Théories géométriques pour l'algèbre des nombres réels sans test de signe ni axiome de choix dépendant

Meeting au CIRM à Luminy
– Ordered Algebraic Structures and Related Topics –
12-16 Octobre 2015

Résumé

On cherche une théorie dynamique aussi complète que possible pour décrire les propriétés algébriques du corps des réels en mathématiques constructives sans axiome du choix dépendant.

Ce texte rend compte d'un travail en cours.
Il est émaillé d'un grand nombre de questions en suspens.
Je remercie Thierry Coquand, Michel Coste et Marie-Françoise Roy pour leurs avis et suggestions.
H. Lombardi. http://hlombardi.free.fr/

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.

L'*algèbre réelle constructive* n'est pas bien comprise ! L'analyse constructive ($\simeq$ les méthodes certifiées en analyse numérique) est nettement mieux étudiée.

D'un point de vue constructif, l'algèbre réelle est *assez éloignée* de la théorie usuelle classique des corps réels clos à la Artin-Schreyer-Tarski, dans laquelle on suppose que l'on a un *test de signe*.

La plupart des algorithmes de l'algèbre réelle classique échouent avec les nombres réels, parce qu'ils requièrent un test de signe.

Même en analyse constructive, on pourrait avoir des retombées intéressantes d'une étude plus approfondie de l'algèbre réelle. Par exemple cela permettrait de mieux comprendre comment éviter le recours à l'axiome du choix dépendant.

La compréhension de l'algèbre réelle constructive peut également être un premier pas pour une théorie constructive (et donc algorithmique) des *structures O-minimales* (cf. [6, 21]).

L'algèbre réelle peut être vue comme la plus simple des structures O-minimales. 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.

Ainsi nous cherchons une théorie dynamique aussi complète que possible pour décrire les propriétés algébriques du corps des réels en mathématiques constructives sans axiome du choix dépendant. Nous évitons aussi l'usage de la négation. Fred Richman [19] montre que les mathématiques constructives sont plus élégantes lorsque l'on se passe de l'axiome du choix dénombrable. Nous pensons qu'elles sont également plus élégantes si l'on se passe de la négation.

1 Théories géométriques du premier ordre

On dira «anneau» pour «anneau commutatif unitaire».

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 :

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

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

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. Seuls 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) est utilisé en tant que règle (2) :

$$A \ \vdash \ \textbf{Introduire}\ \underline{y^1}\ B_1 \ \textbf{ou} \ \cdots \ \textbf{ou Introduire}\ \underline{y^m}\ B_m \tag{2}$$

(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»).

— 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 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.

Par exemple 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 :

$$\textbf{CD} \ \vdash \ x = 0 \ \textbf{ou Introduire}\ y \ \ xy = 1 \tag{3}$$

Pour démontrer la règle dynamique

$$xy = 0 \ \vdash \ x = 0 \ \textbf{ou} \ \ y = 0$$

on ouvre deux branches conformément à l'axiome (3). Dans la première on a $x = 0$ est 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

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

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

Remarque 1.1 Le symbole **ou** doit être compris comme une abréviation pour«**ou**vrir (des branches dans le calcul)». En pratique, dans la suite, nous remplaçons «**Introduire**» et «**ou**» par les symboles traditionnels «$\exists$» et «$\vee$». Cela introduit une confusion avec les formules de la théorie du premier ordre associée à la théorie dynamique que l'on considère, mais nous avons reculé devant l'inflation des notations.

Collapsus

Une règle dynamique s'appelle une *règle de collapsus* lorsque le second membre est la disjonction vide (le faux). Si l'on prouve l'hypothèse d'une règle de collapsus dans une théorie dynamique, la théorie n'admet pas de modèle.

En revanche, si une théorie dynamique ne comporte pas de règle de collapsus, elle admet toujours le modèle réduit à un point où tous les prédicats sont évalués vrai.

Dans la suite nous remplaçons dans les règles de collapsus le faux, i.e. la disjonction vide, par une propriété qui réduit tout modèle à un seul point, en lequel tous les prédicats sont «vrais».

C'est seulement une affaire de goût qui ne change rien au fond des choses [1].

Au lieu de dire qu'une structure algébrique dynamique qui collapse n'a pas de modèle, on dit alors (sans négation) que tout modèle de cette structure algébrique dynamique est trivial, réduit à un point, et que «tout y est vrai» (on retrouve ainsi le ex falso quod libet qui est la règle pertinente concernant le faux en logique intuitionniste).

Dans les théories que nous considérerons, cette propriété de collapsus (qui réduit tout modèle à un point) s'écrira $1 = 0$, car ce sont des théories dynamiques qui étendent celle des anneaux commutatifs.

Théories algébriques

Une règle dynamique qui contient à droite une seule formule atomique (sans $\vee$, ni $\exists$), ou la disjonction vide, est appelée une *régle algébrique*.

Une théorie dynamique est dite *algébrique* lorsqu'elle ne comporte que des règles algébriques. Une théorie algébrique vu comme théorie du premier ordre est parfois appelée une *théorie de Horn universelle*. Lorsque nous parlons de *théorie algébrique* nous la voyons comme une théorie dynamique, une théorie dans laquelle les seules démonstrations sont des démonstrations dynamiques, purement calculatoires, sans logique.

L'*algèbre universelle* correspond aux théories algébriques «purement équationnelles», celles où les seules règles sont des égalités entre termes. En outre l'égalité doit satisfaire les règles usuelles (relation d'équivalence stable par rapport aux termes et aux prédicats).

1. En fait, je dois avoir horreur du vide : le silence de cet espace infini m'effraie.

Dans certaines théories dynamiques avec égalité, comme des théories de groupes ou d'anneaux, il est possible de remplacer le prédicat d'égalité binaire $\cdot = \cdot$ par un prédicat unaire $\cdot = 0$ en confiant à un «calcul automatique externe» les principales règles que doit satisfaire la structure (voir les exemples ci-dessous).

Dans [8], lorsque la théorie formelle ne comporte que des prédicats unaires, les règles algébriques sont classifiées en *règles directes*, *règles de simplification* et *collapsus*. Cela permet d'unifier les démonstrations de plusieurs Nullstellensätze divers et variés. Un Nullstellensatz est un certificat algébrique qui rend évident un fait qui a priori demanderait une démonstration non triviale.

Exemples

1) La théorie purement équationnelle $\mathcal{Ac}$ des anneaux commutatifs est décrite sur la signature $(\cdot = 0, \cdot + \cdot, \cdot \times \cdot, 0, 1, -1)$ et les seules règles directes suivantes :

mc1 $\vdash\ 0 = 0$ **ac1** $x = 0 \ \vdash\ xy = 0$

mc2 $x = 0,\ y = 0 \ \vdash\ x + y = 0$

Le prédicat binaire $\cdot = \cdot$ est alors *défini* par : «$x = y$ signifie $x - y = 0$».

Les règles qui définissent la théorie $\mathcal{Ac}$ des anneaux commutatifs signifient précisément ceci : d'une part la machinerie calculatoire des polynômes commutatifs à coefficients entiers, qui réécrit tout terme (formé sur les constantes et les générateurs) comme un polynôme à coefficients entiers sous une forme normale prédéfinie, d'autre part les trois règles **mc1**, **mc2** et **ac1** telles qu'elles sont énoncées.

La règle de distributivité $x(y+z) = xy+xz$, par exemple, est alors confiée à un calcul automatique qui réduit à 0 tout terme du type $t_1(t_2 + t_3) - (t_1t_2 + t_1t_3)$.

De même la transitivité de l'égalité binaire est gérée par la règle **mc2** et par le calcul automatique qui réduit à $(t_1 - t_3)$ le terme $\big((t_1 - t_2) + (t_2 - t_3)\big)$.

On reconnait dans les trois règles algébriques **mc1**, **mc2** et **ac1** les axiomes des idéaux, qui permettent de créer une structure d'anneau quotient, et qui signifient la compatibilité de l'égalité avec l'addition et la multiplication.

2) La théorie dynamique $\mathcal{Asdz}$ des *anneaux sans diviseur de zéro* est obtenue à partir de la théorie $\mathcal{Ac}$ en ajoutant la règle algébrique [2]

Asdz $xy = 0 \ \vdash\ x = 0 \ \vee\ y = 0$

3) La théorie algébrique $\mathcal{Af}$ des *anneaux avec filtre non trivial* est obtenue à partir de la théorie $\mathcal{Ac}$ en ajoutant un prédicat $F(\cdot)$ et les règles suivantes

fi1 $x = 0,\ F(y) \ \vdash\ F(x + y)$ **Fi1** $F(xy) \ \vdash\ F(x)$

fi2 $\vdash\ F(1)$ $\mathbf{Col_{Af}}$ $F(0) \ \vdash\ 1 = 0$

fi3 $F(x),\ F(y) \ \vdash\ F(xy)$

4) La théorie dynamique $\mathcal{Afp}$ des *anneaux avec filtre premier* est obtenue à partir de la théorie $\mathcal{Af}$ en ajoutant la règle de simplification

FP $F(x + y) \ \vdash\ F(x) \ \vee\ F(y)$

2. Les noms des règles sont calligraphiés comme suit : pour les règles directes, tout en minuscule, pour les autres règles algébriques (les règles de simplification et le collapsus), la première lettre en majuscule, et enfin les autres règles dynamiques, tout en majuscule.

5) La théorie algébrique $\mathcal{Afs}$ des *anneaux avec filtre simplifiable* est obtenue à partir de la théorie $\mathcal{Af}$ en ajoutant la règle de simplification

Fi2 $F(x),\, xy = 0 \;\vdash\; y = 0$

Dans cette théorie, le collapsus se déduit des autres axiomes.

6) La théorie dynamique $\mathcal{Al}$ des *anneaux locaux* est obtenue à partir de la théorie $\mathcal{Afp}$ en ajoutant la règle dynamique

AL $F(x) \;\vdash\; \exists y\, xy = 1$

7) La théorie dynamique $\mathcal{Ai}$ des *anneaux intègres* est obtenue à partir de la théorie $\mathcal{Afs}$ en ajoutant la règle dynamique

AI $\vdash\; x = 0 \vee F(x)$

Structures algébriques dynamiques

Si $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ est une théorie cohérente, 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 une formule atomique $P(\underline{x})$ construite sur le langage $\mathcal{L} \cup G$. Elle correspond à l'axiome (la règle directe) « $\vdash\; P(\underline{x})$ ».

Par exemple le corps dynamique $\mathbf{K} = ((G, R), \mathcal{Cd})$, avec l'ensemble de générateurs $G = \{\, a, b \,\}$ et l'ensemble de relations $R = \left\{\, 105 = 0,\, a^2 + b^2 = 1 \,\right\}$, correspond à n'importe quel corps de caractéristique 3 ou 5 ou 7 engendré par deux éléments a et b vérifiant $a^2 + b^2 = 1$.

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. Une règle dynamique sans hypothèse et avec une seule conclusion sans présence de $\exists$ s'appelle un *fait* (dans $\mathbf{K}$). Un fait concerne uniquement les objets définissables syntaxiquement dans la structure. On peut dire aussi que c'est une règle algébrique sans variable libre.

L'algèbre «concrète» consiste très souvent à prouver des faits ou des règles dynamiques dans des structures algébriques dynamiques particulières. C'est un peu plus général que la théorie (inépuisable) des identités algébriques, c'est-à-dire l'algèbre universelle, à l'œuvre derrière une forte proportion des grands théorèmes d'algèbre abstraite.

