Structures algébriques dynamiques, espaces topologiques sans points et programme de Hilbert

Henri LOMBARDI
Université de Franche-Comté.
`henri.lombardi@univ-fcomte.fr` `http ://hlombardi.free.fr/`

Octobre 2003.

Résumé

Une manière pertinente de revisiter le Programme de Hilbert serait la suivante : « donner une sémantique constructive pour les mathématiques classiques ». Plus précisément donner une interprétation systématique des preuves classiques abstraites (qui utilisent le principe du tiers exclu et l'axiome du choix) au sujet des objets abstraits, en terme de preuves constructives au sujet de contreparties constructives de ces objets abstraits.

Si ce programme est rempli, nous sommes capables « à la fin de l'histoire » d'extraire des preuves constructives de résultats concretr la reference 18 parues abstraites de ces résultats.

Les structures algébriques dynamiques, ou ce qui revient à peu près au même les théories géométriques, semblent être un bon outil pour réaliser ce travail. Dans cette optique, les objets abstraits des mathématiques classiques sont remplacés par des spécifications incomplètes mais concrètes de ces mêmes objets.

La structure des théories géométriques donne naissance de manière naturelle à des treillis distributifs et à des espaces topologiques sans points. Les objets abstraits utilisés par les mathématiques classiques correspondent aux points classiques de ces espaces sans points.

Dans cet article, nous illustrerons ce phénomène principalement avec le spectre de Zariski des treillis distributifs et celui des anneaux commutatifs, en indiquant notamment un équivalent constructif de la notion de dimension de Krull.

Nous insistons sur le caractère extrêmement général de l'interpétation des objets abstraits idéaux des mathématiques classiques comme des points d'espaces spectraux associés à des treillis distributifs qui sont définis de façon naturelle et concrète.

Souligons deux faits d'expérience importants.

Tout d'abord, les preuves abstraites au sujet des points de ces espaces sans points peuvent en général (toujours ?) être relues comme des preuves concernant les parties constructibles de ces espaces.

Enfin, les espaces de fonctions continues sur ces espaces sans points sont souvent utilisés dans d'élégantes théories abstraites. Ces espaces de fonctions sont bien définis constructivement. Cela tient au « théorème de compacité » qui nous dit que dans le cadre en question « tout est fini ». La relecture constructive des preuves abstraites n'est alors rien d'autre que la constatation que les axiomes géométriques sont utilisés de manière correcte.

Abstract

Dynamical algebraic structures, pointfree topological spaces and Hilbert's program

A possible relevant meaning of Hilbert's program is the following one : "give a constructive semantic for classical mathematics". More precisely, give a systematic interpretation of classical abstract proofs (that use Third Excluded Middle and Choice) about abstract objects, as constructive proofs about constructive versions of these objects.

If this program is fulfilled we are able "at the end of the tale" to extract constructive proofs of concrete results from classical abstract proofs of these results.

Dynamical algebraic structures or (this is more ore less the same thing) geometric theories seem to be a good tool for doing this job. In this setting, classical abstract objects are interpreted through incomplete concrete specifications of these objects.

The structure of axioms in geometric theories give rise in a natural way to distributive lattices and pointfree topological spaces. Abstract objects correspond to classical points of these pointfree spaces.

We shall insist on the Zariski spectrum of distributive lattices and commutative rings and give a constructive interpretation of the Krull dimension.

We underline the fact that many abstract objects in classical mathematics can be viewed as points of spectral spaces corresponding to distributive lattices whose definition is concrete and natural.

Two important facts are to be stressed.

First, abstract proofs about points of these pointfree spaces can very often (always ?) be reread as constructive proofs about constructible subsets of these spaces.

Second, function spaces on these pointfree spaces are often explicitely used in elegant abstract theories. The structure of these function spaces is fully constructive : indeed by compactness theorem, "all is finite". The constructive rereading of the abstract proofs is in this setting is nothing but the simple constatation that abstract proofs use correctly (geometric) axioms.

Introduction

En mathématiques classiques les preuves d'existence sont rarement explicites.

Deux obstacles essentiels apparaissent chaque fois qu'on essaie de rendre une telle preuve explicite.

Le premier obstacle est l'application du principe du tiers exclu. Par exemple, si vous considérez la preuve que tout polynome univarié sur un corps $\mathbf{K}$ admet une décomposition en facteurs premiers, vous avez une sorte d'algorithme dont l'ingrédient essentiel est : si P est irréductible c'est bon, si P se décompose en un produit de deux facteurs de degré ≥ 1, c'est bon aussi, par hypothèse de récurrence. Malheureusement la disjonction qui sert à faire fonctionner la preuve « P est irréductible ou P se décompose en un produit de deux facteurs de degré ≥ 1 » n'est pas en général explicite. Autrement dit, même si un corps est défini de manière constructive, on ne peut être certain que cette disjonction puisse être explicitée par un algorithme. Nous nous trouvons ici en présence d'un cas typique où le principe du tiers exclu « pose probème », car l'existence d'un facteur irréductible ne peut pas faire l'objet d'un algorithme général.

Le deuxième obstacle est l'application du lemme de Zorn, qui permet de généraliser au cas non dénombrable les raisonnements par induction usuels dans le cas dénombrable.

Par exemple dans le Modern Algebra de van der Waerden le second écueil est évité en se limitant aux structures algébriques dénombrables.

Par ailleurs l'usage de la théorie des ensembles avec axiome du choix **ZFC** conduit à des résultats hautement indésirables, tels le théorème de Banach-Tarski sur la duplication des boules dans $\mathbb{R}^3$, qui rendent cette théorie sujette à caution. D'autant plus qu'aucune méthode connue ne semble pouvoir jamais démontrer avec un minimum de crédibilité la consistance de la théorie formelle **ZFC**.

En contraste frappant avec les considérations précédentes, nous avons deux faits d'expérience désormais bien établis :

– Les résultats concrets universels démontrés par les méthodes abstraites douteuses ci-dessus n'ont jamais été contredits. On a même très souvent réussi à en fournir des preuves constructives incontestables. Cela signifierait que même si les méthodes abstraites sont quelque part fautives ou contradictoires, elles n'ont jusqu'à présent été utilisées qu'avec suffisamment de discernement (par exemple, on ne cherche guère à débusquer un résultat concret dont la preuve utiliserait comme ingrédient essentiel le théorème de Banach-Tarski).
– Les résultats concrets existentiels démontrés par les méthodes abstraites douteuses n'ont pas non plus été infirmés. Bien au contraire, ils ont souvent été confirmés par des algorithmes démontrés constructivement.

Sur le deuxième point, notre affirmation est moins nette. Si nous revenons à l'exemple de la décomposition d'un polynome en facteurs premiers, il est impossible de réaliser le résultat de manière algorithmique sur certains corps. Cependant le théorème classique n'est pas bien méchant en ce sens qu'on comprend bien pourquoi une conséquence concrète universelle du théorème peut être démontrée en utilisant un substitut constructif au théorème classique : le calcul pratique d'une factorisation d'un polynome chaque fois qu'on trouve dans l'anneau quotient un élément qui n'est ni nul ni inversible. Ainsi d'une part on pourra toujours faire comme si le polynome était irréductible jusqu'à ce qu'un obstacle survienne et nous montre une factorisation, d'autre part dans ce processus on ne pourra jamais décomposer le polynome de degré n en plus que n facteurs. Cela fait que l'hypothèse des mathématiques classiques selon laquelle le polynome est déjà décomposé en facteurs premiers, même si elle n'est pas réalisée, peut toujours être simulée sans risque, jusqu'au moment où le résultat concret universel qui découlait de la preuve classique est obtenu en pratique.

Face à cette situation un peu paradoxale : les méthodes abstraites sont a priori douteuses, mais elles ne nous trompent pas fondamentalement quand elles donnent un résultat de nature concrète, il y a deux réactions possibles.

Ou bien on croit que les méthodes abstraites sont fondamentalement justes parce qu'elles reflètent une « réalité », une sorte d'« univers cantorien idéal » dans lequel se trouve la vraie sémantique de **ZFC**. On pense alors que le théorème de Banach-Tarski est vrai. C'est la position du réalisme platonicien, défendue par exemple par Gödel.

Ou bien on pense que les méthodes abstraites sont vraiment sujettes à caution. Par exemple on pense que le théorème de Banach-Tarski ne correspond à aucune réalité (en ce sens il est donc faux). Mais alors, à moins de croire que les mathématiques relèvent de la magie ou du miracle, il faut expliquer pourquoi les mathématiques classiques se trompent si peu. Si on ne croit ni à Cantor, ni aux miracles, on est conduit à penser que les preuves abstraites de résultats concrets contiennent nécessairement des « ingrédients cachés » suffisants pour construire les preuves concrètes correspondantes.

Cette possibilité de certifier constructivement des résultats concrets obtenus par des méthodes douteuses, si on arrive à la réaliser de manière assez systématique, est dans le droit fil du programme de Hilbert.

Il faut souligner que sous cette formulation, le programme de Hilbert a déjà été confirmé pour une large partie des mathématiques usuelles, celles qui sont « codables » dans le système formel dit « de Peano » et désigné par **PA** : les résultats universels ou existentiels prouvés à l'aide du tiers exclu peuvent également être prouvés constructivement. Plus précisément, toute fonction de $\mathbb{N}$ dans $\mathbb{N}$ qui peut être prouvée récursive dans **PA** peut également être prouvée récursive sans recours au tiers exclu (cf. [21]).

Cependant bien qu'une grande quantité de mathématiques classiques soient codables dans **PA**, cela ne nous éclaire pas suffisamment sur le « fonctionnement des preuves classiques ». Sur la manière qu'elles ont d'introduire des objets abstraits « non crédibles » pour retomber en fin de compte les pieds sur terre et nous affirmer des choses très concrètes, par exemple : oui il y a sûrement là une somme de carrés, même si je ne vous la montre pas[1].

Nous développons depuis quelques années une méthode, que nous espérons assez générale, pour débusquer les « ingrédients cachés » dont nous parlons plus haut : pour forcer la preuve classique à nous montrer sa somme de carrés.

Notre ambition est de « donner une sémantique constructive pour les mathématiques classiques usuellement pratiquées, en particulier pour les méthodes de l'algèbre abstraite ».

Nous remplaçons les objets abstraits des mathématiques classiques par des spécifications incomplètes mais concrètes de ces objets. C'est la contrepartie constructive des objets abstraits.

Plus précisément nous prétendons donner une interprétation systématique de preuves classiques qui utilisent des objets abstraits en les relisant comme des preuves constructives au sujet de contreparties constructives de ces objets abstraits.

Du point de vue du Calcul Formel, c'est ce que l'on appelle de l'« évaluation paresseuse », ou de l'« évaluation dynamique », c'est-à-dire de l'évaluation paresseuse gérée de manière arborescente, comme dans le système D5 [17] qui réalise de manière très innocente ce tour de force : calculer de manière sûre dans la cloture algébrique d'un corps arbitraire, alors même qu'on sait que cet objet (la cloture algébrique) ne peut pas être construit en toute généralité.

1 Bref survol de résultats déjà obtenus

Nous faisons dans cette section un commentaire synthétique sur quelques résultats déjà obtenus dans cette direction.

Les articles correspondants sont réunis en trois groupes.

Le premier groupe contient une série d'articles « Constructions cachées en algèbre abstraite » qui expliquent sur quelques exemples significatifs le mécanisme de relecture constructive sous une forme que nous espérons naturelle.

Nous remplaçons certains objets abstraits des mathématiques classiques par des spécifications incomplètes mais concrètes de ces objets :

- La cloture algébrique d'un corps $\mathbf{K}$ est remplacée par des $\mathbf{K}$-algèbres de type fini zéro dimensionnelles, gérées de manière arborescente.
- Les corps ordonnés $(\mathbf{K}, P)$ sont remplacés par des paires $(\mathbf{A}, C)$ où $\mathbf{A}$ est un anneau et C un cone.
- Les anneaux de valuation d'un corps $\mathbf{K}$ contenant un sous anneau $\mathbf{A}$ (dont $\mathbf{K}$ est le corps des fractions) sont remplacés par des localisations judicieuses de $\mathbf{A}$-algèbres de type fini contenues dans $\mathbf{K}$.

[1] Le 17-ème problème de Hilbert était le suivant : montrer que si un polynome de $\mathbb{R}[x_1, \ldots, x_n]$ est partout ≥ 0 (sur $\mathbb{R}^n$), il est égal à une somme de carrés dans $\mathbb{R}(x_1, \ldots, x_n)$. Une preuve de ce résultat a été obtenue en 1927 par Artin [1]. La preuve était une preuve par l'absurde dans laquelle on ne voyait aucune somme de carrés.

- La localisation en tous les idéaux premiers d'un anneau **A** est remplacée par la localisation en un nombre fini de monoïdes comaximaux décrits en termes finis.
- Les idéaux premiers d'un anneau sont remplacés par des « premiers potentiels ».
- Les chaînes d'idéaux premiers sont remplacées par des « chaînes potentielles ».

Dans chacun de ces articles nous montrons comment certaines preuves des mathématiques classiques qui utilisent ces objets abstraits peuvent être relues comme des preuves constructives au sujet de leurs spécifications incomplètes, et fournissent le résultat concret final sous forme constructive.

Signalons que des travaux de Joyal et Español [24, 20] avaient abouti par des voies différentes à des résultats un peu moins précis, mais tout à fait similaires à ceux de [9] concernant la dimension de Krull. Signalons aussi l'article remarquable [13] de Coquand et Persson concernant la simulation constructive des anneaux de valuation.

Kronecker [32] Lombardi H. *Hidden constructions in abstract algebra (1) Integral dependance.* Journal of Pure and Applied Algebra **167**, (2002) 259–267.

Local-Global-2 [36] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 461–476.

Krull-2 [9] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 477–499.

17-Hilbert-2 [33] Lombardi H. *Constructions cachées en algèbre abstraite (4) La solution du 17ème problème de Hilbert par la théorie d'Artin-Schreier.* Publications Mathématiques de Besançon. Théorie des nombres (2002).

Pfister [35] Lombardi H. *Constructions cachées en algèbre abstraite (5) Principe local-global de Pfister et variantes.* International Journal of Commutative Rings **2** (4), (2003), 157–176.

Local-Global-3 [37] Lombardi H., Quitté C., Yengui I.) *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa.* Preprint 2005.

Les articles qui suivent et que nous commentons maintenant correspondent à la genèse de ces idées, sous une forme directement inspirée de la logique.

Nous avons été frappé lors de notre mise au point d'un algorithme pour le Nullstellensatz réel en 1990 [27], par le fait que nous retrouvions au coeur même de l'algorithme certains arguments purement calculatoires d'Artin-Schreier qui leur permettaient de construire une cloture réelle d'un corps réel (chose assez révoltante a priori d'un point de vue constructif car on connaît des corps réels pour lesquels tout espoir de les munir d'une relation d'ordre explicite est exclu).

L'élucidation de cette coïncidence a fait l'objet des articles [29] et [15].

