorème 1.10. (Skolémisation) *On considère une théorie dynamique* $\mathcal{T}$*. On note* $\mathcal{T}'$ *la théorie* skolémisée*, où l'on a skolémisé tous les axiomes existentiels en remplaçant les* $\exists$ *par l'introduction de symboles de fonctions. Alors* $\mathcal{T}'$ *est une extension conservative de* $\mathcal{T}$*.*

Une preuve en mathématiques classiques avec axiome du choix consiste à constater que les deux théories ont les mêmes modèles. Une démonstration syntaxique et constructive est obtenue en suivant au plus près Shoenfield dans [31, Section 4.5].

1.4 Théorie des modèles

Dans cet article, les théorèmes ou lemmes de mathématiques classiques qui n'ont pas de démonstration constructive connue, et qui souvent ne peuvent pas en avoir, sont indiqués avec une étoile.

Théorème* 1.11. (Théorème de complétude de Gödel, première forme)
Une structure algébrique dynamique qui ne s'effondre pas admet un modèle non trivial.

Théorème* 1.12. (Théorème de complétude, deuxième forme).
On considère une théorie dynamique $\mathcal{T}$ et une structure algébrique dynamique **A** *de type $\mathcal{T}$. Un fait est prouvable dans* **A** *si, et seulement si, il est satisfait dans tous les modèles de* **A**.

Définition 1.13. Soit une théorie dynamique $\mathcal{T}'$ qui étend une théorie dynamique $\mathcal{T}$. Si toute structure algébrique dynamique de type $\mathcal{T}$ s'effondre dès qu'elle s'effondre en tant que structure algébrique dynamique de type $\mathcal{T}'$, on dit que *$\mathcal{T}$ et $\mathcal{T}'$ s'effondrent simultanément.*

Théorème* 1.14. (Collapsus simultané et modèles non triviaux)
Soit $\mathcal{T}$ une théorie dynamique et $\mathcal{T}'$ une extension qui s'effondre simultanément avec $\mathcal{T}$. Si une structure algébrique dynamique de type $\mathcal{T}$ admet un modèle non trivial, elle admet également un modèle non trivial en tant que structure algébrique dynamique de type $\mathcal{T}'$.

Définition 1.15. Soit une théorie dynamique $\mathcal{T}'$ qui étend une théorie dynamique $\mathcal{T}$. Si une règle algébrique formulable dans $\mathcal{T}$ est valide dans $\mathcal{T}$ dès qu'elle est valide dans $\mathcal{T}'$, on dit que *$\mathcal{T}$ et $\mathcal{T}'$ prouvent les mêmes règles algébriques.*

Notons que prouver les mêmes règles algébriques formulables dans $\mathcal{T}$ revient à prouver les mêmes faits dans toutes les structures algébriques dynamiques de type $\mathcal{T}$. Ceci justifie la terminologie adoptée dans [8] : *$\mathcal{T}$ et $\mathcal{T}'$ prouvent les mêmes faits.*

Cela signifie aussi que les deux théories prouvent les mêmes règles algébriques dans toutes les structures algébriques dynamiques de type $\mathcal{T}$.

Théorème* 1.16. (Théorème de plongement) *On considère une théorie dynamique $\mathcal{T}'$ qui étend une théorie algébrique $\mathcal{T}$ et qui prouve les mêmes règles algébriques. Toute structure algébrique M de type $\mathcal{T}$ est isomorphe à une sous-$\mathcal{T}$-structure d'un produit de modèles de la structure algébrique dynamique $\mathcal{T}'(M)$.*

1.5 Théories géométriques infinitaires

Dans une théorie géométrique infinitaire, on autorise des règles dynamiques qui ont des disjonctions infinies dans le second membre, mais les variables sur lesquelles portent une telle disjonction doivent être en nombre fini, précisées d'avance.

Dans les extensions autorisées pour obtenir des théories intuitivement équivalentes on admet de la même manière l'ajout d'un prédicat représentant une disjonction infinie et l'ajout d'une sorte pour une réunion disjointe infinie.

Remarque. Les articles [1, 33] disent pour l'essentiel qu'en mathématiques classiques, deux théories géométriques sont essentiellement équivalentes si, et seulement si, elles sont Morita-équivalentes. ■

Un théorème de Barr, établi en mathématiques classiques (et impossible à démontrer en mathématiques constructives), dit que pour de telles théories géométriques, tout résultat démontré avec la logique classique peut également être démontré avec la logique constructive. C'est une généralisation du théorème 1.9. Elle se trouve confirmée en pratique, même si l'on n'en a pas de certitude complète du point de vue constructif. Une étude récente du problème est faite par Rathjen dans l'article [25] publié dans le livre [24].

Exemple : éléments nilpotents

Un élément x d'un anneau est nilpotent s'il existe un $n \in \mathbb{N}^+$ tel que $x^n = 0$. Si l'on introduit un prédicat $\mathrm{Z}(x)$ pour « x est nilpotent », il sera soumis aux axiomes naturels suivants :

nil1 $\vdash \mathrm{Z}(0)$
nil2 $\mathrm{Z}(x), \mathrm{Z}(y) \vdash \mathrm{Z}(x+y)$
NIL1 $Z(x) \vdash \exists z\ z(1+x) = 1$
nil3 $\mathrm{Z}(x) \vdash \mathrm{Z}(xy)$
Nil $\mathrm{Z}(x^2) \vdash \mathrm{Z}(x)$

Dans la théorie dynamique correspondante, les seuls termes pour lesquels on pourra démontrer $\mathrm{Z}(t)$ seront ceux pour lesquels on pourra démontrer $t^n = 0$ pour un $n > 0$. Rien ne garantit cependant que dans un modèle de la théorie, le prédicat $\mathrm{Z}(x)$ corresponde bien à « x est nilpotent ».

La seule manière de s'en assurer est d'introduire la règle dynamique infinitaire

NIL $\mathrm{Z}(x) \vdash \bigvee_{n\in\mathbb{N}^+} x^n = 0$

Cette préoccupation est en relation directe avec la dimension de Krull des anneaux commutatifs, qui peut être définie dans le cadre des théories géométriques infinitaires.

2 Théories dynamiques pour les corps ordonnés

2.1 Une théorie dynamique naturelle pour les corps ordonnés discrets

On rappelle ici la théorie dynamique des corps ordonnés discrets $\mathcal{Cod}$ donnée dans [8].

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

Si l'on veut donner un corps ordonné discret dynamique, i.e. une structure algébrique dynamique de type $\mathcal{Cod}$, on ajoute à la signature une présentation par générateurs et relations de la structure algébrique dynamique considérée. Par exemple cela peut être la présentation vide, ou un ensemble dénombrable de générateurs, sans aucune relation, ou encore cela peut être basé sur une structure algébrique existante dans laquelle on demande de préserver certaines relations, par exemple le diagramme positif de la structure. Ainsi tout anneau définit un corps ordonné discret dynamique.

Abréviations

- $x \# 0$ signifie $x^2 > 0$
- $x = y$ signifie $x - y = 0$
- $x > y$ signifie $x - y > 0$
- $x \geqslant y$ signifie $x - y \geqslant 0$
- $x \# y$ signifie $x - y \# 0$
- $x \leqslant y$ signifie $y \geqslant x$

Axiomes

Règles directes

ga0 $\vdash 0 = 0$
ga2 $x = 0, y = 0 \vdash x + y = 0$
gao1 $x = 0 \vdash x \geqslant 0$
gao2 $x \geqslant 0, y \geqslant 0 \vdash x + y \geqslant 0$
aso1 $\vdash 1 > 0$
aso2 $x > 0 \vdash x \geqslant 0$
ac1 $x = 0 \vdash xy = 0$
ao1 $\vdash x^2 \geqslant 0$
ao2 $x \geqslant 0, y \geqslant 0 \vdash xy \geqslant 0$
aso3 $x > 0, y \geqslant 0 \vdash x + y > 0$
aso4 $x > 0, y > 0 \vdash xy > 0$

Collapsus

col$_\#$ $0 > 0 \vdash 1 = 0$ (i.e. $0 \# 0 \vdash 1 = 0$)

Règles de simplification

Gao $x \geqslant 0, x \leqslant 0 \vdash x = 0$ **Iv** $xy = 1 \vdash x \# 0$

Règles dynamiques

IV $x > 0 \vdash \exists y\, xy = 1$ **OT** $\vdash x \geqslant 0$ **ou** $x \leqslant 0$

ED$_\#$ $\vdash x = 0$ **ou** $x \# 0$

Les règles **gao1** et **gao2** expriment, dans le contexte des groupes, la réflexivité et la transitivité de la relation d'ordre (compatible avec la loi de groupe). La règle **Gao** correspond à l'antisymétrie pour la relation d'ordre.