À une structure algébrique dynamique pour une théorie algébrique, correspond une structure algébrique usuelle, définie par générateurs et relations, satisfaisant les règles algébriques requises. C'est le modèle générique de la théorie dynamique associée à cette structure algébrique dynamique. Les autres modèles minimaux de la théorie dynamique associée sont simplement les quotients du modèle générique : on est donc dans le cadre des structures algébriques usuelles, que nous pouvons qualifier de «statiques».

La méthode dynamique est souvent un moyen pratique d'accéder à ces identités algébriques (des «Positivstellensätze» par exemple), en suivant au plus près les pistes indiquées dans les preuves données en algèbre abstraite.

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 prouvable). Il est *absolument faux*, ou plus justement *collapsant* si « $P(\underline{t}) \;\vdash$ » est prouvable. Entre les deux existe une grande variété de possibilités : une structure algébrique dynamique n'a pas un modèle figé unique, mais

représente à l'état potentiel toutes les réalisations éventuelles de la structure. Ajouter un fait collapsant comme axiome revient à supprimer tous les modèles [3].

Modèles d'une théorie dynamique

On considère une théorie dynamique $\mathcal{T}$ et une structure algébrique dynamique $\mathbf{A}$ de type $\mathcal{T}$. Un modèle de $(\mathbf{A}, \mathcal{T})$ est une structure algébrique usuelle (statique) dans le langage associé à $(\mathbf{A}, \mathcal{T})$ et vérifiant les axiomes de $(\mathbf{A}, \mathcal{T})$ (ceux de $\mathcal{T}$ et ceux donnés par la présentation de $\mathbf{A}$). On a donc un morphisme de structures algébriques dynamiques de type $\mathcal{T}$, de $\mathbf{A}$ vers un tel modèle.

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.

D'un point de vue constructif on est naturellement intéressés par les modèles qui satisfont les axiomes en respectant le sens intuitif du «ou» et du «il existe» : pour prouver qu'une structure algébrique particulière satisfait les axiomes, on autorise uniquement la logique intuitionniste. Mais on ne précise pas plus les contraintes.

Plus précisément, la théorie naïve des ensembles à laquelle nous nous référons est a priori celle de Bishop. S'il s'agit d'une théorie formelle, à la Aczel, à la Martin-Löf, ou à la HoTT, il se pourrait que cela ait des conséquences en termes de métathéorèmes (les théorèmes de la théorie des modèles «constructive»). Mais comme ce ne sera pas le cas dans nos énoncés relativement simples, nous ne nous en soucierons pas.

En mathématiques classiques on imagine ordinairement les modèles comme jouissant, non seulement de la logique classique avec tiers exclu, mais de toutes les propriétés admises dans la théorie formelle des ensembles classique **ZFC**.

Extensions conservatives d'une théorie dynamique

On dit qu'une théorie dynamique $\mathcal{T}'$ *étend un théorie dynamique* $\mathcal{T}$ si les prédicats et symboles de fonctions de $\mathcal{T}$ sont définis dans $\mathcal{T}'$ et si les axiomes de $\mathcal{T}$ sont des règles dynamiques valides dans $\mathcal{T}'$.

On dit que $\mathcal{T}'$ est une *extension conservative de* $\mathcal{T}$ si les règles dynamiques formulables dans $\mathcal{T}$ et valides dans $\mathcal{T}'$ sont valides dans $\mathcal{T}$.

Cette section est consacrée aux méthodes classiques de constructions d'extensions conservatives d'une théorie dynamique.

En mathématiques classiques, si $\mathcal{T}'$ est une extension conservative de $\mathcal{T}$, tout modèle de $\mathcal{T}$ est une sous-$\mathcal{T}$-structure d'un produit de modèles de $\mathcal{T}'$.

Théorème fondamental des théories dynamiques

On a le théorème fondamental 1.2 ci-après (cf. par exemple le théorème 1 dans [8]). On note que certains modèles constructifs de la première théorie peuvent ne plus correspondre à aucun modèle constructif de la seconde. Néanmoins, ce n'est pas trop grave, comme expliqué dans le théorème fondamental suivant.

Théorème 1.2 (Élimination des coupures)
Pour ce qui concerne les théories dynamiques du premier ordre, la logique, y compris

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

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 prouvable dans une théorie dynamique $\mathcal{T}$ si, et seulement si, elle est prouvable 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.

Skolémisation

Théorème 1.3 (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 $\mathcal{T}$.

Démonstration. 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 [20, Section 4.5]. □

Notons que comme pour le théorème 1.2 une structure algébrique dynamique peut avoir un modèle constructif dans la première théorie et ne plus en avoir (du point de vue constructif) après skolémisation.

2 Rappels sur les corps ordonnés discrets

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].

$$\textbf{Signature :} \quad (\cdot = 0, \cdot > 0, \cdot \geqslant 0, \cdot + \cdot, \cdot \times \cdot, 0, 1, -1).$$

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 toutes les relations d'égalité entre termes construits sur les éléments de la structure. Ainsi tout anneau définit un corps ordonné discret dynamique.

Abréviations

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

Axiomes

Règles directes

On a d'abord mis les axiomes des anneaux commutatifs, puis les règles qui concernent $\cdot = 0$ et $\cdot \geqslant 0$, ensuite les règles qui font intervenir $\cdot > 0$.

mc1 $\vdash\ 0 = 0$

mc2 $x = 0, y = 0 \vdash\ x + y = 0$

ac1 $x = 0 \vdash\ xy = 0$

go1 $x = 0 \vdash x \geqslant 0$

go2 $x \geqslant 0, y \geqslant 0 \vdash x + y \geqslant 0$

aso1 $\vdash 1 > 0$

aso2 $x > 0 \vdash x \geqslant 0$

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 $0 \neq 0 \vdash 1 = 0$

Règles de simplification

Eo $x \geqslant 0, x \leqslant 0 \vdash x = 0$

Iv $xy = 1 \vdash x \neq 0$

Règles dynamiques

IV $x \neq 0 \vdash \exists y\, xy = 1$

ED $\vdash x = 0 \vee x \neq 0$

OT $\vdash x \geqslant 0 \vee x \leqslant 0$

Les règles **go1** et **go2** expriment, dans le contexte des groupes, la réflexivité et la transitivité de la relation d'ordre (compatible avec la loi de groupe). La règle **Eo** 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 valides constructivement pour $\mathbb{R}$. Pour les réels de Bishop **ED** équivaut à **LPO** et **OT** équivaut à **LLPO**.

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

Quelques règles dérivées dans *Cod*

Quatre règles de simplification valides

Anz $x^2 = 0 \vdash x = 0$

Aonz $c \geqslant 0, x(x^2 + c) \geqslant 0 \vdash x \geqslant 0$

Aso1 $x > 0, xy \geqslant 0 \vdash y \geqslant 0$

Aso2 $x \geqslant 0, xy > 0 \vdash y > 0$

Deux règles dynamiques valides

OTF $x + y > 0 \vdash x > 0 \vee y > 0$

OTF$^\times$ $xy < 0 \vdash x < 0 \vee y < 0$

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.

Théories dynamiques plus faibles

La règle **Aonz** implique $x^3 \geqslant 0 \vdash x \geqslant 0$, donc aussi, sous **Eo**, $x^3 = 0 \vdash x = 0$, et a fortiori **Anz**.

Définition 2.1.1
Théories basées sur le langage des anneaux ordonnés $(\cdot = 0, \cdot \geqslant 0, \cdot + \cdot, \cdot \times \cdot, 0, 1, -1)$.

1. *La théorie algébrique* $\mathcal{A}o$ *des* anneaux ordonnés. *Les axiomes sont ceux des anneaux commutatifs, les règles directes* **go1**, **go2**, **ao1**, **ao2** *et la règle de simplification* **Eo**.

2. *La théorie algébrique* $\mathcal{A}onz$ *des* anneaux ordonnés réduits *est obtenue en ajoutant la règle de simplification* **Aonz** *à la théorie* $\mathcal{A}o$.

3. *La théorie dynamique* $\mathcal{A}to$ *des* anneaux totalement ordonnés *est obtenue en ajoutant la règle dynamique* **OT** *à la théorie* $\mathcal{A}o$.

4. *La théorie dynamique* $\mathcal{A}tonz$ *des* anneaux totalement ordonnés réduits *est obtenue en ajoutant la règle dynamique* **Anz** *à la théorie* $\mathcal{A}to$.

Théories basées sur le langage des corps ordonnés $(\cdot = 0, \cdot \geqslant 0, \cdot > 0, \cdot + \cdot, \cdot \times \cdot, 0, 1, -1)$.

5. *La théorie directe* $\mathcal{A}po$ *des* anneaux proto-ordonnés *(cf. [8]). Les axiomes sont ceux des anneaux commutatifs, toutes les règles directes énoncées pour* $\mathcal{C}od$ *(***go1***,* **go2***,* **ao1***,* **ao2***,* **aso1** *à* **aso4***) et le collapsus* **Col**.

6. *La théorie algébrique* $\mathcal{A}so$ *des* anneaux strictement ordonnés *est la théorie* $\mathcal{A}po$ *à laquelle on ajoute les règles de simplification* **Eo**, **Aso1** *et* **Aso2**. *On peut la voir aussi comme construite à partir de* $\mathcal{A}o$ *en ajoutant le prédicat* $\cdot > 0$ *dans le langage, les règles directes* **aso1** *à* **aso4** *et les règles de simplification* **Aso1** *et* **Aso2**.

7. *La théorie algébrique* $\mathcal{A}sto$ *des* anneaux strictement totalement ordonnés *est la théorie* $\mathcal{A}so$ *à laquelle on ajoute la règle dynamique* **OT**. *On peut la voir aussi comme construite à partir de* $\mathcal{A}to$ *en ajoutant le prédicat* $\cdot > 0$ *dans le langage, les règles directes* **aso1** *à* **aso4** *et les règles de simplification* **Aso1** *et* **Aso2**.

8. *La théorie algébrique* $\mathcal{A}sonz$ *des* anneaux strictement ordonnés réduits *(« quasi-ordered rings» dans [8]) est obtenue en ajoutant la règle de simplification* **Aonz** *à* $\mathcal{A}so$. *On peut aussi la voir comme la théorie* $\mathcal{A}po$ *à laquelle on ajoute les règles de simplification* **Eo**, **Aonz**, **Aso1** *et* **Aso2**.

9. *La théorie dynamique* $\mathcal{A}lsonz$ *des* anneaux locaux strictement ordonnés réduits *est obtenue en ajoutant les règles dynamiques* **IV** *et* **OTF** *à* $\mathcal{A}sonz$.

Corps réels clos discrets

On introduit aussi les règles dynamiques suivantes pour décrire les corps réels clos discrets.

$\mathbf{RCF}_n \quad a \leqslant b,\ P(a)P(b) < 0 \ \vdash\ \exists x\, P(x) = 0 \qquad (P \text{ polynôme de degré} \leqslant n)$

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 2.1.2 *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* $\mathbf{RCF}_n$.

Positivstellensatz formel

Le Positivstellensatz formel des mathématiques classiques admet la version constructive suivante. Voir [8] et pour des bornes de complexité [12].

Théorème 2.1.3 (Positivstellensatz formel, 1)

1. *Les théories dynamiques* $\mathcal{A}po$, $\mathcal{A}so$, $\mathcal{C}od$ *et* $\mathcal{C}rcd$ *collapsent simultanément.*

2. *Les théories dynamiques* $\mathcal{A}sonz$, $\mathcal{C}od$ *et* $\mathcal{C}rcd$ *prouvent les mêmes faits.*

Le collapsus d'une structure algébrique dynamique dans $\mathcal{Apo}$ est donné par un certificat algébrique d'impossibilité, que l'on appelle un *Positivstellensatz*.