On y introduit les structures algébriques dynamiques et les théories dynamiques. Les théories dynamiques ne sont pas vraiment nouvelles car elles ressemblent comme deux gouttes d'eau aux théories géométriques étudiées en théorie des topos (cf. [38]). Ce qu'il y a de nouveau c'est qu'on exclut tout traitement « logique » au profit d'un traitement purement calculatoire. En particulier, si une structure algébrique dynamique est définie à l'aide d'un certain nombre de fonctions et de prédicats, la machinerie calculatoire arborescente de la théorie dynamique ne concerne que les prédicats qui définissent la structure : les prédicats composés au moyen des connecteurs logiques et des quantificateurs ne sont jamais introduits ni utilisés. En particulier la négation est absente. Le théorème crucial dans [15] est justement qu'on ne rajoute aucun résultat nouveau en introduisant les prédicats composés et en utilisant le principe du tiers exclu, c'est-à-dire en passant d'une théorie dynamique à la théorie géométrique correspondante (avec la logique classique).

Dans [15] on obtient notamment un « Positivstellensatz » général pour les corps valués algébriquement clos, inconnu auparavant.

Néanmoins, dans ces trois articles, on s'appuie de manière essentielle sur le fait que les théories utilisées (corps réels clos, corps algébriquement clos, corps valués algébriquement clos) sont des théories complètes. Aussi l'article [30] marque un tournant car il montre comment la machinerie calculatoire « dynamique » peut être mise en oeuvre dans un cadre très général, celui de l'algèbre abstraite usuelle.

Enfin la découverte que, en suivant cette méthode, la dimension de Krull d'un anneau commutatif arbitraire avait une formulation entièrement constructive (cf. [31]) a achevé d'emporter notre conviction d'être sur une bonne voie.

Positivstellensatz [27] Lombardi H. *Effective real nullstellensatz and variants*, dans : Effective Methods in Algebraic Geometry. Eds. Mora T., Traverso C.. Birkhaüser (1991). Progress in Math. n°94 (MEGA 90), 263–288

17-Hilbert-1 [29] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier.* Annals of Pure and Applied Logic **91**, (1998), 59–92.

Nullstellensätze [15] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256.

Local-Global-1 [30] 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. Fascicule 94–95 & 95–96, (1997).

Krull-1 [31] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242**, (2002), 23–46.

Enfin les articles qui suivent utilisent la méthode générale des « spécifications incomplètes » à coté d'autres méthodes constructives plus habituelles.

En particulier dans les articles [19] et [34], la méthode dynamique intervient presque toujours seulement à titre heuristique. En effet les algorithmes produits par la méthode se simplifient et fournissent un exposé constructif indépendant, où les traces du décryptage de preuves classiques ne sont plus guère visibles. Néanmoins l'essentiel des algorithmes provient de ce décryptage. L'article [19] (qui fait suite à la thèse de Maimouna Salou [42]) peut aussi être vu comme une mise en oeuvre d'un programme de travail initié par Buchman et Lenstra dans [6]. En particulier on obtient la possibilité de travailler dans les anneaux d'entiers de corps de nombres sans avoir à factoriser le discriminant, ce que ne savent pas faire les logiciels usuels utilisés en théorie des nombres. La notion d'anneau de Prüfer à factorisation partielle développée dans [19] peut être vue comme une version dynamique et constructive des anneaux de Dedekind, qui ne sont rien d'autre que des anneaux de Prüfer à factorisation totale.

Prüfer [34] Lombardi H. *Platitude, localisation et anneaux de Prüfer, une approche constructive.* Publications Mathématiques de Besançon. Théorie des nombres. 2002.

Corps valués [25] Kuhlmann F.-V., Lombardi H., Perdry H. *Dynamic computations inside the algebraic closure of a valued field.*. A paraître dans : Valuation Theory and its Applications. Vol 2. Eds. F.-V. Kuhlmann, S. Kuhlmann and M. Marshall. Fields Institute Communications (2003)

Krull-3 [11] Coquand T., Lombardi H. *Going up, Going down, une approche constructive.* En préparation.

Krull-4 [12] Coquand T., Lombardi H. *Le théorème de l'idéal principal de Krull et la dimension des anneaux noethériens, une approche constructive.* En préparation.

Dedekind [19] Ducos L., Lombardi H., Quitté C., Salou M. *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Journal of Algebra. **281**, (2004), 604–650.

Les sous-produits de notre méthode sont de diverses sortes et certains devraient intéresser mêmes ceux qui dédaignent les résultats sous forme constructive.

– La mise au point d'algorithmes constructivement prouvés pour réaliser explicitement des résultats concrets (voir par exemple [18, 19, 27, 36, 37]).

– L'obtention de bornes générales uniformes sur la taille des objets ainsi produits (cf. [28]).

– La découverte de preuves plus élémentaires pour l'existence (parfois purement idéale) de certains objets abstraits (cf. [10]).

– La découverte de nouveaux théorèmes d'existence (parfois purement idéale) de certains objets abstraits (cf. le Positivstellensatz pour les corps valués dans [15], le théorème de Krull généralisé 2.4 et son corollaire 2.3, le Nullstellensatz généralisé dans [31]).

2 Les premiers potentiels comme contrepartie constructive des idéaux premiers

On sait à quel point les idéaux premiers sont omniprésents en algèbre commutative. Ils servent à ramener les cas généraux apparemment inextricables à des cas plus simples, celui des corps ou celui des anneaux locaux.

Dans un anneau commutatif, une spécification incomplète pour un idéal premier $\mathfrak{p}$ est donnée lorsqu'on précise des éléments dans l'idéal et d'autres éléments dans son complémentaire. En pratique on manipule essentiellement des spécifications incomplètes finies, mais on n'introduit pas de restriction de ce type dans la définition générale qui suit.

Définition 2.1 (Premiers potentiels)

1. *Un* premier potentiel *dans un anneau commutatif* $\mathbf{A}$ *est donné par un couple* $P = (I; U)$ *de parties de* $\mathbf{A}$*.*
2. *On dit que le premier potentiel* $P_1 = (I_1; U_1)$ raffine *le premier potentiel* $P = (I; U)$*, et on écrit* $P \le P_1$ *si* $I \subseteq I_1$ *et* $U \subseteq U_1$*.*
3. *On dit que le premier potentiel* $P_1 = (I_1; U_1)$ contient *le premier potentiel* $P = (I, U)$*, et on écrit* $P \subseteq P_1$ *si* $I \subseteq I_1$ *et* $U_1 \subseteq U$*.*
4. *Un idéal premier* $\mathfrak{p}$ *définit le premier potentiel* $(\mathfrak{p}\,;\mathbf{A}\backslash\mathfrak{p})$*, qu'on note encore* $\mathfrak{p}$*. On considère qu'un premier potentiel* P *est une spécification incomplète pour un idéal premier* $\mathfrak{p}$ *qui le raffinerait.*
5. *Le monoïde* $\mathcal{S}(P)$ *associé au premier potentiel* P *est l'ensemble* $\langle I\rangle_{\mathbf{A}} + \mathcal{M}(U)$*, où* $\langle I\rangle_{\mathbf{A}}$ *est l'idéal de* $\mathbf{A}$ *engendré par* I *et* $\mathcal{M}(U)$ *est le monoïde (multiplicatif) engendré par* U*. On note* $\mathbf{A}_P$ *le localisé* $\mathcal{S}(P)^{-1}\mathbf{A}$*, on dit qu'il s'agit du localisé de* $\mathbf{A}$ *en* P*.*
6. *On dit que le premier potentiel* P collapse *si* $0 \in \mathcal{S}(P)$*, c'est-à-dire encore si le localisé* $\mathbf{A}_P$ *est un anneau trivial.*
7. *Le premier potentiel* $P = (I; U)$ *est dit* complet *si* I *est un idéal,* U *un monoïde et* $I + U = U$*. Il est dit* saturé *si :*
$$\begin{array}{lll} (I, x; U) \text{ collapse} & \text{implique} & x \in U, \quad \text{et} \\ (I; U, x) \text{ collapse} & \text{implique} & x \in I. \end{array}$$

Notez que si l'anneau $\mathbf{A}$ est non trivial[2], un idéal premier n'est autre qu'un premier potentiel $(I; U)$ qui ne collapse pas et qui vérifie $\mathbf{A} = I \cup U$.

[2] Pour l'anneau trivial, tout dépend de la définition générale qu'on donne d'un idéal premier. La définition la plus confortable est que c'est un idéal I tel que A/I soit intègre et tel que $1 \in I \Rightarrow \mathbf{A} = 0$.

2.1 La version constructive du théorème de Krull

Maintenant voyons notre premier exemple typique concernant la signification concrète d'un théorème affirmant l'existence d'un certain objet abstrait.

Théorème concret 2.1 *Soit $P = (I;U)$ un premier potentiel et x un élément de $\mathbf{A}$. Si les premiers potentiels $(I,x;U)$ et $(I;U,x)$ collapsent, alors P collapse.*

Preuve Si $(I,x;U)$ collapse on a une égalité $i_1 + ax = u_1$ avec $i_1 \in \langle I\rangle$, $a \in \mathbf{A}$, $u_1 \in \mathcal{M}(U)$. Si $(I;U,x)$ collapse on a une égalité $i_2 = u_2x^n$ avec $i_2 \in \langle I\rangle$, $n \in \mathbb{N}$, $u_2 \in \mathcal{M}(U)$. L'élimination de x donne alors le résultat cherché : $a^nx^nu_2 = i_2a^n = (-i_1 + u_1)^nu_2$ et donc $u_1^nu_2 \in \mathcal{M}(U) \cap \langle I\rangle$. □

Théorème abstrait 2.1 (Théorème de Krull et Nullstellensatz formel) *Soit $\mathbf{A}$ un anneau commutatif non trivial.*

1. *Soit $P = (I;U)$ un premier potentiel qui ne collapse pas, alors il existe un idéal premier $\mathfrak{p}$ qui raffine P.*
2. *Soit $P = (f_1,\ldots,f_n;g)$ un premier potentiel. Les propriétés suivantes sont équivalentes :*
   - *P collapse, c'est-à-dire il existe un entier k et des éléments $a_1,\ldots,a_n$ tels que $g^k = a_1f_1 + \cdots + a_nf_n$.*
   - *« g s'annule aux zéros de $(f_1,\ldots,f_n)$ », plus précisément : pour tout corps $\mathbf{K}$ et tout homomorphisme $\varphi : \mathbf{A} \to \mathbf{K}$ on a l'implication :*
   $$\varphi(f_1) = \cdots = \varphi(f_n) = 0 \;\Rightarrow\; \varphi(g) = 0.$$

Remarquons tout d'abord que la preuve du théorème concret 2.1 est élémentaire et se trouve sous une forme plus ou moins déguisée dans toute preuve du théorème de Krull. Remarquons aussi que la version « Nullstellensatz formel » n'est autre qu'une contraposée du théorème de Krull (du point de vue des mathématiques classiques).

Maintenant l'important est de voir que la version concrète et la version abstraite se déduisent l'une de l'autre en deux lignes, du point de vue des mathématiques classiques.

Supposons la version abstraite et démontrons la version concrète. Puisqu'on est en mathématiques classiques on raisonne par l'absurde. Si P ne collapsait pas, il se raffinerait en un idéal premier $\mathfrak{p}$. Par principe du tiers exclu $x \in \mathfrak{p}$ ou $x \notin \mathfrak{p}$. Si $x \in \mathfrak{p}$ alors $\mathfrak{p}$ raffine $(I,x;U)$ et donc $(I,x;U)$ ne collapse pas. Si $x \notin \mathfrak{p}$ alors $\mathfrak{p}$ raffine $(I;U,x)$ et donc $(I;U,x)$ ne collapse pas.

Supposons la version concrète et démontrons la version abstraite. Par Zorn, considérons parmi les premiers potentiels qui raffinent P et qui ne collapsent pas un premier potentiel $P_1 = (I_1,U_1)$ maximal pour la relation de raffinement. Je dis que P_1 est un idéal premier, c'est-à-dire que $\mathbf{A} = U_1 \cup I_1$. Si ce n'était pas le cas, soit $x \in \mathbf{A} \setminus (U_1 \cup I_1)$. Alors les deux premiers potentiels $(I_1,x;U_1)$ et $(I_1;U_1,x)$ ne peuvent collapser tous les deux, par application du théorème concret. Donc, par application du tiers exclu l'un des deux ne collapse pas, et ceci contredit la maximalité de P_1.

Les deux preuves établissent le lien entre la version concrète et la version abstraite, à grand renfort d'arguments non constructifs. Finalement, du point de vue constructif, il reste la version concrète avec sa preuve élémentaire, et du point de vue classique, il reste deux versions tellement proches l'une de l'autre que l'on ne voit guère pourquoi en préférer une.

Notons pour terminer le raffinement suivant du théorème de Krull, qui est aussi une conséquence immédiate du théorème concret 2.1 en mathématiques classiques.

Soit $P = (I;U)$ un premier potentiel qui ne collapse pas. Soit (J,V) le premier potentiel obtenu en saturant P. Alors l'intersection des $\mathfrak{p}$ qui raffinent P est égale à J, et l'intersection des $\mathbf{A}\setminus\mathfrak{p}$ est égale à V.

2.2 Principes local-global

Les différentes formes du principe local-global en algèbre commutative classique sont des conséquences du théorème abstrait ci-après (ou d'une variante de ce théorème). Nous commençons par la version constructive la plus élémentaire du théorème.

On considère un système linéaire écrit sous forme matricielle : $MX = C$.

Théorème concret 2.2 *Soit $P = (I; U)$ un premier potentiel de $\mathbf{A}$, et $a \in \mathbf{A}$. Notons $P_1 = (I, a; U)$ et $P_2 = (I; U, a)$. Si le système linéaire $MX = C$ admet une solution dans $\mathbf{A}_{P_1}$ et dans $\mathbf{A}_{P_2}$ alors il admet une solution dans $\mathbf{A}_P$.*

Preuve En appliquant la définition du localisé $S^{-1}\mathbf{A}$ on voit qu'une solution du système linéaire dans $S^{-1}\mathbf{A}$ est donnée par un vecteur Y à coordonnées dans $\mathbf{A}$ et par $s, s' \in S$ tels qu'on ait dans $\mathbf{A}$: $s'MY = ss'C$. Ceci se réécrit $MZ = s''C$ avec Z à coordonnées dans $\mathbf{A}$ et $s'' \in S$. On a donc par hypothèse, Z_1 et Z_2 à coordonnées dans $\mathbf{A}$ et $s_1 \in \mathcal{S}(P_1)$, $s_2 \in \mathcal{S}(P_2)$ avec $MZ_1 = s_1 C$ et $MZ_2 = s_2 C$. On écrit $s_1 + j_1 - u_1 = ax$ et $s_2 + j_2 = a^m u_2$ avec $j_1, j_2 \in \langle I \rangle$, $u_1, u_2 \in \mathcal{M}(U)$. On élève la première égalité à la puissance m et on la multiplie par u_2, cela donne une égalité $s_1 z_1 + j_3 + u_3 = a^m u_2 x^m$ avec $j_3 \in \langle I \rangle$ et $u_3 = u_1^m u_2 \in \mathcal{M}(U)$. On multiplie la seconde égalité par x^m on obtient $s_2 z_2 + j_4 = a^m u_2 x^m$ avec $j_4 \in \langle I \rangle$. On obtient donc $s_2 z_2 - s_1 z_1 = j_5 + u_3 = s \in \mathcal{S}(P)$. On pose $X = -s_1 z_1 Z_1 + s_2 z_2 Z_2$, d'où $MX = sC$ et X/s est une solution à coordonnées dans $\mathbf{A}_P$. □

Théorème abstrait 2.2 (Résolution locale d'un système linéaire) *Si le système linéaire $MX = C$ admet une solution dans tous les localisés $\mathbf{A}_\mathfrak{p}$ (où $\mathfrak{p}$ parcourt* $\operatorname{Spec} \mathbf{A}$*) alors il admet une solution dans $\mathbf{A}$.*

La preuve du théorème concret est élémentaire, son contenu calculatoire est clair.

