Dimension de Krull, Nullstellensätze et Évaluation Dynamique

Henri Lombardi [1]

sept 2000

Résumé

Nous démontrons un Nullstellensatz qui établit une équivalence entre l'existence d'une identité algébrique d'un certain type, d'une part, et l'impossibilité de trouver une suite croissante de variétés irréductibles répondant à certaines contraintes d'autre part. De ce point de vue le Nullstellensatz usuel correspond au cas des variétés réduites à un point. Nous établissons aussi un Nullstellensatz formel du même type, en relation avec les suites croissantes d'idéaux premiers. Un cas particulier important est donné par la notion de suite pseudo régulière, plus générale que la notion de suite régulière. Nous obtenons de cette manière une nouvelle caractérisation de la dimension de Krull d'un anneau : un anneau a une dimension de Krull $\geq \ell$ si et seulement si il existe une suite pseudo régulière de longueur ℓ dans l'anneau. Dans les cas où ces résultats peuvent avoir une signification constructive précise, nos preuves y aboutissent constructivement. Nous pensons avoir donné ainsi quelques éléments en vue d'une interprétation constructive de la théorie de la dimension de Krull des anneaux commutatifs. Notre méthode utilise la notion de structure algébrique dynamique introduite dans des articles précédents.

Abstract

We prove constructively a Nullstellensatz giving an equivalence between the existence of a certain kind of algebraic identity on one hand, and the impossibility of finding an increasing sequence of irreducible varieties obeying certain constraints on the other hand. The ususal Nullstellensatz corresponds to the case of varieties that are reduced to a point. We settle also a similar formal Nullstellensatz related to increasing sequences of primes. An important particular case is given by the notion of pseudo regular sequence. This allows a new characterisation of the Krull dimension of a ring. This characterisation via pseudo regular sequences is elementary and constructive. Our method uses dynamical algebraic structures which were introduced in previous papers.

MSC : 13C15, 03F65, 13A15, 13E05

Mots clés : Dimension de Krull, Nullstellensatz, Mathématiques constructives, Structures algébriques dynamiques.

Key Words : Krull Dimension, Nullstellensatz, Constructive Mathematics, Dynamical Algebraic Structures.

[1] Équipe de Mathématiques, CNRS UMR 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25 030 BESANCON cedex, FRANCE, email : lombardi@math.univ-fcomte.fr

Introduction

Dans cet article nous nous intéressons à une approche constructive des anneaux commutatifs dont la dimension de Krull est au moins égale à ℓ. Le concept est difficile à manipuler constructivement car en général on n'a pas un accès explicite aux idéaux premiers d'un anneau commutatif.

Suites pseudo régulières et dimension de Krull

Nous introduisons la notion de suite pseudo régulière, qui donne un test explicite concernant la dimension de Krull d'un anneau commutatif. Nous appelons *suite pseudo régulière de ℓ éléments* (dans un anneau commutatif A) une suite $(x_1, \ldots, x_\ell)$ telle que pour tous $a_1, \ldots, a_\ell \in A$ et tous $m_1, \ldots, m_\ell \in \mathbb{N}$ on ait

$$x_1^{m_1}(x_2^{m_2} \cdots (x_\ell^{m_\ell}(1 + a_\ell x_\ell) + \cdots + a_2 x_2) + a_1 x_1) \neq 0$$

Une suite pseudo régulière de longueur ℓ permet de spécifier incomplètement une chaîne strictement croissante de $\ell + 1$ idéaux premiers, conformément au théorème suivant que nous démontrons dans la section 4.

Théorème 5 (suites pseudo régulières et chaînes croissantes d'idéaux premiers) *Dans un anneau A une suite $(x_1, \ldots, x_\ell)$ est pseudo régulière si et seulement si il existe $\ell + 1$ idéaux premiers $P_1 \subset \cdots \subset P_\ell \subset P_{\ell+1}$ avec $x_1 \in P_2 \setminus P_1$, $x_2 \in P_3 \setminus P_2, \ldots$ $x_\ell \in P_{\ell+1} \setminus P_\ell$.*

Etant donnée une suite pseudo régulière de longueur ℓ notre preuve ne peut pas fournir un procédé de construction explicite des idéaux premiers $P_1, \ldots, P_{\ell+1}$, sauf dans certains cas particuliers (voir l'énoncé complet du théorème 5 dans la section 4).

Nouveaux Nullstellensätze

La description de la dimmension de Krull à travers les suites pseudo régulières apparaît comme un cas particulier d'un Nullstellensatz formel plus général démontré dans la section 2.

Théorème 2 (Nullstellensatz formel pour les chaînes d'idéaux premiers, en mathématiques classiques) *Soit A un anneau et $J_1, \ldots, J_\ell$, $U_1, \ldots, U_\ell$ 2ℓ parties de A. Les deux propriétés suivantes sont équivalentes :*

(*a*) *il n'existe pas ℓ idéaux premiers $P_1 \subset \cdots \subset P_\ell$ ([1]) tels que $J_i \subset P_i$, $U_i \cap P_i = \emptyset$, $(i = 1, \ldots, \ell)$,*

(*b*) *il existe j_i dans l'idéal engendré par J_i, $(i = 1, \ldots, \ell)$, u_i dans le monoïde engendré par U_i, $(i = 1, \ldots, \ell)$, vérifiant l'égalité*

$$u_1(\ldots(u_\ell + j_\ell) + \ldots) + j_1 = 0 \quad (*)$$

Ce résultat, énoncé de manière aussi générale, ne peut pas être constructif. Nous en donnons deux versions constructives, une générale sous forme d'un collapsus simultané (théorème 1), une autre particulière lorsque l'anneau A vérifie des hypothèses adéquates quant à la possibilité d'y mener des calculs sur les idéaux premiers (théorème 3).

Nous démontrons enfin dans la section 3 le Nullstellensatz suivant dans le cas géométrique.

Théorème 4 *Soit $\mathbf{K}$ un corps contenu dans un corps algébriquement clos discret $\mathbf{L}$. Soient $J_1, \ldots, J_\ell, U_1, \ldots, U_\ell$ 2ℓ familles finies de polynomes de $\mathbf{K}[x_1, \ldots, x_n] = \mathbf{K}[\mathbf{x}]$.*
Soient $\mathcal{I}_i$ l'idéal de $\mathbf{K}[\mathbf{x}]$ engendré par J_i et $\mathcal{M}_i$ le monoïde engendré par U_i, $(i = 1, \ldots, \ell)$.
On a alors l'équivalence suivante

[1] Dans tout l'article le symbole $\subset$ est mis pour l'inclusion au sens large.

(*a*) *Il n'existe pas* ℓ *variétés irréductibles* $V_\ell \subset \cdots \subset V_1 \subset \mathbf{L}^n$ *qui vérifient les conditions suivantes*

$$\forall f \in J_i \;\; f|_{V_i} = 0|_{V_i}, \quad \forall g \in U_i \;\; g|_{V_i} \neq 0|_{V_i} \quad (i = 1, \ldots, \ell)$$

(*b*) *Il existe des* $u_i \in \mathcal{M}_i$ *et* $j_i \in \mathcal{I}_i$ $(i = 1, \ldots, \ell)$ *tels que*

$$u_1(\ldots(u_\ell + j_\ell) + \ldots) + j_1 = 0$$

En outre on a un procédé explicite qui construit, à partir de la donnée $J_1, \ldots, J_\ell, U_1, \ldots, U_\ell$, *ou bien une identité algébrique comme en* (*b*) *(si une telle identité existe), ou bien (dans l'autre cas) un système fini de générateurs pour chacun des idéaux premiers correspondant aux variétés irréductibles vérifiant les conditions décrites au point* (*a*).

La méthode dynamique

D'un point de vue dynamique (l'annexe reprend, pour la commodité de la lecture, des définitions relatives aux structures algébriques dynamiques données dans [1] et [10]), on accepte de ne pas spécifier complètement la chaîne croissante d'idéaux premiers, et on s'intéresse aux conditions dans lesquelles une telle structure collapse.

Un idéal premier est incomplètement spécifié par la donnée d'éléments dans l'idéal et d'éléments dans la partie multiplicative complémentaire de l'idéal.

Si ensuite on retourne dans une situation concrète où les chaînes croissantes d'idéaux premiers sont complètement explicitables, on obtient un Nullstellensatz effectif. C'est le cas de l'anneau $\mathbf{L}[x_1, \ldots, x_n]$ lorsque $\mathbf{L}$ est un corps algébriquement clos.

Une structure algébrique dynamique est une *structure algébrique incomplètement spécifiée*. Pour cela on donne les axiomes que doit vérifier la structure, des générateurs et des relations. Le fait que la structure est *algébrique* tient à ce que les axiomes ont une forme particulièrement simple. Ils peuvent être mis en oeuvre à l'intérieur d'un calcul arborescent dans lequel la logique sous sa forme usuelle sophistiquée ne joue plus aucun role. Aucune formule compliquée avec connecteurs ou quantificateurs n'est mise en oeuvre. Seuls apparaissent les prédicats donnés au départ dans la structure. En particulier, on peut éviter tout recours à la négation. Et le calcul mis en oeuvre est, le long de chaque branche du calcul arborescent, de l'algèbre pure, en fait surtout de la réécriture. L'arborescence elle-même est gouvernée par des axiomes simples. Elle est pour l'essentiel une discussion cas par cas.

Cet article constitue une confirmation de la souplesse d'utilisation des structures algébriques dynamiques (cf. [1, 7, 8, 9, 10, 11, 12, 13]). La plupart des théorèmes d'algèbre abstraite, dans la preuve desquels l'axiome du choix et le principe du tiers exclu semblent offrir un obstacle sérieux à une interprétation explicite en termes de calculs algébriques, auraient ainsi une version dynamique constructive, à partir de laquelle l'utilisation du théorème de complétude de Gödel fournirait la version classique abstraite. Lorsque ces théorèmes abstraits sont ensuite utilisés pour prouver l'existence d'objets concrets, la version dynamique donnera alors ipso facto une construction explicite de ces objets concrets.

1 Théorie dynamique des chaînes croissantes d'idéaux premiers

Nous donnons tout le traitement avec $\ell = 3$, laissant au lecteur le soin de remplacer éventuellement 3 par ℓ et de rajouter les *trois petits points* aux endroits nécessaires([2]).

[2] S'il le désire, il pourra même faire des preuves par récurrence sur ℓ. Il aura alors la satisfaction secrète de savoir que ses énoncés sont prouvés rigoureusement pour tout entier ℓ même dans le cas où on dispose d'entiers

Lorsqu'on examine des structures algébriques "au dessus" d'une structure d'anneau commutatif, on peut se passer de la relation d'égalité binaire et de la plupart des axiomes des anneaux commutatifs. On introduit le prédicat unaire $x = 0$ et on considère que $x = y$ est une abréviation pour $x - y = 0$. Les axiomes usuels des anneaux commutatifs sont alors remplacés par du calcul algébrique dans les anneaux de polynomes à coefficients entiers : on considère que tout terme doit être réécrit sous une forme réduite dans l'anneau des polynomes correspondant. Par exemple l'axiome $a + b = b + a$ est remplacé par le calcul qui réduit $(a + b) - (b + a)$ à 0 dans $\mathbb{Z}[a, b]$. Les seuls axiomes qui restent nécessaires sont alors les suivants.