Nous examinons maintenant ce que deviennent les résultats précédents en l'absence du prédicat $\cdot > 0$ dans la présentation d'une structure algébrique dynamique.

Théorème 2.1.4 (Positivstellensatz formel, 1bis, avec seulement $\cdot \geqslant 0$)
(Pour une présentation donnée dans le langage des anneaux ordonnés.)

1. *Les théories dynamiques $\mathcal{Ao}$, $\mathcal{Apo}$, $\mathcal{Ato}$, $\mathcal{Cod}$ et $\mathcal{Crcd}$ collapsent simultanément.*
2. *Les théories dynamiques $\mathcal{Aonz}$, $\mathcal{Atonz}$, $\mathcal{Cod}$ et $\mathcal{Crcd}$ prouvent les mêmes faits.*

Positivstellensatz concret

Voici un énoncé équivalent au Positivstellensatz de Krivine-Stengle, donné ici dans le langage des structures algébriques dynamiques. Il se déduit du Positivstellensatz formel et du fait que la théorie des corps réels clos discrets est complète. Si $\mathbf{K}$ un corps ordonné discret, on note $\mathcal{Cod}(\mathbf{K})$ la théorie dynamique $\mathcal{Cod}$ à laquelle on a ajouté le *diagramme positif de* $\mathbf{K}$: les constantes sont les éléments de $\mathbf{K}$ et les relations sont les relations « $t = 0$ » ou « $t \geqslant 0$ » ou « $t > 0$ » qui ont lieu dans $\mathbf{K}$ pour un terme clos arbitraire construit sur les constantes. Une preuve constructive du théorème se trouve dans [8], pour des bornes de complexité voir [12].

Théorème 2.1.5 *Soit $\mathbf{K}$ un corps ordonné discret et $\mathbf{R}$ un corps réel clos discret contenant $\mathbf{K}$, par exemple sa clôture réelle. On considère une structure algébrique dynamique $\mathbf{A} = \big((G, Rel), \mathcal{Cod}(\mathbf{K})\big)$ où $G = (x_1, \ldots, x_n)$ et Rel est fini.*

1. *La structure algébrique dynamique $\mathbf{A}$ collapse si, et seulement si, il est impossible de trouver un modèle de $\mathbf{A}$ contenu dans $\mathbf{R}$.*
2. *Le collapsus s'il a lieu est donné par un certificat algébrique conformément au point 1 du théorème 2.1.3.*
3. *On a un algorithme qui décide si $\mathbf{A}$ collapse et qui en cas de réponse négative décrit un système $(\xi_1, \ldots, \xi_n)$ dans $\mathbf{R}^n$ qui satisfait les contraintes énoncées dans Rel.*

Cet énoncé n'est pas valable sous cette forme générale si on prend $\mathbf{K} = \mathbf{R} = \mathbb{R}$ car il n'y a pas de test de signe dans $\mathbb{R}$ et l'algorithme du point *3* utilise 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 $x \neq 0$ désigne le prédicat d'inversibilité, on a l'équivalence

$$\exists y \;\; x^2 y = x \iff x = 0 \vee x \neq 0. \tag{4}$$

En effet supposons $x(1 - xy) = 0$. Si xy est inversible, alors x est inversible, et si $1 - xy$ est inversible, alors $x = 0$.

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 « $x = 0 \vee x \neq 0$ » est indécidable dans $\mathbb{R}$.

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

Question 2.1.6 Déterminer quelles propriétés algébriques de $\mathbb{R}$ permettent de démontrer les formes constructivement satisfaisantes de Positivstellensätze prouvées pour $\mathbb{R}$ dans [10]. Par exemple déterminer si la théorie des corps ordonnés avec racines virtuelles (introduite plus loin) permet d'obtenir ces résultats.

2.2 Corps ordonné discret avec sup

Dans un ensemble totalement ordonné et a fortiori dans un corps ordonné discret toute paire d'éléments admet une borne supérieure : le plus grand des deux. On ne change donc rien d'essentiel à la théorie $\mathcal{Cod}$ en ajoutant un symbole fonctionnel $\cdot\vee\cdot$ soumis au trois axiomes « qui définissent le sup de deux éléments » quand il existe.

Définition 2.2.1 *La théorie dynamique des* corps ordonnés discrets avec sup $\mathcal{Codsup}$ *est la théorie dynamique des corps ordonnés discrets à laquelle on ajoute un symbole de fonction* $\cdot\vee\cdot$ *et pour axiomes les règles algébriques* **sup1**, **sup2** *et* **Sup** *suivantes.*

sup1 $\vdash\ x\vee y\geqslant x$ **sup2** $\vdash\ x\vee y\geqslant y$ **Sup** $\ z\geqslant x,\ z\geqslant y\ \vdash\ z\geqslant x\vee y$

Cette théorie est pour l'essentiel identique à la théorie $\mathcal{Cod}$.

2.3 Corps ordonné de Heyting ?

En première approximation, et en suivant une suggestion de Heyting, on peut choisir comme théorie formelle du premier ordre pour les propriétés algébriques de $\mathbb{R}$ la théorie $\mathcal{Alsonz}$ à laquelle on ajoute l'axiome **HOF** non géométrique, donc indésirable.

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

On a un anneau local, car **OTF** implique que pour tout x, x ou $1-x$ est inversible. Et **HOF** signifie que le radical de Jacobson est réduit à 0.

Outre le caractère indésirable de **HOF**, la théorie formelle présente un inconvénient majeur, qui est de ne pas pouvoir démontrer l'existence de la borne supérieure de deux éléments : la règle dynamique suivante ne peut pas être démontrée (voir [5]).

Sup1 $\vdash\ \exists z\ \big((z-x)(z-y)=0,\ z\geqslant x,\ z\geqslant y\big)$

L'axiome **Sup1** est vérifié constructivement par les nombres réels, et il est très naturel. Il est donc légitime d'explorer les possibilités qu'offre l'ajout d'une loi pour cette borne supérieure, avec les règles adéquates.

Ceci nous invite à faire un détour (section 3) du coté des anneaux fortement réticulés.

3 Anneaux fortement réticulés

Dans cette section on dit « groupe » pour « groupe abélien ». Et les anneaux sont commutatifs unitaires comme dans tout l'article. Nous examinons les structures algébriques dynamiques définies à partir de certaines règles dynamiques satisfaites par les corps ordonnés discrets avec sup, en excluant les règles qui ne sont pas valides pour $\mathbb{R}$, par exemple **OT** et **ED**.

La principale de ces structures est celle d'anneau fortement réticulé (les f-rings dans la littérature anglaise). Nous commençons par les groupes réticulés.

3.1 Groupes réticulés (ℓ-groups)

Définition de la théorie purement équationnelle $\mathcal{Grl}$

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

Le symbole $\vee$ utilisé pour la borne supérieure binaire ne doit pas être confondu avec le symbole $\vee$ de la disjonction logique.

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 $x - y = 0$
- $x \perp y$ signifie $|x| \wedge |y| = 0$
- $x \geqslant y$ signifie $x \vee y = x$

Axiomes

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

eqsup1 $x = 0 \vdash (x + y) \vee z = y \vee z$

eqsup2 $x = 0 \vdash y \vee (x + z) = y \vee z$

Règles directes

mc1 $\vdash 0 = 0$

mc2 $x = 0, y = 0 \vdash x + y = 0$

ga1 $x = 0 \vdash -x = 0$

NB. Les règles **mc1** et **mc2** et **ga1** définissent la théorie purement équationnelle $\mathcal{Ga}$ des groupes abéliens. On doit alors remplacer, dans l'explication donnée page 6 pour les anneaux commutatifs, la machinerie calculatoire des polynômes commutatifs à coefficients entiers par la machinerie calculatoire des groupes abéliens libres.

Règles équationnelles

Les identités suivantes expriment le fait que $\vee$ définit un sup-demi treillis ainsi que la compatibilité de $\vee$ avec $+$.

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

On obtient ainsi un groupe réticulé (abélien) avec toutes les règles géométriques afférentes (voir [3], [22, Chapitre 2], [Bourbaki, Algèbre, Chapitre 6], et [13, Section XI-2]). En voici quelques unes.

Quelques règles dérivées dans $\mathcal{Grl}$

grl1 $\vdash x \vee (y_1 \wedge y_2) = (x \vee y_1) \wedge (x \vee y_2)$

grl2 $\vdash x \wedge (y_1 \vee y_2) = (x \wedge y_1) \vee (x \wedge y_2)$

grl3 $\vdash (x \wedge y) \vee x = x$

grl4 $\vdash (x \vee y) \wedge x = x$

grl5 $\vdash (x \wedge y) + (x \vee y) = x + y$

grl6 $\vdash x = x^+ - x^-$

grl7 $\vdash |x| = x^+ + x^- = x^+ \vee x^-$

Eo $x \geqslant 0, x \leqslant 0 \vdash x = 0$

Gauss $x \perp y, x \leqslant y + z \vdash x \leqslant z$

Grl1 $y \geqslant 0, z \geqslant 0, y \perp z \vdash (y - z)^+ = y$

Grl2 $nx \geqslant 0 \vdash x \geqslant 0 \quad (n \in \mathbb{N}, n > 1)$

Grl3 $x \leqslant z \vdash (x \wedge y) \vee z = x \wedge (y \vee z)$

Grl4 $nx \geqslant \wedge_{k=1}^{n}(ky + (n-k)x) \vdash x \geqslant y$

Les noyaux des morphismes surjectifs de groupes (abéliens) ordonnés sont les *sous-groupes convexes* : un sous-groupe H est dit convexe s'il vérifie :

$$(x \in H,\, 0 \leqslant y \leqslant x) \Rightarrow y \in H.$$

Les noyaux des morphismes surjectifs de groupes réticulés sont les *sous-groupes solides* : un sous-groupe solide est un sous-groupe réticulé convexe.

Théorème de plongement

En mathématiques classiques tout groupe réticulé est un sous-truc d'un produit de groupes totalement ordonnés.

La méthode de démonstration expliquée en [13, Principe XI-2.10] donne un «équivalent constructif» : *pour prouver un «fait concret» dans un groupe réticulé l'on peut toujours faire comme si l'on était en présence d'un produit de groupes totalement ordonnés.*

En fait, nous avons une «meilleure» formulation (plus formelle) dans le langage des théories dynamiques.

Définition 3.1.1 *La théorie dynamique* $\mathcal{G}$*tosup des* groupes totalement ordonnés avec sup *est la théorie dynamique des groupes réticulés à laquelle on ajoute la règle dynamique suivante (disant que l'ordre est total).*

OT $\vdash\ x \geqslant 0 \vee x \leqslant 0$

Notez que par rapport à la théorie usuelle des groupes totalement ordonnés, nous avons introduit dans la signature la loi $\cdot \vee \cdot$ qui est bien définie.

Théorème 3.1.2 *Les théories dynamiques* $\mathcal{G}rl$ *et* $\mathcal{G}$*tosup trouvent les mêmes faits.*

Comme conséquence en mathématiques classiques on obtient le théorème de plongement suivant.

Tout groupe réticulé est un sous-groupe-réticulé d'un produit de groupes totalement ordonnés.

3.2 Anneaux fortement réticulés (f-rings)

La terminologie «anneau fortement réticulé» pour les «f-rings» de la littérature anglaise se trouve dans les exercices de Bourbaki (Algèbre, chapitre 6). Les anneaux fortement réticulés sont définis par une théorie purement équationnelle (voir [3, 4, 17]).

Nous présentons ici seulement le cas commutatif, sous forme d'une théorie dynamique purement équationnelle.