Voyons de nouveau que les deux versions sont équivalentes de manière immédiate en mathématiques classiques.

Supposons la version abstraite et démontrons la version concrète. Soit $\mathbf{B} = \mathbf{A}_P$. Nous supposons que $MX = C$ admet une solution dans les deux localisés $\mathbf{A}_{P_1}$ et $\mathbf{A}_{P_2}$ de $\mathbf{B}$. Soit $\mathfrak{p} \in \operatorname{Spec} \mathbf{B}$ et $\mathfrak{P}$ l'idéal correspondant dans $\mathbf{A}$ (avec $\mathfrak{P} \cap \mathcal{S}(P) = \emptyset$). Si $a \in \mathfrak{P}$, $\mathfrak{P}$ raffine P_1, $\mathbf{B}_\mathfrak{p}$ est un localisé de $\mathbf{A}_{P_1}$ et donc $MX = C$ admet une solution dans $\mathbf{B}_\mathfrak{p}$. Si $a \notin \mathfrak{P}$, $\mathfrak{P}$ raffine P_2, $\mathbf{B}_\mathfrak{p}$ est un localisé de $\mathbf{A}_{P_2}$ et donc $MX = C$ admet une solution dans $\mathbf{B}_\mathfrak{p}$. Puisque $\mathfrak{p}$ est arbitraire, $MX = C$ admet une solution dans $\mathbf{B}$.

Supposons la version concrète et démontrons la version abstraite, par l'absurde. Nous supposons que $MX = C$ n'admet pas de solution dans $\mathbf{A} = \mathbf{A}_{(0;1)}$. Par Zorn soit $P = (I; U)$ un premier potentiel maximal parmi ceux qui vérifient : $MX = C$ n'admet pas de solution dans $\mathbf{A}_P$. En particulier P ne collapse pas. Et par le théorème concret $\mathbf{A} = I \cup U$, autrement dit P correspond à un idéal premier $\mathfrak{P}$. Contradiction.

Résolution concrète de systèmes linéaires

Dans un anneau non local $\mathbf{B}$ (par exemple un localisé $\mathbf{A}_P$ avec un premier potentiel P), l'idéal maximal doit être remplacé par le *radical de Jacobson* $\operatorname{Rad}(\mathbf{B})$ qui en mathématiques classiques est défini comme l'intersection des idéaux maximaux, et qui est caractérisé constructivement par

$$x \in \operatorname{Rad}(\mathbf{B}) \quad \Longleftrightarrow \quad \forall a \in \mathbf{B}\ \exists y \in \mathbf{B}\ \ y\,(1 + ax) = 1 \tag{1}$$

Supposons maintenant que nous trouvions en mathématiques classiques une preuve qu'un système linéaire $MX = C$ admet une solution en s'appuyant sur le théorème abstrait 2.2. La preuve classique utilise un localisé arbitraire $\mathbf{A}_\mathfrak{p}$ de $\mathbf{A}$ et elle produit un calcul dans ce localisé « purement idéal ».

Selon la preuve classique, certains calculs sont faisables dans $\mathbf{A}_\mathfrak{p}$ en appliquant le fait que l'anneau est local, ce qui peut se traduire en disant que le quotient de l'anneau par son radical de Jacobson est un corps discret. Autrement dit la preuve met en oeuvre le principe suivant :

$$\forall x \in \mathbf{A}_\mathfrak{p} \qquad \big(x \in \mathbf{A}_\mathfrak{p}^\times \ \vee\ x \in \mathrm{Rad}(\mathbf{A}_\mathfrak{p})\big)\,, \tag{2}$$

principe qui est appliqué à des éléments x provenant de la preuve elle-même. Dans chacun des deux cas la preuve classique indique le calcul qu'il faudrait faire.

Nous remarquons que la preuve classique n'utilise pas complètement le fait que $\mathbf{A}_\mathfrak{p}$ est un anneau local. En particulier, l'idéal maximal $\mathfrak{P}$ de $\mathbf{A}_\mathfrak{p}$ intervient seulement en tant que radical de Jacobson. Or justement, dans un localisé (non local en général) $\mathbf{A}_P$ de $\mathbf{A}$ en un premier potentiel $P = (I;U)$ tous les éléments de I sont dans le radical de Jacobson.

Notre méthode consiste alors à répéter la preuve classique, en remplaçant chaque disjonction « x est une unité ou x est dans le radical de Jacobson », par la considération de deux anneaux $\mathbf{B}_1 = \mathbf{A}_{(I;U,x)}$ et $\mathbf{B}_2 = \mathbf{A}_{(I,x;U)}$, où $\mathbf{B} = \mathbf{A}_{(I;U)}$ est la localisation « courante » de l'anneau $\mathbf{A}$ de départ, à l'endroit de la preuve où on se trouve. Autrement dit si $\mathbf{B} = \mathbf{A}_{(a_1,\dots,a_k;u_1,\dots u_\ell)}$ les deux nouvelles localisations considérées sont $\mathbf{A}_{(a_1,\dots,a_k;u_1,\dots u_\ell,x)}$ et $\mathbf{A}_{(a_1,\dots,a_k,x;u_1,\dots u_\ell)}$.

Le calcul indiqué dans la preuve classique pour le cas où $x \in \mathbf{A}_\mathfrak{p}^\times$ est possible dans la première localisation puisque $x \in \mathbf{B}_1^\times$, et celui indiqué pour le cas où $x \in \mathrm{Rad}(\mathbf{A}_\mathfrak{p})$ est possible dans la deuxième localisation puisque $x \in \mathrm{Rad}(\mathbf{B}_2)$.

Lorsque la preuve initiale est ainsi déployée, on a construit en fin de compte un certain nombre, fini parce que la preuve est finie, de localisés $\mathbf{A}_{P_i}$, pour lesquels la propriété est vraie. Et le théorème concret 2.2 implique que, vue la manière dont l'arbre a été construit, le système linéaire a une solution à chacun des noeuds de l'arbre (on part des feuilles et on remonte l'histoire à l'envers), et donc en particulier à sa racine, c'est-à-dire dans $\mathbf{A}$. Et cette fois-ci, la résolution du système linéaire est entièrement explicite.

Dans l'article [36] nous avons appliqué cette méthode de relecture constructive dans deux cas importants. Il s'agit d'une preuve du théorème de Quillen-Suslin et d'une preuve du théorème de stabilité de Suslin (pour le cas des corps). Dans l'article [37] ces résultats sont étendus au cas des anneaux de Bezout de dimension ≤ 1, sans aucune hypothèse de noethériannité. En comparaison notons que les algorithmes ad hoc imaginés dans le cas des corps discrets par d'autres auteurs qui utilisent les bases de Gröbner ne s'appuient que partiellement sur la preuve classique et ne peuvent être étendus au cas non noethérien.

2.3 Anneaux de valuation

Les deux théorèmes concrets regroupés dans le théorème 2.3 correspondent à très peu près au même calcul (celui d'un résultant, cf. par exemple [32]).

Théorème concret 2.3 *Soit $\mathbf{A}$ un sous anneau d'un corps $\mathbf{K}$ et $a, b \in \mathbf{K}$ tels que $ab = 1$.*

1. *Soit $P = (I;U)$ un premier potentiel de $\mathbf{A}$. Si P collapse dans $\mathbf{A}[a]$ et dans $\mathbf{A}[b]$ alors P collapse dans $\mathbf{A}$.*
2. *Soit $x \in \mathbf{K}$. Si x est entier sur $\mathbf{A}[a]$ et sur $\mathbf{A}[b]$ alors x est entier sur $\mathbf{A}$.*

Leurs traductions sous forme abstraite via Zorn et le tiers exclu sont deux théorèmes classiques de la théorie des anneaux de valuation.

Théorème abstrait 2.3 *Soit $\mathbf{A}$ un sous anneau d'un corps $\mathbf{K}$.*

1. (Théorème de Chevalley) *Si $\mathfrak{p}$ est un idéal premier de $\mathbf{A}$ il existe un anneau de valuation $(\mathbf{V}, \mathfrak{m})$ de $\mathbf{K}$ tel que $\mathbf{A} \subset \mathbf{V}$ et $\mathfrak{p} = \mathfrak{m} \cap \mathbf{A}$.*

2. (Critère valuatif) *Soit $x \in \mathbf{K}$. Si x est dans tous les anneaux de valuation de $\mathbf{K}$ qui contiennent $\mathbf{A}$ alors x est entier sur $\mathbf{A}$.*

Nous ne reprendrons pas cette fois-ci les preuves d'équivalence entre la version concrète et la version abstraite.

Dans l'article [32] nous avons montré comment des relations de dépendance intégrale obtenues (de manière non effective) en mathématiques classiques en utilisant le critère valuatif pouvaient être obtenues (de manière effective) en relisant la preuve classique et en remplaçant l'usage du théorème abstrait par celui du théorème concret correspondant. Un arbre de calcul similaire à celui qui a été décrit dans la section 2.2 est mis en place pour réaliser l'algorithme.

2.4 Les chaînes potentielles

Définition 2.2 (Les chaînes potentielles)

1. *Une chaîne potentielle C de longueur ℓ dans $\mathbf{A}$ est une liste $(P_0, \ldots, P_\ell)$ de premiers potentiels de $\mathbf{A}$. Elle est considérée comme une spécification incomplète pour une chaîne d'idéaux premiers $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_\ell$ où chaque $\mathfrak{p}_i$ raffinerait le P_i correspondant.*
2. *La chaîne potentielle C est dite* complète *si chaque P_i est complet et si $P_0 \subseteq \cdots \subseteq P_\ell$. On notera $\overline{C}$ la chaîne potentielle obtenue en complétant C.*
3. *Supposons $P_i = (I_i, U_i)$. On dit que la chaîne potentielle C* collapse *si dans $\overline{C}$ le premier des monoïdes contient 0. Autrement dit s'il existe pour $i = 0, \ldots, \ell$, $a_i \in \langle I_i \rangle$ et $u_i \in \mathcal{M}(U_i)$ tels que*
$$u_0 \cdot (u_1 \cdot (\cdots (u_\ell + a_\ell) + \cdots) + a_1) + a_0 = 0.$$
4. *On dit que la chaîne potentielle $C' = (P'_0, \ldots, P'_\ell)$* raffine *la chaîne potentielle C si chacun des P'_i raffine le P_i correspondant.*
5. *La chaîne potentielle C est dite* saturée *si pour chaque i :*
$$\begin{array}{llll} (P_0, \ldots, P_{i-1}, (I_i, x; U_i), P_{i+1}, \ldots, P_n) \text{ collapse} & \text{implique} & x \in U_i, & \text{et} \\ (P_0, \ldots, P_{i-1}, (I_i; U_i, x), P_{i+1}, \ldots, P_n) \text{ collapse} & \text{implique} & x \in I_i. & \end{array}$$

Une généralisation du théorème de Krull aux chaînes d'idéaux premiers

Théorème concret 2.4 *Soit $C = (P_0, \ldots, P_\ell)$ une chaîne potentielle avec $P_i = (I_i; U_i)$, et x un élément de $\mathbf{A}$.*
Si $(P_0, \ldots, P_{i-1}, (I_i, x; U_i), P_{i+1}, \ldots, P_n)$ et $(P_0, \ldots, P_{i-1}, (I_i; U_i, x), P_{i+1}, \ldots, P_n)$ collapsent, alors C collapse.

Théorème abstrait 2.4 (Théorème de Krull généralisé)
Soit C une chaîne potentielle, les propriétés suivantes sont équivalentes :

- *La chaîne potentielle C ne collapse pas.*
- *Il existe une chaîne d'idéaux premiers qui raffine C.*

Ce théorème abstrait (inconnu auparavant semble-t-il) implique la caractérisation constructive suivante de la dimension de Krull d'un anneau (l'équivalence est établie en mathématiques classiques et la caractérisation sert de définition en mathématiques constructives).

Corollaire 2.3 *Pour tout anneau $\mathbf{A}$ les propriétés suivantes sont équivalentes :*

- *La dimension de Krull de $\mathbf{A}$ est $\leq \ell - 1$.*
- *Pour tous $x_1, \ldots, x_\ell \in \mathbf{A}$ la chaîne potentielle $((0; x_1), (x_1; x_2), \ldots, (x_{\ell-1}; x_\ell), (x_\ell, 1))$ collapse.*

– *Pour tous* $x_1, \ldots, x_\ell \in \mathbf{A}$ *il existe* $a_1, \ldots, a_\ell \in \mathbf{A}$ *et* $m \in \mathbb{N}$ *tels que*
$$x_1^m(x_2^m \cdots (x_\ell^m(1 + a_\ell x_\ell) + \cdots + a_2x_2) + a_1x_1) = 0\,.$$

Notons que cette caractérisation permet d'établir de manière particulièrement rapide et élégante la dimension d'un anneau de polynomes sur un corps ([10]).

Going up et Going down

Dans ce paragraphe nous donnons à titre d'exemple des versions concrètes (et constructivement prouvées, cf. [11]) du Going up et du Going down. Elles sont équivalentes (en trois lignes de Zorn et de tiers exclu) aux versions abstraites usuelles de ces théorèmes en mathématiques classiques.

Si $\mathbf{A} \subset \mathbf{B}$ et si $C = ((I_0, U_0), \ldots, (I_\ell, U_\ell))$ est une chaîne potentielle de $\mathbf{B}$ on note $C|_\mathbf{A}$ sa trace sur $\mathbf{A}$ c'est-à-dire la chaîne potentielle $((I_0 \cap \mathbf{A}, U_0 \cap \mathbf{A}), \ldots, (I_\ell \cap \mathbf{A}, U_\ell \cap \mathbf{A}))$.

Nous notons $L \bullet L'$ la concaténation de deux listes L et L'.

Théorème concret 2.5 (Going up) *Soit* $\mathbf{A} \subseteq \mathbf{B}$ *des anneaux commutatifs avec* $\mathbf{B}$ *entier sur* $\mathbf{A}$*. Soit* C_1 *une chaîne potentielle saturée de* $\mathbf{B}$ *et* C_2 *une chaîne potentielle de* $\mathbf{A}$*. La chaîne potentielle* $C = C_1 \bullet C_2$ *collapse dans* $\mathbf{B}$ *si et seulement si la chaîne potentielle* $C_1|_\mathbf{A} \bullet C_2$ *collapse dans* $\mathbf{A}$*.*

On obtient également que $\mathbf{B}$ et $\mathbf{A}$ ont la même dimension de Krull. La signification de cette affirmation est beaucoup plus riche que la signification usuelle classique. En effet, outre le résultat classique abstrait, la preuve constructive montre qu'une certaine machinerie de fabrication d'identités algébriques dans $\mathbf{A}$ permet de construire une machinerie analogue dans $\mathbf{B}$, et vice-versa.