Les règles **ED**$_\#$ et **OT** expriment que l'égalité est discrète et l'ordre total. Elles ne sont pas satisfaites constructivement pour $\mathbb{R}$. Pour les réels de Bishop, la règle **ED**$_\#$ équivaut au principe d'omniscience **LPO** et **OT** équivaut au principe **LLPO**. Notons aussi que le principe « tout élément régulier de $\mathbb{R}$ est inversible » équivaut au principe de Markov [6] **MP**.

Vue la forme sans négation adoptée ici pour le collapsus, l'anneau trivial est un corps ordonné discret, et l'axiome de collapsus **col**$_\#$ est une conséquence de **IV**.

Quelques règles dérivées dans $\mathcal{Cod}$

Quatre règles de simplification valides

Anz $x^2 = 0 \vdash x = 0$ **Aso1** $x > 0, xy \geqslant 0 \vdash y \geqslant 0$

Aonz $c \geqslant 0, x(x^2 + c) \geqslant 0 \vdash x \geqslant 0$ **Aso2** $x \geqslant 0, xy > 0 \vdash y > 0$

Deux règles dynamiques valides

OTF $x + y > 0 \vdash x > 0$ **ou** $y > 0$ **OTF**$^\times$ $xy < 0 \vdash x < 0$ **ou** $y < 0$

Théorème 2.1. *Hormis les règles* **ED**$_\#$ *et* **OT**, *toutes les règles énoncées précédemment sont valides constructivement pour* $\mathbb{R}$, *sans utilisation de l'axiome du choix dépendant.*

Définition 2.2. *(Théories dynamiques plus faibles)*
Théories basées sur le langage des anneaux ordonnés $(\cdot = 0, \cdot \geqslant 0\,; \cdot + \cdot, \cdot \times \cdot, - \cdot, 0, 1)$.

1. La théorie algébrique $\mathcal{Ao}$ des *anneaux ordonnés*. Les axiomes sont ceux des anneaux commutatifs, les règles directes **gao1**, **gao2**, **ao1**, **ao2** et la règle de simplification **Gao**.
2. La théorie dynamique $\mathcal{Ato}$ des *anneaux totalement ordonnés* est obtenue en ajoutant la règle dynamique **OT** à la théorie $\mathcal{Ao}$. La théorie dynamique $\mathcal{Atonz}$ des *anneaux totalement ordonnés réduits* est obtenue en ajoutant la règle dynamique **Anz** à la théorie $\mathcal{Ato}$.

Théories basées sur le langage des corps ordonnés (on ajoute $\cdot > 0$).

3. La théorie directe $\mathcal{Apo}$ des *anneaux proto-ordonnés* (cf. [8]). Les axiomes sont ceux des anneaux commutatifs, toutes les règles directes énoncées pour $\mathcal{Cod}$ (**gao1**, **gao2**, **ao1**, **ao2**, **aso1** à **aso4**) et le collapsus **col**$_\#$.
4. La théorie algébrique $\mathcal{Asonz}$ des *anneaux strictement ordonnés réduits* (*quasi-ordered rings* dans [8]) est obtenue en ajoutant à $\mathcal{Apo}$ les règles de simplification **Gao**, **Aonz**, **Aso1** et **Aso2**.

La théorie directe $\mathcal{Apo}$ est celle dans laquelle le collapsus est le plus clair, directement donné par un certificat algébrique.

6. Suggéré par F. Richman.

Lemme 2.3 ([8, Proposition 3.1]). *Soit* $\mathbf{K}$ *une structure algébrique dynamique de type* $\mathcal{A}po$ *donnée par une présentation* $(G; R_{>0}, R_{\geqslant 0}, R_{=0})$ *avec la signification suivante : G est l'ensemble des générateurs de la structure, $R_{>0}$, $R_{\geqslant 0}$ et $R_{=0}$ sont trois parties de $\mathbb{Z}[G]$, les éléments de $R_{>0}$ (resp. $R_{\geqslant 0}$, $R_{=0}$) sont supposés > 0 (resp. $\geqslant 0$, $= 0$) dans la structure. La structure algébrique dynamique* $\mathbf{K}$ *s'effondre si, et seulement si, on a dans $\mathbb{Z}[G]$ une égalité*

$$s + p + z = 0$$

où s est dans le monoïde multiplicatif engendré par $R_{>0}$, p est dans le cône engendré par $R_{>0} \cup R_{\geqslant 0}$ et z dans l'idéal engendré par $R_{=0}$.

L'égalité $s + p + z = 0$ dans le lemme est appelée un *certificat algébrique d'effondrement* ou encore un *Positivstellensatz*.

2.2 Corps réels clos discrets

On introduit les règles dynamiques suivantes pour les corps réels clos discrets : pour $n \geqslant 2$ et $P_n(x) = \sum_{k=0}^{n} a_k x^k$

$\mathsf{RCF}_n \quad a < b,\ P_n(a)P_n(b) < 0 \ \vdash\ \exists x \left(P_n(x) = 0,\ a < x < b\right)$

Un théorème essentiellement équivalent à cette règle est démontré par Bishop pour le corps $\mathbb{R}$, mais en utilisant l'axiome du choix dépendant.

Définition 2.4. La théorie dynamique $\mathcal{C}rcd$ des *corps réels clos discrets* est obtenue à partir de la théorie $\mathcal{C}od$ en ajoutant les règles dynamiques RCF_n.

Positivstellensätze formels

Le Positivstellensatz formel des mathématiques classiques ([4, Theorem 4.4.2]) admet la version constructive suivante.

Théorème 2.5. (Positivstellensatz formel, 1) [8]

1. *Les théories dynamiques $\mathcal{A}po$, $\mathcal{C}od$ et $\mathcal{C}rcd$ s'effondrent simultanément.*
2. *Les théories dynamiques $\mathcal{A}sonz$, $\mathcal{C}od$ et $\mathcal{C}rcd$ prouvent les mêmes règles algébriques.*

Une conséquence du point *1* en mathématiques classiques (via le théorème 1.14) est qu'un corps $\mathbf{K}$ dans lequel -1 n'est pas une somme de carrés peut être ordonné. En revanche, la seule signification calculatoire connue de ce résultat des mathématiques classiques est que la théorie $\mathcal{C}od(\mathbf{K})$ s'effondre si, et seulement si, -1 est une somme de carrés dans $\mathbf{K}$.

La force démonstrative des Positivstellensätze formels

Les théories dynamiques que nous explorons dans la suite pour décrire les propriétés algébriques des nombres réels sont des extensions de $\mathcal{A}sonz$ (si le prédicat $\cdot > 0$ est présent) ou $\mathcal{A}onz$ (dans le cas contraire). En outre les théories explorées sont toujours plus faibles que $\mathcal{C}rcd$. Et toute règle algébrique valide dans la théorie dynamique $\mathcal{C}rcd$ est valide dans $\mathcal{A}sonz$ (dans $\mathcal{A}onz$ si le prédicat $\cdot > 0$ est absent).

Or $\mathbb{R}$ constitue un modèle constructif de la théorie $\mathcal{A}sonz$ pour le langage basé sur la signature $(\cdot = 0, \cdot > 0, \cdot \geqslant 0\,; \cdot + \cdot, \cdot \times \cdot, - \cdot, 0, 1)$ (théorème 2.1). Ainsi du point de vue des seules règles algébriques, les Positivstellensätze formels nous disent que la théorie $\mathcal{C}rcd$ est entièrement satisfaisante, y compris pour $\mathbb{R}$, qui ne satisfait pourtant ni $\mathsf{ED}_{\#}$ ni OT. Cependant, pour tempérer cette déclaration optimiste, voici le résultat précis. On notera aussi qu'il ne s'applique que pour les règles algébriques, pas pour les autres règles dynamiques.

Théorème 2.6. *Considérons une règle algébrique formulée dans la structure algébrique dynamique* $\mathbf{R} = \mathcal{A}sonz(\mathbb{R})$. *Si les constantes qui interviennent dans la règle font partie d'un sous-corps discret* $\mathbf{R}_0$ *de* $\mathbb{R}$, *pour que la règle soit valide dans* $\mathbf{R}$, *il suffit qu'elle soit valide dans* $\mathcal{C}rcd(\mathbf{R}_0)$.

Positivstellensatz concret

On rappelle tout d'abord le théorème fondamental de Tarski. Pour une démonstration simple, dite à la Cohen-Hormander, voir [4, Section 1.4], ou [8, Lemme 3.12]. Quelques commentaires instructifs se trouvent dans [17, theorems 10 et 11].

Théorème 2.7. *La théorie formelle intuitioniste du premier ordre associée à la théorie dynamique $\mathcal{Crcd}$ admet l'élimination des quantificateurs. Elle est complète et décidable.*

Voici maintenant un théorème équivalent au Positivstellensatz de Krivine-Stengle, énoncé ici dans le langage des structures algébriques dynamiques.