Les axiomes sont ceux des anneaux commutatifs, ceux des groupes réticulés. et la règle équationnelle **afr** qui exprime la compatibilité de $\vee$ par rapport à la multiplication [4]. Voici tout en détail.

4. Par rapport à la théorie $\mathcal{G}rl$, on a ajouté la loi $\cdot \times \cdot$ et les règles **ac1** et **afr**. En outre, la machinerie calculatoire qui réduit tout terme à son écriture canonique dans le groupe abélien libre $\mathbb{Z}^n$ a été remplacée par la machinerie calculatoire qui réduit tout élément de $\mathbb{Z}[X_1, \ldots, X_n]$ à une forme normale.

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

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

Abréviations : comme pour les groupes réticulés.

Axiomes

Règles des anneaux commutatifs

mc1 $\vdash\ 0 = 0$

mc2 $x = 0,\ y = 0\ \vdash\ x + y = 0$

ac1 $x = 0\ \vdash\ xy = 0$

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

eqsup1 $x = 0\ \vdash\ (x + y) \vee z = y \vee z$

eqsup2 $x = 0\ \vdash\ y \vee (x + z) = y \vee z$

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

Note sur les anneaux réticulés (ℓ-rings)

La théorie $\mathcal{A}r\ell$ des anneaux réticulés (ℓ-rings dans la littérature anglaise) est définie en remplaçant la règle **afr** par les règles **ao1** et **ao2** des anneaux ordonnés, valides dans $\mathcal{A}fr$.

ao1 $\vdash\ a^2 \geqslant 0$

ao2 $x \geqslant 0,\ y \geqslant 0\ \vdash\ xy \geqslant 0$

Dans un anneau réticulé on a $|ab| \leqslant |a|\ |b|$. Pour le lemme suivant voir [3].

Lemme 3.2.1 *Sur la théorie des anneaux réticulés les règles suivantes sont toutes équivalentes.*

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

afr1 $\vdash\ |a|\ |b| = |ab|$

afr2 $\vdash\ (ab)^+ = a^+b^+ + a^-b^-$

afr3 $\vdash\ (ab)^- = a^+b^- + a^-b^+$

afr4 $\vdash\ c^+ |a| = |c^+a|$

Afr $a \geqslant 0\ \vdash\ a(b \vee c) = ab \vee ac$

Afr1 $a \wedge b = 0,\ x \geqslant 0\ \vdash\ a \wedge bx = 0$

Afr2 $a \perp b\ \vdash\ ca \perp cb$

Afr3 $a \wedge b = 0,\ c \geqslant 0\ \vdash\ ac \wedge bc = 0$

Autrement dit chacune de ces règles peut servir à définir les anneaux fortement réticulés.

Quelques règles dérivées dans $\mathcal{A}fr$

Outre les règles dérivées pour les groupes réticulés et celles signalées dans le paragraphe précédent, voici des règles classiques fort utiles où intervient la multiplication.

ao1 $\vdash\ a^2 \geqslant 0$

ao2 $x \geqslant 0,\ y \geqslant 0\ \vdash\ xy \geqslant 0$

afr5 $\vdash\ (a \wedge b)(a \vee b) = ab$

afr6 $\vdash\ a^2 = (a^+)^2 + (a^-)^2 = |a|^2$

Afr4 $a \wedge b = 0\ \vdash\ ab = 0$

Ato1 $y \geqslant 0,\ xy = 1\ \vdash\ x \geqslant 0$

Ato2 $c \geqslant 0,\ x(x^2 + c) \geqslant 0\ \vdash\ x^3 \geqslant 0$

afr7 $\vdash\ ab^+ = (ab \wedge (a^2+1)b) \vee (-(a^2+1)b \wedge 0)$

Remarque. La règle **afr7** sert à montrer la possibilité d'une forme simplifiée pour les termes dans un anneau fortement réticulé libre (voir le lemme 3.2.5). ■

Un exemple avec des nilpotents

L'exemple ici est celui que l'on doit garder en tête pour bien comprendre la différence entre les anneaux totalement ordonnés et les anneaux totalement ordonnés intègres.

Il s'agit de l'anneau totalement ordonné $\mathbb{Q}[\alpha]$ où $\alpha > 0$ et $\alpha^6 = 0$ (α est un infinitésimal > 0 nilpotent). Soit c un élément tel que $c^2 = 0$ (par exemple $c = \alpha^5$). Le système d'inégalités

$$(x-c)(x+c) = 0,\ x \geqslant c,\ x \geqslant -c,$$

qui a été suggéré pour décrire $c \vee -c$ sans utiliser le test de signe dans le cas d'un corps ordonné, admet maintenant une infinité de solutions : tous les $r\alpha^3 + y\alpha^4$ où $r > 0$ dans $\mathbb{Q}$ et y arbitraire dans $\mathbb{Q}[\alpha]$.

Structures quotients

Les noyaux des morphismes surjectifs d'anneaux fortement réticulés sont les *idéaux solides*[5] : un idéal est dit solide s'il est solide en tant que sous-groupe. L'idéal solide engendré par un élément a est $\mathcal{I}(a) = \{\ x \mid \exists y,\ |x| \leqslant |ya|\ \}$. On a $\mathcal{I}(a) = \mathcal{I}(|a|)$, $\mathcal{I}(a) \cup \mathcal{I}(b)$ engendre l'idéal solide $\mathcal{I}(|a| + |b|) = \mathcal{I}(|a| \vee |b|)$, et $\mathcal{I}(a) \cap \mathcal{I}(b) = \mathcal{I}(|a| \wedge |b|)$.

Collapsus et théorème de plongement pour les anneaux fortement réticulés

Définition 3.2.2 *La théorie dynamique* $\mathcal{A}$*tosup des* anneaux totalement ordonnés avec sup *est la théorie dynamique des anneaux totalement ordonnés à laquelle on ajoute un symbole de fonction* $\cdot \vee \cdot$ *qui doit satisfaire les règles algébriques suivantes.*

sup1 $\vdash\ x \vee y \geqslant x$ **Sup** $z \geqslant x,\ z \geqslant y\ \vdash\ z \geqslant x \vee y$

sup2 $\vdash\ x \vee y \geqslant y$

On peut aussi la voir comme la théorie des anneaux fortement réticulés à laquelle on ajoute comme axiome la règle dynamique **OT** *(disant que l'ordre est total).*

OT $\vdash\ x \geqslant 0 \vee x \leqslant 0$

Vu l'existence unique du sup dans un anneau totalement ordonné, la théorie dynamique des anneaux totalement ordonnés avec sup est essentiellement identique à la théorie des anneaux totalement ordonnés. En particulier, les théories $\mathcal{A}$*to* et $\mathcal{A}$*tosup* prouvent les mêmes règles dynamiques (lorsqu'elles sont formulées sans utiliser $\vee$).

Le théorème pour les anneaux fortement réticulés analogue au théorème 3.1.2 est le suivant.

Théorème 3.2.3 *Les théories* $\mathcal{A}$*fr et* $\mathcal{A}$*tosup prouvent les mêmes faits.*

5. L'ouvrage [3] dit un ℓ-idéal, ce qui semble correspondre à la terminologie dans la littérature anglaise.

Comme conséquence du théorème 3.2.3 on obtient en mathématiques classiques le théorème de plongement suivant

Tout anneau fortement réticulé est un sous-anneau-fortement-réticulé d'un produit d'anneaux totalement ordonnés.

Théorème 3.2.4 (Collapsus simultané)
Les théories Afr, Atosup et Codsup collapsent simultanément.

Localisation d'un anneau fortement réticulé

On considère un monoïde S dans un anneau fortement réticulé $\mathbf{A}$ et l'on construit la solution du problème universel (dans la catégorie des anneaux fortement réticulés) consistant à inverser les éléments de S.

Pour cela, il suffit de considérer le localisé usuel $S^{-1}\mathbf{A}$ et de définir correctement la loi $\vee$. Comme inverser s ou inverser s^2 revient au même, on peut ne considérer que des fractions à dénominateur $\geqslant 0$. On définit alors

$$\frac{a}{s} \vee \frac{b}{t} := \frac{at \vee bs}{st} \qquad (s, t \geqslant 0).$$

Réécriture de termes dans les anneaux fortement réticulés

Contrairement à la théorie des anneaux commutatifs où les termes se réécrivent sous une forme normale unique, on n'a pas pour les anneaux fortement réticulés un résultat aussi satisfaisant. On a néanmoins une réécriture sous une forme simplifiée (à l'image de la forme normale conjonctive dans les treillis distributifs).

Lemme 3.2.5 *Soit* $\mathbf{A}$ *un anneau fortement réticulé et* t *un terme écrit sur des éléments* $x_1, \ldots, x_n$ *de* $\mathbf{A}$. *Ce terme se réécrit sous forme*

$$\sup_{i \in I} \left(\inf_{j \in J_i} (f_{i,j}(\underline{x})) \right)$$

pour une famille finie convenable de polynômes $f_{i,j} \in \mathbb{Z}[X_1, \ldots, X_n]$.

Démonstration. Vu les réécritures usuelles dans les treillis distributifs et vu que $x \mapsto -x$ échange $\vee$ et $\wedge$, il suffit de savoir réécrire $a + (b \vee c)$ et $a\,(b \vee c)$ sous la forme voulue. Cela résulte des règles équationnelles **grl**, **grl6** et **afr7**. □

Notation 3.2.6 Soit $\mathbf{B}$ un anneau fortement réticulé dynamique (par exemple un simple anneau commutatif). Comme la théorie *Afr* est algébrique, $\mathbf{B}$ engendre un anneau fortement réticulé «statique» que l'on note AFR($\mathbf{B}$). Les éléments de cet anneau peuvent tous s'écrire sous la forme donnée dans le lemme 3.2.5.

Anneaux de fonctions fortement réticulés, semipolynômes

Pour tout ensemble E et tout anneau fortement réticulé $\mathbf{A}$ l'anneau des fonctions $f : E \to \mathbf{A}$ est muni d'une structure naturelle d'anneau fortement réticulé (c'est la structure produit).

Définition et notation 3.2.7 *Soit* $\varphi : \mathbf{A} \to \mathbf{B}$ *un morphisme d'anneaux fortement réticulés. L'anneau des* $\mathbf{A}$-semipolynômes (dans la littérature anglaise, les «SIPD») en n variables sur $\mathbf{B}$ *est le sous-anneau fortement réticulé de fonctions* $f : \mathbf{B}^n \to \mathbf{B}$ *engendré*

par les constantes dans $\varphi(\mathbf{A})$ et les fonctions coordonnées. On le notera $\mathrm{SIPD}_n(\mathbf{A},\mathbf{B})$. *On abrège* $\mathrm{SIPD}_n(\mathbf{A},\mathbf{A})$ *en* $\mathrm{SIPD}_n(\mathbf{A})$.
La définition s'étend au cas où $\mathbf{A}$ *et/ou* $\mathbf{B}$ *sont des anneaux totalement ordonnés, que l'on considère comme des anneaux fortement réticulés.*

Lemme 3.2.8 *Tout élément de* $\mathrm{SIPD}_n(\mathbf{A},\mathbf{B})$ *se réécrit sous forme* $\sup_{i\in I}\left(\inf_{j\in J_i}(f_{i,j})\right)$ *pour une famille finie convenable de polynômes* $f_{i,j}\in\mathbf{A}[x_1,\dots,x_n]$.

