Constructions cachées en algèbre abstraite (4)
La solution du 17ème problème de Hilbert par la théorie d'Artin-Schreier

H. Lombardi
Équipe de Mathématiques, (UMR CNRS 6623)
Université de Franche-Comté, 25030 BESANÇON cedex, France.
email lombardi@math.univ-fcomte.fr

juin 2001

Résumé

Nous expliquons comment la théorie abstraite d'Artin-Schreier qui résoud le 17ème problème de Hilbert peut être interprétée comme une invitation à vraiment construire des sommes de carrés. Pour cela nous remplaçons les objets "trop abstraits" dont parle la preuve classique par des spécifications incomplètes de ces mêmes objets.

Mots-clés 17ème problème de Hilbert. Théorie d'Artin-Schreier. Mathématiques constructives. Programme de Hilbert.

Abstract

We explain how it is possible to construct explicit sums of squares by deciphering an abstract proof giving a positive answer to the 17th Hilbert's Problem. When doing this job we replace abstract objects in the classical proof by incomplete specifications of these objects.

Key-words : 17–th Hilbert problem. Artin-Schreier Theory. Constructive mathematics . Hilbert Program.

MSC 2000 : 03F65, 03B35, 12D15, 12J15, 14Q20

Introduction

Soit $\mathbf{K}$ un corps ordonné où les positifs sont des sommes de carrés, $\mathbf{R}$ sa cloture réelle, $P(x_1, \ldots, x_n)$ un polynome de $\mathbf{K}[x_1, \ldots, x_n]$ partout ≥ 0 sur $\mathbf{R}^n$. Le 17ème problème de Hilbert demande d'écrire P comme une somme de carrés dans $\mathbf{K}(x_1, \ldots, x_n)$.

En deux mots voici comment fonctionne la preuve d'Artin-Schreier.

Dans une première étape on démontre concernant un corps arbitraire $\mathbf{K}$ avec un élément spécifié a que les propriétés suivantes sont équivalentes :

– $\mathbf{K}$ est réel, c.-à-d. -1 n'est pas une somme de carrés dans $\mathbf{K}$
– $\mathbf{K}$ peut être ordonné
– $\mathbf{K}$ peut être plongé dans un corps réel clos

de même les propriétés suivantes sont équivalentes :

– $-a$ n'est pas une somme de carrés dans $\mathbf{K}$
– $\mathbf{K}$ peut être ordonné avec $a > 0$
– $\mathbf{K}$ peut être plongé dans un corps réel clos avec $a > 0$

En théorie des modèles, les équivalences ci-dessus se relisent en disant que les propriétés suivantes sont équivalentes :

– -1 est une somme de carrés dans $\mathbf{K}$
– La théorie formelle des corps réels extensions du corps $\mathbf{K}$ prouve prouve $-1 \geq 0$
– La théorie formelle des corps ordonnés extensions du corps $\mathbf{K}$ prouve $-1 \geq 0$

de même les propriétés suivantes sont équivalentes :

– $-a$ est une somme de carrés dans $\mathbf{K}$
– La théorie formelle des corps ordonnés extensions du corps $\mathbf{K}$, avec $a > 0$, prouve $-1 \geq 0$
– La théorie formelle des corps réels clos extensions du corps $\mathbf{K}$, avec $a > 0$, prouve $-1 \geq 0$

Nous donnons des versions constructives simples "purement algébriques" (sans logique ni théorie des modèles) de ces équivalences. Nous appelons *corps ordonné idéel* (en anglais : an *idealistic ordered field*) une spécification incomplète pour un corps ordonné (voir section 1.1). Un tel corps ordonné idéel *collapse* lorsqu'une condition algébrique simple est vérifiée. Le collapsus est prouvé être équivalent, en maths classiques, à l'impossibilité de réaliser la spécification incomplète sous forme d'un vrai corps ordonné.

Nous remplaçons systématiquement les théorèmes classiques d'existence abstraite par des théorèmes constructifs de collapus simultanés, qui leur sont équivalents en maths classiques.

Ensuite nous interprétons les preuves de la théorie classique qui parlent de corps ordonnés hypothétiques construits en utilisant le tiers exclu et l'axiome du choix comme des preuves constructives de faits classiques) concernant des corps ordonnés idéels bien concrets. Autrement dit les preuves constructives sont simplement cachées à l'intérieur des preuves classiques.