Théorème 2.8. (Positivstellensatz concret) *Soit $\mathbf{K}$ un corps ordonné discret et $\mathbf{R}$ un corps réel clos discret contenant $\mathbf{K}$, (par exemple la clôture réelle de $\mathbf{K}$). Soit $\mathbf{A} = \big((G, Rel), \mathcal{Cod}(\mathbf{K})\big)$ une structure algébrique dynamique avec le système générateur $G = (x_1, \ldots, x_n)$ et où Rel est fini.*

1. *La structure algébrique dynamique $\mathbf{A}$ s'effondre si, et seulement si, il est impossible de trouver un modèle de $\mathbf{A}$ contenu dans $\mathbf{R}$.*
2. *L'effondrement s'il a lieu est donné par un certificat algébrique conformément au point 1 du théorème 2.5 et au lemme 2.3.*
3. *On a un algorithme qui décide si $\mathbf{A}$ s'effondre et qui en cas de réponse négative donne la description d'un système $(\xi_1, \ldots, \xi_n)$ dans $\mathbf{R}^n$ qui satisfait les contraintes données dans les relations Rel.*

Une preuve constructive du théorème 2.8 se trouve dans [8]. Elle est fondée sur le Positivstellensatz formel d'une part et sur le lemme 3.12 de [8], variante du théorème de Tarski. Pour des bornes de complexité voir [15]. Pour la construction de la clôture réelle d'un corps ordonné discret voir [17].

Le théorème 2.8 n'est pas valable sous cette forme générale si l'on prend $\mathbf{K} = \mathbf{R} = \mathbb{R}$ car il n'y a pas de test de signe dans $\mathbb{R}$ et les algorithmes qui explicitent le théorème [7] utilisent de manière cruciale ce test de signe.

Voici un petit exemple des problèmes auxquels on se heurte. Sur $\mathbb{R}$, comme sur un anneau local arbitraire dans lequel $x \# 0$ désigne le prédicat d'inversibilité, on a l'équivalence

$$\exists y \;\; x^2 y = x \iff x = 0 \;\vee\; x \# 0. \tag{2.1}$$

Ce cas simple d'élimination du quantificateur $\exists$ montre que l'on aboutit dans les calculs à des impasses du point de vue de la décidabilité, puisque « $x = 0$ ou $x \# 0$ » est indécidable dans $\mathbb{R}$.

Néanmoins, dans la section finale de l'article [10], on trouve une forme constructive entièrement satisfaisante pour le 17e problème de Hilbert sur $\mathbb{R}$. Et d'autres cas de Positivstellensätze constructivement prouvables sur $\mathbb{R}$ sont également traités.

2.3 Corps ordonnés *non* discrets

En première approximation, et en suivant une suggestion de Heyting, on pourrait choisir comme théorie formelle du premier ordre pour les propriétés algébriques de $\mathbb{R}$ la théorie $\mathcal{Asonz}$ (vue comme théorie du premier ordre) à laquelle on ajoute les axiomes géométriques **IV** et **OTF** ainsi que l'axiome **HOF** non géométrique, donc indésirable.

HOF $\quad (x > 0 \Rightarrow 1 = 0) \Rightarrow x \leqslant 0$

Cela revient à remplacer dans la théorie $\mathcal{Cod}$, les axiomes $\mathbf{ED}_{\#}$ et **OT** par les axiomes **OTF** et **HOF**. On a alors une structure d'anneau local, car la règle **OTF** implique que pour tout x, x ou $1 - x$ est inversible [8]. Dans ce cadre l'axiome **HOF** signifie que le radical de Jacobson est réduit à 0.

7. Ces algorithmes sont fournis par la preuve constructive du théorème.
8. Pour le traitement constructif des anneaux locaux, du radical de Jacobson et des corps de Heyting voir par exemple [16, section IX-1]

Notons que l'axiome **HOF** formulable au premier ordre, même s'il n'entre pas dans le cadre des théories dynamiques, est satisfait de manière indirecte (comme métathéorème) sous la forme suivante : *dans une structure algébrique dynamique de type $\mathcal{A}sonz$, si un terme clos t vérifie $t > 0 \vdash \bot$, alors il vérifie aussi $\vdash t \leqslant 0$.* Cela résulte du Positivstellensatz formel.

À vrai dire on a même : si un terme clos t vérifie $t \geqslant 0 \vdash \bot$, alors il vérifie aussi $\vdash t < 0$. Cela signifie que le principe de Markov, qui s'exprime sur $\mathbb{R}$ par l'implication $\neg\neg(t < 0) \Rightarrow t < 0$ vaut comme métathéorème.

Outre le caractère indésirable de **HOF**, la théorie formelle ainsi définie présente un inconvénient majeur, qui est de ne pas pouvoir démontrer l'existence de nombreuses fonctions « rationnelles » comme la borne supérieure de deux éléments : voir à ce sujet [5].

Définition de la théorie purement équationnelle $\mathcal{A}fr$

Définition 2.9. Une première approximation de la théorie des corps ordonnés *non* discrets est donnée par la théorie des *anneaux fortement réticulés* (f-rings en anglais) définie comme suit.

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

Abréviations

Symboles fonctionnels

- $x \wedge y$ signifie $-(-x \vee -y)$
- $|x|$ signifie $x \vee -x$
- x^+ signifie $x \vee 0$
- x^- signifie $-x \vee 0$

Prédicats

- $x = y$ signifie $x - y = 0$
- $x \leqslant y$ signifie $y \geqslant x$
- $x \geqslant y$ signifie $x \vee y = x$

Axiomes

Règles des anneaux commutatifs

ga0 $\vdash 0 = 0$

ga2 $x = 0, y = 0 \vdash x + y = 0$

ac1 $x = 0 \vdash xy = 0$

Règles de compatibilité de $\vee$ avec l'égalité

sup1$_=$ $x = 0 \vdash (x + y) \vee z = y \vee z$

sup2$_=$ $x = 0 \vdash y \vee (x + z) = y \vee z$

Règles équationnelles

sdt1 $\vdash x \vee x = x$

sdt2 $\vdash x \vee y = y \vee x$

sdt3 $\vdash (x \vee y) \vee z = x \vee (y \vee z)$

grl $\vdash x + (y \vee z) = (x + y) \vee (x + z)$

afr $\vdash x^+ (y \vee z) = (x^+ y) \vee (x^+ z)$

Théorème de plongement pour les anneaux fortement réticulés

Définition 2.10. La théorie dynamique $\mathcal{A}tosup$ des *anneaux totalement ordonnés avec sup* est la théorie dynamique obtenue à partir de $\mathcal{A}fr$ en ajoutant comme axiome la règle dynamique **OT** (disant que l'ordre est total).

OT $\vdash x \geqslant 0$ **ou** $x \leqslant 0$

Vu l'existence unique du sup dans un anneau totalement ordonné, les théories $\mathcal{A}to$ et $\mathcal{A}tosup$ sont essentiellement équivalentes.

Théorème 2.11. *Les théories $\mathcal{A}fr$ et $\mathcal{A}tosup$ prouvent les mêmes règles algébriques.*

La traduction en mathématiques classiques est que tout anneau fortement réticulé est isomorphe à un sous-truc d'un produit d'anneaux totalement ordonnés.

Une première théorie $\mathcal{Co0}$ pour les corps ordonnés *non* discrets

Définition 2.12. Une théorie dynamique pour les corps ordonnés notée $\mathcal{Co0}$ est obtenue en ajoutant à la théorie $\mathcal{Afr}$ le symbole de relation $\cdot > 0$ ainsi que les axiomes suivants.

aso1	$\vdash\ 1 > 0$	**aso3**	$x > 0,\ y \geqslant 0\ \vdash\ x + y > 0$
aso2	$x > 0\ \vdash\ x \geqslant 0$	**aso4**	$x > 0,\ y > 0\ \vdash\ xy > 0$
Aso1	$x > 0,\ xy \geqslant 0\ \vdash\ y \geqslant 0$	**Aso2**	$x \geqslant 0,\ xy > 0\ \vdash\ y > 0$
Aonz	$c \geqslant 0,\ x(x^2 + c) \geqslant 0\ \vdash\ x \geqslant 0$	**Iv**	$xy = 1\ \vdash\ x^2 > 0$
col$_{\#}$	$0 > 0\ \vdash\ 1 = 0$	**OTF**	$x + y > 0\ \vdash\ x > 0$ **ou** $y > 0$
IV	$x > 0\ \vdash\ \exists y\, xy = 1$		

Si l'on omet les règles **IV** et **OTF** cela définit la théorie algébrique $\mathcal{Asr}$ des *anneaux strictement réticulés*. Si l'on omet seulement la règle **OTF** cela définit la théorie dynamique $\mathcal{Arftr}$ des *anneaux réticulés fortement réels*.

Ajout de fractions bien définies.

Certaines fonctions «rationnelles», comme la fraction $f = \dfrac{xy(x+y)}{x^2+y^2}$, bien définies sur $\mathbb{R}$, se semblent pas définissables dans $\mathcal{Co0}$. Cette fraction est du type $z = u/v$ avec $u^2 \leqslant v^3$. Elle est caractérisée par les relations $zv = u$ et $|z|^2 \leqslant |v|$. Or les règles dynamiques suivantes sont satisfaites pour $\mathbb{R}$, et aussi bien pour les corps réels clos discrets :

$$\textbf{FRAC}_n \quad |u|^n \leqslant |v|^{n+1}\ \vdash\ \exists z\ (zv = u,\ |z|^n \leqslant |v|) \qquad (n \geqslant 1)$$

L'existence de la fraction f résulte de la règle $\textbf{FRAC}_2$.