De manière générale, la caractérisation de la dimension de Krull en terme de machinerie de fabrication d'identités algébriques ouvre l'espoir de fournir des versions algorithmiques générales pour des théorèmes où la dimension de Krull figure dans les hypothèses de départ. Cette perspective était impossible auparavant, et il fallait se limiter à des cas particuliers (comme les algèbres de présentation finie sur les corps) où on avait accès par d'autres moyens à la dimension de Krull de manière explicite.

Nous donnons maintenant sans commentaire une version constructive du Going down, en laissant le soin au lecteur de prouver l'équivalence avec la version usuelle en mathématiques classiques, via le théorème abstrait 2.4.

Théorème concret 2.6 (Going down) *Soit* $\mathbf{A} \subseteq \mathbf{B}$ *des anneaux intègres avec* $\mathbf{B}$ *entier sur* $\mathbf{A}$ *et* $\mathbf{A}$ *intégralement clos. Soit* C_1 *une chaîne potentielle saturée de* $\mathbf{A}$ *et* C_2 *une chaîne potentielle saturée de* $\mathbf{B}$*, non vides. Soit* I_ℓ *le dernier des idéaux dans la chaîne potentielle* C_1 *et* $I_{\ell+1}$ *le premier des idéaux dans la chaîne potentielle* $C_2|_\mathbf{A}$*. On suppose* $I_\ell \subseteq I_{\ell+1}$*. Si la chaîne potentielle* $C_1 \bullet C_2$ *collapse dans* $\mathbf{B}$*, alors la chaîne potentielle* C_2 *collapse dans* $\mathbf{B}$*.*

3 La cloture algébrique d'un corps

Dans cette section, nous donnons un aperçu du traitement constructif, par la méthode dynamique, de la cloture algébrique d'un corps (et de son utilisation) en mathématiques classiques.

Le système de calcul formel D5 (cf. [17]) a constitué la première mise en oeuvre systématique de l'évaluation dynamique comme moyen efficace de contourner les problèmes posés par la difficulté, voire l'impossibilité, de décomposer en facteurs premiers un polynome en une variable sur un corps.

Le fait qu'un tel système de calcul remplit les mêmes objectifs que la considération de la cloture algébrique en mathématiques classiques fournissait, pour la première fois, une sémantique constructive claire et très simple pour cet « objet abstrait » qui semblait auparavant nous échapper des mains comme une savonnette.

3.1 Corps incomplètement spécifiés

Un *corps incomplètement spécifié* est donné par un anneau $\mathbf{A}$ et un premier potentiel $P = (I; U)$ de $\mathbf{A}$ qui ne collapse pas. Éventuellemnt l'anneau $\mathbf{A}$ peut être décrit par générateurs et relations.

Si $\mathfrak{p}$ est un idéal premier qui raffine P, le couple $(\mathbf{A}, P)$ est considéré comme une spécification incomplète du corps des fractions de $\mathbf{A}/\mathfrak{p}$.

Si $(J; V)$ est le saturé de P l'anneau intègre $\mathbf{A}/\mathfrak{p}$ est un quotient de $\mathbf{A}/J$ (qui est un anneau réduit).

En général, un couple $\mathbf{K} = (\mathbf{A}, P)$ est appelé un *corps dynamique*, et si P collapse dans $\mathbf{A}$ on dit que le corps dynamique $\mathbf{K}$ *collapse*. L'évaluation dynamique de $\mathbf{K}$ consiste à explorer les raffinements possibles de P au sein d'un arbre de calcul, dont toutes les feuilles sont « orthogonales », c'est-à-dire ne peuvent être spécifiées que de manières contradictoires.

La considération d'un élément a de $\mathbf{A}$ en un point de l'arbre où P a été raffiné en $P' = (I'; U')$ conduit à poser la question : « a est-il nul ou inversible dans le corps dynamique $(\mathbf{A}, P')$? ». Si $(I'; U', a)$ collapse on peut répondre que a est nul (et le rajouter dans I'). De même, si $(I', a; U')$ collapse on peut répondre que a est inversible (et le rajouter dans U'). Si on ne sait répondre à aucune des deux questions, on ouvre deux branches, l'une avec le premier potentiel $(I'; U', a)$ et l'autre avec le premier potentiel $(I', a; U')$. Lorsqu'on développe les calculs on peut s'apercevoir qu'un premier potentiel collapse et on ferme la branche de calcul correspondante. Vu le théorème concret 2.1, si au départ on est certain que $\mathbf{K}$ ne collapse pas, alors on est certain qu'il est impossible que toutes les branches d'une évaluation dynamique de $\mathbf{K}$ meurent simultanément.

A titre d'exemple une évaluation dynamique du corps dynamique $(\mathbb{Z}, (0; 1))$ peut consister à créer pour des nombres premiers entre eux deux à deux $q_1, \ldots, q_n$ les branches correspondantes, c'est-à-dire à créer n branches « $\mathbb{Z}/\langle q_i \rangle$ » (chacune correspond à différentes possibilités de corps finis $\mathbb{Z}/\langle p \rangle$, ceux pour lesquels p divise q_i) et une branche où tous les q_i sont inversibles, qui correspond d'une part à $\mathbb{Q}$, et d'autre part aux autres corps finis $\mathbb{Z}/\langle p \rangle$ (ceux pour lesquels p ne divise aucun des q_i).

On voit assez clairement sur cet exemple, le rapport qu'il y a entre d'une part une évaluation dynamique d'un anneau en tant que corps et d'autre part une partition du spectre de l'anneau en un nombre fini de constructibles. Dans le cas d'un anneau arbitraire $\mathbf{A}$, l'avantage des évaluations dynamiques est qu'il n'y a nullement besoin de connaître les points du spectre pour travailler concrètement sur le spectre.

3.2 Cloture algébrique

Etant donné un corps dynamique $\mathbf{K} = (\mathbf{A}, P)$ on peut vouloir utiliser les facilités qu'offre la considération de la cloture algébrique. Le fait que ceci est toujours possible (sans danger de créer un collapsus général) résulte du théorème concret suivant.

Théorème concret 3.1 (Rajouter formellement un zéro d'un polynome unitaire)
Soit un corps dynamique $\mathbf{K} = (\mathbf{A}, P)$, $f \in \mathbf{A}[X]$ *unitaire et* $\mathbf{B} = \mathbf{A}[x] = \mathbf{A}[X]/\langle f \rangle$. *Si le corps dynamique* $\mathbf{K}[x] = (\mathbf{B}, P)$ *collapse, alors* $\mathbf{K}$ *collapse.*

La preuve de ce théorème concret revient à dire que $\mathbf{B}$ est un $\mathbf{A}$-module libre ayant pour base $1, x, \ldots, x^{\deg f - 1}$ ce qui résulte fondamentalement de l'algorithme de la division euclidienne, argument qui intervient aussi dans la construction en mathématiques classiques des extensions algébriques de corps.

Au moyen d'une zornette pas très agréable (voir les livres d'algèbre usuels) le théorème concret précédent donne l'existence en mathématiques classiques de la cloture algébrique d'un corps arbitraire $\mathbf{L}$ (il faut en gros introduire un idéal premier dans une $\mathbf{L}$-algèbre contenant des zéros formels en quantité suffisante).

En fait le système de calcul formel D5 fait un travail beaucoup plus précis que le théorème concret 3.1, et il est donc nettement plus informatif que la simple considération de la cloture algébrique. En effet les conceptrices du système ont mis au point un système de discussion des cas automatique (une recherche certifiée de collapsus) qui aboutit au théorème concret qui va suivre (après quelques précisions concernant la terminologie).

Définition 3.1 *Soit* $\mathbf{L}$ *un corps.*

1. *Une* $\mathbf{L}$*-algèbre de présentation finie* $\mathbf{A}$ *est dite* triangulaire *à* n *étages si elle est isomorphe à une algèbre* $\mathbf{L}_{(P_1,\ldots,P_n)} := \mathbf{L}[X_1,\ldots,X_n]/\langle P_1,\ldots,P_n\rangle$ *où chaque* P_i *est un polynome* X_i*-unitaire de* $\mathbf{L}[X_1,\ldots,X_{i-1}][X_i]$.
2. *Deux algèbres triangulaires* $\mathbf{L}_{(P_1,\ldots,P_n)}$ *et* $\mathbf{L}_{(Q_1,\ldots,Q_m)}$ *sont dites orthogonales si il existe* k *tel que :* $P_1 = Q_1, \ldots, P_k = Q_k$*, et on connaît* $A, B \in \mathbf{L}_{(P_1,\ldots,P_k)}[X_{k+1}]$ *tels que* $AP_{k+1} + BQ_{k+1} = 1$ *dans* $\mathbf{L}_{(P_1,\ldots,P_k)}[X_{k+1}]$.
3. *Si* $\mathbf{A}$ *est une algèbre triangulaire on note* $\widetilde{\mathbf{A}}$ *le quotient de* $\mathbf{A}$ *par son nilradical.*

Le calcul de générateurs du nilradical d'une algèbre triangulaire n'est pas évident (il est possible en caractéristique nulle et avec les corps parfaits). On a néanmoins un test facile d'appartenance au nilradical. Le sytème D5 obtient de façon tout à fait explicite, comme résultat final d'une évaluation dynamique bien menée le théorème de factorisation suivant :

Théorème concret 3.2 (Factorisation d'une algèbre triangulaire)
Soit $\mathbf{L}$ *un corps dans lequel l'égalité est décidable,* $\mathbf{A} = \mathbf{L}_{(P_1,\ldots,P_n)}$ *une* $\mathbf{L}$*-algèbre triangulaire et* $a_1, \ldots, a_s$ *des éléments de* $\mathbf{A}$*. Alors il existe des* $\mathbf{L}$*-algèbres triangulaires* $(\mathbf{A}_j)_{j=1,\ldots,r}$ *deux à deux orthogonales avec :*

– $\widetilde{\mathbf{A}} \simeq \widetilde{\mathbf{A}_1} \times \cdots \times \widetilde{\mathbf{A}_s}$.

– *Dans chaque* $\widetilde{\mathbf{A}_j}$ *chaque* a_i *est nul ou inversible.*

Notez qu'en mathématiques classiques l'égalité dans $\mathbf{L}$ est toujours décidable en vertu du tiers exclu.

L'idée de la preuve est que lorsqu'on demande « est-ce que $g(x)$ est inversible dans $\mathbf{A} = \mathbf{L}[x] = \mathbf{L}[X]/\langle f(X)\rangle$? », on peut pour répondre à cette question, au moyen de calculs de pgcds, décomposer $f(X)$ en un produit $f_1 f_2$ où f_1 est étranger à g et f_2 divise une puissance de g. Ce calcul permet aussi de remplacer éventuellement f_1 (resp. f_2) par un diviseur h_1 (resp. h_2) qui possède les mêmes zéros (resp. qui possède les mêmes zéros et en outre divise g). On a alors en posant $\mathbf{A}_1 = \mathbf{L}[X]/\langle h_1(X)\rangle$ et $\mathbf{A}_2 = \mathbf{L}[X]/\langle h_2(X)\rangle$: $\widetilde{\mathbf{A}} \simeq \widetilde{\mathbf{A}_1} \times \widetilde{\mathbf{A}_2}$, g inversible dans $\mathbf{A}_1$ et nul dans $\mathbf{A}_2$.

Ensuite, il faut gérer ce calcul de manière récursive, c'est-à-dire montrer qu'on peut remplacer le corps $\mathbf{L}$ par une $\mathbf{L}$-algèbre triangulaire, quitte à la factoriser lorsque les calculs présentent une ambigüité.

3.3 Le Nullstellensatz de Hilbert

Le Nullstellensatz de Hilbert est plus sophistiqué que le Nullstellensatz formel (théorème abstrait 2.1).

En mathématiques classiques il peut être vu comme une conséquence du Nullstellensatz formel. On utilise alors le fait que la théorie des corps algébriquement clos contenant un corps fixé est complète, via un algorithme d'élimination des quantificateurs. Cet algorithme peut être vu comme une recherche systématique de collapsus pour le premier potentiel P qui apparaît dans l'énoncé ci-après.

Ainsi même si le corps $\mathbf{L}$ sur lequel on travaille ne possède pas de cloture algébrique au sens constructif, on obtient une sémantique constructive claire pour le Nullstellensatz.

Théorème concret 3.3 (Nullstellensatz concret)
Soit $\mathbf{L}$ un corps où l'égalité est décidable. Soit $P = (f_1, \ldots, f_n; g)$ un premier potentiel fini dans $\mathbf{L}[X_1, \ldots, X_m]$.

1. *On a un test explicite (à la D5) pour décider si P collapse.*
2. *Les propriétés suivantes sont équivalentes :*
   (a) *P collapse, c'est-à-dire $g \in \sqrt{\langle f_1, \ldots, f_n \rangle}$.*
   (b) *« g s'annule aux zéros algébriques de $(f_1, \ldots, f_n)$ », plus précisément, pour toute $\mathbf{L}$-algèbre triangulaire $\mathbf{A}$ et tout $\xi = (\xi_1, \ldots, \xi_m) \in \widetilde{\mathbf{A}}^m$ on a l'implication dans $\widetilde{\mathbf{A}}$:*
   $$f_1(\xi) = \cdots = f_n(\xi) = 0 \Rightarrow g(\xi) = 0\,.$$
   (c) *« g s'annule aux zéros de $(f_1, \ldots, f_n)$ » : pout toute $\mathbf{L}$-algèbre réduite $\mathbf{B}$ et pour tout $\xi = (\xi_1, \ldots, \xi_m) \in \mathbf{B}^m$ on a l'implication dans $\mathbf{B}$:*
   $$f_1(\xi) = \cdots = f_n(\xi) = 0 \Rightarrow g(\xi) = 0\,.$$

Notez qu'en mathématiques classiques l'égalité est toujours décidable en vertu du tiers exclu, et que le théorème concret implique le Nullstellensatz habituel. En effet le point 2b peut être remplacé par d'autres formulations plus usuelles lorsque le corps $\mathbf{L}$ vérifie des hypothèses ad hoc :

(b') (dans le cas où toute $\mathbf{L}$-algèbre triangulaire contient un idéal premier)
Tout $\xi = (\xi_1, \ldots, \xi_m)$ zéro de $\langle f_1, \ldots, f_n \rangle$ dans une extension finie de $\mathbf{L}$ est aussi un zéro de g.

(b") (dans le cas où $\mathbf{L}$ possède une cloture algébrique $\mathbf{M}$)
g s'annule aux zéros de $\langle f_1, \ldots, f_n \rangle$ dans $\mathbf{M}^m$.

Pour plus de détails on pourra consulter [15].

3.4 Isomorphisme de deux clotures séparables

En mathématiques classiques l'existence d'un $\mathbf{L}$-isomorphisme entre deux clotures algébriques de $\mathbf{L}$ résulte (par Zorn) de l'existence d'un $\mathbf{L}$-isomorphisme entre deux corps de décomposition d'un même polynome.

Pour cet isomorphisme un raisonnement par induction permet de se limiter au cas où on rajoute les zéros d'un polynome irréductible.