Ici nous obtenons, concernant un corps ordonné idéel $\mathbf{L}$, que les propriétés suivantes sont équivalentes :

– -1 est ≥ 0 dans $\mathbf{L}$ (si $\mathbf{L}$ est un corps ordinaire, cela signifie que -1 est une somme de carrés dans $\mathbf{L}$)
– le corps ordonné idéel $\mathbf{L}$ prouve $-1 \geq 0$
– le corps réel clos idéel $\mathbf{L}$ prouve $-1 \geq 0$

de même, si a est inversible et si $\mathbf{L}$ est basé sur un corps, les propriétés suivantes sont équivalentes :

– $-a$ est une somme de carrés dans $\mathbf{L}$
– le corps ordonné idéel $\mathbf{L}$ avec $a \geq 0$ prouve $-1 \geq 0$
– le corps réel clos idéel $\mathbf{L}$ avec $a \geq 0$ prouve $-1 \geq 0$

La deuxième étape de la preuve d'Artin-Schreier est de nature différente. Si $\mathbf{K}$ est un corps ordonné où les positifs sont des sommes de carrés, $\mathbf{R}$ sa cloture réelle, et $P(x_1, \ldots, x_n)$ un polynome partout ≥ 0 sur $\mathbf{R}^n$, il faut en déduire qu'il n'existe pas d'ordre rendant P négatif sur le corps de fractions rationnelles $\mathbf{K}(x_1, \ldots, x_n)$. Pour ceci nous suivons une méthode inspirée de celle exposée dans [1]. Nous considérons une preuve élémentaire (par l'algorithme de Cohen-Hörmander) du fait que $P(x_1, \ldots, x_n)$ est un polynome partout ≥ 0 dans $\mathbf{R}$ et nous regardons ce que dit cette preuve dans une hypothétique cloture réelle de $\mathbf{K}(x_1, \ldots, x_n)$: elle nous dit que le corps réel clos idéel $\mathbf{K}(x_1, \ldots, x_n)$ avec $-P(x_1, \ldots, x_n) \geq 0$ prouve $-1 \geq 0$.

En résumé, c'est la version "théorie des modèles" de la preuve d'Artin-Schreier, avec utilisation du principe de transfert de Tarski-Seidenberg (ce qui est vrai dans un corps réel clos est vrai dans toutes ses extensions réelles closes), que nous interprétons comme une preuve constructive cachée.

Pour d'autres exemples de la méthode présente, qui met à jour des preuves constructives cachées dans les preuves classiques, voir [2, 3, 7, 8, 9]. Enfin remarquons que l'article présent peut aussi être considéré comme une version plus simple et plus algébrique de l'article [6].

1 Corps ordonnés idéels

Dans l'article tous les anneaux considérés sont commutatifs unitaires, et 2 est inversible.

Si $\mathbf{A}$ est un anneau on note $\mathbf{A}^{(2)}$ l'ensemble des carrés de $\mathbf{A}$ et $\sum \mathbf{A}^{(2)}$ l'ensemble des sommes de carrés de $\mathbf{A}$.

Un *corps discret* est un anneau commutatif $\mathbf{A}$ qui vérifie l'axiome

$$\forall x \quad x = 0 \ \vee \ x \text{ inversible}$$

Dans tout l'article nous disons corps au lieu de corps discret.

Un corps *collapse* si $1 = 0$.

Nous évitons systématiquement le recours à la négation (sauf en quelques endroits où nous raisonnons en maths classiques) que nous remplaçons par sa version très légèrement affaiblie, le collapsus.

1.1 Rappels et définitions

Un *corps ordonné discret* est un couple $(\mathbf{K}, \mathbf{P})$ où $\mathbf{K}$ est un corps discret et où

$$\mathbf{P} \times \mathbf{P} \subseteq \mathbf{P}, \quad \mathbf{P} + \mathbf{P} \subseteq \mathbf{P}, \quad \mathbf{K}^{(2)} \subseteq \mathbf{P}, \quad \mathbf{P} \cup -\mathbf{P} = \mathbf{K}.$$

Dans tout l'article nous disons corps ordonné au lieu de corps ordonné discret. Si $(\mathbf{K}, \mathbf{P})$ est un corps ordonné, $\mathbf{P}$ est appelé un *ordre sur* $\mathbf{K}$. Si $\mathbf{P} \cap -\mathbf{P}$ contient un inversible de $\mathbf{K}$, on a $\mathbf{P} = \mathbf{K}$ et on dit que *le corps ordonné* $(\mathbf{K}, \mathbf{P})$ *collapse.*

Dans un anneau $\mathbf{A}$ un *cone* est une partie $\mathbf{C}$ telle que

$$\mathbf{C} \times \mathbf{C} \subseteq \mathbf{C}, \quad \mathbf{C} + \mathbf{C} \subseteq \mathbf{C}, \quad \mathbf{A}^{(2)} \subseteq \mathbf{C}$$

Puisque 2 est inversible on a

$$-1 \in \mathbf{C} \ \Leftrightarrow \ \mathbf{C} = \mathbf{A}$$

(car $x = 1/4((1+x)^2 + (-1)(1-x)^2)$).

Si C est une partie arbitraire de $\mathbf{A}$, on note $\mathcal{M}(C)$ le monoïde multiplicatif engendré par C et le cone engendré par C est alors

$$\mathbf{C} = \left\{ x \in \mathbf{A} \quad | \quad x = \sum c_i x_i^2, \ c_i \in \mathcal{M}(C), \ x_i \in \mathbf{A} \right\}$$

L'ensemble vide engendre le cone $\sum \mathbf{A}^{(2)}$.