D'où la théorie dynamique suivante pour les corps ordonnés *non* discrets.

Définition 2.13. Une théorie dynamique pour les corps ordonnés notée $\mathcal{Co}$ est obtenue en ajoutant à la théorie $\mathcal{Co0}$ les règles $\textbf{FRAC}_n$.

Si l'on ajoute l'axiome $\textbf{ED}_{\#}$ à la théorie $\mathcal{Co0}$ ou à $\mathcal{Co}$, la règle **OT** est valide, donc on retrouve une théorie essentiellement équivalente à $\mathcal{Cod}$.

Exemples 2.14. De nombreux sous-corps naturels de $\mathbb{R}$ sont *non* discrets, par exemple le corps énumérable $\mathbb{R}_{\textbf{PR}}$ des réels calculables en temps primitif récursif, ou le corps énumérable des réels calculables en temps polynomial, ou encore le corps *non* énumérable des réels récursifs. Une théorie dynamique satisfaisante pour les propriétés algébriques des nombres réels devrait très probablement accepter pour modèles ces sous-corps naturels de $\mathbb{R}$. Notons que le caractère complet de $\mathbb{R}$ semble relever plus de l'analyse que de l'algèbre.
Notons aussi que l'on ne connait pas en mathématiques constructives de corps ordonné «de Heyting» qui soit non archimédien. En fait le «corps» des séries de Puiseux sur $\mathbb{R}$ ne semble pas satisfaire **OTF** (pour n'importe quelle tentative de définition raisonnable pour la relation d'ordre).

3 Corps ordonnés réels clos *non* discrets

3.1 Le principe de prolongement par continuité

On note $\mathbf{R}_{\mathrm{a}}$ le corps des réels algébriques. On rappelle que $\mathbf{R}_{\mathrm{a}}$ est un corps réel clos discret au sens constructif. La propriété de completion de $\mathbb{R}$ s'exprime naturellement sous la forme suivante, sans interférence avec l'axiome du choix dépendant.

Théorème 3.1. *Si une fonction $f : \mathbb{Q}^n \to \mathbb{R}$ est uniformément continue sur tout borné elle se prolonge de manière unique en une fonction $\widetilde{f} : \mathbb{R}^n \to \mathbb{R}$ uniformément continue sur tout borné.*

Ce théorème est un théorème d'analyse et ne peut pas s'exprimer directement dans le cadre d'une théorie dynamique qui vise les propriétés algébriques de $\mathbb{R}$, car la propriété «être uniformément continue» n'est pas géométrique. Néanmoins c'est essentiellement ce théorème qui nous guide dans notre quête. Nous remplacerons pour cela la propriété «être uniformément continue» par une formulation où la continuité uniforme est contrôlée a priori et ne cache plus de $\forall\exists\forall$.

Tout d'abord nous rappelons que la continuité uniforme sur tout borné d'une fonction semialgébrique continue $\mathbf{R}_{\mathrm{a}}^n \to \mathbf{R}_{\mathrm{a}}$ est contrôlée à la Łojasiewicz précisément comme suit.

Lemme 3.2. *Soit* $\mathbf{R}$ *un corps réel clos discret et soit* $f : \mathbf{R}^n \to \mathbf{R}$ *une fonction semialgébrique continue. Alors* f *possède un module de continuité uniforme sur tout borné qui s'exprime à la Łojasiewicz comme suit (avec un* $c \in \mathbf{R}$ *et* k, ℓ *entiers* $\geqslant 1$*)*

$$\forall \underline{\xi}, \underline{\xi}' \in \mathbf{R}^n \ \left|f(\underline{\xi}) - f(\underline{\xi}')\right|^\ell \leqslant |c| \ \left(1 + \| \underline{\xi} \|^2 + \| \underline{\xi}' \|^2\right)^k \| \underline{\xi} - \underline{\xi}' \|^2. \tag{3.1}$$

Démonstration. Le corollaire 2.6.7 de [4] a pour conséquence une inégalité de ce type, sans le facteur $\left(1+\| \underline{\xi} \|^2+\| \underline{\xi}' \|^2\right)^k$, pour une fonction semialgébrique continue sur un fermé borné semialgébrique K. On se ramène à ce cas «compact» en divisant f par une puissance suffisante de $1+\| \underline{\xi} \|^2+\| \underline{\xi}' \|^2$, la nouvelle fonction tend vers 0 à l'infini et peut être vue comme une fonction semialgébrique continue sur $[-1, 1]^n$ (nulle sur le bord). □

Dans le cas d'un sous-corps de $\mathbb{R}$ on ne peut pas accepter, d'un point de vue constructif, la définition usuelle des fonctions semialgébriques continues car elle est donnée pour le cas d'un corps réel clos discret et suppose implicitement l'utilisation d'un test de signe. Nous proposons donc la définition suivante, qui n'utilise aucun test de signe.

Définition 3.3. Soit $\mathbf{R}$ un sous-corps de $\mathbb{R}$. Une fonction $f : \mathbf{R}^n \to \mathbf{R}$ est dite *semialgébrique continue* si elle satisfait les deux propriétés suivantes.

1. La fonction f est algébrique sur $\mathbf{R}[x_1, \ldots, x_n] = \mathbf{R}[\underline{x}]$: précisément, on a un polynôme $g = \sum_{k=0}^m g_k(\underline{x}) y^k \in \mathbf{R}[\underline{x}, y]$, avec au moins un des coefficients d'un $g_k(\underline{x})$ inversible, tel que $g(\underline{\xi}, f(\underline{\xi})) = 0$ pour tout $(\underline{\xi}) \in \mathbf{R}^n$.
2. La fonction f possède un module de continuité uniforme sur tout borné à la Łojasiewicz, donné par une inégalité (3.1) comme dans le lemme 3.2.

Cette définition est légitime pour le corps $\mathbb{R}$ car
— elle est valable en mathématiques classiques,
— elle a une signification constructive claire,
— les fonctions continues qui prolongent par continuité les fonctions semialgébriques continues $\mathbf{R}_{\mathrm{a}}^n \to \mathbf{R}_{\mathrm{a}}$ satisfont bien la définition.

On sera assez satisfait d'une théorie dynamique pour les propriétés algébriques de $\mathbb{R}$ si les axiomes permettent de capturer dans la théorie toutes les fonctions répondant à la définition 3.3. Le problème ici revient donc à algébriser cette définition ! La section 3.2 essaie de préciser ce point.

En outre il se pose la question légitime suivante.

Question 3.4. Si une fonction $f : \mathbb{R}^n \to \mathbb{R}$ est algébrique sur $\mathbb{R}[\underline{x}]$ (point *1* de la définition 3.3) et si elle est uniformément continue sur tout borné, est-ce qu'elle possède un module de continuité uniforme à la Łojasiewicz, comme dans le lemme 3.2 ?

NB : la réponse est positive en mathématiques classiques, mais elle semble nettement plus délicate en mathématiques constructives.

3.2 Théories dynamiques raisonnables pour l'algèbre des nombres réels

Voici maintenant les propriétés que nous avons en vue pour une théorie dynamique $\mathcal{C}rc$ des corps réels clos (*non* discrets), décrites ici de manière plutôt informelle.

Propriétés attendues 3.5.

1. La théorie $\mathcal{C}rc$ est une extension de $\mathcal{C}o$.

2. Le corps $\mathbb{R}$ est un modèle constructif de $\mathcal{C}rc$.
3. La théorie $\mathcal{C}rc$ devient essentiellement équivalente à $\mathcal{C}rc\acute{d}$ lorsqu'on lui ajoute l'axiome $\mathbf{ED}_{\#}$.
4. Tous les symboles de fonction de $\mathcal{C}rc$ définissent sur $\mathbb{R}$ des fonctions semialgébriques continues de leurs variables (définition 3.3).
5. Le langage de $\mathcal{C}rc$ est énuméré de manière naturelle et dans ce cadre les axiomes sont décidables de manière primitive récursive.
6. Les fonctions semialgébriques continues $\mathbf{R}_{\mathrm{a}}^n \to \mathbf{R}_{\mathrm{a}}$ sont définissables dans le langage de $\mathcal{C}rc$ et les règles algébriques qu'elles satisfont sont valides dans la théorie.
7. Des principes de prolongement par continuité (les plus larges possibles) sont satisfaits sous une forme convenable dans la théorie dynamique.
8. Des principes de recollement (les plus larges possibles) pour des fonctions définies sur un recouvrement fini par des ouverts semialgébriques, ou par des fermés semialgébriques, sont satisfaits sous une forme convenable dans la théorie dynamique.
9. Toute fonction semialgébrique continue $\mathbb{R}^n \to \mathbb{R}$ peut s'exprimer au moyen d'un terme de $\mathcal{C}rc(\mathbb{R})$.