- $\vdash\ 0 = 0$ $\quad(\mathrm{Aco}_1)$
- $(x = 0,\ y = 0)\ \vdash\ x + y = 0$ $\quad(\mathrm{Aco}_2)$
- $x = 0\ \vdash\ ax = 0$ $\quad(\mathrm{Aco}_3)$
- $1 = 0\ \vdash\ \mathsf{Faux}$ $\quad(\mathrm{Aco}_{col})$

La théorie dynamique qu'on obtient est dite directe si en outre tous les prédicats sont unaires et tous les axiomes sont "algébriques directs" en un sens convenable (pour plus de détails, voir [1]). Les théories dynamiques directes sont particulièrement bien adaptées aux preuves de Nullstellensätze.

Rappelons qu'un Nullstellensatz est un théorème qui affirme que certains systèmes de conditions algébriques sont incompatibles si et seulement si il existe un certificat algébrique simple d'incompatibilité. Par exemple le Nullstellensatz faible usuel dit qu'un système d'équations polynomiales n'admet aucun zéro (dans une cloture algébrique du corps des coefficients) si et seulement si 1 est dans l'idéal engendré par les équations.

La théorie dynamique des anneaux commutatifs avec trois idéaux premiers emboités est basée sur la théorie directe $\mathcal{P}_{3,dir}$ suivante.

Le langage $\mathcal{L}_{\mathcal{P},3}$ est celui des anneaux commutatifs, avec le prédicat unaire $x = 0$ et six prédicats unaires $\mathrm{Ide}_1(x)$, $\mathrm{Ndz}_1(x)$, $\mathrm{Ide}_2(x)$, $\mathrm{Ndz}_2(x)$, $\mathrm{Ide}_3(x)$, $\mathrm{Ndz}_3(x)$. Si $P_1 \subset P_2 \subset P_3$ sont les trois idéaux premiers que nous avons en vue, $\mathrm{Ide}_i(x)$ signifie $x \in P_i$ et $\mathrm{Ndz}_i(x)$ signifie $x \notin P_i$ ou plutot que x est non diviseur de zéro modulo P_i.

Nous donnons les axiomes de cette théorie directe sous forme de trois groupes distincts, réservant au troisième groupe, pour des raisons de commodité dans l'exposé qui suit, certains axiomes pour les parties multiplicatives.

Le premier groupe d'axiomes, noté (A_0) est formé par les 4 axiomes des anneaux commutatifs non triviaux.

- $\vdash\ 0 = 0$ $\quad(\mathrm{Aco}_1)$
- $(x = 0,\ y = 0)\ \vdash\ x + y = 0$ $\quad(\mathrm{Aco}_2)$
- $x = 0\ \vdash\ ax = 0$ $\quad(\mathrm{Aco}_3)$
- $1 = 0\ \vdash\ \mathsf{Faux}$ $\quad(\mathrm{Aco}_{col})$

Le deuxième groupe d'axiomes, noté (A_1) est le suivant. Un axiome indiqué avec un indice i est répété pour $i = 1, 2, 3$, sauf si $i + 1$ intervient également dans l'axiome, auquel cas l'axiome est répété pour $i = 1, 2$.

- $(x = 0)\ \vdash\ \mathrm{Ide}_i(x)$ $\quad(\mathrm{P}_{3,dir,1,i})$
- $(\mathrm{Ide}_i(x),\ \mathrm{Ide}_i(y))\ \vdash\ \mathrm{Ide}_i(x + y)$ $\quad(\mathrm{P}_{3,dir,2,i})$
- $\mathrm{Ide}_i(x)\ \vdash\ \mathrm{Ide}_i(ax)$ $\quad(\mathrm{P}_{3,dir,3,i})$
- $\mathrm{Ide}_i(x)\ \vdash\ \mathrm{Ide}_{i+1}(x)$ $\quad(\mathrm{P}_{3,dir,4,i})$
- $\mathrm{Ide}_i(1)\ \vdash\ \mathsf{Faux}$ $\quad(\mathrm{P}_{3,col,1,i})$

non standard.

- $\vdash \ \mathrm{Ndz}_i(1)$ $\qquad (\mathrm{P}_{3,dir,5,i})$
- $(\mathrm{Ndz}_i(x),\ \mathrm{Ndz}_i(y)) \ \vdash \ \mathrm{Ndz}_i(xy)$ $\qquad (\mathrm{P}_{3,dir,6,i})$
- $(x=0,\ \mathrm{Ndz}_i(y)) \ \vdash \ \mathrm{Ndz}_i(x+y)$ $\qquad (\mathrm{P}_{3,dir,7,i})$

Le troisième groupe d'axiomes, noté (A_2) est le suivant.

- $\mathrm{Ndz}_i(0) \ \vdash \ \mathsf{Faux}$ $\qquad (\mathrm{P}_{3,col,2,i})$
- $(\mathrm{Ide}_i(x),\ \mathrm{Ndz}_i(y)) \ \vdash \ \mathrm{Ndz}_i(x+y)$ $\qquad (\mathrm{P}_{3,dir,8,i})$
- $\mathrm{Ndz}_{i+1}(x) \ \vdash \ \mathrm{Ndz}_i(x)$ $\qquad (\mathrm{P}_{3,dir,9,i})$

Notation 1.1 Nous notons $\mathcal{P}_{3,dir}$ la théorie directe $(\mathcal{L}_{\mathcal{P}_3}|\mathrm{A}_0,\mathrm{A}_1,\mathrm{A}_2)$.

On a le lemme suivant qui sera utilisé implicitement dans la suite.

Lemme 1.2 *Pour une structure algébrique dynamique de type $\mathcal{P}_{3,dir}$ si on a établi deux faits* $\mathrm{Ndz}_i(t)$ *et* $\mathrm{Ide}_i(t)$ *pour un même terme t, cela collapse.*

Preuve On a en effet $\mathrm{Ide}_i(-t)$ par $(\mathrm{P}_{3,dir,3,i})$ donc $\mathrm{Ndz}_i(t+(-t))$ par $(\mathrm{P}_{3,dir,8,i})$ c.-à-d. $\mathrm{Ndz}_i(0)$ □

Pour obtenir la théorie dynamique correspondant vraiment à un sytème de trois idéaux premiers emboités nous devons rajouter le groupe d'axiomes suivant, noté (A_5).

- $\vdash \ (\mathrm{Ide}_i(x)\ \mathsf{ou}\ \mathrm{Ndz}_i(y))$ $\qquad (\mathrm{P}_{3,dyn,1,i})$

Si enfin nous réclamons que l'emboitement des idéaux soit strict, nous rajouterons le groupe d'axiomes suivant, noté (A_6).

- $\vdash \ \mathsf{E}\, x_i \ (\mathrm{Ide}_{i+1}(x_i),\ \mathrm{Ndz}_i(x_i))$ $\qquad (\mathrm{P}_{3,dyn,2,i})$

Notation 1.3 Nous noterons
$\mathcal{P}_{3,dyn1} = (\mathcal{L}_{\mathcal{P}_3}|\mathrm{A}_0,\mathrm{A}_1,\mathrm{A}_2,\mathrm{A}_5)$ et $\mathcal{P}_{3,dyn2} = (\mathcal{L}_{\mathcal{P}_3}|\mathrm{A}_0,\mathrm{A}_1,\mathrm{A}_2,\mathrm{A}_5,\mathrm{A}_6)$.

En pratique, on sera plutot intéressé par des structures algébriques dynamiques de type $\mathcal{P}_{3,dyn1}$ avec une présentation pour laquelle on peut trouver deux termes u et v tels que $\mathrm{Ide}_2(u),\mathrm{Ndz}_1(u),\mathrm{Ide}_3(v),\mathrm{Ndz}_2(v)$ soient des faits prouvables.

Lemme 1.4 *La théorie $\mathcal{P}_{3,dyn1}$ prouve les* règles de simplification *suivantes : tout d'abord un groupe d'axiomes* (A_3)

- $(\mathrm{Ide}_i(xy),\ \mathrm{Ndz}_i(y)) \ \vdash \ \mathrm{Ide}_i(x)$ $\qquad (\mathrm{P}_{3,sim,1,i})$

ensuite un groupe d'axiomes (A_4)

- $\mathrm{Ndz}_i(xy) \ \vdash \ (\mathrm{Ndz}_i(x),\ \mathrm{Ndz}_i(y))$ $\qquad (\mathrm{P}_{3,sim,2,i})$
- $\mathrm{Ide}_i(x^2) \ \vdash \ \mathrm{Ide}_i(x)$ $\qquad (\mathrm{P}_{3,sim,3,i})$

Preuve Par exemple pour la première règle. On suppose $\mathrm{Ide}_1(xy)$, $\mathrm{Ndz}_1(y)$ on ouvre deux branches, la première avec $\mathrm{Ide}_1(x)$ et la deuxième avec $\mathrm{Ndz}_1(x)$. Dans la deuxième on a $\mathrm{Ndz}_1(xy)$ et $\mathrm{Ide}_1(-xy)$ donc $\mathrm{Ndz}_1(xy+(-xy))$ c.-à-d. $\mathrm{Ndz}_1(0)$ et elle meurt. □

Notation 1.5 Nous noterons $\mathcal{P}_{3,sim1} = (\mathcal{L}_{\mathcal{P}_3}|\mathrm{A}_0,\mathrm{A}_1,\mathrm{A}_2,\mathrm{A}_3,\mathrm{A}_4)$ et $\mathcal{P}_{3,sim2} = (\mathcal{L}_{\mathcal{P}_3}|\mathrm{A}_0,\mathrm{A}_1,\mathrm{A}_3)$.

Une structure algébrique ordinaire qui vérifie les axiomes de $\mathcal{P}_{3,sim2}$ est donnée par un anneau commutatif, trois idéaux emboités $I_1 \subset I_2 \subset I_3$ et trois monoïdes multiplicatifs $S_1,\ S_2,\ S_3$. Les éléments de S_i doivent être non diviseurs de zéro modulo I_i. Un exemple est donné en prenant pour S_i tous les non diviseurs de zéro modulo I_i. Par contre on ne demande pas d'inclusion entre les S_i, et les idéaux ne sont pas nécessairement premiers.