Définition 1 *Un* corps ordonné idéel *est un couple* $\mathbf{L} = (\mathbf{A}, \mathbf{C})$ *où* $\mathbf{A}$ *est un anneau et* $\mathbf{C}$ *un cone. Le corps ordonné idéel* collapse *si* $-1 \in \mathbf{C}$ *(c'est par exemple le cas si* $1 =_{\mathbf{A}} 0$*). Un* homomorphisme *du corps ordonné idéel* $\mathbf{L} = (\mathbf{A}, \mathbf{C})$ *vers le corps ordonné idéel* $\mathbf{L}' = (\mathbf{A}', \mathbf{C}')$ *est un homomorphisme de* $\mathbf{A}$ *vers* $\mathbf{A}'$ *qui envoie* $\mathbf{C}$ *dans* $\mathbf{C}'$*.*

Notation 2 On pratiquera quelques abus de notations : si C est une partie arbitraire de $\mathbf{A}$ qui engendre un cone $\mathbf{C}$, on notera $(\mathbf{A}, C)$ au lieu de $(\mathbf{A}, \mathbf{C})$; si $x \in \mathbf{A}$ et si $C \cup \{x\}$ engendre le cone $\mathbf{C}'$, on notera $(\mathbf{A}; C, x)$ au lieu de $(\mathbf{A}, \mathbf{C}')$. Dans la suite, nous écrivons $(\mathbf{A}, \mathbf{C})$ avec un $\mathbf{C}$ gras pour indiquer qu'il s'agit bien d'un cone.

Si φ est un homomorphisme de $\mathbf{L} = (\mathbf{A}, \emptyset)$ vers un corps ordonné $(\mathbf{K}, \mathbf{P})$ l'image réciproque de $\mathbf{P}$ est un *cone premier*, c'est-à-dire un cone $\mathbf{C}$ de $\mathbf{A}$ qui vérifie

$$\forall x, y \in \mathbf{A} \quad (-xy \in \mathbf{C} \ \Rightarrow \ (x \in \mathbf{C} \vee y \in \mathbf{C}))$$

Le noyau de φ est alors $\mathbf{C} \cap -\mathbf{C}$. Réciproquement, si $\mathbf{C}$ est un cone premier de $\mathbf{A}$ et $J = \mathbf{C} \cap -\mathbf{C}$, J est un idéal premier, et le corps des fractions de $\mathbf{A}/J$ est ordonné par le cone engendré par $\mathbf{C}/J$ (petits calculs immédiats, voir par exemple [1]).

1.2 Tout corps réel peut être ordonné

Un corps ordonné idéel qui ne collapse pas représente une *spécification incomplète pour un corps ordonné qui ne collapse pas* en vertu du théorème de maths classiques suivant :

Théorème* 3 *Le corps ordonné idéel* $\mathbf{L} = (\mathbf{A}, C)$ *collapse si et seulement si pour tout homomorphisme de* $\mathbf{L}$ *vers un corps ordonné* $(\mathbf{K}, \mathbf{P})$, $(\mathbf{K}, \mathbf{P})$ *collapse.*
De manière équivalente : dans un anneau un cone strict est contenu dans un cone premier strict.
En particulier,

- *un corps où* -1 *n'est pas une somme de carrés peut être ordonné sans collapser,*
- *tout cone strict dans un corps* $\mathbf{K}$ *peut être étendu en un ordre sur* $\mathbf{K}$*,*
- *si* $\mathbf{C}$ *est un cone strict d'un corps* $\mathbf{K}$ *et* $-a \notin \mathbf{C}$*, il existe un ordre strict de* $\mathbf{K}$ *qui contient* a *et* $\mathbf{C}$*.*

L'étoile * de théorème* est mise pour signifier que le théorème n'est valable qu'en maths classiques.

Un équivalent constructif de ce théorème de maths classiques est donné par un théorème de collapsus simultané.

Théorème 4 *Soit un corps ordonné idéel* $\mathbf{L} = (\mathbf{A}, C)$ *et* $a \in \mathbf{A}$*.*

- *Si* $(\mathbf{A}; C, a)$ *et* $(\mathbf{A}; C, -a)$ *collapsent, alors* $\mathbf{L}$ *collapse.*
- *Si* $(\mathbf{A}/\langle a\rangle\,; C)$ *et* $(\mathbf{A}[1/a]; C)$ *collapsent, alors* $\mathbf{L}$ *collapse.*

Preuve Facile. □

Le théorème précédent a la signification pratique que tant qu'il s'agit de démontrer un collapsus d'un corps ordonné idéel $\mathbf{L}$, on peut toujours faire comme si $\mathbf{L}$ était un vrai corps ordonné (pour plus de détails voir section 1.3).

La proposition qui suit a la même signification intuitive (voir le commentaire après).