Démonstration. C'est à très peu près le lemme 3.2.5. □

Exemple 3.2.9
1. Les deux éléments $x\vee(1-x)$ et $1\vee x\vee(1-x)$ définissent la même fonction dans $\mathrm{SIPD}_1(\mathbb{Z})$, mais pas dans $\mathrm{SIPD}_1(\mathbb{Q})$.
2. Soit $\mathbf{K}=\mathbb{Q}(\epsilon)$ avec ϵ infinitésimal positif et $\mathbf{R}$ la clôture réelle de $\mathbf{K}$. Le semipolynôme $f=0\wedge-(x^2-\epsilon)(x^3-\epsilon)$ définit la fonction nulle sur $\mathbf{K}$ mais ne définit pas une fonction nulle sur $\mathbf{R}$: l'intervalle $[\epsilon^{1/2},\epsilon^{1/3}]$ est invisible sur $\mathbf{K}$. On peut «améliorer» cet exemple en prenant $\mathbf{K}=\mathbb{Q}[\epsilon]$ avec $\epsilon>0$ nilpotent convenable.

Anneaux strictement réticulés

On peut vouloir considérer une structure d'anneau fortement réticulé dans laquelle serait défini un prédicat $\cdot>0$ de manière aussi raisonnable que possible.

Nous avons mis le prédicat $\cdot\geqslant 0$ directement dans le langage plutôt que le définir à partir de $\cdot\vee\cdot$.

Définition 3.2.10 *La théorie algébrique* $\mathcal{Asr}$ *des* anneaux strictement réticulés *est basée sur le langage* $(\cdot=0,\cdot\geqslant 0,\cdot>0,\cdot+\cdot,\cdot\times\cdot,\cdot\vee\cdot,0,1,-1)$. *Les axiomes sont les suivants.*
- *les règles de la théorie purement équationnelle* $\mathcal{Afr}$ *(théorie des anneaux fortement réticulés),*
- *les règles directes de* **aso1** *à* **aso4**,
- *les règles algébriques* **Eo**, **Col**, **Iv**, **Aso1** *et* **Aso2**,
- *enfin, on a deux règles* **sge** *et* **Sge** *pour relier* $\cdot\geqslant 0$ *et* $\cdot\vee\cdot$ *:*

sge $\vdash\ x\vee y\geqslant x$ **Sge** $z\geqslant x,\ z\geqslant y\ \vdash\ z\geqslant x\vee y$

En passant de $\mathcal{Afr}$ à $\mathcal{Asr}$ on sort du cadre des théories purement équationnelles.

Définition 3.2.11 *La théorie dynamique* $\mathcal{Asto}$ *des* anneaux strictement totalement ordonnés *est la théorie* $\mathcal{Asr}$ *à laquelle on ajoute l'axiome* **OT**.
On peut aussi voir la théorie $\mathcal{Asto}$ *comme la théorie* $\mathcal{Atosup}$ *à laquelle on ajoute un prédicat* $\cdot>0$ *et les règles que l'on a ajoutées à* $\mathcal{Afr}$ *pour définir* $\mathcal{Asr}$.

Théorème 3.2.12 (Collapsus simultané)
Les théories $\mathcal{Afr}$, $\mathcal{Asr}$, $\mathcal{Asto}$, $\mathcal{Codsup}$ *et* $\mathcal{Crcdsup}$ *collapsent simultanément.*

3.3 Anneaux fortement réticulés réduits

Nous examinons ici la théorie algébrique $\mathcal{Afrnz}$ des anneaux fortement réticulés réduits. On ajoute donc à $\mathcal{Afr}$ la règle **Anz** des anneaux réduits, qui est algébrique.

Anz $a^2=0\ \vdash\ a=0$

En passant de *Afr* à *Afrnz* on sort du cadre des théories purement équationnelles.

Quelques règles dérivées dans Afrnz

Afrnz1 $x^3 \geqslant 0 \ \vdash \ x \geqslant 0$

Notez que de **Afrnz1** on déduit la même règle pour un exposant impair arbitraire qui remplace l'exposant 3.

On a aussi la réciproque suivante de la règle **Afr4**.

Afrnz2 $ab = 0 \ \vdash \ |a| \wedge |b| = 0$

Ainsi, pour $a, b \geqslant 0$, $ab = 0$ équivaut à $a \wedge b = 0$.

Aonz $c \geqslant 0,\ x(x^2 + c) \geqslant 0 \ \vdash \ x \geqslant 0$

Lemme 3.3.1 *Dans la théorie Afr les règles* **Afrnz1**, **Afrnz2**, **Aonz** *et* **Anz** *sont équivalentes.*

Les éléments réguliers $\geqslant 0$ dans un anneau fortement réticulé réduit

Lemme 3.3.2 *Soit* $\mathbf{A}$ *un anneau fortement réticulé réduit et* S^+ *le monoïde des éléments réguliers* $\geqslant 0$*.*

1. *Si l'on définit «* $x > 0$ *» par «* $x \in S^+$ *», l'anneau vérifie tous les axiomes algébriques de la théorie dynamique des corps ordonnés discrets.*
2. *L'anneau* $\mathbf{B} = S^{-1}\mathbf{A}$ *est muni d'une unique structure d'anneau fortement réticulé qui prolonge celle de* $\mathbf{A}$*. Si l'on définit «* $x > 0$ *» (dans* $\mathbf{B}$*) par «* x *est inversible et* $\geqslant 0$ *», l'anneau vérifie les axiomes algébriques de la théorie dynamique des corps ordonnés discrets ainsi que la règle dynamique* **IV***.*

Anneaux strictement réticulés réduits et anneaux fortement réels

Le lemme 3.3.2 légitime l'introduction de la notion suivante.

Définition 3.3.3

1. *La théorie algébrique Asrnz des* anneaux strictement réticulés réduits *est la théorie obtenue à partir de la théorie Asr en ajoutant la règle algébrique* **Anz***.*
2. *La théorie dynamique Aftr des* anneaux fortement réels *est la théorie Asrnz à laquelle on ajoute la règle dynamique* **IV***.*

De manière équivalente, un anneau fortement réel est une $\mathbb{Q}$-algèbre fortement réticulée réduite dans laquelle les éléments inversibles et $\geqslant 0$ (que l'on dit > 0) vérifient la règle **aso3**, c'est-à-dire ici : tout élément plus grand qu'un élément inversible positif est inversible.

Théorèmes de plongement

Un anneau totalement ordonné réduit est sans diviseur de zéro. En effet si $ab = 0$, alors $|a| \wedge |b| = 0$ (**Afrnz2**), et comme l'ordre est supposé total l'un des deux est nul.

La théorie *Atosupnz* (*anneaux totalement ordonnés avec sup réduits*) est obtenue à partir de la théorie *Afrnz* en ajoutant la règle **OT** (ordre total). On peut aussi la voir comme la théorie *Atosup* (anneaux totalement ordonnés avec sup) à laquelle on ajoute la règle **Anz**.

Théorème 3.3.4 (Positivstellensatz formel, 2)

1. *Les théories dynamiques* ***Asrnz****,* ***Aftr****,* ***Codsup*** *et* ***Crcdsup*** *prouvent les mêmes faits (formulés dans le langage des anneaux strictement réticulés).*
2. *Les théories dynamiques* ***Afrnz****,* ***Atosupnz****,* ***Codsup*** *et* ***Crcdsup*** *prouvent les mêmes faits (formulés dans le langage des anneaux fortement réticulés).*

En mathématiques classiques on en déduit le théorème de plongement suivant.

Un anneau fortement réticulé réduit est un sous-truc d'un produit d'anneaux totalement ordonnés intègres

Anneaux de fonctions fortement réticulés réduits

L'anneau $\mathrm{SIPD}_n(\mathbf{A})$ des semipolynômes sur $\mathbf{A}$ en n variables est défini en 3.2.7.

Théorème 3.3.5

1. *Soit* $\mathbf{K}$ *un corps ordonné discret et* $\mathbf{R}$ *sa clôture réelle. L'anneau* $\mathrm{SIPD}_n(\mathbf{K},\mathbf{R})$ *s'identifie à l'anneau fortement réticulé engendré par* $\mathbf{K}[x_1,\dots,x_n]$*. Plus précisément : la structure de* $\mathbf{K}$ *confère à* $\mathbf{K}[x_1,\dots,x_n]$ *une structure d'anneau fortement réticulé dynamique et l'unique* $\mathbf{K}$*-morphisme d'anneaux fortement réticulés de* $\mathrm{AFR}(\mathbf{K}[x_1,\dots,x_n])$ *vers* $\mathrm{SIPD}_n(\mathbf{K},\mathbf{R})$ *est un isomorphisme.*
2. *Soit* $\mathbf{K}$ *un corps ordonné discret et* $\mathbf{R}$ *sa clôture réelle. Si tout ouvert semialgébrique de* $\mathbf{R}^n$ *contient des points de* $\mathbf{K}^n$ *l'anneau* $\mathrm{SIPD}_n(\mathbf{K})$ *s'identifie à l'anneau fortement réticulé engendré par* $\mathbf{K}[x_1,\dots,x_n]$*.*
3. *Si* $\mathbf{K}$ *est une* $\mathbb{Q}$*-algèbre contenue dans* $\mathbb{R}$*, l'anneau* $\mathrm{SIPD}_n(\mathbf{K})$ *s'identifie à l'anneau fortement réticulé engendré par* $\mathbf{K}[x_1,\dots,x_n]$*.*

4 Corps ordonnés généraux

Rappelons les règles dynamiques suivantes satisfaites par les corps ordonnés discrets.

IV	$x^2>0 \vdash \exists y\, xy=1$	**OT**	$\vdash x\geqslant 0 \vee x\leqslant 0$
ED	$\vdash x\neq 0 \vee x=0$	**OTF**	$x+y>0 \vdash x>0 \vee y>0$

Le corps des réels ne vérifie ni **ED**, ni **OT**.

4.1 Corps ordonnés avec sup

La théorie dynamique ***Codsup*** des corps ordonnés discrets avec sup n'est pas acceptable pour le corps des réels. Par contre la théorie suivante donne une bonne base de travail.

Définition 4.1.1 *La* théorie dynamique de base pour les corps ordonnés avec sup*, notée* ***BasicCosup****, est la théorie des anneaux strictement réticulés réduits locaux : plus précisément, on ajoute comme axiomes à la théorie* ***Asrnz*** *(définition 3.2.10) la règle algébrique* **Anz** *et les règles dynamiques* **OTF** *et* **IV***.*
NB. On peut aussi la voir comme la théorie ***Codsup*** *(définition 2.2.1) dans laquelle on a remplacé les axiomes* **DE** *et* **OT** *par l'axiome* **OTF***.*

Théorème 4.1.2 (Positivstellensatz formel, 3)
Les théories dynamiques suivantes prouvent les mêmes faits (formulés dans le langage des anneaux strictement réticulés).

1. *La théorie* $\mathcal{A}srnz$ *des anneaux strictement réticulés réduits.*
2. *La théorie* $\mathcal{A}ftr$ *des anneaux fortement réels.*
3. *La théorie de base des corps ordonnés avec sup :* $\mathcal{B}asicCosup$.
4. *La théorie* $\mathcal{A}tosupnz$ *des anneaux totalement ordonnés réduits.*
5. *La théorie* $\mathcal{C}odsup$ *des corps ordonnés discrets avec sup.*
6. *La théorie* $\mathcal{C}rcdsup$ *des corps réels clos discrets avec sup.*

Remarque. La morale de la chose est la suivante : dans [8], on a des résultats analogues sans la fonction $\cdot\vee\cdot$; on en déduit le résultat pour $\mathcal{A}srnz$, $\mathcal{C}odsup$ et $\mathcal{C}rcdsup$. Les autres théories sont intermédiaires. ■

On prend désormais pour point de départ la «théorie de base des corps ordonnés avec sup» $\mathcal{B}asicCosup$ (définition 4.1.1), et l'on explore les règles dynamiques à ajouter pour mieux approcher les propriétés algébriques de $\mathbb{R}$ lorsqu'elles sont démontrables en mathématiques constructives sans utiliser l'axiome du choix dépendant.