2 Collapsus simultanés et Nullstellensätze formels

Dans une théorie dynamique comme $\mathcal{P}_{3,dir}$, on peut donner une description simplifiée pour la présentation d'une structure algébrique dynamique S. L'ensemble des générateurs est G et les relations de départ peuvent être données par 7 parties de $\mathbb{Z}[G]$, $R_{=0}$, R_{Ide_i}, R_{Ndz_i} $(i = 1, 2, 3)$. La partie $R_{=0}$ donne l'ensemble des termes $t \in \mathbb{Z}[G]$ pour lesquels on a la relation de départ $t = 0$, la partie R_{Ide_1} donne l'ensemble des termes $t \in \mathbb{Z}[G]$ pour lesquels on a la relation de départ $\mathrm{Ide}_1(t)$, etc... Le lemme suivant est à la fois très simple et fondamental.

Lemme 2.1 *Soit* $S = (\mathcal{P}_{3,dir}, (G|R))$ *avec* $R = (R_{=0}, R_{\mathrm{Ide}_1}, \ldots, R_{\mathrm{Ndz}_3})$ *une structure algébrique dynamique de type* $\mathcal{P}_{3,dir}$*. Notons* $\mathcal{M}_{\mathrm{Ndz}_i}$ *le monoide (multiplicatif) dans* $\mathbb{Z}[G]$ *engendré par* R_{Ndz_i} $(i = 1, 2, 3)$*. Notons* $\mathcal{I}_{=0}$ *l'idéal de* $\mathbb{Z}[G]$ *engendré par* $R_{=0}$ *et* $\mathcal{I}_{\mathrm{Ide}_i}$ *l'idéal de* $\mathbb{Z}[G]$ *engendré par* R_{Ide_i} $(i = 1, 2, 3)$*.*
Alors la structure algébrique dynamique S *collapse si et seulement si on a une identité algébrique du type suivant dans* $\mathbb{Z}[G]$

$$u_1(u_2(u_3 + j_3) + j_2) + j_1 + j_0 = u_1u_2u_3 + u_1u_2j_3 + u_1j_2 + j_1 + j_0 = 0$$

avec $u_i \in \mathcal{M}_{\mathrm{Ndz}_i}$ *et* $j_i \in \mathcal{I}_{\mathrm{Ide}_i}$ *pour* $(i = 1, 2, 3)$ *et* $j_0 \in \mathcal{I}_{=0}$*.*

Preuve On voit tout d'abord facilement qu'on peut supposer que le seul axiome de collapsus est $\mathrm{Ndz}_1(0) \vdash \mathsf{Faux}$. On considère alors les faits prouvables par évaluation dynamique avant un collapsus.
Notons $\mathcal{I}_0 = \mathcal{I}_{=0}$, $\mathcal{I}_1 = \mathcal{I}_{=0} + \mathcal{I}_{\mathrm{Ide}_1}$, $\mathcal{I}_2 = \mathcal{I}_{=0} + \mathcal{I}_{\mathrm{Ide}_1} + \mathcal{I}_{\mathrm{Ide}_2}$, $\mathcal{I}_3 = \mathcal{I}_{=0} + \mathcal{I}_{\mathrm{Ide}_1} + \mathcal{I}_{\mathrm{Ide}_2} + \mathcal{I}_{\mathrm{Ide}_3}$.
Vu l'enchainement des axiomes directs, on voit alors que les éléments $t \in \mathbb{Z}[G]$ pour lesquels le fait $t = 0$ est prouvable sont exactement les éléments de $\mathcal{I}_0 = \mathcal{I}_{=0}$. Ensuite les éléments $t \in \mathbb{Z}[G]$ pour lesquels le fait $\mathrm{Ide}_1(t)$ est prouvable sont exactement les éléments de $\mathcal{I}_1$. Même chose pour $\mathrm{Ide}_2(t)$ et $\mathcal{I}_2$, puis pour Ide_3 et $\mathcal{I}_3$.
Ensuite les éléments $t \in \mathbb{Z}[G]$ pour lesquels le fait Ndz_3 est prouvable sont exactement les éléments de la forme $u_3 + k_3$ avec $u_3 \in \mathcal{M}_{\mathrm{Ndz}_3}$ et $k_3 \in \mathcal{I}_3$ (notez que le produit de deux éléments de cette forme est encore un élément de cette forme). Puis les éléments $t \in \mathbb{Z}[G]$ pour lesquels le fait Ndz_2 est prouvable sont exactement les éléments de la forme $u_2(u_3 + k_3) + k_2$ avec $u_3 \in \mathcal{M}_{\mathrm{Ndz}_3}$, $u_2 \in \mathcal{M}_{\mathrm{Ndz}_2}$, $k_3 \in \mathcal{I}_3$ et $k_2 \in \mathcal{I}_2$ (notez à nouveau que le produit de deux éléments de cette forme est encore un élément de cette forme). Enfin les éléments $t \in \mathbb{Z}[G]$ pour lesquels le fait Ndz_1 est prouvable sont exactement les éléments de la forme $u_1(u_2(u_3 + k_3) + k_2) + k_1$ avec $u_3 \in \mathcal{M}_{\mathrm{Ndz}_3}$, $u_2 \in \mathcal{M}_{\mathrm{Ndz}_2}$, $u_1 \in \mathcal{M}_{\mathrm{Ndz}_1}$, $j_3 \in \mathcal{I}_3$, $j_2 \in \mathcal{I}_2$ et $j_1 \in \mathcal{I}_1$.
On termine en remarquant que les éléments $u_1(u_2(u_3 + k_3) + k_2) + k_1$ de la forme précédente sont exactement les éléments de la forme $u_1(u_2(u_3 + j_3) + j_2) + j_1 + j_0$ avec $u_i \in \mathcal{M}_{\mathrm{Ndz}_i}$ et $j_i \in \mathcal{I}_{\mathrm{Ide}_i}$ pour $(i = 1, 2, 3)$ et $j_0 \in \mathcal{I}_{=0}$. □

Nous sommes maintenant en mesure d'établir un théorème de collapsus simultané.

Théorème 1 (théorème de collapsus simultané) *Les théories dynamiques* $\mathcal{P}_{3,dir}$*,* $\mathcal{P}_{3,dyn1}$*,* $\mathcal{P}_{3,sim1}$ *et* $\mathcal{P}_{3,sim2}$ *collapsent simultanément. Les théories dynamiques* $\mathcal{P}_{3,dyn1}$ *et* $\mathcal{P}_{3,sim1}$ *prouvent les mêmes faits.*

Avant de prouver ce théorème, donnons une version classique (obtenue en supposant le théorème de complétude de Gödel) pour le collapsus simultané de $\mathcal{P}_{3,dir}$ et $\mathcal{P}_{3,dyn1}$.

Théorème 2 (Nullstellensatz formel pour les chaînes d'idéaux premiers, en mathématiques classiques) *Soit* A *un anneau et* J_1*,* J_2*,* J_3*,* U_1*,* U_2*,* U_3 *six parties de* A*. Les deux propriétés suivantes sont équivalentes :*

(*a*) *il n'existe pas 3 idéaux premiers* $P_1 \subset P_2 \subset P_3$ *tels que* $J_1 \subset P_1$*,* $U_1 \cap P_1 = \emptyset$*,* $J_2 \subset P_2$*,* $U_2 \cap P_2 = \emptyset$*,* $J_3 \subset P_3$*,* $U_3 \cap P_3 = \emptyset$

(b) *il existe j_1 dans l'idéal engendré par J_1, j_2 dans l'idéal engendré par J_2, j_3 dans l'idéal engendré par J_3, u_1 dans le monoïde engendré par U_1, u_2 dans le monoïde engendré par U_2, u_3 dans le monoïde engendré par U_3, vérifiant l'égalité*

$$u_1(u_2(u_3 + j_3) + j_2) + j_1 = 0. \quad (*)$$

Preuve du théorème 2 Il est clair qu'une égalité $(*)$ interdit la possibilité des trois idéaux premiers. Si par contre la structure algébrique dynamique de type $\mathcal{P}_{3,dyn1}$ correspondant aux données A, J_1, J_2, J_3, U_1, U_2 et U_3 ne collapse pas (c.-à-d. s'il n'y a pas d'égalité du type $(*)$), alors la théorie formelle du premier ordre correspondante est cohérente (cf. [1] théorème 1.1) et par le théorème de complétude de Gödel elle admet un modèle. Ce modèle est donné par un anneau B avec trois idéaux premiers $Q_1 \subset Q_2 \subset Q_3$, avec un homomorphisme $\varphi : A \to B$ vérifiant $\varphi(J_1) \subset Q_1$, $\varphi(U_1) \cap Q_1 = \emptyset$, $\varphi(J_2) \subset Q_2$, $\varphi(U_2) \cap Q_2 = \emptyset$, $\varphi(J_3) \subset Q_3$, $\varphi(U_3) \cap Q_3 = \emptyset$. Il suffit alors de prendre pour P_i les $\varphi^{-1}(Q_i)$.
Une preuve classique plus usuelle serait la suivante.
Considérons les systèmes $(J'_1, J'_2, J'_3, U'_1, U'_2, U'_3)$ où les J'_i sont des idéaux de A, les U'_i sont des monoïdes, avec $J_i \subset J'_i$, $U_i \subset U'_i$, $J'_1 \subset J'_2 \subset J'_3$, $U'_3 \subset U'_2 \subset U'_1$, avec la condition supplémentaire qu'une égalité de type $(*)$ est impossible. Ordonnons l'ensemble de ces systèmes par l'ordre produit de l'ordre de l'inclusion. On est dans les conditions d'application du lemme de Zorn. On considère un système maximal $(J'_1, J'_2, J'_3, U'_1, U'_2, U'_3)$. Si on n'a pas $J'_1 \cup U'_1 = A$ soit $t \in A \setminus (J'_1 \cup U'_1)$. Si on rajoute t à J'_1, puisque le système est maximal, on a une égalité $u_1(u_2(u_3 + j_3) + j_2) + j_1 + at = 0$. Si on rajoute t à U'_1, puisque le système est maximal, on a une égalité $t^m u_1(u_2(u_3 + j_3) + j_2) + j_1 = 0$. Ici on fait un calcul algébrique qui se trouve dans la preuve du lemme 2.2 ci-après, pour obtenir une contradiction. Même chose dans les cas où $J'_2 \cup U'_2 \neq A$ ou $J'_3 \cup U'_3 \neq A$. □

La preuve précédente montre qu'un contenu constructif du théorème 2 est exactement le théorème 1. Plus exactement, le théorème 1 et le lemme 2.1 (qui sont tous deux constructifs) donnent la condition nécessaire et suffisante de collapsus pour la théorie dynamique $\mathcal{P}_{3,dyn1}$ donc aussi pour la théorie formelle du premier ordre correspondante. Or, via le théorème de complétude de Gödel, cette condition de collapsus équivaut facilement au théorème 2.