Proposition 5 *Soit un corps ordonné idéel* $\mathbf{L} = (\mathbf{A}, C)$ *et* $x, y \in \mathbf{A}$*. Si* $(\mathbf{A}; C, x)$ *et* $(\mathbf{A}; C, y)$ *collapsent, alors* $(\mathbf{A}; C, -xy)$ *collapse.*

Preuve Immédiate. □

En maths classiques un corollaire de la proposition 5 est le théorème 3. On considère un $\mathbf{L} = (\mathbf{A}, C)$ qui ne collapse pas. Soit alors par Zorn un cone maximal C' parmi ceux qui contiennent C mais ne contiennent pas -1. Alors ce cone est premier en vertu de la proposition 5.

On peut aussi déduire le théorème 3 du théorème 4, mais la zornification est à peine plus délicate.

Enfin, le théorème 3 implique sans difficulté la proposition 5 et le théorème 4. Cette implication est même constructive, mais le théorème 3 n'est pas prouvable constructivement.

1.3 Preuves arborescentes de collapsus

Si nous sommes en face d'une preuve classique du style : tel corps ne peut pas être ordonné en respectant telles contraintes de signes, d'où on déduit, par application du théorème 3 que quelque chose est une somme de carrés, nous avons maintenant une recette pour transformer de manière à peu près automatique la preuve abstraite en une preuve constructive du résultat final.

Nous supposons que la preuve abstraite est de nature élémentaire et fonctionne cas par cas, pour aboutir à une contradiction, avec le corps ordonné hypothétique de départ, en utilisant systématiquement les deux axiomes disjonctifs des corps ordonnés

$$\forall x \quad x = 0 \ \vee \ x \text{ inversible}$$

et

$$\forall x \quad x \geq 0 \ \vee \ x \leq 0$$

La relecture consiste à partir du corps ordonné idéel correspondant aux contraintes initiales et à le faire évoluer au fur et à mesure que se déroule la preuve classique. On crée ainsi un grand arbre binaire. Si à un moment donné de la preuve on se trouve à une feuille provisoire (qui deviendra un noeud) de notre arbre avec un corps ordonné idéel $(\mathbf{A}_i, C_i)$ et si la preuve classique fait intervenir le premier axiome avec un élément a, nous créons un embranchement avec les deux fils $(\mathbf{A}_i/\langle a\rangle, C_i)$ et $(\mathbf{A}_i[1/a], C_i)$ de $(\mathbf{A}_i, C_i)$. De même, si la preuve classique fait intervenir le deuxième axiome avec un élément a, nous créons un embranchement avec les deux fils $(\mathbf{A}_i; C_i, a)$ et $(\mathbf{A}_i; C_i, -a)$ de $(\mathbf{A}_i, C_i)$. Quand la relecture est terminée, toutes les feuilles de l'arbre collapsent, donc la racine également, par applications répétées du théorème 4.

Définition 6 *Lorsque nous avons ce type de construction arborescente ayant à sa racine un corps ordonné idéel* $\mathbf{L}$*, dont les embranchements correspondent aux deux axiomes disjonctifs des corps ordonnés, et dont toutes les feuilles collapsent, nous disons que* le corps ordonné idéel $\mathbf{L}$ prouve $-1 \geq 0$.

Naturellement, d'après le théorème 4, "$\mathbf{L}$ prouve $-1 \geq 0$" est équivalent au collapsus de $\mathbf{L}$, mais subjectivement c'est très différent. Au départ, on ne dispose que de générateurs du cone. On mime un raisonnement classique qui n'avait pas l'air constructif du tout. À l'arrivée on a une preuve explicite que -1 est dans le cone.

Le théorème 4 se relit donc, concernant un corps ordonné idéel $\mathbf{L}$, en disant que les propriétés suivantes sont équivalentes :

- -1 est ≥ 0 dans $\mathbf{L}$ (autrement dit $\mathbf{L}$ collapse : si $\mathbf{L} = (\mathbf{A}, \emptyset)$, cela signifie que -1 est une somme de carrés dans $\mathbf{A}$)
- le corps ordonné idéel $\mathbf{L}$ prouve $-1 \geq 0$

de même, si a est inversible et si $\mathbf{L} = (\mathbf{K}, C)$ où $\mathbf{K}$ est un corps ordinaire, nous avons que les propriétés suivantes sont équivalentes :

- $-a$ est dans le cone engendré par C (dans $\mathbf{K}$)
- le corps ordonné idéel $\mathbf{L}$ avec $a \geq 0$ (c'est-à-dire le corps ordonné idéel $(\mathbf{K}; C, a)$) prouve $-1 \geq 0$.

Un exemple.
Supposons qu'une preuve classique fasse usage du prédicat $x > 0$ dans un corps ordonné hypothétique[1], par exemple en utilisant la règle

$$(x > 0, \ y \geq 0) \Rightarrow x + y > 0$$

Comment nous débrouillons-nous dans ce cas de figure ? Nous considérons $x > 0$ comme une abréviation de : $x \geq 0$ et x est inversible. On ouvre deux branches. La première avec $x + y = 0$, la seconde avec $x + y$ inversible (c'est-à-dire une branche où on rajoute formellement un inverse de $x + y$). Dans la première branche, on a $ux = 1$ (par hypothèse) pour un certain u donc $-1 = -u^2x^2 = u^2xy \geq 0$: cela collapse. Dans la deuxième branche on a $x + y > 0$. Tout est donc OK.