Le point *4* est facultatif. Le point *5* peut être sujet à discussion, et le point *9* semble difficile à atteindre (c'est le Graal). Une manière un peu brutale d'obtenir une réponse relativement satisfaisante est de prendre au sérieux le point *6* ci-dessus. Voici ce que cela donne.

Définition 3.6. La théorie dynamique $\mathcal{C}rc1$ est obtenue à partir de la théorie dynamique $\mathcal{C}o0$ en ajoutant un symbole de fonction et des axiomes convenables pour chaque fonction semialgébrique continue $f : \mathbf{R}_{\mathrm{a}}^n \to \mathbf{R}_{\mathrm{a}}$. Plus précisément on procède comme suit. On commence par ajouter le diagramme positif du corps $\mathbf{R}_{\mathrm{a}}$ dans la théorie dynamique $\mathcal{C}o0$. Ensuite on note que l'ensemble des fonctions semialgébriques continues définies sur $\mathbf{R}_{\mathrm{a}}$ peut être énuméré de façon explicite. Par exemple d'après le théorème de finitude, le graphe G_f de la fonction f peut être décrit comme l'ensemble des zéros d'une *fonction semipolynôme* $F : \mathbf{R}_{\mathrm{a}}^{n+1} \to \mathbf{R}_{\mathrm{a}}$ écrite sous la forme

$$\sup_i (\inf_{ij} p_{ij}) \quad \text{où } p_{ij} \in \mathbf{R}_{\mathrm{a}}[x_1, \ldots, x_n, y]$$

On sait décider si un tel graphe est celui d'une fonction semialgébrique continue. Chaque fois qu'une telle fonction semipolynôme F définit une fonction semialgébrique continue, nous introduisons un symbole de fonction fsa_F avec l'axiome correspondant :

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

Enfin, pour un terme arbitraire t avec n variables libres ($n \geqslant 1$) dans le langage ainsi défini, lorsque ce terme définit la fonction identiquement nulle sur $\mathbf{R}_{\mathrm{a}}^n$, on introduit l'axiome correspondant $\vdash t = 0$.

Naturellement, une telle théorie dynamique semble a priori difficile à pratiquer d'un point de vue concret. Nous verrons cependant qu'une manière plus naturelle, que nous proposons par la suite, aboutit probablement à une théorie essentiellement équivalente à $\mathcal{C}rc1$. Ceci est étroitement lié à la théorie des anneaux réels clos et à sa réécriture sous forme concrète dans [32].

3.3 Rappels concernant les racines virtuelles

Références [11, 7, 2, 9].

Lemme 3.7.

1. *Une fonction continue strictement monotone $f : [a, b] \to \mathbb{R}$ ($a \leqslant b \in \mathbb{R}$) atteint son minimum en valeur absolue en un unique $x \in [a, b]$. Nous notons $\mathrm{R}(a, b, f)$ ce réel. On a $(x - a)(x - b)f(x) = 0$, et x est l'unique réel vérifiant le système d'inégalités suivant, où $\Delta = f(b) - f(a)$:*

- $a \leqslant x \leqslant b$
- $(x-a)f(a)\Delta \leqslant 0$
- $(x-b)f(b)\Delta \leqslant 0$
- $(x-a)f(x)\Delta \leqslant 0$
- $(x-b)f(x)\Delta \leqslant 0$

2. *Si $f : [a,+\infty[\to \mathbb{R}$ est une fonction continue strictement croissante qui atteint une valeur > 0, alors elle atteint son minimum en valeur absolue en un unique $x \in [a,+\infty[$. Nous notons $\mathrm{R}(a,+\infty,f)$ ce réel. On a $(x-a)f(x) = 0$, et x est l'unique réel vérifiant le système d'inégalités suivant :*
   - $a \leqslant x$
   - $(x-a)f(a) \leqslant 0$
   - $(x-a)f(x) \leqslant 0$
   - $f(x) \geqslant 0$
3. *Des énoncés analogues au précédent, laissés au lecteur, pour une fonction continue strictement monotone $f :]-\infty, a] \to \mathbb{R}$.*

Ce lemme est également valable pour un corps réel clos discret $\mathbf{R}$ *si f est une fonction semialgébrique continue.*

Pour un polynôme f unitaire de degré d, nous notons $f^{[k]}$ la dérivée k-ème de f divisée par son coefficient dominant $(0 \leqslant k < d)$: c'est un polynôme unitaire de degré $d-k$.

Proposition et définition 3.8. *Soit* $\mathbf{R}$ *un corps réel clos discret ou le corps $\mathbb{R}$. Pour tout polynôme unitaire*

$$f(X) = X^d - (a_{d-1}X^{d-1} + \cdots + a_1X + a_0) \quad (d \geqslant 1)$$

on définit les fonctions racines virtuelles de f

$$\rho_{d,j}(f) = \rho_{d,j}(a_{d-1}, \ldots, a_0)$$

pour $1 \leqslant j \leqslant d$ par récurrence sur d : (on abrège $\rho_{k,j}(f^{[d-k]})$ en $\rho_{k,j}$)

— $\rho_{1,1}(X-a) = \rho_{1,1}(a) := a$;
— $\rho_{d,j} := \mathrm{R}(\rho_{d-1,j-1}, \rho_{d-1,j}, f)$ *pour $1 \leqslant j \leqslant d \leqslant 2$;*

(on a posé par convention $\rho_{d,0} = -\infty$ et $\rho_{d,d+1} = +\infty$ pour tout $d \geqslant 1$).

Cette proposition se démontre simultanément avec les points 3d et 3e du théorème qui suit.

Théorème 3.9. (Quelques propriétés des racines virtuelles, [11, 7]) *Soit* $\mathbf{R}$ *un corps réel clos discret ou le corps $\mathbb{R}$.*

1. *Vu le lemme 3.7, pour un f donné de degré d, les $\frac{d(d+1)}{2}$ réels $\rho_{k,j}(f^{[d-k]})$, sont définis par un système d'inégalités larges.*
2. *Chaque fonction $\rho_{d,j} : \mathbf{R}^d \to \mathbf{R}$ est uniformément continue sur toute boule*[9] $\mathrm{B}_{d,M}$.
3. *Soit f unitaire de degré d, on note $\widetilde{f} = \prod_{j=1}^{d}(X - \rho_{d,j}(f))$ et $f^\star = \prod_{j=0}^{d-1} f^{[j]}$.*
   On utilise les conventions $\rho_{d,0}(f) = (-1)^d\infty$ et $\rho_{d,d+1}(f) = +\infty$.
   Dans la suite, on fixe f et on note $\rho_{\delta,j} = \rho_{\delta,j}(f^{[d-\delta]})$ pour $1 \leqslant j \leqslant \delta \leqslant d$.
   (a) *On a $\rho_{d,1} \leqslant \rho_{d-1,1} \leqslant \rho_{d,2} \leqslant \rho_{d-1,2} \leqslant \cdots \leqslant \rho_{d,d-1} \leqslant \rho_{d-1,d-1} \leqslant \rho_{d,d}$.*
   (b) *Si $d \geqslant 2$ et $f = X^d - a$, alors $\rho_{d,d} = \sqrt[d]{a^+}$; et pour d impair, $\rho_{d,1} + \rho_{d,d} = \sqrt[d]{a}$.*
   (c) *Si $f = \prod_{i=1}^{d}(X - \xi_i)$ pour des $\xi_i \in \mathbf{R}$, alors $\widetilde{f} = f$. En conséquence $\rho_{d,1} = \wedge_i \xi_i$, $\rho_{d,d} = \vee_i \xi_i$ et $\rho_{d,k} = \wedge_{J \subseteq [\![1..d]\!], \#J=k}(\vee_{i \in J} \xi_i)$.*
   (d) *Si $\rho_{d-1,j} < \rho_{d-1,j+1}$, $(0 \leqslant j \leqslant d-1)$, alors f est strictement monotone sur l'intervalle, croissante si $d-j$ impair, décroissante sinon.*
   (e) *Si $\rho_{d,j} < \xi < \rho_{d,j+1}$, $(0 \leqslant j \leqslant d)$, alors $(-1)^{d-j}f(\xi) > 0$.*

9. $\mathrm{B}_{d,M} := \{\ (a_{d-1}, \ldots, a_0) \mid \sum_i a_i^2 \leqslant M\ \}$, $(M > 0)$. La continuité peut être donnée sous forme complètement explicite à la Łojasiewicz.