Preuve du théorème 1 Nous reprenons concernant la présentation $(G|R)$ d'une structure algébrique dynamique de type $\mathcal{P}_{3,dir}$ les notations du lemme 2.1. Supposons tout d'abord que nous avons le collapsus simultané de $\mathcal{P}_{3,dir}$ et $\mathcal{P}_{3,dyn1}$, alors nous en déduisons celui de $\mathcal{P}_{3,sim1}$ qui est une théorie intermédiaire entre ces deux extrêmes. Par ailleurs $\mathcal{P}_{3,sim2}$ est plus faible que $\mathcal{P}_{3,sim1}$. Il suffit donc de montrer qu'une égalité $u_1(u_2(u_3 + j_3) + j_2) + j_1 = 0$ avec $u_i \in \mathcal{M}_{\mathrm{Ndz}_i}$ et $j_i \in \mathcal{I}_{\mathrm{Ide}_i}$ pour $(i = 1, 2, 3)$ fait collapser la structure algébrique dynamique S' de type $\mathcal{P}_{3,sim2}$ et de présentation $(G|R)$. Tout d'abord, il est clair qu'on a les faits $\mathrm{Ndz}_1(u_1)$, $\mathrm{Ndz}_2(u_2)$, $\mathrm{Ndz}_3(u_3)$, $\mathrm{Ide}_1(j_1)$, $\mathrm{Ide}_2(j_2)$, $\mathrm{Ide}_3(j_3)$. Posons $v = u_2(u_3 + j_3) + j_2$. Comme $u_1 v = -j_1$ la règle de simplification $(\mathrm{P}_{3,sim,1,1})$ nous permet de conclure $\mathrm{Ide}_1(v)$. Donc on a $\mathrm{Ide}_2(v)$ c.-à-d. $\mathrm{Ide}_2(u_2(u_3+j_3)+j_2)$. Comme $\mathrm{Ide}_2(-j_2)$ on en déduit $\mathrm{Ide}_2(u_2(u_3+j_3))$. La règle de simplification $(\mathrm{P}_{3,sim,1,2})$ nous permet de conclure $\mathrm{Ide}_2(u_3 + j_3)$ donc $\mathrm{Ide}_3(u_3 + j_3)$. On en déduit $\mathrm{Ide}_3(u_3)$, comme on a aussi $\mathrm{Ndz}_3(u_3)$, la régle de simplification $(\mathrm{P}_{3,sim,1,3})$ donne $\mathrm{Ide}_3(1)$ et cela collapse.

Montrons maintenant le collapsus simultané de $\mathcal{P}_{3,dir}$ et $\mathcal{P}_{3,dyn1}$. Pour cela il nous suffit de voir qu'un usage une fois de l'un des trois axiomes supplémentaires $(\mathrm{P}_{3,dyn,1,i})$ ne change pas les conditions du collapsus. Cela signifie qu'il nous faut prouver le lemme suivant :

Lemme 2.2 *Soit $S = (\mathcal{P}_{3,dir}, (G|R))$ une structure algébrique dynamique (notations du lemme 2.1). Soit t un terme de $\mathbb{Z}[G]$. Notons $R \cup \{\mathrm{Ide}_1(t)\}$ le système de relations obtenu en rajoutant $\mathrm{Ide}_1(t)$, c.-à-d. en remplaçant R_{Ide_1} par $R_{\mathrm{Ide}_1} \cup \{t\}$. Notons en outre $S \cup (\emptyset|\{\mathrm{Ide}_1(t)\})$ la structure algébrique dynamique $(\mathcal{P}_{3,dir}, (G|R \cup \{\mathrm{Ide}_1(t)\}))$*

— *Si les structures* $S \cup (\emptyset|\{\mathrm{Ide}_1(t)\})$ *et* $S \cup (\emptyset|\{\mathrm{Ndz}_1(t)\})$ *collapsent alors la strucure* S *collapse.*
— *Si les structures* $S \cup (\emptyset|\{\mathrm{Ide}_2(t)\})$ *et* $S \cup (\emptyset|\{\mathrm{Ndz}_2(t)\})$ *collapsent alors la strucure* S *collapse.*
— *Si les structures* $S \cup (\emptyset|\{\mathrm{Ide}_3(t)\})$ *et* $S \cup (\emptyset|\{\mathrm{Ndz}_3(t)\})$ *collapsent alors la strucure* S *collapse.*

Preuve du lemme 2.2

— La structure $S \cup (\emptyset|\{\mathrm{Ide}_1(t)\})$ collapse si et seulement si on a une égalité dans $\mathbb{Z}[G]$

$$u_1(u_2(u_3 + j_3) + j_2) + j_1 + at + j_0 = 0 \qquad (1)$$

avec $a \in \mathbb{Z}[G]$, $u_i \in \mathcal{M}_{\mathrm{Ndz}_i}$, $j_0 \in \mathcal{I}_{=0}$ et $j_i \in \mathcal{I}_{\mathrm{Ide}_i}$ pour $(i = 1, 2, 3)$. La structure $S \cup (\emptyset|\{\mathrm{Ndz}_1(t)\})$ collapse si et seulement si on a une égalité dans $\mathbb{Z}[G]$

$$t^m v_1(v_2(v_3 + k_3) + k_2) + k_1 + k_0 = 0 \qquad (2)$$

avec $m \in \mathbb{N}$, $v_i \in \mathcal{M}_{\mathrm{Ndz}_i}$, $k_0 \in \mathcal{I}_{=0}$ et $k_i \in \mathcal{I}_{\mathrm{Ide}_i}$ pour $(i = 1, 2, 3)$. On peut terminer par l'usuel truc de Rabinovitch. Dans (1) on met $-at$ dans le second membre, on élève à la puissance m on obtient une égalité dans $\mathbb{Z}[G]$ qui se réécrit sous la forme

$$u'_1(u'_2(u'_3 + j'_3) + j'_2) + j'_1 + j'_0 = bt^m \qquad (3)$$

avec $b \in \mathbb{Z}[G]$, $u'_i \in \mathcal{M}_{\mathrm{Ndz}_i}$, $j'_0 \in \mathcal{I}_{=0}$ et $j'_i \in \mathcal{I}_{\mathrm{Ide}_i}$ pour $(i = 1, 2, 3)$. Il reste à multiplier (2) par b puis à remplacer bt^m par sa valeur donnée en (3). On obtient

$$(u'_1(u'_2(u'_3 + j'_3) + j'_2) + j'_1 + j'_0)v_1(v_2(v_3 + k_3) + k_2) + bk_1 + bk_0 = 0 \qquad (4)$$

qui se réécrit sous la forme voulue.

— On reprend le même style de notations, sans forcément donner toutes les précisions. La structure $S \cup (\emptyset|\{\mathrm{Ide}_2(t)\})$ collapse si et seulement si on a une égalité dans $\mathbb{Z}[G]$

$$u_1(u_2(u_3 + j_3) + j_2 + at) + j_1 + j_0 = 0 \qquad (5)$$

La structure $S \cup (\emptyset|\{\mathrm{Ndz}_2(t)\})$ collapse si et seulement si on a une égalité dans $\mathbb{Z}[G]$

$$v_1(t^m v_2(v_3 + k_3) + k_2) + k_1 + k_0 = 0 \qquad (6)$$

On réécrit (5) sous la forme (7)

$$u_1(u_2(u_3 + j_3) + j_2) + j_1 + j_0 = \; - u_1 at \qquad (7)$$

En élevant ceci à la puissance m on obtient

$$u'_1(u'_2(u'_3 + j'_3) + j'_2) + j'_1 + j'_0 = u'_1 bt^m \qquad (8)$$

On multiplie (6) par $u'_1 b$ on obtient

$$v_1(u'_1 bt^m v_2(v_3 + k_3) + u'_1 k'_2) + k'_1 + k'_0 = 0 \qquad (9)$$

En utilisant (8) cela donne

$$v_1((u'_1(u'_2(u'_3 + j'_3) + j'_2) + j'_1)v_2(v_3 + k'_3) + u'_1 k'_2) + k'_1 + k'_0 = 0 \quad (10)$$

ce qui se réécrit

$$v_1 u'_1((u'_2(u'_3 + j'_3) + j'_2)v_2(v_3 + k'_3) + k'_2) + j''_1 + j''_0 = 0 \quad (11)$$

enfin $(u'_2(u'_3 + j'_3) + j'_2)v_2(v_3 + k'_3) + k'_2$ se réécrit $u''_2(u''_3 + j''_3) + j''_2$.

— Le troisième cas est essentiellement le même que le second. □

Montrons enfin que $\mathcal{P}_{3,dyn1}$ et $\mathcal{P}_{3,sim1}$ prouvent les mêmes faits. Comme $\mathcal{P}_{3,sim1}$ est plus faible que $\mathcal{P}_{3,dyn1}$ et comme les deux théories collapsent simultanément, il nous suffit de vérifier le lemme suivant.

Lemme 2.3 *Soit S une structure algébrique dynamique de type $\mathcal{P}_{3,sim1}$ et t un élément de S (plus précisément t est un élément de $\mathbb{Z}[G]$ si G est l'ensemble générateur de S). Alors*

— *un fait* $\mathrm{Ide}_i(t)$ *est vrai dans S si et seulement si rajouter* $\mathrm{Ndz}_i(t)$ *aux relations de S produit un collapsus,*

— *un fait* $\mathrm{Ndz}_i(t)$ *est vrai dans S si et seulement si rajouter* $\mathrm{Ide}_i(t)$ *aux relations de S produit un collapsus.*

Naturellement ce résultat vaut aussi pour $\mathcal{P}_{3,dyn1}$

Preuve du lemme 2.3 Supposons par exemple que la structure $S \cup (\emptyset|\{\mathrm{Ide}_2(t)\})$ collapse : on a une égalité dans $\mathbb{Z}[G]$

$$u_1(u_2(u_3 + j_3) + j_2 + at) + j_1 + j_0 = 0 \qquad (5)$$

On a donc $\mathrm{Ide}_1(u_1(u_2(u_3+j_3)+j_2+at))$ et en appliquant $(\mathrm{P}_{3,sim,1,1})$ on obtient $\mathrm{Ide}_1(u_2(u_3+j_3)+j_2+at)$ donc $\mathrm{Ide}_2(u_2(u_3+j_3)+j_2+at)$ donc $\mathrm{Ide}_2(u_2(u_3+j_3)+at)$. Posons $j = u_2(u_3+j_3)+at$. Comme on a $-at = -j + (u_2(u_3+j_3))$, $\mathrm{Ide}_2(-j)$ et $\mathrm{Ndz}_2(u_2(u_3+j_3))$, on obtient $\mathrm{Ndz}_2(-at)$. Et finalement $\mathrm{Ndz}_2(t)$ en appliquant $(\mathrm{P}_{3,sim,2,2})$.
Supposons maintenant par exemple que la structure $S \cup (\emptyset|\{\mathrm{Ndz}_2(t)\})$ collapse : on a une égalité dans $\mathbb{Z}[G]$

$$v_1(t^m v_2(v_3 + k_3) + k_2) + k_1 + k_0 = 0 \qquad (6)$$

Comme précédemment on obtient $\mathrm{Ide}_2(t^m v_2(v_3+k_3)+k_2)$, puis par $(\mathrm{P}_{3,sim,1,2})$, $\mathrm{Ide}_2(t^m)$, donc aussi $\mathrm{Ide}_2(t^{2^\ell})$ pour un certain ℓ. En appliquant ℓ fois $(\mathrm{P}_{3,sim,3,2})$ il vient $\mathrm{Ide}_2(t)$. □

□

Revenons maintenant au Nullstellensatz formel (théorème 2), pour la preuve duquel on a besoin de l'axiome du choix[3]. Il existe des cas où ce théorème est vrai d'un point de vue constructif.