On justifierait de manière analogue la possibilité d'utiliser les règles usuelles suivantes

$$\begin{array}{rcl} x > 0, \ xy \geq 0 & \Rightarrow & y \geq 0 \\ x \geq 0, \ xy > 0 & \Rightarrow & y > 0 \\ -x^2 \geq 0 & \Rightarrow & x = 0 \\ & & x \geq 0 \ \vee \ x < 0 \\ xy = 0 & \Rightarrow & x = 0 \ \vee \ y = 0 \end{array}$$

(les deux dernières sont exprimées sous forme de collapsus simultanés).

[1] La preuve classique a pour but de montrer qu'un tel corps ordonné ne peut exister.

1.4 Corps réels clos

Rappelons qu'un *corps réel clos* est un corps ordonné où tout polynome qui change de signe possède un zéro. Dans un corps réel clos, les positifs sont des carrés.

Théorème 7 *Soit un corps ordonné idéel* $\mathbf{L} = (\mathbf{A}, C)$, $a, b \in \mathbf{A}$ *et* $P(X) \in \mathbf{A}[X]$. *Soit* $\mathbf{A}[x] = \mathbf{A}[X]/\langle P\rangle$. *Si* $(\mathbf{A}[x]; C, -P(a)P(b))$ *collapse, alors* $(\mathbf{A}; C, -P(a)P(b))$ *collapse.*

Preuve Les manipulations d'identités algébriques que nous allons faire sont présentes dans la preuve classique que tout corps ordonné peut être plongé dans un corps réel clos.
On fait une preuve par récurrence sur le degré de P. Comme la récurrence risque de faire descendre le degré de 2 il nous faut deux initialisations.
Initialisation avec $\deg(P) = 0$. Si $P = e \in \mathbf{A}$, on ouvre deux branches en dessous de $(\mathbf{A}; C, -e^2)$: $(\mathbf{A}[1/e]; C, -e^2)$ et $(\mathbf{A}/\langle e\rangle; C, -e^2)$. Dans le première e est inversible, donc -1 est dans le cone engendré par $-e^2$, la branche collapse. Dans la seconde $\mathbf{A}[x] = (\mathbf{A}/\langle e\rangle)[X]$, le collapsus de $(\mathbf{A}[x]; C, -e^2)$ se spécialise en faisant $X = 0$ en un collapsus de $(\mathbf{A}/\langle e\rangle; C, -e^2)$.
Initialisation avec $\deg(P) = 1$. Si $P = cX + e \in \mathbf{A}$, on ouvre deux branches en dessous de $(\mathbf{A}; C, -P(a)P(b))$. Dans la première $c = 0$ et on est ramené au cas précédent. Dans la deuxième c possède un inverse u et $P(-eu) = 0$, le collapsus de $(\mathbf{A}[x]; C, -P(a)P(b))$ se spécialise en faisant $x = -eu$ en un collapsus de $(\mathbf{A}[u]; C, -P(a)P(b))$.
Nous passons à la récurrence proprement dite. Soit P de degré $d+2$. Soit C' le cone de $\mathbf{A}$ engendré par C et $-P(a)P(b)$. Nous supposons que $(\mathbf{A}[x]; C')$ collapse et nous voulons montrer que $(\mathbf{A}; C')$ collapse.
Cas particulier. Supposons tout d'abord P unitaire. Le collapsus de $(\mathbf{A}[x]; C')$ s'écrit

$$-1 = \sum_i c_i Q_i(X)^2 + P(X)S(X)$$

avec $c_i \in C'$ et $Q_i, P, S \in \mathbf{A}[X]$. On peut diviser les Q_i par P et on obtient une autre égalité

$$-1 = \sum_i c_i R_i(X)^2 + P(X)T(X) \quad (*)$$

avec $\deg(R_i) \leq d+1$ et donc $\deg(T) \leq d$. En outre

$$P(a)P(b)T(a)T(b) = (1 + \sum_i c_i R_i(a)^2)(1 + \sum_i c_i R_i(b)^2) \quad (**)$$

On ouvre deux branches en dessous de $(\mathbf{A}; C')$. La première $(\mathbf{A}; C', T(a)T(b))$ collapse en utilisant $(**)$. La seconde $(\mathbf{A}; C', -T(a)T(b))$ collapse en vertu de l'hypothèse de récurrence en degré d car $(*)$ constitue un collapsus de $(\mathbf{A}[y]; C', -T(a)T(b))$ où $\mathbf{A}[y] = \mathbf{A}[Y]/\langle T(Y)\rangle$.
Supposons maintenant P quelconque. Soit c le coefficient de X^{d+2} dans P. On ouvre deux branches en dessous de $(\mathbf{A}; C')$. Dans la première on a $c = 0$ et on utilise l'hypothèse de récurrence en degré $d+1$. Dans la seconde c possède un inverse u, on considère $P_1 = uP$ qui est unitaire et qui vérifie $-P_1(a)P_1(b) \in C''$ (le cone engendré par C' dans $\mathbf{A}[u]$) et on est ramené au cas particulier unitaire, déjà traité. □

Le théorème précédent a la signification pratique que tant qu'il s'agit de démontrer un collapsus d'un corps ordonné idéel $\mathbf{L}$, on peut toujours faire comme si $\mathbf{L}$ était un corps réel clos (voir section 1.5).