(f) *Les zéros de f sont des zéros de $\widetilde{f}$, avec une multiplicité supérieure ou égale dans $\widetilde{f}$. Plus précisément :*
- *Si $f(\xi)=0$, alors $\widetilde{f}(\xi)=0$;*
- *Si $\widetilde{f}(\xi)\#0$, alors $f(\xi)\#0$;*
- *Si $f^{[j]}(\xi)=0$ pour $j\in[\![1..k]\!]$, alors $\widetilde{f}^{[j]}(\xi)=0$ pour $j\in[\![1..k]\!]$;*
- *Si $f^{[j]}(\xi)=0$ pour $j\in[\![1..k]\!]$ et $\widetilde{f}^{[k+1]}(\xi)\#0$, alors $f^{[k+1]}(\xi)\#0$.*

(g) *Chaque $\rho_{d,j}$ est un zéro de $f^\star$; le polynôme $\widetilde{f}$ divise $(f^\star)^d$.*

(h) (Compte de Budan Fourier) *Soit $a\in\mathbf{R}$ tel que les $f^{[k]}(a)\#0$ pour $0\leqslant k\leqslant d$, et soit r le nombre de changements de signes dans la suite des $f^{[k]}(a)$ $(k=d,\dots,0)$, $(r\in[\![0..d]\!])$. Alors $\rho_{d,d-r}<a<\rho_{d,d-r+1}$.*

(i) (Théorème de la valeur intermédiaire)
Si $a<b$ et $f(a)f(b)<0$, on a $\prod_{j=1}^d f(\mu_j)=0$, où $\boxed{\mu_j=a\vee(b\wedge\rho_{d,j})}$.
Cas particuliers.
- *Si d est impair, alors $\prod_{j=1}^d f(\rho_{d,j})=0$.*
- *Si $0\leqslant k<\ell\leqslant d$ et $f(\rho_{d-1,k})f(\rho_{d-1,\ell})<0$, alors $\prod_{j=k}^{\ell-1} f(\rho_{d,j})=0$.*
- *Si, selon le point 3h on a $\rho_{d,k}<a<\rho_{d,k+1}<b<\rho_{d,k+2}$, alors $f(\rho_{d,k+1})=0$.*

(j) (Théorème des valeurs extrema) *Le polynôme unitaire f atteint sa borne supérieure et sa borne inférieure sur tout intervalle fermé borné au sens précis suivant : si $a<b$, on a*

$$\sup_{\xi\in[a,b]} f(\xi)=f(a)\vee f(b)\vee\sup_{j=1}^{d-1} f(\nu_j)\quad\text{où}\quad\boxed{\nu_j=a\vee(b\wedge\rho_{d-1,j})},$$
$$\inf_{\xi\in[a,b]} f(\xi)=f(a)\wedge f(b)\wedge\inf_{j=1}^{d-1} f(\nu_j)\,.$$

Si f est de signe strict constant ε sur $[a,b]$, on a $\inf_{\xi\in[a,b]}\big(\varepsilon\,f(\xi)\big)>0$.

(k) (Théorème du minimum en valeur absolue et de la non valeur intermédiaire) *Si $a<b$, on a*

$$\inf_{\xi\in[a,b]}|f(\xi)|=|f(a)|\wedge|f(b)|\wedge\inf_{j=1}^{d}|f(\mu_j)|\,.$$

En outre, si le second membre est >0, f est de signe constant sur $[a,b]$.

(l) (Une borne) *Si $f(x)=x^d+\sum_{k=0}^{d-1}a_kx^k$, on a $|\rho_{d,j}|\leqslant\sup_{k=0}^d(1+|a_k|)$.*

Un résultat à la Pierce-Birkhoff

On appelle *fonction polyracine* une fonction $\mathbf{R}^m\to\mathbf{R}$ qui peut s'écrire sous la forme $\rho_{d,j}(f_1,\dots,f_d)$ pour des entiers $1\leqslant j\leqslant d$ et des polynômes $f_j\in\mathbf{R}[x_1,\dots,x_m]$.

Théorème 3.10. ([11, Theorem 6.4]) *Soit $\mathbf{R}$ un corps réel clos discret et soit $g:\mathbf{R}^m\to\mathbf{R}$ une fonction semialgébrique continue entière sur l'anneau $\mathbf{R}[x_1,\dots,x_m]$ (vu comme un anneau de fonctions). Alors g est une combinaison par $\vee$, $\wedge$ et $+$ de fonctions polyracines $\mathbf{R}^m\to\mathbf{R}$. Plus précisément, si $g(\underline{x})$ annule le polynôme Y-unitaire $P(Y,\underline{x})$ de degré d, elle s'exprime comme sup-inf combinaison de fonctions de la forme*

$$\rho_{d,j}(P)+\sqrt[r]{R_\ell^+\cdot\big(1+\|\,\underline{x}\,\|^2\big)^s}\tag{3.2}$$

pour des $R_\ell\in\mathbf{R}[x_1,\dots,x_m]$ (le deuxième terme dans la somme (3.2) est aussi une fonction polyracine, voir le point 3b du théorème 3.9).

Remarque. Lorsque la fonction g est polynomiale par morceaux, elle annule un polynôme unitaire $P(Y)=\prod_{i=1}^d(Y-f_i)$ pour des $f_i\in\mathbf{R}[x_1,\dots,x_m]$. Dans l'expression obtenue en (3.2) pour g, c'est l'inégalité de Łojasiewicz qui est responsable de l'extraction de racine r-ème dans la formule. ∎

3.4 Corps ordonnés avec racines virtuelles

Les théories dynamiques $\mathcal{C}or\mathcal{v}$ et $\mathcal{C}o0r\mathcal{v}$

Définition 3.11.

1. La théorie dynamique $\mathcal{C}or\mathcal{v}$ des *corps ordonnés avec racines virtuelles* est obtenue comme suit à partir de la théorie dynamique $\mathcal{C}o$.
   — Pour $1 \leqslant j \leqslant d$ dans $\mathbb{N}$, on ajoute un symbole de fonction $\rho_{d,j}$ d'arité d ;
   — on ajoute comme axiomes les inégalités décrites dans le point 1 du théorème 3.9.
2. La théorie dynamique $\mathcal{C}o0r\mathcal{v}$ est obtenue de la même manière à partir de la théorie $\mathcal{C}o0$.

La théorie $\mathcal{C}rc\mathcal{d}$ est essentiellement équivalente à la théorie obtenue en ajoutant à $\mathcal{C}o0r\mathcal{v}$ l'axiome $\mathbf{ED}_{\#}$.

Anneaux fortement réticulés avec racines virtuelles

Définition 3.12. La théorie purement équationnelle $\mathcal{A}fr\mathcal{rv}$ des *anneaux fortement réticulés avec racines virtuelles* est obtenue à partir de la théorie algébrique $\mathcal{A}f\mathcal{r}$ de la même manière que la théorie $\mathcal{C}or\mathcal{v}$ est obtenue à partir de la théorie $\mathcal{C}o$ (définition 3.11). En outre on ajoute la règle $\mathbf{vrsup} \vdash \rho_{2,2}(a+b,-ab) = a \vee b$.

Lemme 3.13.

1. *Un anneau fortement réticulé avec racines virtuelles est réduit.*
2. *Un anneau intègre totalement ordonné avec racines virtuelles est intégralement clos et son corps de fractions est réel clos discret.*

Anneaux de Pierce-Birkhoff

Définition 3.14. Soit $\mathbf{A}$ un anneau, ou plus généralement une présentation dans le langage des anneaux fortement réticulés.

1. L'anneau AFRNZ($\mathbf{A}$) est l'*anneau fortement réticulé réduit engendré par* $\mathbf{A}$.
2. L'anneau AFRRV($\mathbf{A}$) est l'*anneau fortement réticulé avec racines virtuelles engendré par* $\mathbf{A}$.
3. L'anneau PPM($\mathbf{A}$) est défini comme le sous-anneau de AFRRV($\mathbf{A}$) formé par les éléments x qui annulent un polynôme $\prod_{i=1}^{k}(X - a_i)$ pour des $a_i \in \mathbf{A}$.
4. Un anneau $\mathbf{A}$ est appelé un *anneau de Pierce-Birkhoff* lorsque le morphisme naturel AFRNZ($\mathbf{A}$) $\to$ PPM($\mathbf{A}$) est un isomorphisme.

Question 3.15.
1) En mathématiques classiques, la définition d'un anneau de Pierce-Birkhoff donnée ci-dessus coïncide-t-elle avec la notion définie dans [19, Madden] ?
2) Si c'est bien le cas, se pose le problème de donner des preuves constructives pour des résultats sophistiqués, comme le fait qu'un anneau cohérent noethérien régulier de dimension $\leqslant 2$ est un anneau de Pierce-Birkhoff [18].
3) La conjecture de Pierce-Birkhoff usuelle est démontrée dans [20] pour $\mathbf{R}[x,y]$ lorsque $\mathbf{R}$ est un corps réel clos discret mais il n'est pas si clair qu'il y ait une preuve constructive pour $\mathbb{R}[x,y]$.

3.5 Une théorie purement équationnelle pour les anneaux réels clos

La structure d'*anneau réel clos* est définie par N. Schwartz de manière très abstraite dans [27]. Alexander Prestel et Niels Schwartz présentent une axiomatisation au premier ordre en une théorie cohérente dans [23]. Une version plus élémentaire, semblable à celle que nous proposons, se trouve dans [32].