Pour la définition d'un anneau de Lasker-Noether nous renvoyons à [14]. En mathématiques classiques tout anneau noethérien est un anneau de Lasker-Noether.

Théorème 3 (Nullstellensatz formel pour les chaînes d'idéaux premiers, en mathématiques constructives) *Soit A un anneau de Lasker-Noether. Soient J_1, J_2, J_3, U_1, U_2, U_3 six parties finies de A. Les deux propriétés suivantes sont équivalentes :*

(*a*) *il n'existe pas 3 idéaux premiers $P_1 \subset P_2 \subset P_3$ de type fini tels que $J_1 \subset P_1$, $U_1 \cap P_1 = \emptyset$, $J_2 \subset P_2$, $U_2 \cap P_2 = \emptyset$, $J_3 \subset P_3$, $U_3 \cap P_3 = \emptyset$*

(*b*) *il existe j_1 dans l'idéal engendré par J_1, j_2 dans l'idéal engendré par J_2, j_3 dans l'idéal engendré par J_3, u_1 dans le monoïde engendré par U_1, u_2 dans le monoïde engendré par U_2, u_3 dans le monoïde engendré par U_3, vérifiant l'égalité*

$$u_1(u_2(u_3 + j_3) + j_2) + j_1 = 0 \quad (*)$$

Plus précisément, il existe un algorithme qui construit ou bien une égalité du type $(*)$ en (b) ou bien trois idéaux premiers vérifiant les conditions requises en (a).

---

[3] Le théorème de complétude de Gödel est, du point de vue classique, équivalent à une forme faible de l'axiome du choix. Dans le cas d'une théorie dynamique avec un langage dénombrable et dont les axiomes peuvent être énumérés, le théorème de complétude de Gödel est, du point de vue constructif, équivalent au principe d'omniscience **LLPO** qui affirme que tout nombre réel est ≤ 0 ou ≥ 0. Ceci dans la mesure où on considère comme non problématique l'axiome du choix dénombrable.

Preuve Notons $I_1 = (J_1)$, $I_2 = (J_1) + (J_2)$ et $I_3 = (J_1) + (J_2) + (J_3)$. Notons V_3 la partie multiplicative engendrée par U_3, V_2 la partie multiplicative engendrée par U_3 et U_2, V_1 la partie multiplicative engendrée par U_3, U_2 et U_1.
Dans l'anneau A il est possible de construire explicitement la famille finie des idéaux premiers minimaux au dessus d'un idéal de type fini donné. En outre si P est un idéal premier de type fini explicite et U une partie multiplicative de type fini explicite, il est possible de tester si $P \cap U = \emptyset$. En effet, cela équivaut à $u \notin P$ pour chacun des générateurs de U.
Si trois idéaux premiers P_1, P_2, P_3 vérifiant les conditions requises existent, alors on peut tout d'abord remplacer P_1 par un idéal premier Q_1 minimal au dessus de I_1 et contenant P_1. Ensuite on peut remplacer P_2 par un idéal premier Q_2 minimal au dessus de $I_2 + Q_1$ et contenant P_2. Enfin, on peut remplacer P_3 par un idéal premier Q_3 minimal au dessus de $I_3 + Q_2$ et contenant P_3.
Partant de I_1, I_2, I_3 il n'y a qu'un nombre fini de possibilités, qu'on peut toutes expliciter, pour trois idéaux Q_1, Q_2, Q_3 vérifiant : Q_1 est minimal au dessus de I_1, Q_2 est minimal au dessus de $I_2 + Q_1$ et Q_3 est minimal au dessus de $I_3 + Q_2$. Pour chaque triplet (Q_1, Q_2, Q_3) ainsi sélectionné, il reste à tester si $Q_1 \cap V_1 = Q_2 \cap V_2 = Q_3 \cap V_3 = \emptyset$.
Nous venons de voir que l'existence éventuelle de trois idéaux premiers vérifiant les conditions requises peut être testée explicitement, avec construction d'un triplet convenable en cas de réponse positive.
Il nous reste à voir qu'en cas de réponse négative nous avons un collapsus de la structure algébrique dynamique correspondante, ce qui d'après le lemme 2.1 et le théorème de collapsus simultané (théorème 1), donnera une égalité du type $(*)$. Il s'agit de la structure algébrique dynamique $S = (\mathcal{P}_{3,dyn1}, (G|R))$ avec $G = A$, $R = (R_{=0}, R_{\mathrm{Ide}_1}, \ldots, R_{\mathrm{Ndz}_3}) = (R_{=0}, J_1, J_2, J_3, U_1, U_2, U_3)$ où $R_{=0}$ est le *diagramme de l'anneau* A([4]).
Considérons les idéaux premiers minimaux $Q_{1,\ell}$ $(\ell = 1, \ldots, n_1)$ au dessus de I_1, que nous avons de manière explicite. Nous savons que le radical de I_1 est l'intersection de ces idéaux premiers. Supposons tout d'abord que la construction soit bloquée ici par le fait que $U_1 \cup U_2 \cup U_3$ coupe chacun des $Q_{1,\ell}$. En faisant le produit des éléments en question, on obtient de manière explicite un élément v de $V_1 \cap \sqrt{I_1}$. Puisque les preuves dans [14] sont constructives, nous connaissons un exposant m tel que v^m est dans I_1 de manière explicite. Ceci produit un collapsus de la structure S.
Supposons maintenant par exemple que $U_1 \cup U_2 \cup U_3$ (donc aussi V_1) coupe tous les $Q_{1,\ell}$ sauf $Q_{1,1}$, $Q_{1,2}$ et $Q_{1,3}$. Nous allons voir que nous pouvons construire une évaluation dynamique de S dans laquelle toutes les branches meurent sauf certaines réparties en trois types. Dans les branches du premier type sont vrais les $\mathrm{Ide}_1(a_i)$ pour un nombre fini de a_i qui engendrent $Q_{1,1}$. Dans les branches du second type sont vrais les $\mathrm{Ide}_1(b_j)$ pour un nombre fini de b_j qui engendrent $Q_{1,2}$. Dans les branches du troisième type sont vrais les $\mathrm{Ide}_1(c_k)$ pour pour un nombre fini de c_k qui engendrent $Q_{1,3}$.
Pour ce faire nous procédons comme suit : nous choisissons pour chaque $\ell \neq 1, 2, 3$ un élément dans $Q_{1,\ell} \cap (U_1 \cup U_2 \cup U_3)$, nous appelons u leur produit. On a évidemment $\mathrm{Ndz}_1(u)$. Si maintenant nous choisissons un élément a de $Q_{1,1}$, un élément b de $Q_{1,2}$ et un élément c de $Q_{1,3}$. On a $uabc$ dans le radical de I_1. D'où une égalité explicite entre un élément de I_1 et $(uabc)^m$ pour un certain m. On a donc $\mathrm{Ide}_1((uabc)^m)$ et $\mathrm{Ndz}_1(u)$ d'où on tire $\mathrm{Ide}_1(abc)$.
Après avoir sélectionné n_1 éléments a_i qui engendrent $Q_{1,1}$, n_2 éléments b_j qui engendrent $Q_{1,2}$ et n_3 éléments c_k qui engendrent $Q_{1,3}$, on applique systématiquement les axiomes $\mathrm{Ide}_1(x) \vee \mathrm{Ndz}_1(x)$ à ces éléments, ce qui donne $2^{n_1+n_2+n_3}$ branches. Toute branche où on a pour un triplet

[4] $R_{=0}$ contient les éléments suivants de $\mathbb{Z}[G]$: $1_{\mathbb{Z}[G]} - 1_A$, $0_{\mathbb{Z}[G]} - 0_A$ ainsi que tous les $a +_{\mathbb{Z}[G]} b -_{\mathbb{Z}[G]} c$ et les $a \times_{\mathbb{Z}[G]} b -_{\mathbb{Z}[G]} d$ lorsque $a +_A b =_A c$ et $a \times_A b =_A d$.

(a_i, b_j, c_k), $\mathrm{Ndz}_1(a_i)$, $\mathrm{Ndz}_1(b_j)$ et $\mathrm{Ndz}_1(c_k)$ meurt puisqu'on a aussi $\mathrm{Ide}_1(a_i b_j c_k)$. Toute branche qui reste en vie est donc de l'un des trois types annoncé.
Dans les branches du premier type, nous considérons la liste finie des idéaux premiers minimaux au dessus de $I_2+Q_{1,1}$. Supposons par exemple que chacun de ces idéaux premiers coupe $U_2 \cup U_3$ (donc aussi V_2). En considérant un produit des éléments en question, on tombe explicitement dans le radical de $I_2 + Q_{1,1}$ et cela fait mourir la branche. etc...
En définitive l'obstruction à la construction des idéaux premiers vérifiant les conditions requises produit bien un collapsus de la structure algébrique dynamique S. □

3 Un Nullstellensatz lié à la théorie de la dimension

Théorème 4 *Soit* $\mathbf{K}$ *un corps contenu dans un corps algébriquement clos discret* $\mathbf{L}$*. Soient* $J_1, J_2, J_3, U_1, U_2, U_3$ *six familles finies de polynomes de* $\mathbf{K}[x_1, \ldots, x_n] = \mathbf{K}[\mathbf{x}]$*.*
Soient $\mathcal{I}_i$ *l'idéal de* $\mathbf{K}[\mathbf{x}]$ *engendré par* J_i *et* $\mathcal{M}_i$ *le monoïde engendré par* U_i*,* $(i = 1, 2, 3)$*.*
On a alors l'équivalence suivante

- (a) *Il n'existe pas trois variétés irréductibles* $V_3 \subset V_2 \subset V_1 \subset \mathbf{L}^n$ *qui vérifient les conditions suivantes*
$$\forall f \in J_i \ \ f|_{V_i} = 0|_{V_i}, \quad \forall g \in U_i \ \ g|_{V_i} \neq 0|_{V_i} \quad (i = 1, 2, 3)$$
- (b) *Il existe des* $u_i \in \mathcal{M}_i$ *et* $j_i \in \mathcal{I}_i$ $(i = 1, 2, 3)$ *tels que*
$$u_1(u_2(u_3 + j_3) + j_2) + j_1 = 0$$