Un corollaire du théorème 7 en maths classiques est :

Théorème* 8 *Soit un corps ordonné idéel* $(\mathbf{K}, C)$ *où* $\mathbf{K}$ *est un corps. Si* $(\mathbf{K}, C)$ *ne collapse pas, il peut être plongé dans un corps réel clos qui ne collapse pas.*

Preuve* On considère dans la cloture algébrique de $\mathbf{K}$ un corps ordonné idéel $(\mathbf{K}', C')$ où $\mathbf{K}'$ est un corps, et qui est maximal parmi ceux qui ne collapsent pas et qui prolongent $(\mathbf{K}, C)$. Alors, par le théorème 4 on obtient un corps ordonné, et par le théorème 7, il doit être réel clos : sinon, on considère un polynome qui change de signe et qui n'a pas de zéros ; un facteur irréductible de ce polynome change aussi de signe, on applique le théorème 7 et on obtient une extension algébrique stricte de la précédente, qui ne collapse pas, ce qui est contradictoire. □

1.5 Preuves arborescentes de collapsus avec des corps réels clos idéels

Ce que nous avons développé dans la section 1.3 peut être maintenant amélioré.

En cas d'une preuve classique par contradiction qui fait appel au théorème 8, et qui utilise uniquement des arguments simples faisant un appel immédiat aux deux axiomes cités dans la section 1.3 et à l'axiome qui permet d'introduire un zéro pour un polynome qui change de signe, nous pouvons construire une arborescence de corps ordonnés idéels, qui suit la preuve classique pas à pas, et se termine par des feuilles qui collapsent toutes.

La seule chose à rajouter par rapport à la section 1.3 est, lorsqu'on fait appel à l'existence d'un zéro réel d'un polynome P qui change de signe, si nous sommes en un point de notre arborescence où nous avons un corps ordonné idéel $(\mathbf{A}_i; C_i)$ avec $-P(a)P(b) \in C_i$, alors nous avons le droit de prolonger cette branche avec le corps ordonné idéel $(\mathbf{A}_i[X]/\langle P\rangle ; C_i, -P(a)P(b))$, c'est-à-dire de rajouter un zéro formel au polynome P.

Définition 9 *Lorsque nous avons ce type de construction arborescente ayant à sa racine un corps ordonné idéel* $\mathbf{K}$*, construction qui mime l'utilisation des axiomes des corps réels clos, et dont toutes les feuilles collapsent nous disons que* le corps réel clos idéel $\mathbf{K}$ prouve $-1 \geq 0$.

Et nous obtenons alors une nouvelle version constructive du théorème classique affirmant que tout corps réel peut être plongé dans un corps réel clos, version plus directement utilisable que le théorème 7.

Théorème 10 *Pour tout corps ordonné idéel* $\mathbf{L}$ *les propriétés suivantes sont équivalentes :*
- *le corps ordonné idéel* $\mathbf{L}$ *collapse*
- *le corps ordonné idéel* $\mathbf{L}$ *prouve* $-1 \geq 0$
- *le corps réel clos idéel* $\mathbf{L}$ *prouve* $-1 \geq 0$

Dans ces preuves arborescentes, on peut mimer toutes les règles de déduction simples usuelles dans les corps réels clos. On a par exemple le corollaire suivant du théorème 7.

Proposition 11 *Soit un corps ordonné idéel* $\mathbf{L} = (\mathbf{A}, C)$*,* $a, b \in \mathbf{A}$ *et* $P(X) \in \mathbf{A}[X]$*. Soit* $\mathbf{A}[x] = \mathbf{A}[X]/\langle P\rangle$*.*
- *Si* $(\mathbf{A}[x]; C, (x-a)(b-x), -P(a)P(b))$ *collapse, alors* $(\mathbf{A}; C, -P(a)P(b))$ *collapse.*
- *Si* $(\mathbf{A}[x]; C, x-a, b-x, -P(a)P(b))$ *collapse, alors* $(\mathbf{A}; C, -P(a)P(b), b-a)$ *collapse.*