Le but était de donner une description abstraite des anneaux de fonctions semialgébriques continues sur les fermés semialgébriques pour un corps réel clos fixé $\mathbf{R}$, et de définir des *espaces réels clos* abstraits.

Voici une définition des anneaux réels clos en mathématiques classiques [28].

Définition* 3.16. Un anneau *réel clos* est un anneau réduit $\mathbf{A}$ vérifiant les propriétés suivantes.

1. L'ensemble des carrés de $\mathbf{A}$ est l'ensemble des éléments $\geqslant 0$ d'un ordre partiel qui fait de $\mathbf{A}$ un anneau fortement réticulé.
2. Si $0 \leqslant a \leqslant b$, il existe z tel que $zb = a^2$.
3. Pour tout idéal premier $\mathfrak{p}$, l'anneau résiduel $\mathbf{A}/\mathfrak{p}$ est intégralement clos et son corps de fractions est un corps réel clos.

L'article [23] montre en mathématiques classiques que la structure d'anneau réel clos précédente est décrite par une théorie cohérente. Les axiomes existentiels proposés par les auteurs pour remplacer le point *3* ci-dessus sont très sophistiqués et la démonstration est également un tour de force remarquable. Il semble que le fait que la théorie des anneaux réels clos est essentiellement équivalente à une théorie purement équationnelle (proposition 3.21 et théorème 3.18) se trouve déjà dans la littérature ([32], et peut-être avant).

La définition 3.16 nous conduit à proposer la définition suivante en mathématiques constructives.

Définition 3.17. La théorie dynamique $\mathcal{A}rc$ des *anneaux réels clos* est obtenue à partir de la théorie $\mathcal{A}frrv$ (anneaux fortement réticulés avec racines virtuelles) en ajoutant les règles dynamiques $\mathbf{FRAC}_n$ page 14.

Théorème 3.18. *La théorie $\mathcal{A}rc$ est essentiellement équivalente à une théorie* purement équationnelle *notée $\mathcal{A}rc1$, décrite dans la démonstration qui suit.*

Démonstration. On obtient une théorie algébrique essentiellement équivalente à $\mathcal{A}rc$ en ajoutant un symbole de fonction $\mathrm{Fr}_n(\cdot,\cdot)$ correspondant aux fractions définies en application d'un axiome $\mathbf{FRAC}_n$ et en ajoutant les règles algébriques convenables. Rappelons cette règle :

$$\mathbf{FRAC}_n \quad |u|^n \leqslant |v|^{n+1} \vdash \exists z\ (zv = u,\ |z|^n \leqslant |v|) \qquad (n \geqslant 1)$$

On peut forcer l'hypothèse en remplaçant u par $u' = -a \vee (u \wedge a)$ avec $a = |v|^{\frac{n+1}{n}}$. Les règles que l'on impose à $\mathrm{Fr}_n(\cdot,\cdot)$ sont alors les suivantes

$$\mathbf{fr0}_n \quad \vdash \mathrm{Fr}_n(u,v) = \mathrm{Fr}_n(u',v) \qquad \mathbf{fr2}_n \quad \vdash \mathrm{Fr}_n(u,v) \leqslant |v|^{\frac{1}{n}}$$
$$\mathbf{fr1}_n \quad \vdash \mathrm{Fr}_n(u,v)v = u'$$

Par ailleurs une inégalité $x \leqslant y$ dans une règle algébrique peut toujours être remplacée par une égalité $x \vee y = y$. La théorie purement équationnelle en question est donc obtenue à partir de la théorie $\mathcal{A}frrv$ en ajoutant, pour chaque entier $n \geqslant 1$, les symboles de fonction $\mathrm{Fr}_n(\cdot,\cdot)$ et les règles $\mathbf{fr0}_n$, $\mathbf{fr1}_n$ et $\mathbf{fr2}_n$. □

Proposition 3.19. *Dans un anneau réel clos (définition 3.17), si l'on définit le prédicat « $x > 0$ » par « x est inversible et $\geqslant 0$ » les axiomes des anneaux réticulés fortement réels sont satisfaits.*

Lemme 3.20. (Structure quotient) *Soit $\mathbf{A}$ un anneau réel clos (définition 3.17) et I un idéal radical. Alors $\mathbf{A}/I$ est un anneau réel clos.*

Proposition* 3.21. *En mathématiques classiques les définitions 3.17 et 3.16 sont équivalentes.*

3.6 Une théorie dynamique des corps réels clos *non* discrets

Définition 3.22. La *théorie dynamique de base pour les corps réels clos*, notée $\mathcal{C}rc2$, est l'extension de la théorie purement équationnelle $\mathcal{A}rc1$ obtenue en ajoutant la règle $\mathbf{OTF}$. Elle est essentiellement équivalente à la théorie $\mathcal{C}orv$ des corps ordonnés avec racines virtuelles.

Remarques 3.23.
1) Le corps $\mathbb{R}$ est un modèle constructif de la théorie $\mathcal{C}rc2$.

2) La théorie $\mathcal{C}rcd$ est essentiellement équivalente à la théorie obtenue en ajoutant à $\mathcal{C}rc2$ l'axiome $\mathbf{ED}_{\#}$.

3) La théorie $\mathcal{C}rc2$ permet de démontrer l'existence d'une racine carrée pour un nombre complexe de module 1. On recouvre le cercle unité $\{\, x^2+y^2=1 \,\}$ par les ouverts $\{\, x>-1 \,\}$ et $\{\, x<1 \,\}$, sur chacun desquels l'existence est assurée par une fonction continue. Cependant, cette existence ne semble pas pouvoir être démontrée dans $\mathcal{A}rc1$, car dans cette théorie seules les fonctions semialgébriques continues partout définies ont droit de cité.

4) La théorie $\mathcal{C}rc2$ n'est rien d'autre que la théorie des anneaux réels clos locaux. Cependant, il existe des anneaux réels clos locaux qui ne sont pas des corps au sens de Heyting. Considérons par exemple l'anneau $\mathbf{A}$ des fonctions semialgébriques continues sur $\mathbf{R}_a$, et soit $\mathbf{B}=S^{-1}\mathbf{A}$ où S est le monoïde des fonctions f telles que $f(0)\neq 0$. C'est l'anneau des germes en (0) des fonctions $f\in\mathbf{A}$. Un élément $f\in\mathbf{A}$ est >0 dans $\mathbf{B}$ (resp. $\leqslant 0$ dans $\mathbf{B}$) si, et seulement si, $f(0)>0$ dans $\mathbf{R}_{\mathrm{a}}$ (resp. $f(x)\leqslant 0$ au voisinage de 0). Ceci montre que **HOF** n'est pas satisfait dans $\mathbf{B}$, car il ne suffit pas que $f(0)\leqslant 0$ pour que f soit $\leqslant 0$ au voisinage de 0. Notons que cet anneau réel clos local admet deux idéaux premiers minimaux, avec pour localisés respectifs les germes de fonctions à droite (ou à gauche) de 0.

Question 3.24. Est-ce que les théories $\mathcal{C}rc1$ et $\mathcal{C}rc2$ sont essentiellement équivalentes ? On a une démonstration en mathématiques classiques, mais d'un point de vue constructif, la théorie $\mathcal{C}rc2$, plus naturelle que $\mathcal{C}rc1$, est a priori un peu plus faible.

Question 3.25. Montrer que le théorème de la valeur intermédiaire, énoncé sous la forme de la règle $\mathbf{RCF}_n$ page 11, n'est pas valide dans la théorie $\mathcal{C}rc2$. Montrer de même que le théorème qui affirme que tout nombre complexe a une racine carrée n'est pas une règle valide dans la théorie $\mathcal{C}rc2$.

Le 17-ème problème de Hilbert

Question 3.26. Dans quelle mesure la solution constructive du 17e problème de Hilbert pour $\mathbb{R}$ (voir [10, section 6.1]) s'applique-t-elle à tout anneau fortement réticulé avec racines virtuelles ? Si ce n'est pas le cas, quelle théorie plus forte ferait l'affaire : $\mathcal{A}rc$ (définition 3.17), $\mathcal{C}rc2$ (définition 3.22), $\mathcal{C}rca$ (définition 3.27) ?

3.7 Corps réel clos archimédien *non* discret

Pour mieux décrire les propriétés algébriques de $\mathbb{R}$, on fait une tentative de ne pas quitter les théories dynamiques tout en conservant l'essence de la règle non dynamique **HOF**.

La règle suivante, qui signifie que le corps est archimédien, est satisfaite sur $\mathbb{R}$. Cette règle est acceptable dans le cadre des théories dynamiques infinitaires.

$$\mathbf{AR1} \;\vdash\; \mathbf{OU}_{n\in\mathbb{N}}\ |x|\leqslant n \qquad\qquad (\textbf{Archimède 1})$$

Définition 3.27. On définit la théorie $\mathcal{C}rca$ des corps réels clos archimédiens comme la théorie géométrique obtenue en ajoutant l'axiome **AR1** à la théorie $\mathcal{C}rc2$.