Quelle contrepartie constructive nous donne la méthode dynamique pour le théorème concernant les extensions finies ?

Nous ne ferons qu'esquisser une réponse en nous limitant à la cloture séparable. Ce serait un théorème du style du théorème 3.4, pour lequel nous indiquerons uniquement une preuve en mathématiques classiques. Avec ce théorème, il s'agit aussi d'une approche dynamique de la théorie de Galois.

Rappelons que si $f \in \mathbf{L}[X]$ est un polynome unitaire de degré n, *l'algèbre de décomposition universelle de f au dessus de* $\mathbf{L}$ est l'algèbre triangulaire (de dimension $n!$) obtenue en rajoutant formellement toutes les racines de f. Nous la noterons $\mathbf{L}[(x_i)_{x_i:f}]$. Par exemple on peut poser

$$\mathbf{L}[(x_i)_{x_i:f}] = \mathbf{L}[x_1, \ldots, x_n], \text{ avec } \mathbf{L}[x_1] = \mathbf{L}[X_1]/\langle f_1(X_1)\rangle,\ \mathbf{L}[x_1, x_2] = \mathbf{L}[x_1][X_2]/\langle f_2(X_2)\rangle, \ldots$$

avec $f_1 = f$,

$$f_2(X_2) = \frac{f_1(X_2) - f_1(x_1)}{X_2 - x_1}, \ \ldots\ , f_{i+1}(X_{i+1}) = \frac{f_i(X_{i+1}) - f_i(x_i)}{X_{i+1} - x_i}, \ldots.$$

Cette algèbre peut également être décrite, de manière plus symétrique, comme quotient de $\mathbf{L}[X_1, \ldots, X_n]$ par l'idéal obtenu en identifiant les fonctions symétriques élémentaires des X_i aux coefficients de f (aux signes près).

Théorème concret 3.4 (Factorisation de l'algèbre de décomposition universelle d'un polynome séparable)
Soit $\mathbf{L}$ un corps où l'égalité est décidable. Soit $f \in \mathbf{L}[X]$ un polynome séparable et $\mathbf{A} = \mathbf{L}[(x_i)_{x_i:f}]$ sa $\mathbf{L}$-algèbre de décomposition universelle. Soit $\mathbf{B}$ une $\mathbf{L}$-algèbre dans laquelle f se décompose en facteurs de degré 1. Soit $\mathbf{C}$ la sous-algèbre de $\mathbf{B}$ engendrée par les zéros de f dans cette décomposition. Alors il existe un idempotent e de $\mathbf{A}$ tel que, en notant $\mathbf{A}_1$ l'algèbre $\mathbf{A}[1/e] \simeq e\mathbf{A} \simeq \mathbf{A}/\langle 1 - e\rangle$ on ait :

(1) *L'orbite de e sous l'action du groupe symétrique est une famille $(e_i)_{i=1,\ldots,p}$ qui forme un système fondamental d'idempotents orthogonaux, de sorte que $\mathbf{A} \simeq (\mathbf{A}_1)^p$.*

(2) *L'algèbre $\mathbf{C}$ est isomorphe à une puissance de $\mathbf{A}_1$.*

En mathématiques classiques, le théorème se démontre comme suit : on sait que l'algèbre de décomposition universelle est isomorphe à $\mathbf{L}_1^k$ où $\mathbf{L}_1$ est le corps des racines de f dans une cloture séparable de $\mathbf{L}$ et k est l'indice du groupe de Galois dans le groupe symétrique. En outre le groupe symétrique opère sur $\mathbf{A}$ en permutant transitivement les k facteurs de $\mathbf{L}_1^k$.

Par ailleurs, dans une $\mathbf{L}$-algèbre quelconque, si on a $f(X) = \prod_{i=1}^n (X - \xi_i)$, alors la sous-algèbre $\mathbf{L}[\xi_1, \ldots, \xi_n]$ est un quotient de l'algèbre de décomposition universelle, donc est isomorphe à une puissance de $\mathbf{L}_1$.

Donc en mathématiques classiques, on peut imposer en plus que $\mathbf{A}_1$ soit un corps. Mais seul le théorème sous la forme énoncée ci-dessus pourra être établi en mathématiques constructives, et pourra fournir un algorithme général. Peut-être en outre, il faudra introduire une hypohèse supplémentaire du style : $\mathbf{B}$ admet une base en tant que $\mathbf{L}$-espace vectoriel.

Enfin, comme le calcul itératif procèdera dans des algèbres plutot que des corps, on devrait établir une variante dans laquelle on supposerait seulement que $\mathbf{L}$ est un corps dynamique et f est un polynome étranger à sa dérivée (c'est-à-dire engendrant avec sa dérivée l'idéal $\langle 1\rangle$).

4 Théories dynamiques, treillis distributifs et espaces sans points

4.1 Treillis distributifs

Nous présentons dans cette section les travaux [8] et [9] sur les treillis distributifs.

Idéaux, filtres et spectre

Un treillis distributif est un ensemble ordonné avec sup et inf finis, un élément minimum (noté 0) et un élément maximum (noté 1). On demande que les lois sup et inf soient distributives l'une par rapport à l'autre. On note ces lois $\vee$ et $\wedge$. La relation $a \leq b$ peut être définie par $a \vee b = b$. La théorie des treillis distributifs est alors purement équationnelle. Il y a donc des treillis distributifs définis par générateurs et relations.

On note $\mathcal{P}_{\mathrm{f}}(X)$ l'ensemble des parties finies d'un ensemble X.

Si A est une partie finie d'un treillis distributif T on note :

$$\bigvee A := \bigvee_{x \in A} x \qquad \text{et} \qquad \bigwedge A := \bigwedge_{x \in A} x\,.$$

On note $A \vdash B$ ou $A \vdash_T B$ la relation définie comme suit sur l'ensemble $\mathcal{P}_{\mathrm{f}}(T)$ des parties finies d'un treillis distributif T :

$$A \vdash B \quad \overset{\mathrm{def}}{\Longleftrightarrow} \quad \bigwedge A \leq \bigvee B\,.$$

Cette relation vérifie les axiomes suivants, dans lesquels on écrit x pour $\{x\}$ et A, B pour $A \cup B$.

$$\begin{array}{rcrcll} & & a & \vdash & a & (R)\\ A \vdash B & \Longrightarrow & A, A' & \vdash & B, B' & (M)\\ (A, x \vdash B)\ \&\ (A \vdash B, x) & \Longrightarrow & A & \vdash & B & (T)\end{array}$$

on dit que la relation est réflexive, monotone et transitive. La troisième règle (transitivité) s'appelle aussi la règle de coupure.

Proposition 4.1 *Soit T un treillis distributif et (J, F) un couple de parties de T. On considère le treillis distributif T' engendré par T et par les relations $x = 0$ pour les $x \in J$ et $y = 1$ pour les $y \in F$ (T' est un quotient de T). Alors on a :*

$$a \leq_{T'} b \quad \Longleftrightarrow \quad \exists J_0 \in \mathcal{P}_{\mathrm{f}}(J), \exists F_0 \in \mathcal{P}_{\mathrm{f}}(F),\ \ a, F_0 \vdash_T b, J_0 \tag{3}$$

Dans la proposition ci-dessus la classe d'équivalence de 0 est appelée un *idéal* du treillis. Si $F = \emptyset$, c'est *l'idéal engendré par J*, on le note $\langle J \rangle_T$. Un idéal I est soumis aux seules contraintes suivantes :

$$\begin{array}{rcl} & & 0 \in I\\ x, y \in I & \Longrightarrow & x \vee y \in I\\ x \in I,\ z \in T & \Longrightarrow & x \wedge z \in I\end{array} \tag{4}$$

(la dernière se réécrit $(x \in I,\ y \leq x) \Rightarrow y \in I$).

Un *idéal principal* est un idéal engendré par un élément a. On a $\langle a \rangle_T = \{x \in T\ ;\ x \leq a\}$. Tout idéal de type fini est principal.

La notion duale de celle d'idéal est la notion de *filtre*. Il est soumis aux seules contraintes

$$\begin{array}{rcl} & & 1 \in F\\ x, y \in F & \Longrightarrow & x \wedge y \in F\\ x \in F,\ z \in T & \Longrightarrow & x \vee z \in F\end{array} \tag{5}$$

Nous noterons $T/(J = 0, F = 1)$ le treillis quotient T' décrit à la proposition 4.1. Soit $\psi : T \to T'$ la projection canonique. Si I est l'idéal $\psi^{-1}(0)$ et F le filtre $\psi^{-1}(1)$, on dit que *l'idéal I et le filtre F sont conjugués*. Un idéal I et un filtre F sont conjugués si et seulement si on a :

$$(f \in F,\ x \wedge f \in I) \Longrightarrow x \in I \quad \text{et} \quad (j \in I,\ x \vee j \in F) \Longrightarrow x \in F$$

Lorsqu'un idéal I et un filtre F sont conjugués, on a

$$1 \in I \iff 0 \in F \iff (I, F) = (T, T)$$

Le treillis quotient $T/(J = 0, F = 1)$ sera aussi noté $T/(I, F)$. Tout homomorphisme φ de T vers un autre treillis distributif T_1 vérifiant $\varphi(J) = \{0\}$ et $\varphi(F) = \{1\}$ se factorise de manière unique par le treillis quotient $T/(I, F)$.

On note $\mathbf{1}$ le treillis trivial à un seul élément et $\mathbf{2}$ le treillis à deux éléments.

En mathématiques classiques un *idéal premier* I d'un treillis $T \neq \mathbf{1}$ est un idéal dont le complémentaire F est un filtre, qui est alors un *filtre premier*. Il revient au même de dire, pour le filtre F, que

$$0 \in F \implies 1 = 0 \qquad \text{et} \qquad (x \vee y) \in F \implies (x \in F \text{ ou } y \in F) \tag{6}$$

ou encore de dire que I est le noyau d'un homorphisme de T vers $\mathbf{2}$. En mathématiques constructives il semble logique de choisir la définition (6) qui est moins contraignante, sans supposer $T \neq \mathbf{1}$ mais en donnant sa pleine signification constructive au “ou”. On définit la notion d'idéal premier de manière duale.

En mathématiques classiques on appelle *spectre du treillis distributif* T et on note $\mathrm{Spec}(T)$ l'ensemble ordonné $\mathrm{Hom}(T, \mathbf{2})$. Lorsque $T \neq \mathbf{1}$ il revient au même de considérer l'ensemble des filtres premiers de T. La relation d'ordre correspond alors à l'inclusion des filtres premiers ou si on préfère à l'inclusion renversée des idéaux premiers.

Définition 4.2 *En mathématiques constructives nous définissons* $\mathrm{Spec}(T)$ *comme l'ensemble ordonné des filtres premiers de T : un filtre premier est un filtre F qui vérifie l'axiome (6).*

Relations implicatives

Une manière intéressante d'aborder la question des treillis distributifs définis par générateurs et relations est de considérer la relation $A \vdash B$ définie sur l'ensemble $\mathcal{P}_{\mathrm{f}}(T)$ des parties finies d'un treillis distributif T. En effet, si $S \subseteq T$ engendre T comme treillis, alors la connaissance de la relation $\vdash$ sur $\mathcal{P}_{\mathrm{f}}(S)$ suffit à caractériser sans ambigüité le treillis T, car tout terme sur S peut être réécrit, au choix, en forme normale conjonctive (inf de sups dans S) ou normale disjonctive (sup de infs dans S). Donc si on veut comparer deux éléments du treillis engendré par S on écrit le premier en forme normale disjonctive, le second en forme normale conjonctive, et on remarque que

$$\bigvee_{i \in I} \Big(\bigwedge A_i \Big) \leq \bigwedge_{j \in J} \Big(\bigvee B_j \Big) \qquad \iff \qquad \&_{(i,j) \in I \times J} \; (A_i \vdash B_j)\,.$$

Définition 4.3 *Pour un ensemble S arbitraire, une relation sur $\mathcal{P}_{\mathrm{f}}(S)$ qui est réflexive, monotone et transitive (voir page 17) est appelée une* relation implicative *sur S (en anglais :* entailment relation*).*

L'origine des relations implicatives se trouve dans le calcul des séquents de Gentzen, qui mit le premier l'accent sur la règle (T) (la coupure). Le lien avec les treillis distributifs a été mis en valeur dans [8]. Le théorème suivant (cf. [8]) est fondamental. Il dit que les trois axiomes des relations implicatives sont exactement ce qu'il faut pour que l'interprétation en forme de treillis distributif soit adéquate.

Théorème 4.1 (théorème fondamental des relations implicatives) *On considère un ensemble S avec une relation implicative $\vdash_S$ sur S. On considère le treillis distributif T défini par* *générateurs et relations comme suit : les générateurs sont les éléments de S et les relations sont les*

$$A \;\vdash_T\; B$$

chaque fois que $A \;\vdash_S\; B$. Alors pour toutes parties finies A et B de S on a

$$A \;\vdash_T\; B \Longrightarrow A \;\vdash_S\; B$$

Premiers potentiels, chaînes potentielles et dimension de Krull

Définition 4.4 *Soit T un treillis distributif.*

- *Un* premier potentiel *dans T est donné par un couple $(J;U)$ de parties de T. Nous le considérons comme une spécification incomplète pour un idéal premier P qui vérifie $J \subseteq P$ et $U \cap P = \emptyset$. Il est dit* fini *si J et U sont finis,* trivial *si $J = U = T$.*
- *Un premier potentiel $(J;U)$ est dit* saturé *si J est un idéal, U un filtre et si J et U sont conjugués. Tout premier potentiel engendre un premier potentiel saturé $(I;F)$ décrit à la proposition 4.1.*
- *On dit que le premier potentiel $(J;U)$* collapse *si le premier potentiel saturé $(I;F)$ qu'il engendre est trivial, autrement dit il existe une partie finie J_0 de J et une partie finie U_0 de U telles que :*
$$U_0 \vdash_T J_0\,.$$

On a le théorème suivant analogue au théorème concret 2.1.

Théorème concret 4.1 (Collapsus simultané pour les premiers potentiels)
Soit un premier potentiel $(J;U)$ et un élement x dans un treillis distributif T. Si les premiers potentiels $(J,x;U)$ et $(J;U,x)$ collapsent, alors $(J;U)$ collapse également.

Le théorème abstrait immédiatement équivalent en mathématiques classiques peut se reformuler comme suit.

Théorème abstrait 4.1 (Théorème de représentation)
L'application $\theta_T : T \to \mathcal{P}(\mathrm{Spec}(T))$ définie par $a \mapsto \{\varphi \in \mathrm{Spec}(T)\ ;\ \varphi(a) = 1\}$ est un homomorphisme injectif de treillis distributifs. Autrement dit, tout treillis distributif peut être représenté comme un treillis de parties d'un ensemble.

Nous passons maintenant aux chaînes d'idéaux premiers et à leurs spécifications incomplètes.