En outre, on a un procédé explicite qui construit, à partir de la donnée $J_1, \ldots, J_3, U_1, \ldots, U_3$*, ou bien une identité algébrique comme en* (b) *(si une telle identité existe), ou bien (dans l'autre cas) un système fini de générateurs pour chacun des idéaux premiers correspondant aux variétés irréductibles vérifiant les conditions décrites au point* (a)*.*

Preuve (constructive) Si $\mathbf{K} = \mathbf{L}$ c'est une conséquence immédiate du Nullstellensatz formel donné au théorème 3. En effet on sait que l'anneau $\mathbf{L}[x_1, \ldots, x_n]$ est un anneau de Lasker-Noether (cf. [14] chap. 8 th. 9.6).
Si $\mathbf{K}$ n'est pas algébriquement clos, on se ramène au cas précédent en vérifiant que la condition (b) vue dans $\mathbf{L}[\mathbf{x}]$ équivaut à la condition (b) vue dans $\mathbf{K}[\mathbf{x}]$. Considérons la structure algébrique dynamique S définie dans la preuve du théorème 3. Nous rajoutons les axiomes de cloture algébrique relatifs à $\mathbf{K}$. Nous obtenons une structure algébrique dynamique S'. Pour voir qu'un collapsus de S' produit un collapsus de S, il suffit de considérer le cas où on a utilisé une seule fois un de ces nouveaux axiomes. On suppose donc qu'on a une égalité $u_1(u_2(u_3+j_3(x))+j_2(x))+j_1(x) = 0$ où x est un nouveau paramètre et en présence d'un nouvel axiome $P(x) = 0$ où P est un polynome unitaire à coefficients dans $\mathbf{K}$. En fait $j_1(x)$ est explicté sous forme $\sum_k j_{1,k} R_{1,k}(x)$ avec les $j_{1,k}$ dans $\mathcal{I}_1$. Même chose pour $j_2(x)$ et $j_3(x)$. Après division des $R_{i,j}$ par P relativement à la variable x, on obtient une égalité $u_1(u_2(u_3 + j_3'(x)) + j_2'(x)) + j_1'(x) = P(x)Q(x)$ avec $\deg(j_i'[x]) < \deg(P)$ $(i = 1, 2, 3)$. Cela implique que Q est identiquement nul. Il reste alors à considérer le coefficient constant de cette identité lorsqu'on voit le premier membre comme un polynome en x. □

Remarque 3.1 Si on ne sait pas construire une cloture algébrique de $\mathbf{K}$, on peut quand même faire l'évaluation dynamique de la structure S' où on a rajouté les axiomes de cloture algébrique relatifs à $\mathbf{K}$. Le théorème précédent admet alors la variante suivante : ou bien cette structure collapse et cela nous permet de produire une identité (b) à coefficients dans $\mathbf{K}$, ou bien on peut construire un système triangulaire d'équations et inéquations polynomiales à coefficients dans

K tel que dans la branche correspondante de S' (qui est une branche qui ne collapse surement pas) on ait la construction explicite des idéaux premiers définissant les variétés irréductibles V_i, avec la preuve que le point (a) est bien vérifé.

4 Suites régulières et pseudo régulières

Définition 4.1 *Soit $(x_1, \ldots, x_\ell)$ dans un anneau commutatif A.*

- *On dit que la suite $(x_1, \ldots, x_\ell)$ est une* suite pseudo singulière *lorsqu'il existe $a_1, \ldots, a_\ell \in A$ et $m_1, \ldots, m_\ell \in \mathbb{N}$ tels que*

$$x_1^{m_1}(x_2^{m_2} \cdots (x_\ell^{m_\ell}(1 + a_\ell x_\ell) + \cdots + a_2x_2) + a_1x_1) =$$
$$x_1^{m_1} \cdots x_\ell^{m_\ell} + a_\ell x_1^{m_1} \cdots x_{\ell-1}^{m_{\ell-1}} x_\ell^{1+m_\ell} + \cdots + a_2 x_1^{m_1} x_2^{1+m_2} + a_1 x_1^{1+m_1} = 0$$

- *On dit que la suite $(x_1, \ldots, x_\ell)$ est une* suite pseudo régulière *lorsque pour tous $a_1, \ldots, a_\ell \in A$ et tous $m_1, \ldots, m_\ell \in \mathbb{N}$ on a* ([5])

$$x_1^{m_1}(x_2^{m_2} \cdots (x_\ell^{m_\ell}(1 + a_\ell x_\ell) + \cdots + a_2x_2) + a_1x_1) \neq 0$$

Une suite pseudo régulière ne contient ni inversible ni nilpotent. Dans le cas d'un anneau local on se limite à examiner les cas avec les x_i dans l'idéal maximal, et $(1 + a_\ell x_\ell)$ peut être remplacé par 1.

La proposition suivante est une conséquence immédiate du lemme 2.1 qui caractérise le collapsus d'une structure algébrique dynamique de type $\mathcal{P}_{\ell,dir}$ (ici $\ell = 4$)

Proposition 4.2 *Soit A un anneau commutatif et (x_1, x_2, x_3) trois éléments de A. Soit B la structure algébrique dynamique de type $\mathcal{P}_{4,dir}$ obtenue à partir du diagramme de A comme anneau commutatif (avec le prédicat $x = 0$), en rajoutant les relations suivantes dans la présentation*

$$\mathrm{Ndz}_1(x_1),\ \mathrm{Ide}_2(x_1),\ \mathrm{Ndz}_2(x_2),\ \mathrm{Ide}_3(x_2),\ \mathrm{Ndz}_3(x_3),\ \mathrm{Ide}_4(x_3)$$

Alors B ne collapse pas si et seulement si la suite (x_1, x_2, x_3) est pseudo régulière

Preuve Vue la présentation de B, et vu le lemme 2.1 un collapsus de B donne une égalité dans A du type

$$u_1(u_2(u_3(u_4 + j_4) + j_3) + j_2) + j_1 = 0$$

avec $u_1 = x_1^{m_1}$, $u_2 = x_2^{m_2}$, $u_3 = x_3^{m_3}$, $u_4 = 1$, $j_1 = 0$, $j_2 = a_1x_1$, $j_3 = a_2x_2$, $j_4 = a_3x_3$, c.-à-d.

$$x_1^{m_1}(x_2^{m_2}(x_3^{m_3}(1 + a_3x_3) + a_2x_2) + a_1x_1) = 0$$

□

Le lien avec les suites régulières est donné par la proposition suivante.

[5] Dans un cadre constructif, il est parfois préférable de considérer une relation d'inégalité $x \neq 0$ qui ne soit pas simplement l'impossibilité de $x = 0$. Par exemple un nombre réel est dit $\neq 0$ lorsqu'il est inversible, c'est-à-dire clairement non nul. Chaque fois que nous mentionnons une relation d'inégalité $x \neq 0$, nous supposons donc toujours implicitement que cette relation a été définie au préalable dans l'anneau que nous considérons. Nous demandons que cette relation soit une inégalité standard, c'est-à-dire qu'elle puisse être démontrée équivalente à $\neg(x = 0)$ en utilisant le principe du tiers exclu. Nous demandons en outre que l'on ait constructivement $(x \neq 0,\ y = 0) \Rightarrow x + y \neq 0$, $xy \neq 0 \Rightarrow x \neq 0$, et $\neg(0 \neq 0)$. Enfin $x \neq y$ est défini par $x - y \neq 0$. En l'absence de précisions concernant $x \neq 0$, on peut toujours considérer qu'il s'agit de la relation $\neg(x = 0)$. Lorsque l'anneau est un ensemble discret, c'est-à-dire lorsqu'il possède un test d'égalité à zéro, on choisit toujours l'inégalité $\neg(x = 0)$. Néanmoins ce serait une erreur de principe grave de considérer que l'algèbre commutative ne doit travailler qu'avec des ensembles discrets.

Proposition 4.3 *Considérons un anneau commutatif A et trois éléments x_1, x_2, x_3 de A. Si la suite (x_1, x_2, x_3) est régulière alors elle est pseudo régulière.*

Preuve Supposons la suite régulière et montrons qu'une égalité $x_1^{m_1}(x_2^{m_2}(x_3^{m_3}(1+a_3x_3)+a_2x_2)+a_1x_1) = 0$ est impossible. Si on a une égalité de ce type, comme x_1 est non diviseur de zéro on en déduit $x_2^{m_2}(x_3^{m_3}(1 + a_3x_3) + a_2x_2) + a_1x_1 = 0$.
Comme x_2 est non diviseur de zéro modulo x_1A on en déduit $x_3^{m_3}(1 + a_3x_3) + a_2x_2 = dx_1$
Donc $x_3^{m_3}(1 + a_3x_3) \in (x_1A + x_2A)$. Puisque x_3 est non diviseur de zéro modulo $x_1A + x_2A$ on obtient $1 + a_3x_3 = ex_1 + e'x_2$ ce qui est contradictoire avec $x_1A + x_2A + x_3A \neq A$. □

La version "Nullstellensatz formel" de la proposition 4.2, qu'on déduit immédiatement des théorème 2 et 3 est le théorème suivant.

Théorème 5 (suites pseudo régulières et chaînes croissantes d'idéaux premiers)

(en mathématiques classiques) *Dans un anneau A une suite (x_1, x_2, x_3) est pseudo régulière si et seulement si il existe quatre idéaux premiers $P_1 \subset P_2 \subset P_3 \subset P_4$ avec $x_1 \in P_2 \setminus P_1$, $x_2 \in P_3 \setminus P_2$ et $x_3 \in P_4 \setminus P_3$.*

(en mathématiques constructives) *Ce théorème est valable constructivement lorsque A est un anneau de Lasker-Noether. (cf. [14])*

5 Vers une théorie constructive de la dimension de Krull

Ainsi, le fait qu'un anneau est de dimension $\geq \ell$ équivaut (en mathématiques classiques) à l'existence d'une suite pseudo régulière de longueur ℓ. Il serait intéressant de développer un traitement constructif de la théorie de la dimension de Krull basé sur les suites pseudo régulières. On donnerait les définitions suivantes.

Définition 5.1 *Un anneau A est dit* de dimension -1 *lorsque $1_A = 0_A$. Dans le cas contraire il est dit de dimension ≥ 0. Soit maintenant $\ell \geq 1$. L'anneau est dit* de dimension $\geq \ell$ *s'il existe une suite pseudo régulière de longueur ℓ. Il est dit* de dimension $\leq \ell - 1$ *si toute suite $(x_1, \ldots, x_\ell)$ de longueur ℓ dans A est pseudo singulière. L'anneau est dit* de dimension ℓ *s'il est à la fois de dimension $\geq \ell$ et $\leq \ell$. Il est dit* de dimension $< \ell$ *lorsqu'il est impossible qu'il soit de dimension $\geq \ell$.*

Notez que $\mathbb{R}$ est un anneau local de dimension < 1, mais qu'on ne peut pas prouver constructivement qu'il est de dimension ≤ 0.