Preuve Le second item se déduit facilement du premier. Démontrons celui-ci.
On fait une preuve par recurrence sur le degré de P.
On initialise la récurrence. Si P est une constante $e \in \mathbf{A}$, on ouvre deux branches en dessous de $(\mathbf{A}; C, -e^2)$: $(\mathbf{A}[1/e]; C, -e^2)$ et $(\mathbf{A}/\langle e\rangle ; C, -e^2)$. Dans la première e est inversible, donc -1 est dans le cone engendré par $-e^2$, la branche collapse. Dans la seconde $\mathbf{A}[x] = (\mathbf{A}/\langle e\rangle)[X]$, le collapsus de $(\mathbf{A}[x]; C, (x-a)(b-x), -e^2)$ se spécialise, en faisant $X = a$ en un collapsus de $(\mathbf{A}/\langle e\rangle ; C, -e^2)$.
Soit maintenant P de degré $d+1$. Nous supposons que $(\mathbf{A}[x]; C, (x-a)(b-x), -P(a)P(b))$ collapse et nous voulons montrer que $(\mathbf{A}; C, -P(a)P(b))$ collapse. Par application du théorème 7, il nous suffit de montrer que $(\mathbf{A}[x]; C, -P(a)P(b))$ collapse. Pour cela, on ouvre deux branches en dessous de $(\mathbf{A}[x]; C, -P(a)P(b))$. Dans le première $(x-a)(b-x) \geq 0$, cela collapse par hypothèse. Dans la

seconde $(x-a)(b-x) < 0$. Dans $\mathbf{A}[x][T]$ on a $P(T) = (T-x)Q(T)$ avec $\deg(Q) = d$ et en remplaçant T par a puis par b on obtient $-P(a)P(b) = -(x-a)(x-b)Q(a)Q(b)$ et on peut utiliser la règle de déduction valide (cf. fin de la section 1.3)

$$u > 0,\ uv \geq 0\ \Rightarrow v \geq 0$$

(avec $u = (x-a)(x-b)$ et $v = -Q(a)Q(b)$) ce qui nous ramène au degré d et à l'hypothèse de récurrence. □

1.6 Variantes

Dans de nombreux exposés classiques, un corps réel clos est défini comme un corps ordonné R où les positifs sont des carrés et où tout polynome de degré impair possède un zéro. On montre ensuite que $R[\sqrt{-1}]$ est algébriquement clos, puis que tout polynome de $R[X]$ se décompose en produit de facteurs de degrés 1 ou 2 (ces derniers partout > 0). Enfin on montre que tout polynome qui change de signe possède un zéro réel (cf. par exemple [1] chapitre 1). L'avantage d'un tel exposé, outre qu'il est plus conforme à l'original d'Artin-Schreier, est surtout que l'existence d'un corps réel clos qui est une extension d'un corps ordonné ou d'un corps réel donné est facile à établir via le lemme de Zorn (et le principe du tiers exclu) en utilisant le résultat facile suivant.

Proposition 12 *Si* $\mathbf{K}$ *est un corps réel et* P *un polynome irréductible de degré impair, alors* $\mathbf{K}[X]/\langle P\rangle$ *est aussi un corps réel.*

Nous aurions pu suivre de plus près cette démarche classique, mais cela aurait demandé des efforts supplémentaires, qui auraient beaucoup rallongé cet article et obscurci notre propos.

2 Solution du 17ème problème de Hilbert

Théorème 13 (17ème problème de Hilbert) *Soit* $(\mathbf{K}, \mathbf{P})$ *un corps ordonné,* $\mathbf{R}$ *sa cloture réelle,* $F(x_1, \ldots, x_n)$ *un polynome de* $\mathbf{K}[x_1, \ldots, x_n]$ *partout* ≥ 0 *sur* $\mathbf{R}^n$*. Alors on peut écrire* F *comme une somme*

$$\sum_i p_i\, G_i^2 \qquad (p_i \in \mathbf{P},\ \ G_i \in \mathbf{K}(x_1, \ldots, x_n)).$$

Preuve classique D'après le théorème* 3 il suffit de montrer que F est ≥ 0 pour tout ordre de $\mathbf{K}(x_1, \ldots, x_n)$ qui prolonge $\mathbf{P}$. D'après le théorème* 8 il suffit de montrer que F est ≥ 0 dans tout corps réel clos R contenant $\mathbf{K}(x_1, \ldots, x_n)$ et dont l'ordre prolonge $\mathbf{P}$. Or si F est partout ≥ 0 sur $\mathbf{R}^n$, il est partout ≥ 0 dans n'importe quelle extension réelle close de $(\mathbf{K}, \mathbf{P})$) (principe de transfert de Tarski-Seidenberg). En particulier F est ≥ 0 au point $(x_1, \ldots, x_n)$ de R, c'est-à-dire F est ≥ 0 dans R.