4.2 Des règles pour d'autres opérations «rationnelles» continues

On note $\mathbf{R}_{\mathrm{a}}$ le corps des réels algébriques.

On rappelle que $\mathbf{R}_{\mathrm{a}}$ est un corps réel clos discret an sens constructif.

Dans la section 3 on a beaucoup insisté sur la fonction sup, mais d'autres fonctions «rationnelles» posent le même type de problèmes. Un exemple pour commencer

$$\frac{(ax+by)xy}{x^2+y^2} \tag{5}$$

Cette fraction rationnelle est le prototype d'une famille (paramétrée par a, b) de fonctions réelles continues $\mathbb{R}^2 \to \mathbb{R}$ (ou d'une fonction réelle continue $\mathbb{R}^4 \to \mathbb{R}$).

Une règle dynamique «définit» cette fonction :

$$\vdash\ \exists z\quad \big(z(x^2+y^2) = (ax+by)xy,\ |z| \leqslant |ax+by|\,\big) \tag{6}$$

et elle ne semble pas valide dans la théorie de base $\mathcal{B}asicCosup$.

Question 4.2.1 La règle algébrique (6) qui équivaut à l'existence de la fonction (5) n'est pas prouvable dans $\mathcal{B}asicCosup$?

Dans cet exemple, si $a = b = 1$, la 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 la règle dynamique suivante est valide pour $\mathbb{R}$, et aussi bien pour les corps réels clos discrets :

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

Intuitivement cette règle signifie que la fraction u/v est bien définie : si $v \neq 0$ c'est clair, si $v = 0$ on force $z = 0$. On vérifie d'ailleurs que l'existence est bien unique en s'appuyant uniquement sur les axiomes de $\mathcal{A}frnz$ comme suit.
Si $zv = u$, $|z|^n \leqslant |v|$, $z'v = u$, $|z'|^n \leqslant |v|$, on pose $w = |z - z'|$ et l'on obtient : $w\,|v| = 0$, $w \leqslant |z| + |z'| \leqslant 2|v|^{\frac{1}{n}}$, $w^n \leqslant 2^n|v|$, $0 \leqslant w^{n+1} \leqslant 2^n\,|v|\,w = 0$, donc $w^{n+1} = 0$ et enfin $w = 0$.

Définition 4.2.2 *La* théorie dynamique de base des corps ordonnés, *notée* $\mathcal{BasicCo}$, *est l'extension de la théorie* $\mathcal{BasicCosup}$ *obtenue en ajoutant les règles dynamiques* FRAC_n *pour les entiers* $n \geqslant 1$.

Question 4.2.3 Dans la théorie des anneaux réels clos en mathématiques classiques (voir [18]), les auteurs ont introduit l'axiome :

$$\text{Si } 0 \leqslant a \leqslant b \text{ alors } b \text{ divise } a^2.$$

Pour assurer l'unicité, on peut considérer la règle dynamique suivante

$$\mathsf{FRAC} \quad 0 \leqslant a \leqslant b \ \vdash \ \exists z \ (zb = a^2,\ 0 \leqslant z \leqslant a)$$

Elle signifie que la fraction a^2/b est bien définie. Cette règle découle de FRAC_1 en posant $u = a^2$ et $v = b$.
La question qui se pose est la suivante : est-ce que dans le cadre de la théorie $\mathcal{BasicCosup}$, ou dans la cadre de la théorie $\mathcal{Covr}$ (section 5) la règle **FRAC** implique les règles FRAC_n **?**

Question 4.2.4 Soit $\mathbf{R}$ un corps réel clos discret. Disons qu'une fonction semialgébrique continue $\mathbf{R}^n \to \mathbf{R}$ est «rationnelle» si elle est, sur un ouvert semialgébrique dense, égale à un quotient de deux semipolynômes.
Est-ce que la théorie $\mathcal{BasicCo}(\mathbf{R})$ permet de capturer toutes les fonctions semialgébriques continues rationnelles ?

Exemple 4.2.5 De nombreux sous-corps «naturels» de $\mathbb{R}$ sont *non* discrets, par exemple le corps énumérable $\mathbb{R}_{\mathsf{PR}}$ des réels calculables en temps primitif récursif, ou celui des réels calculables en temps polynomial, ou encore celui des réels récursifs. Ce sont des modèles de $\mathcal{BasicCo}$, et aussi de certaines extensions de $\mathcal{BasicCosup}$ que nous définissons par la suite, comme $\mathcal{Covr}$ ou $\mathcal{Crc}$.

4.3 Axiomes de clôture réelle valides sur $\mathbb{R}$

Comme axiomes de clôture réelle acceptables constructivement pour le corps des réels, on doit au minimum introduire les (fonctions) **racines virtuelles** des polynômes unitaires (voir [11, 7]). Avec les axiomes adéquats (qui sont des règles dynamiques).

En fait il est probable qu'il faille introduire un symbole de fonction pour toute fonction semialgébrique continue $\mathbf{R}_{\mathrm{a}}^n \to \mathbf{R}_{\mathrm{a}}$. En effet, une fonction semialgébrique continue $\mathbf{R}^n \to \mathbf{R}$ est localement uniformément continue, donc prolongeable sur $\mathbb{R}^n$.

L'ajout de ces fonctions et des axiomes adéquats peut se faire en restant dans le cadre des théories dynamiques. En outre, les fonctions semialgébriques continues $\mathbf{R}_{\mathrm{a}}^n \to \mathbf{R}_{\mathrm{a}}$ sont définies sur $\mathbb{Q}$.

Nous approfondissons ces questions dans les sections 5 et 6.

Auparavant nous proposons la définition suivante en mathématiques constructives.

Définition 4.3.1 *Une fonction* $f : \mathbb{R}^n \to \mathbb{R}$ *est dite* semialgébrique continue *si*

1. f *est algébrique sur* $\mathbb{R}[X_1, \ldots, X_n] = \mathbb{R}[\underline{X}]$ *: précisément, on a un polynôme* $g \in \mathbb{R}[\underline{X}, Y]$ *ayant au moins un de ses coefficients en* Y *(éléments de* $\mathbb{R}[\underline{X}]$*) clairement non nul tel que* $P(\underline{x}, f(\underline{x})) = 0$ *pour tout* $(\underline{x}) \in \mathbb{R}^n$.
2. f *possède un «module de continuité uniforme sur tout compact» à la Łojasiewicz.*

Cette définition est légitime 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 serait assez satisfait d'une théorie dynamique des propriétés algébriques de $\mathbb{R}$ si les axiomes permettaient de capturer dans la théorie toutes les fonctions répondant à la définition 4.3.1. Le problème revient donc à algébriser cette définition !

5 Corps ordonnés avec racines virtuelles

L'idée des racines virtuelles est d'avoir pour un polynôme unitaire réel des fonctions continues des coefficients qui recouvrent les racines réelles. Quand une racine réelle s'évanouit dans le plan complexe, on peut la relayer par la racine de la dérivée qui coïncide avec la racine réelle double au moment où elle disparaît.

Par exemple les racines carrées virtuelles d'un réel arbitraire a sont $\pm\sqrt{a}$ lorsque $a \geqslant 0$, et dans le cas contraire, elles sont nulles : c'est la valeur qu'elles avaient au moment de disparaître.

5.1 Rappels concernant les racines virtuelles

Références [11, 7, 1, 2, 9].

Définition et premières propriétés

Rappelons tout d'abord le théorème algébrique des accroissements finis.

Lemme 5.1.1 (Théorème algébrique des accroissements finis, [15, 14])
Il existe deux familles $(\lambda_{i,j})_{1\leqslant i\leqslant j\leqslant n}$ et $(r_{i,j})_{1\leqslant i\leqslant j\leqslant n}$ dans $\mathbb{Q}\cap\,]0,1[$ avec $\sum_{i=1}^n r_{i,n} = 1$ pour tout $n \geqslant 1$ et telles que, pour tout polynôme $f \in \mathbb{Q}[X]$ de degré $\leqslant n$, on ait dans $\mathbb{Q}[a,b]$:

$$f(b) - f(a) = (b-a) \times \sum_{i=1}^{n} r_{i,n} \cdot f'(a + \lambda_{i,n}(b-a)).$$

Le résultat s'applique à toute $\mathbb{Q}$-algèbre $\mathbf{A}$ (en particulier aux corps ordonnés sans test de signe). Si $\mathbf{A}$ est un anneau fortement réticulé, cela montre qu'un polynôme dont la dérivée est $\geqslant 0$ sur un intervalle est une fonction croissante sur l'intervalle. Si $\mathbf{A}$ est strictement réticulé, cela montre qu'un polynôme dont la dérivée est > 0 sur un intervalle est une fonction strictement croissante sur l'intervalle.

Exemple 5.1.2 *Par exemple pour les polynômes de degré $\leqslant 4$ on a avec $\Delta = b - a$*

$$f(b) - f(a) = \Delta \cdot \big(\tfrac{1}{3}\, f'(a + \tfrac{5}{6}\Delta) + \tfrac{1}{6}\, f'(a + \tfrac{2}{3}\Delta) + \tfrac{1}{6}\, f'(a + \tfrac{1}{3}\Delta) + \tfrac{1}{3}\, f'(a + \tfrac{1}{6}\Delta)\big).$$

Ce qui est affirmé en 5.1.3, 5.1.4 et 5.1.5 pour $\mathbb{R}$ est également valable sur tout corps réel clos discret.

Lemme 5.1.3

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 $x \in [a, b]$. 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. *Un énoncé analogue au précédent, laissé au lecteur, pour une fonction continue strictement monotone $f :]-\infty, a] \to \mathbb{R}$.*

Le lemme est également valable pour un corps réel clos discret si f est une fonction semialgébrique continue.

À partir de cette constatation on obtient la construction des «racines virtuelles» pour un polynôme unitaire de degré d : d'une part elles «couvrent» toutes les racines réelles, d'autre part elles varient continument en fonction des coefficients du polynôme.

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

Proposition et définition 5.1.4 *Pour tout polynôme unitaire*

$$f(X) = X^{d+1} - (a_d X^d + \cdots + a_1 X + a_0)$$

on définit les fonctions racines virtuelles de f

$$\rho_{d+1,j}(f) = \rho_{d+1,j}(a_d, \ldots, a_0)$$

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

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

Cette proposition se démontre simultanément avec les points *3d* et *3e* du théorème qui suit, en utilisant le lemme 5.1.1.

Théorème 5.1.5 (Quelques propriétés des racines virtuelles, [11, 7])

1. *Vu le lemme 5.1.3, 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 $\rho_{d,j} : \mathbb{R}^d \to \mathbb{R}$ est uniformément continue sur toute boule*[6] $\mathrm{B}_{d,M}$.

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

3. Pour un 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 $\rho_{d,1} \leqslant \rho_{d-1,1} \leqslant \cdots \leqslant \rho_{d-1,j} \leqslant \rho_{d,j+1} \leqslant \rho_{d-1,j+1} \leqslant \cdots \leqslant \rho_{d-1,d-1} \leqslant \rho_{d,d}$.

(b) Si $d \geqslant 2$ et $f = X^d - a$, alors $\rho_{d,d} = \sqrt[d]{a^+}$; pour d impair, $\rho_{d,1} + \rho_{d,d} = \sqrt[d]{a}$.