Définition 4.5 *Dans un treillis distributif T*

- *Une* spécification partielle pour une chaîne d'idéaux premiers *(ce que nous abrégeons en* chaîne potentielle*) est définie comme suit. Une chaîne potentielle de longueur ℓ est un liste de $\ell + 1$ premiers potentiels de T : $C = ((J_0;U_0), \ldots, (J_\ell;U_\ell))$. La chaîne potentielle est dite finie si toutes les parties sont finies. Une chaîne potentielle de longueur 0 n'est autre qu'un* premier potentiel.
- *Une chaîne potentielle est dite* saturée *si les $(J_i;U_i)$ sont des couples d'idéaux et filtres conjugués, et si on a les relations $J_i \subseteq J_{i+1}$, $U_{i+1} \subseteq U_i$ $(i = 0, \ldots, \ell - 1)$.*
- *On dit qu'une chaîne potentielle $C' = ((J'_0;U'_0), \ldots, (J'_\ell;U'_\ell))$ est* un raffinement de la chaîne potentielle *$C = ((J_0;U_0), \ldots, (J_\ell;U_\ell))$ si on a $J_k \subseteq J'_k$, $U_k \subseteq U'_k$,*
- *On dit qu'une chaîne potentielle C* collapse *si la seule chaîne potentielle saturée qui raffine C est la chaîne potentielle triviale $((T;T), \ldots, (T;T))$.*

On a une caractérisation du collapsus d'une chaîne potentielle sous forme purement algébrique (nous nous limitons ici au cas fini) :

Proposition 4.6 *Soit une chaîne potentielle finie $C = ((J_0; U_0), \dots, (J_\ell; U_\ell))$ dans un treillis distributif T. La chaîne potentielle C collapse si et seulement si il existe $a_1, \dots, a_\ell \in T$, avec les relations suivantes dans T :*

$$\begin{array}{rcl} a_1,\ U_0 & \vdash & J_0 \\ a_2,\ U_1 & \vdash & J_1,\ a_1 \\ \vdots & \vdots & \vdots \\ a_\ell,\ U_{\ell-1} & \vdash & J_{\ell-1},\ a_{\ell-1} \\ U_\ell & \vdash & J_\ell,\ a_\ell \end{array}$$

La véritable raison de ces identités provient de l'introduction d'un nouveau treillis $\mathrm{Kr}_\ell(T)$ dont les idéaux premiers correspondent aux chaines d'idéaux premiers de longueur ℓ de T. Ce treillis que nous ne décrivons pas ici a été introduit par Joyal. Pour plus de précisions voir [9, 20, 24].

Théorème concret 4.2 (Collapsus simultané pour les chaînes potentielles dans les treillis distributifs)
Soit une chaîne potentielle $C = ((J_0; U_0), \dots, (J_\ell; U_\ell))$ dans un treillis distributif T. Soit $x \in T$. Supposons que les chaînes potentielles $((J_0; U_0), \dots, (J_i, x; U_i), \dots, (J_\ell; U_\ell))$ et $((J_0; U_0), \dots, (J_i; U_i, x), \dots, (J_\ell; U_\ell))$ collapsent toutes les deux, alors C collapse également.

Le théorème abstrait correspondant est le suivant.

Théorème abstrait 4.2 (Nullstellensatz formel pour les chaînes d'idéaux premiers dans un treillis distributif) *Soit T un treillis distributif et $((J_0; U_0), \dots, (J_\ell; U_\ell))$ une chaîne potentielle dans T. Les propriétés suivantes sont équivalentes :*

(*a*) *Il existe $\ell + 1$ idéaux premiers $P_0 \subseteq \cdots \subseteq P_\ell$ tels que $J_i \subseteq P_i$, $U_i \cap P_i = \emptyset$, $(i = 0, \dots, \ell)$.*

(*b*) *La chaîne potentielle ne collapse pas.*

Ceci conduit à la définition constructive suivante de la dimension de Krull, de manière entièrement analogue au cas des anneaux commutatifs.

Définition 4.7 *Un treillis distributif T engendré par une partie A est dit* de dimension $\leq \ell - 1$ *s'il vérifie la condition suivante : pour tous $x_1, \dots, x_\ell \in A$ la chaîne potentielle $((0, x_1), (x_1, x_2), \dots, (x_{\ell-1}, x_\ell), (x_\ell, 1))$ collapse, ce qui revient à dire qu'il existe a_1, a_2,$\dots a_\ell$ vérifiant :*

$$a_1,\, x_1 \vdash 0\,, \quad a_2,\, x_2 \vdash a_1,\, x_1\,, \dots, \quad a_\ell,\, x_\ell \vdash a_{\ell-1},\, x_{\ell-1}\,, \quad 1 \vdash a_\ell,\, x_\ell.$$

En particulier un treillis distributif est de dimension ≤ 0 si et seulement si on a $\forall x\, \exists a\, (\, x \wedge a = 0,\ x \vee a = 1)$ c'est-à-dire si c'est une algèbre de Boole.

Cas des algèbres de Heyting

Un treillis distributif T est appelé un *treillis implicatif* [16] ou une *algèbre de Heyting* [23] lorsqu'il existe une opération binaire $\to$ vérifiant pour tous a, b, c :

$$a,\, b \vdash c \quad \Longleftrightarrow \quad a \vdash b \to c\,,$$

auquel cas l'opération $\to$ est déterminée de manière unique par la structure du treillis. On définit alors la loi unaire $\neg x = x \to 0$.

Le collapsus d'une chaîne potentielle finie s'écrit alors sous la forme simple suivante.

Théorème 4.2 *Soit une chaîne potentielle finie $C = ((J_0; U_0), \ldots, (J_\ell; U_\ell))$ dans un treillis implicatif T. Alors la chaîne potentielle C collapse si et seulement si*

$$1 = u_\ell \to (j_\ell \vee (u_{\ell-1} \to (j_{\ell-1} \vee \cdots (u_0 \to j_0) \cdots)))$$

où $u_j = \bigwedge U_j$ et $j_k = \bigvee J_k$.

Comme conséquence on obtient la dimension de Krull sous forme d'identités algébriques dans la structure du treillis implicatif.

Corollaire 4.8 *Un treillis implicatif T est de dimension $\leq \ell - 1$ si et seulement si pour toute suite $x_1, \ldots, x_\ell$ dans T on a l'égalité*

$$1 = x_\ell \vee (x_\ell \to \cdots (x_2 \vee (x_2 \to (x_1 \vee \neg x_1))) \cdots)$$

Le lien avec la dimension de Krull des anneaux commutatifs

Cette sous-section a sa véritable origine dans les travaux de Joyal (cf. [9, 20, 24]).

Dans un anneau commutatif $\mathbf{A}$, le *treillis de Zariski* $\mathrm{Zar}(\mathbf{A})$ a pour éléments les radicaux d'idéaux de type fini (la relation d'ordre est l'inclusion, $\sqrt{I_1} \wedge \sqrt{I_2} = \sqrt{I_1 I_2}$ et $\sqrt{I_1} \vee \sqrt{I_2} = \sqrt{I_1 + I_2}$). Le treillis de Zariski de $\mathbf{A}$ est toujours un treillis distributif, mais en général l'égalité n'est pas testable. Néanmoins une inclusion $\sqrt{I_1} \subseteq \sqrt{I_2}$ peut être certifiée de manière finie si l'anneau $\mathbf{A}$ est discret. Ce treillis contient toutes les informations nécessaires au développement du point de vue constructif concernant la théorie abstraite et non constructive du spectre de Zariski. Nous notons $\widetilde{a}$ pour $\sqrt{\langle a \rangle}$. Pour une partie S de $\mathbf{A}$ nous notons $\widetilde{S}$ la partie de $\mathrm{Zar}(\mathbf{A})$ formée des $\widetilde{s}$ pour $s \in S$.

Soient U et J deux familles finies dans $\mathbf{A}$, on a

$$\widetilde{U} \vdash_{\mathrm{Zar}(\mathbf{A})} \widetilde{J} \quad \Longleftrightarrow \quad \prod_{u \in U} u \in \sqrt{\langle J \rangle} \quad \Longleftrightarrow \quad \mathcal{M}(U) \cap \langle J \rangle \neq \emptyset$$

c'est-à-dire encore

$$(J, U) \text{ collapse dans } \mathbf{A} \quad \Longleftrightarrow \quad (\widetilde{J}, \widetilde{U}) \text{ collapse dans le treillis } \mathrm{Zar}(\mathbf{A})$$

Cela suffit à décrire ce treillis. Plus précisément on a :

Proposition 4.9 *Le treillis $\mathrm{Zar}(\mathbf{A})$ d'un anneau commutatif $\mathbf{A}$ est (à isomorphisme près) le treillis engendré par $(\mathbf{A}, \vdash)$ où $\vdash$ est la plus petite relation implicative vérifiant*

$$0_{\mathbf{A}} \ \vdash \quad ; \quad \vdash \ 1_{\mathbf{A}} \quad ; \quad x + y \ \vdash \ x,\, y \quad ; \quad xy \ \vdash \ x \quad ; \quad x,\, y \ \vdash \ xy$$

On reconnaît là une réécriture des axiomes qui définissent un idéal premier $\mathfrak{P}$ si on interprète x comme signifiant $x \notin \mathfrak{P}$, et les autres symboles avec leur signification usuelle en logique : $\vdash$ pour « implique », la virgule avant $\vdash$ pour la conjonction, et la virgule après $\vdash$ pour la disjonction.

Le treillis dual serait défini par les relations

$$\vdash \ 0_{\mathbf{A}} \quad ; \quad 1_{\mathbf{A}} \ \vdash \quad ; \quad x,\, y \ \vdash \ x + y \quad ; \quad x \ \vdash \ xy \quad ; \quad xy \ \vdash \ x,\, y$$

avec l'interprétation de x comme signifiant $x \in \mathfrak{P}$.

Ainsi le treillis de Zariski est le treillis distributif « des axiomes des idéaux premiers » ou si l'on préfère, celui des « axiomes des anneaux intègres ». En outre on vérifie facilement que son spectre est le spectre premier de l'anneau. Tout l'avantage est qu'on n'a pas besoin des points du spectre pour parler du treillis de Zariski.

En outre la théorie de la dimension de Krull des anneaux devient un simple cas particulier de la théorie de la dimension de Krull des treillis distributifs.

La dualité entre treillis distributifs et espaces spectraux

En mathématiques classiques on a une dualité canonique entre treillis distributifs et *espaces spectraux*, introduite par Stone dans [44].

Pour un treillis T, Stone définit la topologie suivante sur $\mathrm{Spec}(T)$, vu comme ensemble ds filtres premiers de T : une base d'ouverts est donnée par les

$$U(a) = \{\, \mathfrak{T} \in \mathrm{Spec}(T)\,;\, a \in \mathfrak{T}\,\} \qquad (a \in T).$$

On a alors

$$U(0) = \emptyset,\; U(1) = T,\; U(a \wedge b) = U(a) \cap U(b) \;\text{ et }\; U(a \vee b) = U(a) \cup U(b).$$

Pour cette topologie (dite spectrale) les ouverts quasi-compacts sont exactement les $U(a)$ ce qui permet de récupérer le treillis à partir de l'espace topologique $\mathrm{Spec}(T)$.

Les espaces topologiques de ce type sont appelés des espaces spectraux et ils peuvent être caractérisés par les propriétés suivantes :

– L'espace est de type T_0 : étant donnés deux points il existe un voisinage de l'un des deux qui ne contient pas l'autre.

– L'espace est quasi-compact, l'intersection de deux ouverts quasi-compacts est un ouvert quasi-compact, et tout ouvert est réunion d'ouverts quasi-compacts.

– Pour tout fermé F et pour tout ensemble S d'ouverts quasicompacts tels que $F \cap \bigcap_{U \in S'} U \neq \emptyset$ pour toute partie finie S' de S, on a aussi $F \cap \bigcap_{U \in S} U \neq \emptyset$.

Le foncteur Spec établit une équivalence entre la catégorie des treillis distributifs et la catégorie opposée à la catégorie des espaces spectraux.

Bien que cette équivalence soit « bien connue » des mathématiciens de la théorie des topos, selon nous, l'accent n'avait pas encore été suffisamment mis sur le caractère constructif de l'aspect « treillis distributif », qui résulte du fait que « le treillis admet une description explicite par générateurs et relations ». En mathématiques classiques les gens pensent mieux comprendre les choses dans leur version « espaces spectraux » et ils ont naturellement tendance à définir le treillis distributif à partir de son spectre plutot que le contraire, ce qui enlève au treillis son caractère d'objet concret.

Notre thèse est que tout argument classique du coté des espaces spectraux se relit en un argument constructif du coté des treillis distributifs.

Dans notre mise en pratique de cette thèse, chaque fois que nous avons réussi le décryptage, la preuve classique abstraite s'est avérée être en fait un double renversement par l'absurde de la preuve constructive qu'elle cache.

Par exemple, la preuve classique de la solution positive pour le 17-ème problème de Hilbert dans [2] procède comme suit. On considère un polynome $P \in \mathbf{R}[X_1, \ldots, X_n]$ partout ≥ 0 (avec $\mathbf{R}$ réel clos). Si P n'était pas une somme de carrés dans $\mathbf{R}(X_1, \ldots, X_n)$, le corps réel $\mathbf{R}(X_1, \ldots, X_n)$ pourrait être ordonné avec $P < 0$. Notons $\mathbf{R}_1$ la cloture réelle de ce corps ordonné. Le fait que P est partout ≥ 0 peut être prouvé dans la théorie de corps réels clos (car elle est complète), et cette preuve s'applique à $\mathbf{R}_1$. Or P évalué en $(X_1, \ldots, X_n) \in \mathbf{R}_1^n$ est égal à P donc est < 0. Contradiction.

Ainsi le recours à l'objet idéal $\mathbf{R}_1$ dans la preuve classique est utilisé essentiellement à travers le fait que son existence supposée conduit à une contradiction. Et cet objet idéal existe lui-même en vertu d'une présupposition fausse, à savoir que P ne serait pas une somme de carrés.

La preuve constructive cachée dans cette preuve consiste à « remettre les choses à l'endroit » (cf. [15, 33]). On part de la preuve en théorie des corps réels clos que P est partout ≥ 0 (cette preuve existe en vertu d'un algorithme d'élimination des quantificateurs). On en déduit que la structure algébrique dynamique de corps réels clos basée sur le corps réel $\mathbf{R}(X_1, \ldots, X_n)$ avec la relation $P < 0$ collapse. On montre ensuite que ce collapsus se transfère à la structure algébrique dynamique de corps ordonné basée sur la même présentation : pour ce faire, on reprend des calculs algébriques présents dans la preuve par Artin qu'un corps ordonné possède une cloture réelle. Enfin on en déduit que P est une somme de carrés : pour ce faire, on reprend des calculs explicites présents dans la preuve par Artin qu'un corps réel peut être ordonné avec $P < 0$ si P n'est pas une somme de carrés. Ces calculs disent exactement que si un corps réel collapse comme corps ordonné après qu'on ait rajouté la relation $P < 0$ c'est que P est une somme de carrés.

4.2 Théories géométriques et structures algébriques dynamiques

Théories géométriques

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

$$A \implies \exists \underline{y}^1 \, B_1 \ \vee \ \cdots \ \vee \ \exists \underline{y}^m \, B_m \tag{7}$$

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.

Théories dynamiques

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

– 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 (7) est utilisé en tant que règle (8) :

$$A \ \vdash \ \exists \underline{y}^1 \, B_1 \text{ ou } \cdots \text{ ou } \exists \underline{y}^m \, B_m \tag{8}$$

(voir le point 4 et l'exemple qui suit).