Un anneau est local zéro-dimensionnel si et seulement si on a

$$\forall x \in A \quad x \text{ est inversible ou nilpotent}$$

Il serait souhaitable d'obtenir, sous des hypothèses convenables une forme constructive générale du Principal Ideal Theorem de Krull.

Ce pourrait être quelque chose du genre suivant.

Théorème 6 *Soit A un anneau local noetherien cohérent à idéaux détachables dont l'idéal maximal $\mathcal{M}$ est de type fini. Il existe $x_1, \ldots, x_\ell \in \mathcal{M}$ et un entier $n \in \mathbb{N}$ tels que*

$$\mathcal{M}^n \subset x_1A + \cdots + x_\ell A$$

si et seulement si A est de dimension $\leq \ell$.

Dimension de Krull d'un anneau de polynomes sur un corps discret

Dans ce paragraphe, nous donnons une preuve particulièrement élémentaire de la dimension de Krull d'un anneau de polynomes sur un corps discret. Cette preuve est également valable en mathématiques classiques puisqu'on a établi le théorème 5.

Nous avons tout d'abord.

Proposition 5.2 *Soit* $\mathbf{K}$ *un corps discret,* A *une* $\mathbf{K}$*-algèbre commutative, et* $x_1, \ldots, x_\ell$ *dans* A *algébriquement dépendants sur* $\mathbf{K}$*. Alors la suite* $(x_1, \ldots, x_\ell)$ *est pseudo singulière.*

Preuve Soit $Q(x_1, \ldots, x_\ell) = 0$ une relation de dépendance algébrique sur $\mathbf{K}$. Ordonnons les monomes de Q dont le coefficient est non nul selon l'ordre lexicographique. On peut supposer sans perte de généralité que le coefficient du premier monome non nul (pour cet ordre) est égal à 1. Si $x_1^{m_1} x_2^{m_2} \cdots x_\ell^{m_\ell}$ est ce monome, il est clair que Q s'écrit sous forme

$$Q = x_1^{m_1} \cdots x_\ell^{m_\ell} + x_1^{m_1} \cdots x_\ell^{1+m_\ell} R_\ell + x_1^{m_1} \cdots x_{\ell-1}^{1+m_{\ell-1}} R_{\ell-1} + \cdots + x_1^{m_1} x_2^{1+m_2} R_2 + x_1^{1+m_1} R_1$$

et l'égalité $Q = 0$ fournit donc le collapsus recherché. □

On en déduit.

Théorème 7 *Soit* $\mathbf{K}$ *un corps discret. La dimension de Krull de l'anneau* $\mathbf{K}[X_1, \ldots, X_\ell]$ *est égale à* ℓ*.*

Preuve Vue la proposition 5.2 il suffit de vérifier que la suite $(X_1, \ldots, X_\ell)$ est pseudo régulière. Or elle est régulière. □

Références

[1] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze* à paraître dans Annals of Pure and Applied Logic.

[2] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields* Proceedings Eurocal'85. Lecture Notes in Computer Science 204, 289–290 (1985). (Springer)

[3] Dicrescenzo C., Duval D. *Algebraic extensions and algebraic closure in Scratchpad. Symbolic and algebraic computation* (ISSAC 88). Lecture Notes in Computer Science 358 (Springer), (1989), 440–446.

[4] Duval, D. : *Simultaneous computations in fields of arbitrary characteristic* Computers and Mathematics, Eds Kaltofen E. and Watt S. M., (1989), 321–326. Springer.

[5] Duval D., Reynaud J.-C. *Sketches and Computation (Part I) Basic Definitions and Static Evaluation.* Mathematical Structures in Computer Science, **4**, (1994), 185–238.

[6] Duval D., Reynaud J.-C. *Sketches and Computation (Part II) Dynamic Evaluation and Applications.* Mathematical Structures in Computer Sciencen **4**, (1994), 239–271.

[7] Kuhlmann F.-V., Lombardi H. *Construction du hensélisé d'un corps valué.* Journal of Algebra **228**, (2000), 624–632.

[8] Lombardi H. *Un nouveau positivstellensatz effectif pour les corps valués.* Séminaire "Structures Ordonnées" (Paris 6-7) (18 pages, paru en 96 dans la livraison 94-95. Editeurs : F. Delon, A. Dickmann, D. Gondard)

[9] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini* . Publications Mathématiques de Besançon. Théorie des nombres. (1997). Fascicule 94–95 & 95–96.

[10] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier*. Journal of Pure and Applied Logic, **91**, (1998), 59–92.

[11] Lombardi H. *Platitude, localisation et anneaux de Prüfer : une approche constructive.* Preprint (1999).

[12] Lombardi H. *Constructions cachées en algèbre abstraite (1) Relations de dépendance intégrale.* À paraître dans le Journal of Pure and Applied Algebra.

[13] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Théorème de Horrocks, du local au global.* Preprint (1999).

[14] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988).

Annexe : Théories dynamiques et structures algébriques dynamiques

Cette annexe reprend, pour la commodité de la lecture, des définitions données dans [1] et [10] (voir aussi [8, 9]).

Une structure algébrique dynamique est une *structure algébrique incomplètement spécifiée.* Pour cela on donne les axiomes que doit vérifier la structure, des générateurs et des relations. Le fait que la structure est *algébrique* tient à ce que les axiomes ont une structure particulièrement simple. Ils peuvent être mis en oeuvre à l'intérieur d'un calcul arborescent dans lequel la logique sous sa forme usuelle sophistiquée ne joue plus aucun role. Aucune formule compliquée avec connecteurs ou quantificateurs n'est mise en oeuvre. Seuls apparaissent les prédicats donnés au départ dans la structure. En particulier, on peut éviter tout recours à la négation. Et le calcul mis en oeuvre est, le long de chaque branche du calcul arborescent, de l'algèbre pure, en fait surtout de la réécriture. L'arborescence elle-même est gouvernée par des axiomes simples. Elle est pour l'essentiel une discussion cas par cas.

Les méthodes dynamiques pour l'interprétation constructive de résultats et de méthodes d'algèbre abstraite sont inspirées de la clôture algébrique dynamique implantée en AXIOM suite aux travaux de Dominique Duval (cf. [2, 3, 5, 6])

Nous passons maintenant à des définitions plus formelles.

Une théorie dynamique $\mathcal{T} = (\mathcal{L}|\mathcal{D})$ est donnée par

- Un langage $\mathcal{L}$ comportant des constructeurs de termes (les termes sont construits à partir de variables, de paramètres, de constantes et de symboles de fonctions précisés), et des symboles de prédicat, dont au moins l'égalité. (Notez que les seules formules à notre disposition sont les formules atomiques puisque le langage ne comporte ni connecteur ni quantificateur.)
- Un ensemble $\mathcal{D}$ de règles de déduction, appelées axiomes, de nature élémentaire (on va préciser cela), formulés sans utilisation des paramètres.

Les axiomes sont des *règles dynamiques*, c.-à-d. des règles de déduction du type général suivant :

- $H(\mathbf{x}) \ \vdash \ \big(\mathsf{E}\,\mathbf{y}^1 A_1(\mathbf{x},\mathbf{y}^1)\ \mathsf{ou}\ \ldots\ \mathsf{ou}\ \mathsf{E}\,\mathbf{y}^k A_k(\mathbf{x},\mathbf{y}^k)\big) \qquad \text{(Nom} - \text{Ax)}$

Les $A_i(\mathbf{x},\mathbf{y}^i)$ et $H(\mathbf{x})$ sont des listes de prédicats portant sur des termes construits avec le langage de départ, *sans utilisation des paramètres*[6]. Un $\forall\mathbf{x}$ est implicite devant l'axiome. Le E a la signification d'un "il existe", la virgule dans une liste a la signification d'un "et". Les variables présentes dans la règle sont d'une part les x_h dans $\mathbf{x}$, d'autre part les y^i_j dans les $\mathbf{y}^i$. Aucune variable y^i_j n'est une variable x_h. Mais on peut avoir des variables communes dans deux listes $\mathbf{y}^i$, car les $\mathsf{E}\,\mathbf{y}^i A_i(\mathbf{x},\mathbf{y}^i)$ sont indépendants les uns des autres.

Un axiome est dit *disjonctif* s'il y a effectivement des " ou ", il est dit *existentiel* s'il y a effectivement des variables dans une liste $\mathbf{y}^i$ (c.-à-d. si les listes $\mathbf{y}^i$ ne sont pas toutes vides). Un axiome qui n'est ni disjonctif ni existentiel est dit *universel* ou *purement algébrique*. Une théorie dynamique est dite *purement algébrique* si tous ses axiomes sont purement algébriques.

Dans la liste des axiomes, il y a les *axiomes logiques* usuels relatifs à l'égalité, écrits sous forme de règles dynamiques.

Une structure algébrique dynamique $S = (\mathcal{T},\mathcal{P})$ est donnée par :

— une théorie dynamique $\mathcal{T} = (\mathcal{L}|\mathcal{D})$ qui définit *le type abstrait de la structure algébrique*, d'une part,

— une *présentation* $\mathcal{P} = (G|R)$ *de la structure dynamique* S d'autre part, donnée comme suit

- Un ensemble G de *générateurs*, qu'on peut voir comme de nouvelles constantes. Nous dirons parfois qu'il s'agit des paramètres de départ, particulièrement s'ils ne figurent dans aucune relation. Naturellement $\mathcal{L}\cap G = \emptyset$.
- Et un ensemble de relations R qui sont des *formules (atomiques)* S*-closes*, c.-à-d. des prédicats de $\mathcal{L}$ portant sur des *termes* S*-clos* (c.-à-d. des termes construits à partir des constantes de $\mathcal{L}$ et des générateurs de S au moyen des symboles de fonction de $\mathcal{L}$([7])). On peut voir les relations dans R comme : les faits donnés au départ comme vrais dans la structure. On les appellera les *relations de départ*.

Un *fait* concernant une structure algébrique dynamique $S = (\mathcal{T},\mathcal{P}) = ((\mathcal{L}|\mathcal{D}),(G|R))$ est une affirmation :

Tel(s) terme(s) S-clos satisfait(font) tel prédicat (donné dans la structure).

On pourrait aussi dire que c'est un "fait brut"[8]. Nous donnons plus loin une définition un peu plus formelle de la même chose. Nous avons besoin de préciser auparavant ce que sont les preuves dynamiques.