(c) Si $f = \prod_{i=1}^{d}(X - \xi_i)$ pour des $\xi_i \in \mathbb{R}$, alors $\widetilde{f} = f$. En particulier $\rho_{d,1} = \inf_i(\xi_i)$ et $\rho_{d,d} = \sup_i(\xi_i)$.

(d) Si $\rho_{d-1,j} < \rho_{d-1,j+1}$, alors f est strictement monotone sur l'intervalle, croissante si $d - j$ impair, décroissante sinon ($0 \leqslant j \leqslant d-1$).

(e) Si $\rho_{d,j} < \xi < \rho_{d,j+1}$, alors $(-1)^{d-j} f(\xi) > 0$ ($0 \leqslant j \leqslant d$).

(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 $\widetilde{f}(\xi) \neq 0$, alors $f(\xi) \neq 0$.*
- *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 $\widetilde{f}^{[k+1]}(\xi) \neq 0$, alors $f^{[k+1]}(\xi) \neq 0$.*

(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 $\xi \in \mathbb{R}$ tel que les $f^{[k]}(\xi) \neq 0$ pour $0 \leqslant k \leqslant d$. Soit r le nombre de changements de signes dans la suite des $f^{[k]}(\xi)$.*
Alors $\rho_{d,d-r} < \xi < \rho_{d,d-r+1}$.

(i) (Théorème de la valeur intermédiaire) *Si $a < b$ et $f(a)f(b) < 0$, on a*

$$\prod_{j=1}^{d} f(\mu_j) = 0 \quad \text{où } \mu_j = a \vee (b \wedge \rho_{d,j}).$$

(j) (Théorème de la valeur maximum) *Le polynôme unitaire f atteint sa borne supérieure sur tout intervalle fermé borné. Plus précisément, si $a < b$, on a*

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

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

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

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

Exemple 5.1.6 Nous explicitons ici quelques unes des inégalités évoquées dans le point *1* du théorème précédent pour un polynôme $f(X) = X^4 - (a_3X^3 + a - 2X^2 + a_1X + a_0)$, écrites ici sous forme de règles directes. On reprend les conventions du point *3* du théorème 5.1.5. Ainsi, on pose $\rho_{1,1} = \rho_{1,1}(\frac{a_3}{4})$, $\rho_{2,j} = \rho_{2,j}(\frac{a_3}{2}, \frac{a_2}{6})$, $\rho_{3,j} = \rho_{3,j}(\frac{3a_3}{4}, \frac{a_2}{2}, \frac{a_1}{4})$, $\rho_{4,j} = \rho_{4,j}(a_3, a_2, a_1, a_0)$.

$$\mathbf{vr}_{1,1} \ \vdash \ \rho_{1,1} = \tfrac{a_3}{4}$$

$$\mathbf{vr}_{2,2,0} \ \vdash \ \rho_{1,1} \leqslant \rho_{2,2} \qquad \mathbf{vr}_{2,2,2} \ \vdash \ (\rho_{2,2} - \rho_{1,1})\, f^{[2]}(\rho_{2,2}) \leqslant 0$$
$$\mathbf{vr}_{2,2,1} \ \vdash \ (\rho_{2,2} - \rho_{1,1})\, f^{[2]}(\rho_{1,1}) \leqslant 0 \qquad \mathbf{vr}_{2,2,3} \ \vdash \ f^{[2]}(\rho_{2,2}) \geqslant 0$$

$$\Delta_{3,2} = \rho_{2,2} - \rho_{2,1}$$

$$\mathbf{vr}_{3,2,0} \ \vdash \ \rho_{2,1} \leqslant \rho_{3,2} \leqslant \rho_{2,2}$$
$$\mathbf{vr}_{3,2,1} \ \vdash \ (\rho_{3,2} - \rho_{2,1})\, f^{[1]}(\rho_{2,1})\, \Delta_{3,2} \leqslant 0 \qquad \mathbf{vr}_{3,2,3} \ \vdash \ (\rho_{3,2} - \rho_{2,1})\, f^{[1]}(\rho_{3,2})\, \Delta_{3,2} \leqslant 0$$
$$\mathbf{vr}_{3,2,2} \ \vdash \ (\rho_{3,2} - \rho_{2,2})\, f^{[1]}(\rho_{2,2})\, \Delta_{3,2} \leqslant 0 \qquad \mathbf{vr}_{3,2,4} \ \vdash \ (\rho_{3,2} - \rho_{2,2})\, f^{[1]}(\rho_{3,2})\, \Delta_{3,2} \leqslant 0$$

$$\mathbf{vr}_{4,3,0} \vdash \rho_{3,2} \leqslant \rho_{4,3} \leqslant \rho_{3,3} \qquad \Delta_{4,3} = \rho_{3,3} - \rho_{3,2}$$
$$\mathbf{vr}_{4,3,1} \vdash (\rho_{4,3} - \rho_{3,2})\, f(\rho_{3,2})\, \Delta_{4,3} \leqslant 0 \qquad \mathbf{vr}_{4,3,3} \vdash (\rho_{4,3} - \rho_{3,2})\, f(\rho_{4,3})\, \Delta_{4,3} \leqslant 0$$
$$\mathbf{vr}_{4,3,2} \vdash (\rho_{4,3} - \rho_{3,3})\, f(\rho_{3,3})\, \Delta_{4,3} \leqslant 0 \qquad \mathbf{vr}_{4,3,4} \vdash (\rho_{4,3} - \rho_{3,3})\, f(\rho_{4,3})\, \Delta_{4,3} \leqslant 0$$

Un résultat à la Pierce-Birkhoff

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

Le théorème «à la Pierce-Birhoff» suivant mérite d'être signalé.

Théorème 5.1.7 ([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* $\mathbf{R}[x_1, \ldots, x_m]$ *(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*

$$\rho_{d,j}(P) + \sqrt[r]{R_\ell^+ \cdot \left(1 + \| \underline{x} \|^2\right)^s} \tag{7}$$

pour des $R_\ell \in \mathbf{R}[x_1, \ldots, x_m]$ *(les deux termes dans la somme (7) sont des polyracines).*

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 $f_i \in \mathbf{R}[x_1, \ldots, x_m]$. Dans l'expression obtenue en (7) pour g,, c'est Łojasiewicz qui est responsable de l'extraction de racine r-ème dans la formule. ■

5.2 Corps ordonnés avec racines virtuelles

Définition 5.2.1 *La théorie dynamique* Covr *des* corps ordonnés avec racines virtuelles *est obtenue comme suit à partir de la théorie dynamique* BasicCosup.

- *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 5.1.5.*

Les théories Crcd et Crcdsup sont essentiellement identiques à la théorie obtenue en ajoutant à Covr les axiomes «de tiers exclu» **ED** et **OT**.

Théorème 5.2.2 (Positivstellensatz formel, 4)

1. *Les théories* Asrnz, BasicCosup, Covr *et* Crcdsup *prouvent les mêmes faits (énoncés dans le langage des anneaux strictement réticulés).*
2. *Les points 2 et 3 du théorème 5.1.5 sont valides pour tout corps ordonné avec racines virtuelles.*

Définition 5.2.3 *Soit* $\mathbf{R}$ *un corps ordonné avec racines virtuelles. La famille d'anneaux* $\mathrm{Sace}_m(\mathbf{R})$ *(*$m \in \mathbb{N}$*) est définie comme la plus petite famille stable par composition contenant les fonctions polynômes et les fonctions racines virtuelles. En d'autres mots, un élément de* $\mathrm{Sace}_m(\mathbf{R})$ *est une fonction définie par un terme du langage de* Covr *monté sur des constantes dans* $\mathbf{R}$ *et sur exactement* m *variables* $x_1, \ldots, x_m$.

Il est clair que les éléments de $\mathrm{Sace}_m(\mathbb{R})$ sont des fonctions semialgébriques continues (définition 4.3.1) entières sur le sous-anneau $\mathbb{R}[x_1, \ldots, x_m]$, mais la réciproque n'est pas claire.

Question 5.2.4 Est-ce que toute fonction semialgébrique continue $\mathbb{R}^m \to \mathbb{R}$ entière sur l'anneau des polynômes est un élément de $\mathrm{Sace}_m(\mathbb{R})$?

La réponse est «oui» en mathématiques classiques car en mathématiques classiques on peut appliquer le théorème 5.1.7 à $\mathbb{R}$. La réponse en mathématiques constructives semble nettement plus difficile. Peut-être il faudrait d'abord répondre à la question qui suit.

Question 5.2.5 A-t-on le résultat analogue au théorème 5.1.7 pour tout corps ordonné avec racines virtuelles $\mathbf{R}$? Plus précisément, est-ce que tout élément de $\mathrm{Sace}_m(\mathbf{R})$ est une combinaison par $\vee$, $\wedge$ de fonctions exprimées sous la forme (7) ?

5.3 Construction de la clôture avec racines virtuelles d'un corps ordonné

On considère un «corps ordonné», précisément une structure algébrique $\mathbf{K}$ de type *BasicCosup*. On sait que *Covr* est une extension conservative de *BasicCosup*. Notons $\mathbf{R}$ la structure algébrique dynamique $(\mathbf{K}, \mathit{Covr})$. Tous les termes de $\mathbf{R}$ sont obtenus comme polyracines itérées construits sur des éléments de $\mathbf{K}$.

Ainsi, $\mathbf{R}$ est le candidat naturel pour être la structure algébrique de type *Covr* engendrée par $\mathbf{K}$, si cela a un sens. Mais *Covr* n'est pas une théorie algébrique, donc la réponse n'est pas assurée.

En effet $\mathbf{R}$ est a priori une structure algébrique dynamique de type *Covr*, mais pas forcément un modèle de cette théorie. La question qui se pose semble donc être la suivante : les axiomes dynamiques (non algébriques) de la théorie *Covr*, i.e. **IV** et **OTF** sont-ils satisfaits dans $\mathbf{R}$?

La réponse n'est pas évidente. Le problème essentiel ne semble pas être du coté de l'axiome **IV** (car on saura de tout manière construire l'anneau des fractions dont le dénominateur est un élément > 0), mais du coté de **OTF**. La question vraiment pertinente serait en définitive la suivante.

Question 5.3.1 Avec les notations précédentes, la règle **OTF** est-elle satisfaite dans $\mathbf{R}$? Précisément, étant donnés deux éléments α et β de $\mathbf{R}$ tels que la règle $\vdash\ \alpha + \beta > 0$ est prouvable, est-il vrai que l'une des deux règles $\vdash\ \alpha > 0$, $\vdash\ \beta > 0$ soit prouvable ?

5.4 Anneaux strictement réticulés avec racines virtuelles

Exemple 5.4.1 Nous reprenons l'exemple de la $\mathbb{Q}$-algèbre totalement ordonnée $\mathbb{Q}[\alpha]$, avec $\alpha > 0$ et $\alpha^6 = 0$. Nous allons voir que les contraintes imposées pour $\rho_{2,2}(f)$, où $f = X^2 - a^2$ et $a > 0$, n'impliquent pas nécessairement que $\rho_{2,2} = a$. Les contraintes sont les suivantes pour $x = \rho_{2,2}$ (notez que $\rho_{1,1} = 0$) :

$\mathbf{vr}_{2,2,0}\ \vdash\ 0 \leqslant x$

$\mathbf{vr}_{2,2,1}\ \vdash\ -x\,a^2 \leqslant 0$

$\mathbf{vr}_{2,2,2}\ \vdash\ x\,(x^2 - a^2) \leqslant 0$

$\mathbf{vr}_{2,2,3}\ \vdash\ (x^2 - a^2) \geqslant 0$

Si nous prenons $a = \alpha$, tous les les $x \geqslant 0$ tels que $x^2 = a^2$ conviennent, et donc tous les $\alpha + y\alpha^5$ pour $y \in \mathbb{Q}[\alpha]$ sont solutions. Si nous prenons $a^2 = 0$ les contraintes équivalent à «$x \geqslant 0$ et $x^3 \leqslant 0$» et tout élément de l'intervalle $[0, \alpha^2]$ est solution, y compris $\zeta = \alpha^2$ alors que $\zeta^2 \neq 0$.