Décryptage constructif Nous appliquons la méthode indiquée à la section 1.5 avec la preuve du principe de transfert basée sur l'algorithme de Cohen-Hörmander (cf. [1, 5]). Nous considérons donc le corps ordonné idéel $(\mathbf{K}(x_1, \ldots, x_n), \mathbf{P})$ et nous relisons dans ce corps ordonné idéel la preuve par l'algorithme de Cohen-Hörmander du fait que F est partout positif (sur R^n où R est une extension réelle close de $(\mathbf{K}, \mathbf{P})$). Cette preuve est une preuve élémentaire, c'est-à-dire qui n'utilise les axiomes des corps réels clos que de façon directe, sans appel à des théorèmes généraux mettant en oeuvre des formules avec quantificateurs. Pour s'en convaincre, il suffit de regarder cet algorithme de près. Le seul endroit qui semble utiliser un tel théorème général est celui où on dit qu'un polynome dont la dérivée est > 0 sur un intervalle est croissant sur cet intervalle. En fait ce résultat est certifié par une identité algébrique (théorème algébrique des accroissements finis, cf. [10]). Dans le cas du tableau de Hörmander, on peut aussi utiliser les formules de Taylor généralisées (cf. [5, 13, 14]). Cette preuve élémentaire peut être relue comme une preuve arborescente, comme décrite dans la section

1.5 : le corps réel clos idéel $(\mathbf{K}(x_1,\ldots,x_n);\mathbf{P},-F)$ prouve $-1 \geq 0$. Donc, le corps ordonné idéel $(\mathbf{K}(x_1,\ldots,x_n);\mathbf{P},-F)$ collapse. Donc

$$-1 = (-F)\sum_i r_i R_i^2 + \sum_j q_j Q_j^2$$

avec $r_i, q_j \geq 0$ dans $\mathbf{K}$ et $R_i, Q_j \in \mathbf{K}(x_1,\ldots,x_n)$, ce qui permet d'obtenir l'écriture souhaitée $F = \sum_i p_i G_i^2$. □

Conclusion

Comme dans les articles [2, 8, 9] notre décryptage s'appuie sur une *sémantique constructive* pour les objets mathématiques abstraits hypothétiques dont la "construction" utilise le principe du tiers exclu et le lemme de Zorn : cloture algébrique d'un corps, clotures réelles d'un corps réel, anneaux de valuation hypothétiques contenant un anneau donné, spectre de Zariski, spectre maximal, spectre réel, localisations en tous les idéaux maximaux, chaînes croissantes d'idéaux premiers, idéaux premiers minimaux etc...

Nous interprétons ces objets abstraits comme une invitation à travailler avec des spécifications incomplètes (mais plus concrètes) de ces mêmes objets. L'important n'est pas l'objet abstrait lui-même, mais les preuves qui le concernent, car elles peuvent être comprises également comme des preuves constructives concernant ses spécifications incomplètes. La version constructive des théorèmes abstraits que nous obtenons ainsi a exactement la même force que la version classique du point de vue classique. Mais la version constructive fournit, à la fin du roman, le résultat de l'énigme policière sous une forme explicite : la somme de carrés a bel et bien été construite en suivant la preuve classique abstraite. Il suffisait de savoir lire entre les lignes[2].

Nous pensons que cette méthode générale constitue un espoir de réalisation du programme de Hilbert pour l'algèbre abstraite.

Références

[1] Bochnak, Coste M., Roy M.-F. *Géometrie Algébrique réelle.* Springer-Verlag. Ergeb. M. n°11. 1987. 2, 3, 8

[2] Coquand T., Lombardi H. *Constructions cachées en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down.* Preprint. 2, 9

[3] Coquand T., Lombardi H. *The principal ideal theorem.* In preparation. 2

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

[5] Lombardi H. *Une borne sur les degrés pour le Théorème des zéros réel effectif.* 323–345 in : Real Algebraic Geometry. Proccedings, Rennes 1991, Lecture Notes in Mathematics n°1524. Eds. Coste M., Mahé L., Roy M.-F. (Springer-Verlag, 1992) 8

[6] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier.* Annals of Pure and Applied Logic **91**, (1998), 59–92. 2

[7] Lombardi H. *Platitude, localisation et anneaux de Prüfer : une approche constructive.* Preprint. 2

[8] Lombardi H. *Constructions cachées en algèbre abstraite (1) Relations de dépendance intégrale.* Journal of Pure and Applied Algebra. **167**, (2002) 259–267. 2, 9

[2] Naturellement tous les exposés classiques n'ont pas la même clarté, et il est en général plus facile de décrypter Kaplansky que Bourbaki.

[9] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Théorème de Horrocks, du local au global*. Preprint 1999. 2, 9

[10] Lombardi H., Roy M.-F. *Théorie constructive élémentaire des corps ordonnés.* Publications Mathématiques de Besançon, Théorie des Nombres, 1990-1991.
English abridged version : *Constructive elementary theory of ordered fields.* 249–262. in Effective Methods in Algebraic Geometry. Ed. Mora T., Traverso C. Birkhauser 1991. Progress in Math. n°94. 8

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

[12] Stengle, G. : *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry*. Math. Ann. 207, 87-97 (1974)

[13] Warou H. *An algorithm and bounds for the real effective Nullstellensatz in one variable*. Progress in Math. n°143, Birkhäuser. Basel. 1996. pp. 373–387. 8

[14] Warou H. *Formules de Taylor Généralisées et applications*. Preprint Université de Niamey (1999). 8