– 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 $\mathcal{CD}$ des corps (discrets) est basée sur le langage des anneaux commutatifs et elle a pour axiomes, outre ceux des anneaux commutatifs, celui des corps discrets :

$$\vdash \ x = 0 \ \text{ ou } \ \exists y \, xy = 1 \tag{9}$$

Pour démontrer la règle dynamique

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

on ouvre deux branches conformément à l'axiome (9). Dans la première on a $z = 0$ est la conclusion est prouvée. Dans la deuxième on introduit un paramètre y avec la relation $yz = 1$. Les axiomes des anneaux commutatifs permettent alors de démontrer les égalités $z = 1 \times z = (yz)z = y(z^2) = y \times 0 = 0$, et la conclusion est également prouvée.

On a le théorème fondamental suivant (cf. par exemple le théorème 1 dans [15]) qui est déjà connu pour les théories équationnelles (cf. [41]), et dont nous serions bien téméraires de revendiquer la paternité, tant ce genre de résultat est omniprésent dans la littérature contemporaine (sous des formes plus ou moins déguisées). Du moins la preuve dans [15] est simple et constructive.

Théorème 4.3 (Théorème d'élimination des coupures)
Pour ce qui concerne les théories du premier ordre, si on a affaire uniquement à des axiomes géométriques, la logique (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 géométrique correspondante $\mathcal{T}$ (on utilise dans la théorie géométrique les connecteurs, les quantificateurs et la logique classique du premier ordre).

Structures algébriques dynamiques

Si $\mathcal{T} = (\mathcal{L}, \mathcal{A})$ est une théorie géométrique, 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 $\vdash P(\underline{x})$.

Par exemple le corps dynamique $\mathbf{K} = (\mathcal{CD}, (G, R))$, avec l'ensemble de générateurs $G = \{a, b\}$ et l'ensemble de relations $R = \{105 = 0, a^2 + b^2 = 1\}$, 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 qu'on obtient en élargissant le langage avec les constantes prises dans G et en rajoutant 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*.

L'algèbre « concrète » consiste pour l'essentiel à prouver des faits ou des règles dynamiques dans des structures algébriques dynamiques particulières. Le lecteur pourra se convaincre que tous les « théorèmes concrets » énoncés dans les sections précédentes sont bien de ce type. C'est un peu plus général que la théorie (inépuisable) des identités algébriques, à l'oeuvre derrière la plupart des grands théorèmes d'algèbre abstraite.

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 « $\vdash P(\underline{t})$ » 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. Affirmer un fait collapsant en le rajoutant comme axiome revient à supprimer tous les modèles non triviaux.

4.3 Le treillis de Zariski et le spectre d'une structure algébrique dynamique

Avertissement : *Nous supposons dans cette section que les théories géométriques qui interviennent ont uniquement des axiomes simples du type (10) suivant*

$$P_1(\underline{t_1}), \dots, P_n(\underline{t_n}) \vdash Q_1(\underline{t'_1}), \dots, Q_m(\underline{t'_m}) \tag{10}$$

avec les conventions : chaque P_i et chaque Q_j est un prédicat donné dans la structure, les $\underline{t_i}$ et $\underline{t'_k}$ sont des listes de termes, la virgule avant $\vdash$ représente un « et » et la virgule après $\vdash$ représente un « ou ».

En fait on peut voir que toute théorie géométrique dont les axiomes (7) ne font pas intervenir le quantificateur $\exists$ peut être réécrite sous la forme indiquée ci-dessus.

Le treillis de Zariski d'une structure algébrique dynamique

Définition 4.10 *Le* treillis des faits *de la structure algébrique dynamique* $\mathbf{D} = ((\mathcal{L}, \mathcal{A}), (G, R))$ *est le treillis distributif donné par générateurs et relations comme suit :*

- *les générateurs sont les éléments $P(\underline{t})$ où P est un prédicat arbitraire de $\mathcal{L}$ et $\underline{t}$ une liste de termes clos du langage $\mathcal{L} \cup G$,*
- *les relations sont données par les axiomes (rappelons qu'ils sont tous de la forme (10)) : on y subsitue les variables par des termes clos arbitraires et on relit l'axiome comme une relation implicative.*

En analogie avec le cas de la théorie des anneaux intègres (décrite avec $\neq 0$ comme le seul prédicat[3]*) appliquée à un anneau* $\mathbf{A}$ *(vu comme une présentation d'anneau intègre dynamique), nous l'appellerons le* treillis de Zariski *de la structure algébrique dynamique* $\mathbf{D}$ *et nous le noterons* $\mathrm{Zar}(\mathbf{D})$.

Si la théorie géométrique est une théorie avec égalité, des termes clos prouvablement égaux donnent lieu à des faits équivalents[4]. En conséquence on pourrait remplacer dans la définition du treillis $\mathrm{Zar}(\mathbf{D})$ l'ensemble des termes clos par l'ensemble quotient où on identifie deux termes prouvablement égaux.

En fait les méthodes de preuve à l'oeuvre dans les théories dynamiques ne sont rien d'autre que la traduction des propriétés des relations implicatives des treillis. En conséquence le treillis des faits de $\mathbf{D}$ n'est autre que le treillis des « valeurs de vérité des faits énoncés dans $\mathbf{D}$ ». Précisément on obtient :

Théorème 4.4 *Tout élément de* $\mathrm{Zar}(\mathbf{D})$ *est donné par une conjonction de disjonctions de faits. En outre, pour des faits $P_1(\underline{t_1}), \dots, P_n(\underline{t_n})$ et $Q_1(\underline{t'_1}), \dots, Q_m(\underline{t'_m})$ les propriétés suivantes sont équivalentes :*

- *On a dans* $\mathrm{Zar}(\mathbf{D})$

$$P_1(\underline{t_1}), \dots, P_n(\underline{t_n}) \vdash_{\mathrm{Zar}(\mathbf{D})} Q_1(\underline{t'_1}), \dots, Q_m(\underline{t'_m})\,.$$

---

[3] On pourrait s'étonner que l'égalité ne soit pas présente comme prédicat binaire, ni les axiomes usuels des anneaux commutatifs, qui font intervenir l'égalité. En fait ces axiomes peuvent être gérés sous forme du calcul algébrique dans $\mathbf{A}$ ou dans $\mathbf{A}[X_1, \dots, X_n]$ qui remplace un terme arbitraire par une forme réduite canonique « une fois le calcul effectué ». Pour plus de détails voir [15]. Par ailleurs, on peut également voir ces axiomes comme ceux des anneaux locaux, avec pour seul prédicat le prédicat d'inversibilité.

[4] Si le prédicat $=$ n'est pas présent (cela est parfois bien pratique de ne pas disposer de l'égalité !) on a quand même une relation d'équivalence qui « fait le même travail que l'égalité prouvable » sur l'ensemble des termes clos d'une structure algébrique dynamique.

– *On peut démontrer la règle dynamique*

$$P_1(\underline{t_1}), \ldots, P_n(\underline{t_n}) \vdash Q_1(\underline{t'_1}), \ldots, Q_m(\underline{t'_m})$$

dans la structure algébrique dynamique $\mathbf{D}$ *(ce qui équivaut à la démontrer dans la théorie géométrique correspondante en vertu du théorème fondamental 4.3).*

Dans le corps dynamique donné en exemple ci-dessus, $105 = 0$ est un fait absolument vrai, $11 = 0$ est un fait absolument faux, ou plus précisément un fait collapsant (il fait collapser la structure en un seul point), tandis que $3 = 0$, $5 = 0$ et $7 = 0$ sont des faits vrais « une fois sur trois », le sup de ces trois faits est $105 = 0$, c'est-à-dire le Vrai. Le fait $243 = 0$ représente le même élément du treillis que $3 = 0$ mais $243 = 3$ n'est vrai que si $15 = 0$.

La grande sensibilité au choix des prédicats donnés dans la structure

On peut toujours élargir le langage d'une théorie géométrique $\mathcal{T}$ en rajoutant des prédicats composés (par l'usage des connecteurs et des quantificateurs) soumis aux axiomes adéquats. Si cela ne change pas substantiellement les modèles de la structure algébrique dynamique ni les théorèmes qu'on peut y certifier (c'est justement ce que dit le théorème fondamental 4.3), cela peut changer les stratégies de preuves, et cela change de manière importante le treillis de Zariski des structures algébriques dynamiques de type $\mathcal{T}$.

Par exemple, il est légitime de penser que la dimension de Krull de $\mathrm{Zar}(\mathbf{D})$ est quelque chose d'important à comprendre pour comprendre $\mathbf{D}$ et l'utiliser au mieux.

Mais si on ajoute dans une théorie dynamique le prédicat opposé à tout prédicat de la théorie, les treillis de Zariski des structures algébriques dynamiques deviennent des algèbres de Boole : leur dimension, si pertinente pourtant, s'est évanouie dans les eaux glacées de la logique du tiers exclu.

La logique classique raccourcit les preuves, mais cela se paye. D'une part on mutile les modèles constructifs de structure algébrique dynamique en exigeant la décidabilité des prédicats, d'autre part, on est obligé pour récupérer la dimension de Krull d'introduire des objets idéaux fort justement appelés « spectres ».

Le spectre d'une structure algébrique dynamique

La définition suivante est surtout intéressante en mathématiques classiques.

Définition 4.11 *Le* spectre *de la structure algébrique dynamique* $\mathbf{D}$ *est le spectre de son treillis de Zariski. Nous le noterons* $\mathrm{Spec}(\mathbf{D})$ *ou* $\mathrm{Spec}_{\mathcal{T}}(\mathbf{D})$*. En tant qu'ensemble, il s'identifie aux (classes d'isomorphismes de) modèles minimaux de la théorie du premier ordre associée à* $\mathbf{D}$*.*

Dans le modèle correspondant à un filtre premier $\mathfrak{T} \in \mathrm{Spec}(\mathbf{D})$ tous les faits sont « vrais ou faux » : les faits vrais sont ceux de $\mathfrak{T}$ et les faits faux sont ceux de l'idéal premier $\mathfrak{p} = \mathrm{Zar}(\mathbf{D}) \setminus \mathfrak{T}$. Les éléments du modèle associé à $\mathfrak{T}$ sont définis à partir des termes clos de la structure algébrique dynamique : deux termes clos t et t' définissent le même élément dans le modèle si et seulement si ils sont indiscernables par des faits[5].

On retrouve ainsi le spectre réel, le spectre p-adique et des tas d'autres beaux espaces spectraux des mathématiques classiques.

Du point de vue constructif, les éléments de $\mathrm{Spec}(\mathbf{D})$ sont des objets purement idéaux que l'on ne connaît en général qu'à travers des spécifications incomplètes.

[5] Si la structure a un prédicat d'égalité, cela veut dire que $t = t'$ est dans $\mathfrak{T}$. Si la structure ne comporte que des prédicats unaires, cela veut dire que pour tout prédicat P de la structure, $P(t)$ et $P(t')$ sont ou bien tous deux dans $\mathfrak{T}$, ou bien tous deux dans $\mathfrak{p}$.

La seule réalité tangible et certaine est le treillis de Zariski (le coté « tangible » n'implique pas que l'égalité dans le treillis soit décidable).

Le spectre Spec($\mathbf{D}$) peut être muni de la topologie spectrale introduite par Stone. Une base d'ouverts est fournie par les intersections finies d'ouverts du type suivant :

$$U(P,\underline{a}) = \{\, \mathfrak{T} \in \mathrm{Spec}(\mathbf{D})\,;\, P(\underline{a}) \in \mathfrak{T}\,\},$$

où P est un prédicat de la théorie dynamique et $\underline{a}$ une liste de termes clos de la structure algébrique dynamique.

D'autres topologies sont possibles si on choisit d'autres prédicats qui permettent de définir la même structure (les deux théories dynamiques correspondantes diffèrent par leurs prédicats mais les théories formelles du premier ordre associées sont « les mêmes »).

En particulier si on remplace chaque prédicat par le prédicat opposé, le treillis de Zariski est remplacé par son dual et dans la nouvelle topologie spectrale, les anciens ouverts de base deviennent des complémentaires d'ouverts de base.

De même, si on rajoute pour chaque prédicat P du langage le prédicat « opposé » (avec les axiomes convenables), on obtient pour treillis de Zariski une algèbre de Boole (celle engendrée par le treillis distributif de la première structure algébrique dynamique) et pour topologie la *topologie constructible*.

Un exemple

Voici un exemple dans la lignée de [35].

On considère un corps réel $\mathbf{K}$ muni d'un cone T, c'est-à-dire une partie vérifiant $T+T \subseteq T$, $T \times T \subseteq T$, $\mathbf{K}^2 \subseteq T$ (ici $\mathbf{K}^2$ désigne l'ensemble des carrés de $\mathbf{K}$).

Rappelons qu'un ordre sur $\mathbf{K}$ est un cone $\mathfrak{c}$ qui vérifie $\mathfrak{c} \cap -\mathfrak{c} = \{0\}$ et $\mathfrak{c} \cup -\mathfrak{c} = \mathbf{K}$.

On pose $\dot{\mathbf{K}} = \mathbf{K} \setminus \{0\}$ et $\dot{T} = T \setminus \{0\}$.

L'espace de Harrison $X_{\mathbf{K}}/T$ est formé de tous les ordres de $\mathbf{K}$ qui prolongent le cone T. Il s'identifie donc au spectre de la structure algébrique dynamique de corps ordonné attachée à la présentation définie par $\mathbf{K}$ et T.

En apparence, la théorie classique passe son temps à parler des points $\mathfrak{c}$ de cet espace spectral. En fait elle s'intéresse surtout à ses ouverts de base $U_T(a_1,\ldots,a_k) = \{\, \mathfrak{c} \in X_{\mathbf{K}}/T \mid a_i \in \mathfrak{c}\,\}$ où les a_i sont des éléments de $\dot{\mathbf{K}}/\dot{T}$. Rien de plus concret qu'un tel ouvert, si on veut bien ne pas prêter une trop grande attention à ses points.

En tant qu'espace compact totalement discontinu, l'espace $X_{\mathbf{K}}/T$ est complètement déterminé par l'algèbre de Boole des fonctions continues à valeurs dans $\{0,1\}$: $Cont(X_{\mathbf{K}}/T,\{0,1\}) = B_T(\mathbf{K}) = B_T$. En effet les points de $X_{\mathbf{K}}/T$ s'identifient en mathématiques classiques aux idéaux premiers de cet anneau, qui sont tous maximaux. Et la topologie est la topologie de sous-espace de $\{0,1\}^{X_{\mathbf{K}}/T}$.

Un élément de l'algèbre de Boole B_T peut être vu comme la fonction caractéristique d'un ouvert compact de l'espace. Dans la suite nous notons $\mathring{a}$ la fonction caractéristique de l'ouvert $U_T(a)$. En tant qu'espace de fonctions, la structure de treillis distributif de B_T en mathématiques classiques provient de la structure d'ensemble totalement ordonné de $\{0,1\}$, sa structure d'anneau provient de l'identification de $\{0,1\}$ avec $\mathbb{Z}/2$.