L'exemple précédent justifie en partie les définitions qui suivent.

Définition 5.4.2

1. *La théorie purement équationnelle* $\mathcal{A}frvr$ *des* anneaux fortement réticulés avec racines virtuelles *est obtenue à partir de la théorie algébrique* $\mathcal{A}fr$ *de la même manière que la théorie* $\mathcal{C}ovr$ *est obtenue à partir de la théorie* $\mathcal{B}asicCosup$.
   En outre on ajoute la règle **vrsup** $\vdash \ \rho_{2,2}(a+b,-ab) = a \vee b$.
2. *La théorie algébrique* $\mathcal{A}srvr$ *des* anneaux strictement réticulés avec racines virtuelles *est obtenue à partir de la théorie algébrique* $\mathcal{A}sr$ *des anneaux strictement réticulés de la même manière que la théorie* $\mathcal{C}ovr$ *est obtenue à partir de la théorie* $\mathcal{B}asicCosup$.
   En outre on ajoute la règle **vrsup**.

Notons qu'un anneau fortement réticulé avec racines virtuelles est réduit. En effet, vu la règle **vrsup**, si $a^2 = 0$, on a $0 = \rho_{2,2}(0,0) = \rho_{2,2}(0,a^2) = |a|$.

Théorème 5.4.3 *Le théorème 5.1.5 est entièrement valable pour les anneaux strictement réticulés avec racines virtuelles. Il en va de même pour les anneaux fortement réticulés avec racines virtuelles (théorie purement équationnelle !) si les points qui utilisent* > 0 *sont supprimés ou convenablement reformulés avec* $\geqslant 0$.

Théorème 5.4.4 (Positivstellensatz formel, 5)
Les théories dynamiques suivantes prouvent les mêmes faits (formulés dans le langage des anneaux strictement réticulés avec racines virtuelles).

1. *La théorie* $\mathcal{A}srvr$ *des anneaux strictement réticulés avec racines virtuelles.*
2. *La théorie* $\mathcal{C}ovr$ *des corps ordonnés avec racines virtuelles.*
3. *La théorie* $\mathcal{C}odvr$ *des corps ordonnés discrets avec racines virtuelles.*

Si l'on considère des faits formulés dans le langage des anneaux strictement réticulés, les théories suivantes prouvent également les mêmes faits.

4. *La théorie* $\mathcal{A}srnz$ *des anneaux strictement réticulés réduits.*
5. *La théorie de base des corps ordonnés avec sup :* $\mathcal{B}asicCosup$.
6. *La théorie* $\mathcal{C}odsup$ *des corps ordonnés discrets avec sup.*
7. *La théorie* $\mathcal{C}rcdsup$ *des* corps réels clos discrets avec sup.

Démonstration. Comme pour les Positivstellensätze formels 4.1.2 et 5.2.2 il s'agit d'une variante du théorème 3.3.4. □

17-ème problème de Hilbert

Question 5.4.5 Dans quelle mesure la solution constructive 17-ème problème de Hilbert pour $\mathbb{R}$ (voir [10, section 6.1]) s'applique à tout anneau strictement réticulé avec racines virtuelles ?

Anneaux de Pierce-Birkhoff

Définition 5.4.6 *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* AFRVR(**A**) *est l'*anneau fortement réticulé avec racines virtuelles engendré par **A**.
3. *L'anneau* PPM(**A**) *est défini comme le sous anneau de* AFRVR(**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* **A** *est appelé un* anneau de Pierce-Birkhoff *lorsque le morphisme naturel* AFRNZ(**A**) $\to$ PPM(**A**) *est un isomorphisme.*

Question 5.4.7 En mathématiques classiques, la définition d'un anneau de Pierce-Birkhoff donnée ci-dessus coïncide-t-elle avec la notion définie dans [16, Madden] ?

6 Une théorie dynamique des corps réels clos non discrets

À titre provisoire, on prendra la définition suivante pour la théorie des corps réel clos «non discrets».

Définition 6.1 *La* théorie dynamique de base pour les corps réels clos*, notée* ***BasicCrc****, est l'extension de la théorie* ***Covr*** *obtenue en ajoutant les règles dynamiques* **FRAC**$_n$ *pour les entiers $n \geqslant 1$.*

Remarques 6.2
1) Le corps $\mathbb{R}$ est un modèle constructif de la théorie ***BasicCrc***.

2) La théorie ***Crcd*** est essentiellement identique à la théorie obtenue en ajoutant à ***BasicCrc*** les axiomes **OT** et **DE**.

3) D'un point de vue constructif, si l'on retire les règles dynamiques **IV** et **OTF**, on espère obtenir une théorie dynamique pour les anneaux de fonctions réelles semialgébriques continues sur les compacts semialgébriques. Cette théorie, notée ***Asrrc***, peut être définie comme la théorie ***Asrvr*** à laquelle on ajoute les règles dynamiques **FRAC**$_n$.

4) La théorie dynamique ***Asrrc*** est étroitement reliée à la structure d'*anneau réel clos* définie par N. Schwartz de manière très abstraite, et simplifiée dans [18]. Intuitivement, un anneau réel clos est un anneau fortement réticulé normal sur lequel sont définies toutes les fonctions semialgébriques continues définies sur $\mathbf{R}_{\mathrm{a}}$. Le problème est cependant que $\mathbb{R}$ est un modèle constructif de la théorie ***Asrrc*** mais *n'est pas* normal, car un anneau local normal est sans diviseur de zéro, alors que $\mathbb{R}$ ne satisfait pas la règle correspondante.

Question 6.3 En mathématiques classiques, quels axiomes ajouter à la théorie ***Asrrc*** pour obtenir une théorie équivalente à celle des anneaux réels clos de N. Schwartz ?

Question 6.4
1) Donner une fonction semialgébrique continue $\mathbb{R}^n \to \mathbb{R}$ (définition 4.3.1) qui sorte du cadre de la théorie ***BasicCrc***.
2) Si on en trouve, proposer une extension convenable de la théorie ***BasicCrc***.
3) Si on n'en trouve pas : toute fonction semialgébrique continue $\mathbb{R}^n \to \mathbb{R}$ serait un «point à coordonnées réelles» d'une $\mathbf{R}_{\mathrm{a}}$-famille paramétrée continument de fonctions semialgébriques continues $\mathbf{R}_{\mathrm{a}}^n \to \mathbf{R}_{\mathrm{a}}$?

Question 6.5
On sait qu'on ne peut pas exprimer au premier ordre le fait que $\mathbb{R}$ est archimédien. Cela

peut cependant s'exprimer dans une théorie géométrique infinitaire au moyen de la règle suivante

$$\textbf{AR1} \quad \vdash \bigvee_{n\in\mathbb{N}} |x| \leqslant n \qquad \textbf{(Archimède 1)}$$

La question qui se pose est de savoir si en rajoutant cette règle on obtient une extension conservative de la théorie dynamique $\mathcal{BasicCrc}$, ou si au contraire certaines règles dynamiques au premier ordre, vraies pour $\mathbb{R}$ et qui n'étaient pas démontrables, le deviennent en ajoutant cet axiome.

Question 6.6
Considérons la théorie géométrique infinitaire évoquée dans la question 6.5. La règle suivante n'est pas valide sur $\mathbb{R}$, mais on doit pouvoir démontrer qu'elle est «admissible». Ce serait une sorte de réalisation du programme de Hilbert pour **LPO**.

$$\textbf{AR2} \quad \vdash x = 0 \vee \bigvee_{n\in\mathbb{N}} |x| > 1/2^n \qquad \textbf{(Archimède 2)}$$

Références

[1] Maria 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*, pages 35–42. ACM, New York, 2012. 24

[2] 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*, pages 27–34. ACM, New York, 2011. 24

[3] Alain Bigard, Klaus Keimel, and Samuel Wolfenstein. *Groupes et anneaux réticulés*. Lecture Notes in Mathematics, Vol. 608. Springer-Verlag, Berlin-New York, 1977. 14, 15, 16, 17

[4] Garrett Birkhoff and R. S. Pierce. Lattice-ordered rings. *An. Acad. Brasil. Ci.*, 28 :41–69, 1956. 15

[5] Thierry Coquand and Henri Lombardi. A note on the axiomatisation of real numbers. *Math. Log. Q.*, 54(3) :224–228, 2008. 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. 3

[7] Michel Coste, Tomás Lajous-Loaeza, Henri Lombardi, and Marie-Françoise Roy. Generalized Budan-Fourier theorem and virtual roots. *J. Complexity*, 21(4) :479–486, 2005. 23, 24, 25

[8] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra : effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3) :203–256, 2001. 4, 6, 8, 9, 11, 12, 22

[9] André Galligo. Budan tables of real univariate polynomials. *J. Symbolic Comput.*, 53 :64–80, 2013. 24

[10] Laureano González-Vega and Henri Lombardi. A real Nullstellensatz and Positivstellensatz for the semipolynomials over an ordered field. *J. Pure Appl. Algebra*, 90(2) :167–188, 1993. 12, 13, 29

[11] Laureano González-Vega, Henri Lombardi, and Louis Mahé. Virtual roots of real polynomials. *J. Pure Appl. Algebra*, 124(1-3) :147–166, 1998. 23, 24, 25, 27

[12] Henri Lombardi, Daniel Perrucci, and Marie-Françoise Roy. An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem. Preprint., 2015. 11, 12

[13] Henri Lombardi and Claude Quitté. *Commutative algebra : constructive methods. Finite projective modules. Translated from the french edition (Calvage et Mounet, Paris, 2011).* Springer-Verlag, Berlin-New York, 2015. 14, 15

[14] Henri Lombardi and Marie-Françoise Roy. Elementary constructive theory of ordered fields. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 249–262. Birkhäuser Boston, Boston, MA, 1991. 24

[15] 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, pages x–x+21. Univ. Franche-Comté, Besançon, 1991. 24

[16] James J. Madden. Pierce-Birkhoff rings. *Arch. Math. (Basel)*, 53(6) :565–570, 1989. 30

[17] James J. Madden. On f-rings that are not formally real. *Ann. Fac. Sci. Toulouse Math. (6)*, 19(Fascicule Special) :143–157, 2010. 15

[18] Alexander Prestel and Niels Schwartz. Model theory of real closed rings. In *Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999)*, volume 32 of *Fields Inst. Commun.*, pages 261–290. Amer. Math. Soc., Providence, RI, 2002. 23, 30

[19] Fred Richman. Constructive mathematics without choice. In *Reuniting the antipodes – constructive and nonstandard views of the continuum (Venice, 1999)*, volume 306 of *Synthese Lib.*, pages 199–205. Kluwer Acad. Publ., Dordrecht, 2001. 3

[20] Joseph R. Shoenfield. *Mathematical logic*. Association for Symbolic Logic, Urbana, IL ; A K Peters, Ltd., Natick, MA, 2001. Reprint of the 1973 second printing. 9

[21] Lou van den Dries. *Tame topology and o-minimal structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998. 3

[22] Adriaan C. Zaanen. *Introduction to operator theory in Riesz spaces*. Springer-Verlag, Berlin, 1997. 14