L'exemple donné dans le point 4 de la remarque 3.23 (un anneau réel clos local avec des diviseurs de zéro, modèle de la théorie $\mathcal{C}rc2$) reste un modèle de $\mathcal{C}rca$. Les exemples 2.14 sont également des modèles de la théorie $\mathcal{C}rca$; de manière générale les sous-anneaux de $\mathbb{R}$ stables pour les fonctions racines virtuelles, les fractions Fr_n et les inverses des éléments inversibles, sont des modèles de $\mathcal{C}rca$.

Question 3.28.
On sait qu'on ne peut pas exprimer au premier ordre le fait que $\mathbb{R}$ est archimédien. On l'exprime ici avec la règle infinitaire **AR1**. Une question qui se pose est de savoir si en ajoutant cette règle on obtient une extension conservative de la théorie dynamique $\mathcal{C}rc2$, cela semble probable. Par contre, pour la théorie formelle intuitionniste correspondante dans laquelle on autorise l'introduction de prédicats pour $P\Rightarrow Q$ et $\forall x P$ (avec les règles de déduction de Gentzen) il se pourrait qu'un énoncé comme **HOF** devienne prouvable.

Le Positivstellensatz de Schmüdgen

Références : [26, 29, 30]

Question 3.29. La théorie géométrique $\mathcal{C}rca$ suffit-elle pour développer les théorèmes du type Schmüdgen ?

Conclusion

Cet article, et les questions sans réponse qu'il contient, permet de mesurer notre ignorance de l'algèbre réelle.

Références

[1] Thomas William Barrett and Hans Halvorson, *Morita equivalence.* http://arxiv.org/abs/1506.04675, Manuscript, 2015. 2, 8

[2] Daniel Bembé and André Galligo, *Virtual roots of a real polynomial and fractional derivatives*, ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2011, pp. 27–34. MR 2895191 16

[3] Marc Bezem and Thierry Coquand, *Automating coherent logic.*, 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 (English). 3

[4] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy, *Real algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 36, Springer-Verlag, Berlin, 1998, Translated from the 1987 French original, Revised by the authors. MR MR1659509 (2000a :14067) 11, 12, 15

[5] Thierry Coquand and Henri Lombardi, *A note on the axiomatisation of real numbers*, Math. Log. Q. **54** (2008), no. 3, 224–228. MR 2417794 (2009e :03063) 13

[6] Michel Coste, *An introduction to o-minimal geometry*, Dip. Mat. Univ. Pisa, Dottorato di Ricerca in Matematica, Istituti Editoriali e Poligrafici Internazionali, Pisa, 2000. 2

[7] Michel Coste, Tomás Lajous-Loaeza, Henri Lombardi, and Marie-Françoise Roy, *Generalized Budan-Fourier theorem and virtual roots*, J. Complexity **21** (2005), no. 4, 479–486. MR 2152717 (2006c :12001) 16, 17

[8] Michel Coste, Henri Lombardi, and Marie-Françoise Roy, *Dynamical method in algebra : effective Nullstellensätze*, Ann. Pure Appl. Logic **111** (2001), no. 3, 203–256. MR 1848137 (2003d :03104) 3, 5, 7, 8, 9, 10, 11, 12

[9] André Galligo, *Budan tables of real univariate polynomials*, J. Symbolic Comput. **53** (2013), 64–80. MR 3027983 16

[10] Laureano González-Vega and Henri Lombardi, *A real Nullstellensatz and Positivstellensatz for the semipolynomials over an ordered field*, J. Pure Appl. Algebra **90** (1993), no. 2, 167–188. MR 1250767 (95f :12013) 12, 21

[11] Laureano González-Vega, Henri Lombardi, and Louis Mahé, *Virtual roots of real polynomials*, J. Pure Appl. Algebra **124** (1998), no. 1-3, 147–166. MR 1600281 (98k :14077) 16, 17, 18

[12] Peter T. Johnstone, *Sketches of an elephant : a topos theory compendium. Vol. 2*, Oxford Logic Guides, vol. 44, The Clarendon Press, Oxford University Press, Oxford, 2002. MR 2063092 (2005g :18007) 2

[13] Vladimir Lifschitz, *Semantical completeness theorems in logic and algebra*, Proc. Amer. Math. Soc. **79** (1980), no. 1, 89–96. MR 560591 3

[14] Henri Lombardi, *Structures algébriques dynamiques, espaces topologiques sans points et programme de Hilbert*, Ann. Pure Appl. Logic **137** (2006), no. 1-3, 256–290. MR 2182105 (2006i :03103) 5

[15] Henri Lombardi, Daniel Perrucci, and Marie-Françoise Roy, *An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem. Preprint.* http://arxiv.org/abs/1404.2338, manuscript, 2014. 12

[16] Henri Lombardi and Claude Quitté, *Commutative algebra : constructive methods. finite projective modules*, Algebra and Applications, vol. 20, Springer, Dordrecht, 2015, Translated from the French (Calvage & Mounet, 2011, revised and extended by the authors) by Tania K. Roblot. MR 3408454 12

[17] Henri Lombardi and Marie-Françoise Roy, *Elementary constructive theory of ordered fields*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 249–262. MR 1106427 (92j :12014) 12

[18] F. Lucas, J. Madden, D. Schaub, and M. Spivakovsky, *Approximate roots of a valuation and the Pierce-Birkhoff conjecture*, Ann. Fac. Sci. Toulouse Math. (6) **21** (2012), no. 2, 259–342. MR 2978097 19

[19] James J. Madden, *Pierce-Birkhoff rings*, Arch. Math. (Basel) **53** (1989), no. 6, 565–570. MR 1023972 (90m :14019) 19

[20] Louis Mahé, *On the Pierce-Birkhoff conjecture*, Rocky Mountain J. Math. **14** (1984), no. 4, 983–985, Ordered fields and real algebraic geometry (Boulder, Colo., 1983). MR 773148 (86d :14020) 19

[21] Ju. V. Matijasevi˘ c, *A metamathematical approach to proving theorems in discrete mathematics*, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **49** (1975), 31–50, 177, Theoretical applications of the methods of mathematical logic, I. MR 0376327 3

[22] Dag Prawitz, *Ideas and results in proof theory*, Proceedings of the Second Scandinavian Logic Symposium (Univ. Oslo, Oslo, 1970), North-Holland, Amsterdam, 1971, pp. 235–307. Studies in Logic and the Foundations of Mathematics, Vol. 63. MR 0387024 (52 #7871) 3, 7

[23] Alexander Prestel and Niels Schwartz, *Model theory of real closed rings*, Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 32, Amer. Math. Soc., Providence, RI, 2002, pp. 261–290. MR 1928375 (2003h :13030) 19, 20

[24] 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.*, Berlin : De Gruyter, 2016 (English). 8, 23

[25] Michael Rathjen, *Remarks on Barr's theorem proofs in geometric theories*, Concepts of proof in mathematics, philosophy, and computer science. Based on the Humboldt-Kolleg, Bern, Switzerland, September 9–13, 2013. [24], Berlin : De Gruyter, 2016, pp. 347–374. 8

[26] Konrad Schmüdgen, *The K-moment problem for compact semi-algebraic sets*, Math. Ann. **289** (1991), no. 2, 203–206. MR 1092173 (92b :44011) 22

[27] Niels Schwartz, *Real closed spaces. Habilitationsschrift. München*, 1984. 19

[28] ———, *Real closed rings*, Algebra and order (Luminy-Marseille, 1984), Res. Exp. Math., vol. 14, Heldermann, Berlin, 1986, pp. 175–194. MR 891460 (89b :14035) 20

[29] Markus Schweighofer, *An algorithmic approach to Schmüdgen's Positivstellensatz*, J. Pure Appl. Algebra **166** (2002), no. 3, 307–319. MR 1870623 (2002j :14063) 22

[30] ———, *Iterated rings of bounded elements and generalizations of Schmüdgen's Positivstellensatz*, J. Reine Angew. Math. **554** (2003), 19–45. MR 1952167 (2004b :13028) 22

[31] Joseph R. Shoenfield, *Mathematical logic*, Association for Symbolic Logic, Urbana, IL ; A K Peters, Ltd., Natick, MA, 2001, Reprint of the 1973 second printing. MR 1809685 (2001h :03003) 7

[32] Marcus Tressl, *Super real closed rings*, Fund. Math. **194** (2007), no. 2, 121–177. MR 2310341 (2007m :03078) 2, 16, 19, 20

[33] Dimitris Tsementzis, *A syntactic characterization of Morita equivalence.* http://arxiv.org/abs/1507.02302, Manuscript, 2015. 8

[34] Lou van den Dries, *Tame topology and o-minimal structures*, London Mathematical Society Lecture Note Series, vol. 248, Cambridge University Press, Cambridge, 1998. MR 1633348 (99j :03001) 2