D'un point de vue constructif il nous suffit que l'algèbre de Boole B_T soit un objet bien défini, avec lequel on sache calculer, pour être satisfaits, et pour qu'on puisse interpréter constructivement le discours de la théorie classique.

Dans les bons livres de mathématiques classiques (voir [26]) où l'on parle de l'espace $X_{\mathbf{K}}/T$, on s'intéresse surtout aux anneaux de fonctions continues B_T et $Cont(X_{\mathbf{K}}/T,\mathbb{Z}) = C_T(\mathbf{K}) =$

C_T. L'anneau C_T peut être construit de manière fonctorielle comme l'anneau engendré (en un sens convenable) par l'algèbre de Boole B_T.

On peut montrer que le système de relations suivant liant les $\overset{\circ}{a}$ (pour $a \in \dot{\mathbf{K}}/\dot{T}$), qui engendrent B_T, définit B_T comme treillis distributif : lisez les relations dans la colonne de droite, elles recopient sans rien y changer les axiomes des cones contenant T, écrits dans la colonne de gauche (autrement dit la valeur en $\mathfrak{c}$ de la fonction caractéristique de $a \in \bullet$, c'est $a \in \mathfrak{c}$).

$$\left\{\begin{array}{rclcrcll}
\dot{\mathfrak{c}} + \dot{\mathfrak{c}} & \subset & \dot{\mathfrak{c}} & \qquad & \overset{\circ}{a}\,,\,\overset{\circ}{b} & \vdash & \overset{\circ}{\overline{a+b}} & \\
\dot{\mathfrak{c}}\,\dot{\mathfrak{c}} & \subset & \dot{\mathfrak{c}} & & \overset{\circ}{a}\,,\,\overset{\circ}{b} & \vdash & \overset{\circ}{\overline{ab}} & \\
\dot{\mathfrak{c}} \cap -\dot{\mathfrak{c}} & = & \emptyset & & \overset{\circ}{a}\,,\,\overset{\circ}{\overline{-a}} & \vdash & & \\
\dot{\mathfrak{c}} \cup -\dot{\mathfrak{c}} & = & \dot{\mathbf{K}} & & & \vdash & \overset{\circ}{a}\,,\,\overset{\circ}{\overline{-a}} & \\
\dot{T} & \subset & \dot{\mathfrak{c}} & & & \vdash & \overset{\circ}{t} & \qquad (t \in \dot{T})
\end{array}\right. \tag{11}$$

En fait, considérons la théorie dynamique des corps ordonnés $\mathcal{CO}$ basée sur les prédicats $x = y$ et $x > 0$, et la structure algébrique dynamique de type $\mathcal{CO}$ définie par $(\mathbf{K}, T)$ en un sens évident. Alors le treillis de Zariski de cette structure algébrique dynamique est l'algèbre de Boole B_T et son spectre est l'espace de Harrison $X_{\mathbf{K}}/T$.

Qui marche sur ses pieds, qui marche sur sa tête ? Celui qui définit le treillis de Zariski avant son spectre, ou l'autre ? Celui qui définit l'objet idéal à partir de l'objet concret, ou celui qui définit l'objet concret à partir de son idéalisation ? Question de goût et d'habitude sans doute, mais pas seulement.

Spectre et topologie formelle

En mathématiques classiques une *locale* ou *espace topologique formel* (voir [22, 23], et pour une approche constructive [14]) est un treillis distributif sup-complet (avec la distributivité adéquate pour $\bigvee$ et $\wedge$). En particulier c'est une algèbre de Heyting puisque la flèche $\rightarrow$ peut être définie comme un sup infini. Un morphisme d'une locale L_1 vers une locale L_2 est une application de L_2 dans L_1 qui se comporte convenablement avec les inf finis et les sup arbitraires.

Tout espace topologique usuel définit un espace topologique formel : l'ensemble de ses ouverts. Ceci définit un foncteur de la catégorie des espaces topologiques vers celle des locales[6]. Mais il y a des locales qui ne proviennent pas d'espaces topologiques usuels.

En mathématiques classiques, la locale *engendrée par* le treillis distributif $\mathrm{Zar}(\mathbf{D})$ possède « assez de points » : elle n'est autre que la locale *associée à* l'espace topologique $\mathrm{Spec}(\mathbf{D})$.

La formulation « espace topologique formel » des locales est mieux adaptée à un traitement contructif. Et une version constructive de $\mathrm{Spec}(\mathbf{D})$ n'est en fait rien d'autre que « l'espace topologique formel engendré par $\mathrm{Zar}(\mathbf{D})$ ». Ainsi du point de vue constructif on peut voir $\mathrm{Spec}(\mathbf{D})$ comme un espace topologique formel « qui manque parfois de points » : il ne peut pas toujours être défini à partir de ses points.

Finalement le plus simple est de dire que toute la structure de $\mathrm{Spec}(\mathbf{D})$ se résume à celle de $\mathrm{Zar}(\mathbf{D})$: un bel et bon objet concret parfaitement défini sans recours à Zorn ni au tiers exclu, et qui contient toute l'information nécessaire pour décrypter les discours classiques concernant $\mathrm{Spec}(\mathbf{D})$.

[6] La sous catégorie des espaces topologiques « sobres », qui contient en particulier les espaces spectraux et les espaces séparés, est équivalente par ce foncteur à la catégorie des locales qui possèdent « suffisamment de points » : pour plus de détails voir [23].

Conclusion : les mathématiques constructives et le programme de Hilbert

Voici une tentative pour énoncer le programme de Hilbert de la manière la plus générale et la plus informelle possible.

Programme de travail

(1) *Lorsqu'un résultat concret est démontré en mathématiques par des méthodes douteuses, certifier ce résultat par des méthodes sûres.*

(2) *Réaliser ce travail de manière aussi systématique (voire automatique) que possible.*

Si on entend par « méthodes sûres » les méthodes « finitistes » qui se formalisent dans l'artithmétique primitive récursive **PRA** le programme de Hilbert a été invalidé par le théorème d'incomplétude de Gödel, qui montre (entre autres) que **PRA** ne peut pas prouver la consistance de **PRA**, ni a fortiori celle de **PA**, l'arithmétique de Peano, et encore moins celle de théories comme **ZF**.

Si on entend par « méthodes sûres » les méthodes constructives, alors le programme de Hilbert a déjà été réalisé pour de larges pans des mathématiques.

D'une part il a été prouvé constructivement (voir [21]) que **PA** et **HA** (la version constructive, sans tiers exclu, de **PA**) prouvent les mêmes fonctions récursives : l'usage de la logique classique facilite les preuves, mais les résultats sont les mêmes (donc sûrs) tant que les énoncés ont essentiellement la même signification du point de vue classique et du point de vu constructif. En particulier, la consistance de **HA** entraîne celle de **PA**.

D'autre part les fondements de l'analyse et de l'algèbre ont été réécrits de manière constructive par Bishop, Bridges, Richman, Seidenberg, et bien d'autres qui ont repris le flambeau de Gauss et Kronecker (voir en particulier [3, 4, 5, 7, 39, 43]).

Nous pensons apporter notre contribution à cette tâche en proposant une approche systématique (sinon automatique) de l'algèbre abstraite par la méthode dynamique, dans laquelle les objets abstraits ne sont plus « évités » mais seulement réinterprétés à travers la sémantique constructive des spécifications incomplètes.

Nous pensons en cela être fidèle à l'espoir formulé par Poincaré lors de sa critique contre l'usage abusif de l'infini (notamment lorsqu'il s'en prend au système formel **Z** de Zermelo) : *ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini.*

« M. Zermelo a voulu construire un système impeccable d'axiomes ; mais ces axiomes ne peuvent être regardés comme des décrets arbitraires, puisqu'il faudrait montrer que ces décrets ne sont pas contradictoires, et qu'ayant fait entièrement table rase on n'a plus rien sur quoi l'on puisse appuyer une semblable démonstration. Il faut donc que ces axiomes soient évidents par eux-mêmes. Or quel est le mécanisme par lequel on les a construits ? on a pris des axiomes qui sont vrais des collections finies ; on ne pouvait les étendre tous aux collections infinies, on n'a fait cette extension que pour un certain nombre d'entre eux, choisis plus ou moins arbitrairement. A mon sens d'ailleurs [...] aucune proposition concernant les collections infinies ne peut être évidente par définition. [...]

Quant à moi je proposerais de s'en tenir aux règles suivantes :

1. Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots ;

2. Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini ;

3. Éviter les classifications et les définitions non prédicatives. »

Poincaré, La logique de l'infini [40].

Remerciements Je remercie le referee pour ses remarques détaillées et pertinentes. Je remercie aussi les organisateurs du colloque 2WFTOP pour leur invitation et de leur insistance pour que je rédige ma conférence.

Références

[1] Artin E. *Uber die Zerlegung definiter Funktionen in Quadrate.* Abh. Math. Sem. Hamburg, **5** (1927), 100–115. 4

[2] Bochnak J., Coste M., Roy M.-F. *Géometrie Algébrique réelle.* Springer-Verlag. Ergeb. M. n°11. 1987. 22

[3] Beeson M. *Foundations of Constructive Mathematics.* Springer-Verlag (1985). 29

[4] Bishop E. *Foundations of Constructive Analysis.* McGraw Hill (1967). 29

[5] Bishop E., Bridges D. *Constructive Analysis.* Springer-Verlag (1985). 29

[6] Buchmann J., Lenstra H. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux **6** (2) (1994), 221–260. 6

[7] Bridges D., Richman F. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987). 29

[8] Cederquist J., Coquand T. *Entailment relations and Distributive Lattices.* Logic Colloquium '98 (Prague), 127–139, Lect. Notes Log., 13. Assoc. Symbol. Logic, Urbana, (2000). 16, 18

[9] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 477–499. 5, 16, 20, 21

[10] Coquand T., Lombardi H. *A short proof for the Krull dimension of a polynomial ring.* To appear in American Math. Monthly. 7, 12

[11] Coquand T., Lombardi H. *Going up, Going down, une approche constructive.* En préparation. 6, 12

[12] Coquand T., Lombardi H. *Le théorème de l'idéal principal de Krull et la dimension des anneaux noethériens, une approche constructive.* En préparation. 6

[13] Coquand T., Persson H. *Valuations and Dedekind's Prague Theorem.* Journal of Pure and Applied Algebra **155** (2001) 121–129. 5

[14] Coquand T., Sambin G., Smith J., Valentini S. *Inductively generated formal topologies.* Preprint. 28

[15] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256. 5, 6, 7, 15, 22, 24, 25

[16] Curry, H. B. *Foundations of mathematical logic* McGraw-Hill Book Co., Inc., New York-San Francisco, Calif.-Toronto-London 1963 20

[17] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* EUROCAL '85. Lecture Notes in Computer Science n°204, (Ed. Caviness B.F.) 289–290. Springer 1985. 4, 12

[18] Delzell C., González-Vega L., Lombardi H. *A continuous and rational solution to Hilbert's 17th problem and several Positivstellensatz cases*, in : Computational Algebraic Geometry. Eds. Eyssette F., Galligo A.. Birkhäuser (1993) Progress in Math. n°109. (colloque MEGA 92) (1993), 61–76. 7

[19] Ducos L., Lombardi H., Quitté C., Salou M. *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Journal of Algebra. **281**, (2004), 604–650. 6, 7

[20] Español L. *Constructive Krull dimension of lattices.* Rev. Acad. Cienc. Zaragoza (2) **37** (1982), 5–9. 5, 20, 21

[21] Friedman H. *Classically and intuitionistically provably recursive functions in Peano*, dans : Higher Set Theory. Lecture Notes in Mathematics n°669, 21–27, Springer (1978). 4, 29

[22] Johnstone, P. *The point of pointless topology.* Bull. Amer. Math. Soc. (N.S.) **8** n°1 (1983), 41–53. 28

[23] Johnstone P. *Stone Spaces.* Cambridge Studies in Advanced Mathematics, 3. Cambridge University Press, Cambridge, 1986. 20, 28

[24] Joyal A. *Le théorème de Chevalley-Tarski.* Cahiers de Topologie et Géometrie Differentielle, 1975. 5, 20, 21

[25] Kuhlmann F.-V., Lombardi H., Perdry H. *Dynamic computations inside the algebraic closure of a valued field.*. Valuation Theory and its Applications. Vol 2. Eds. F.-V. Kuhlmann, S. Kuhlmann and M. Marshall. Fields Institute Communications n°33 (2003) 6

[26] Lam T. *Orderings, Valuations, and Quadratic Forms.* CBMS Regional Conference Series in Mathematics, Vol. 52, American Mathematical Society, Providence, R.I., 1983. (Second Printing : 1996.) 27

[27] Lombardi H. *Effective real nullstellensatz and variants*, in : Effective Methods in Algebraic Geometry. Eds. Mora T., Traverso C.. Birkhaüser (1991). Progress in Math. n°94 (MEGA 90), 263–288. 5, 6, 7

[28] Lombardi H. *Une borne sur les degrés pour le Théorème des zéros réel effectif*, in : Real Algebraic Geometry. Proccedings, Rennes 1991, Lecture Notes in Mathematics n°1524. Eds. : Coste M., Mahé L., Roy M.-F.. Springer-Verlag, (1992), 323–345. 7

[29] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier.* Annals of Pure and Applied Logic **91**, (1998), 59–92. 5, 6

[30] 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. Fascicule 94–95 & 95–96, (1997). 6

[31] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242**, (2002), 23–46. 6, 7

[32] Lombardi H. *Hidden constructions in abstract algebra (1) Integral dependance.* Journal of Pure and Applied Algebra **167**, (2002) 259–267. 5, 10, 11

[33] Lombardi H. *Constructions cachées en algèbre abstraite (4) La solution du 17ème problème de Hilbert par la théorie d'Artin-Schreier.* Publications Mathématiques de Besançon. Théorie des nombres. Années 1998-2001. 5, 22

[34] Lombardi H. *Platitude, localisation et anneaux de Prüfer, une approche constructive.* Publications Mathématiques de Besançon. Théorie des nombres. Années 1998-2001. 6

[35] Lombardi H. *Constructions cachées en algèbre abstraite (5) Principe local-global de Pfister et variantes.* International Journal of Commutative Rings **2** (4), (2003), 157–176. 5, 27

[36] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 461–476. 5, 7, 10

[37] Lombardi H., Quitté C., Yengui I. *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa.* Preprint 2005. 5, 7, 10

[38] Makkai M., Reyes G.E. *First Order Categorical Logic.* Springer-Verlag, LNM 611, (1988). 5

[39] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988). 29

[40] Poincaré H. *La logique de l'infini*, Revue de Métaphysique et de Morale **17**, 461–482, (1909) réédité dans « Dernières pensées » Flammarion (1913). 29

[41] Prawitz D. *Ideas and results of proof theory.* Proceedings of the second scandinavian logic symposium (juin 70). Studies in Logic and Foundations of Mathmatics n°63, 235–307. North Holland. 24

[42] Salou Maimouna *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Thèse, avril 2002, Besançon, Université de Franche-Comté. 6

[43] Seidenberg A. *Constructions in Algebra.* Trans. Amer. Math Soc. **197** (1974), 273–313. 29

[44] Stone M.H. *Topological representations of distributive lattices and Brouwerian logics.* Cas. Mat. Fys. **67**, (1937), 1-25. 22

Table des matières