Utilisation légitime d'un axiome comme règle dynamique

De même qu'une théorie purement équationnelle débouche sur un *calcul algébrique pur*, n'utilisant rien d'autre que de la réécriture de manière systématique (le calcul ne fait pas intervenir de

[6] Nous utiliserons souvent par abus de notation les mêmes lettres pour désigner les variables (présentes uniquement dans les axiomes) et les paramètres (présents dans les faits, mais non dans les axiomes). La distinction entre paramètres et variables est en fait bien utile pour éviter les précautions usuelles difficiles à formuler qui gouvernent la légitimité du remplacement d'une variable muette par une variable non muette. Notre point de vue est d'appeler paramètre toute variable non muette et d'adopter des noms radicalement distincts pour les variables et pour les paramètres.

[7] Un terme S-clos ne contient donc ni variables ni paramètres (hormis les générateurs si on les considère comme des paramètres de départ.) Nous dirons parfois *terme clos de* S à la place de "terme S-clos".

[8] De manière générale, l'ensemble des assertions exprimables sous forme de faits dépend de manière critique du langage utilisé. Un langage plus riche permet d'exprimer plus de propriétés sous forme de faits. Par exemple si pour la structure d'anneau, on n'introduisait ni la constante -1, ni l'opération $x\mapsto -x$, on serait contraint à des périphrases bien encombrantes.

logique si ce n'est, implicitement, au travers des axiomes relatifs à l'égalité), de même une théorie dynamique ne doit pas être vue au premier chef comme une variante des théories logiques du premier ordre, mais comme une *pure machinerie calculatoire arborescente.*

Les axiomes n'ont pas pour signification de donner des énoncés élémentaires vrais, mais *d'être utilisés comme règles de déduction*, ou plus précisément comme *règles de constructions d'évaluations dynamiques.* C'est pour cette raison, et non par provocation, que nous n'avons utilisé dans les règles dynamiques aucun des symboles usuels servant à écrire des formules du premier ordre construites à partir des prédicats donnés au départ.

Une évaluation dynamique d'une structure algébrique dynamique $S = (\mathcal{T}, (G|R))$ est un arbre. A la racine de l'arbre, il y a implicitement présents tous les faits concernant S contenus dans les relations de départ. En chaque point de l'arbre des *paramètres existentiels* peuvent avoir été introduits lors de l'utilisation d'axiomes existentiels. Un terme construit sur $\mathcal{L} \cup G$ est appelé un *terme clos* en un point de l'arbre s'il ne contient pas de variable et si les seuls paramètres sont des générateurs de S ou des paramètres existentiels précédemment introduits dans la branche où on est.

Lors de la construction d'un arbre d'évaluation dynamique, voici ce qu'il faut faire pour utiliser *légitimement* un axiome tel que :

- $H(\mathbf{x}) \ \vdash \ \big(\mathsf{E}\,\mathbf{y}^1 A_1(\mathbf{x},\mathbf{y}^1)\ \mathsf{ou}\ \ldots\ \mathsf{ou}\ \mathsf{E}\,\mathbf{y}^k A_k(\mathbf{x},\mathbf{y}^k)\big)$ (Nom – Ax)

On remplace les x_j de la liste $\mathbf{x}$ par des termes t_j qui sont clos (au point où on est) et dont on a établi qu'ils valident l'hypothèse $H(\mathbf{x})$ (au point où on est). Si l'axiome est disjonctif, on produit un noeud à k branches. Dans la i-ème branche, les formules constituant la liste $A_i(\mathbf{t},\mathbf{y}^i)$ sont valides. Si l'axiome est existentiel, on introduit de nouveaux paramètres correspondant aux objets affirmés exister dans l'axiome. Les y^i_j doivent être pris parmi les paramètres non encore utilisés dans la branche où l'on est.

Dans une évaluation dynamique d'une structure algébrique dynamique S les seuls paramètres qui apparaissent sont donc les paramètres de départ et les paramètres existentiels.

En un point d'un arbre d'évaluation dynamique d'une structure S on appelle *fait* une formule atomique $Q(t_1,\ldots,t_n)$ où Q est un prédicat n-aire du langage $\mathcal{L}$ et les t_i sont des termes clos en ce point de l'arbre. Un arbre d'évaluation dynamique est donc un système de preuve extrêmement simple visant à valider des faits.

Définition A.3 (faits vrais dans une structure algébrique dynamique) *Soit* $S = (\mathcal{T},\mathcal{P}) = ((\mathcal{L}|\mathcal{D}),(G|R))$ *une structure algébrique dynamique. Un* fait concernant S *(ou encore, un fait de* S*) est une formule* $Q(t_1,\ldots,t_n)$ *où* Q *est un prédicat figurant dans* $\mathcal{L}$ *et les* t_i *sont des termes* S*-clos de* $\mathcal{L} \cup G$*. Un tel fait est dit* vrai dans la structure algébrique dynamique S *considérée si on a construit un arbre d'évaluation dynamique de la structure, et que ce fait est prouvé vrai à toutes les feuilles de l'arbre.*

Une chose importante est qu'une évaluation dynamique ne s'intéresse qu'aux choses vraies, et pas aux choses fausses. Un fait qui n'est pas prouvable ne peut pas pour autant être déclaré faux. Nous examinerons ceci plus en détail un peu plus loin.

Toute structure algébrique ordinaire S qui satisfait les axiomes d'une théorie dynamique $\mathcal{T}$ (lus comme des axiomes ordinaires) fournit un cas particulier de structure algébrique dynamique $S_1 = (\mathcal{T},(G|\mathrm{Diag}_{\mathcal{T}}(S)))$, en prenant comme générateurs de départ les éléments de S (ou un système de générateurs de S) et comme relations de départ le $\mathcal{T}$-diagramme de S, $\mathrm{Diag}_{\mathcal{T}}(S)$, c'est-à-dire les faits vrais dans S (ou un ensemble de faits vrais dans S qui impliquent, au sens de l'évaluation dynamique, tous les faits vrais dans S). Nous noterons $\widetilde{S}_{\mathcal{T}}$ cette structure algébrique dynamique.

Les faits vrais (au sens usuel) dans la structure ordinaire S sont alors exactement les faits vrais (au sens de l'évaluation dynamique) dans la structure dynamique $\widetilde{S}_{\mathcal{T}}$. A vrai dire dans ce cas, le processus de l'évaluation dynamique n'apporte rien concernant les faits. Si au contraire la structure algébrique ordinaire S ne satisfait pas certains axiomes de $\mathcal{T}$, en particulier si elle ne possède pas tous les prédicats du langage de $\mathcal{T}$, le processus d'évaluation dynamique peut enclancher une exploration des structures correspondantes "idéalement possibles" formées à partir de S quand on impose les contraintes supplémentaires de $\mathcal{T}$.

Une *règle dynamique* a la même forme générale qu'un axiome :

$$H(\mathbf{x}) \ \vdash \ (\mathsf{E}\,\mathbf{y}^1 A_1(\mathbf{x}, \mathbf{y}^1) \ \mathsf{ou} \ \ldots \ \mathsf{ou} \ \mathsf{E}\,\mathbf{y}^k A_k(\mathbf{x}, \mathbf{y}^k))$$

Elle est dite *valide (pour la théorie dynamique considérée)* si elle peut être prouvée à partir des axiomes de la théorie. Cette preuve doit être obtenue en donnant une évaluation dynamique de la structure S de type $\mathcal{T}$ et de présentation $\mathcal{P} = (\mathbf{u}|H(\mathbf{u}))$ (les variables x_i ont été remplacées par des générateurs u_i). A l'extrémité de chaque branche doit être prouvée l'une des conclusions $A_i(\mathbf{u}, \mathbf{t}^i)$ où les t^i_j sont des termes construits au cours de l'évaluation dynamique. Lorsqu'on a prouvé qu'une règle est valide, son utilisation de la même manière que les axiomes est légitime et elle ne permet pas de démontrer d'autres faits que ceux prouvés à partir des axiomes.

La structure réduite à un point et le collapsus

La *structure ponctuelle* est par définition la structure réduite à un point en lequel tous les prédicats sont vrais. Cette structure satisfait toujours les axiomes, ce qui évite radicalement l'usage de la négation.

Dans une évaluation dynamique, une branche *meurt*, ou *collapse*, si elle prouve un fait à partir duquel on sait déduire que tous les faits sont vrais (ce qui correspond à la structure ponctuelle précédemment décrite). Dans le cas de structures qui sont des surstructures de la structure d'anneau, un tel fait est $1 = 0$, (on rajoutera s'il le faut un axiome affirmant, pour chaque nouveau prédicat, qu'il est vrai sous l'hypothèse $1 = 0$). Dans le cas général, on introduit Faux en tant que constante logique, avec les *axiomes logiques* (un pour chaque prédicat n-aire) :

- $\mathsf{Faux} \ \vdash \ A(x_1, x_2, \ldots, x_n)$ $\qquad (\mathsf{Faux}, A)$

(en particulier cela réduit la structure à un point). La connotation inexistentielle du Faux est donc intuitivement remplacée par la connotation de "réduction au cas trivial sans intérêt".

Définition A.4 – *Une structure algébrique dynamique* collapse *si on a construit une évaluation dynamique dans laquelle toutes les branches sont mortes.*

- *Soient $\mathcal{T}_1 = (\mathcal{L}_1|\mathcal{D}_1)$ et $\mathcal{T}_2 = (\mathcal{L}_2|\mathcal{D}_2)$ deux théories dynamiques basées sur des extensions $\mathcal{L}_1$ et $\mathcal{L}_2$ d'un même langage $\mathcal{L} = \mathcal{L}_1 \cap \mathcal{L}_2$.*
  - *On dit que $\mathcal{T}_1$ et $\mathcal{T}_2$* collapsent simultanément *si pour toute présentation $\mathcal{P} = (G|R)$ sur le langage $\mathcal{L}$, la structure $S_1 = (\mathcal{T}_1, \mathcal{P})$ collapse si et seulement si la structure $S_2 = (\mathcal{T}_2, \mathcal{P})$ collapse.*
  - *On dit que les $\mathcal{T}_1$ et $\mathcal{T}_2$* prouvent les mêmes faits *si pour toute présentation $\mathcal{P} = (G|R)$ sur le langage $\mathcal{L}$, la structure $S_1 = (\mathcal{T}_1, \mathcal{P})$ et la structure $S_2 = (\mathcal{T}_2, \mathcal{P})$ prouvent les mêmes faits (écrits dans $\mathcal{L} \cup G$).*

Lorsque $\mathcal{T}_2$ est une extension de $\mathcal{T}_1$ les axiomes et prédicats supplémentaires introduits dans $\mathcal{T}_2$ pour nous faciliter les calculs (il est plus facile de calculer dans un corps réel clos que dans un corps ordonné par exemple) sont en fait inoffensifs, s'il y a collapsus simultané. Les preuves de Nullstellensätze dans [1] sont obtenues notamment par la mise en évidence que certaines théories dynamiques collapsent simultanément. Cette mise en évidence est elle même très proche de certaines preuves classiques abstraites des mêmes Nullstellensätze. La différence avec les preuves classiques en question est que dans [1] tous les Nullstellensätze sont effectifs.