Relecture constructive de la théorie d'Artin-Schreier

H. Lombardi

Annals of Pure and Applied Logic **91**, (1998), 59–92

Équipe de Mathématiques de Besançon, UMR CNRS 6623
Université de Franche-Comté
25030 Besançon Cedex France
email : lombardi@math.univ-fcomte.fr

Résumé

Nous introduisons la notion de structure algébrique dynamique, inspirée de l'évaluation dynamique et de la théorie des modèles. Nous montrons comment cette notion constructive permet une relecture de la théorie d'Artin-Schreier, avec la modification capitale que le résultat final est alors établi de manière constructive. Nous pensons que ce que nous avons réalisé ici sur un cas d'école peut être généralisé à des parties significatives de l'algèbre classique, et est donc une contribution à la réalisation du programme de Hilbert pour l'algèbre classique.

Mots-clés 17ème problème de Hilbert. Théorie d'Artin-Schreier. Évaluation dynamique. Mathématiques constructives. Programme de Hilbert. Sommes de carrés. Cors réels. Corps réels clos.

Abstract

We introduce the notion of "Dynamic Algebraic Structure" (DAS) inspired by Dynamic Evaluation (in computer algebra) and Model Theory. We show that this constructive notion allows a rereading of the Artin-Schreier-Robinson solution for the 17–th Hilbert Problem. So, il we know how to reread the proofs, this kind of abstract theory contains an algorithm which computes the concrete result (here, the sum of squares required by Hilbert). Our method gives a constructive semantic for certain parts af abstract classical mathematic. The idea is the following : replace the classical algebraic structures "constructed" by Choice and Principle of Third Excluded Middle (TEM), by DAS and dynamic evaluations of these DAS. Then TEM is replaced by construction of branching in the trees of dynamic evaluation of the DAS. If Choice is used in the form of Godel completeness theorem, it is not really necessary to use it for obtaining concrete results : in DAS, Choice is simply replaced by ... nothing ! This is because the classical proof is by contradiction : "if there were not a sum of squares then some formal theory would admit a pathological model". The constructive reasoning is more direct : since the pathological theory proves $0 = 1$ we know how to construct the sum of squares ... and classical models have disappeared in the proof. They are replaced by dynamic evaluations of DAS. We think that we have given, for an academic example, a new method, realizing a kind of Hilbert Program for significative parts of classical algebra.

Key-words : 17–th Hilbert problem. Artin-Schreier Theory. Dynamic evaluation. Constructive mathematics . Hilbert Program. Sums of squares. Real Fields. Ordered Fields. Real Closed Fiefds.

Classification AMS : 03F65 03B35 12D15 12J15 14Q20

Table des matières

Introduction

Soit $\mathbf{K}$ un corps ordonné où les positifs sont des 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 17$^{\text{ème}}$ problème de Hilbert demande d'écrire P comme une somme de carrés dans $\mathbf{K}(x_1, \ldots, x_n)$.

Lorsqu'un(e) mathématicien(ne) lit pour la première fois de sa vie la solution du 17$^{\text{ème}}$ problème de Hilbert par la théorie d'Artin-Schreier, il (elle) hésite entre l'admiration et l'incrédulité. Elle (il) se trouve exactement dans la situation du spectateur d'un tour de prestidigitation, avec toutefois le sentiment que les sommes de carrés, en mathématiques, ne devraient pas sortir du chapeau à la manière des lapins de l'homme de l'art.

Convaincu, depuis ma preuve constructive du Positivstellensatz de Stengle ([18], [12], [13], [14]), que la théorie d'Artin-Schreier n'est pas vraiment un tour de passe-passe, mais contient au contraire tous les ingrédients d'une solution explicite du 17$^{\text{ème}}$ problème de Hilbert, j'ai depuis essayé de trouver une clé du mystère. Je livre ici une clé possible. Évidemment, ce mystère n'a pas une seule clé, et d'autres explications, meilleures (plus parlantes pour la majorité des mathématiciens) que celles fournies ici viendront sans doute bientôt à la surface du conscient, issu de l'inconscient collectif des mathématiciens.

L'enjeu est à mon sens avant tout d'ordre épistémologique, une sorte de réhabilitation d'un fragment des mathématiques classiques aux yeux des mathématiciens constructifs, dont je suis. Cependant la méthode de traduction que je propose me semble être assez générale et devrait pouvoir s'appliquer à la plupart des Nullstellensatz et de leurs variantes (p-adiques notamment), et cela devrait intéresser tous les mathématiciens, même ceux pour qui le mot épistémologie provoque un sourire entendu, quand ce n'est pas un franc éclat de rire, pour le déshonneur de l'esprit humain.

Essayons de dire en deux mots comment cela fonctionne.

Tout d'abord nous devons rappeler les deux grandes étapes de la preuve d'Artin-Schreier. Dans une première étape, avec force recours aux méthodes non constructives (tiers exclu et axiome du choix), on démontre les équivalences suivantes, concernant un corps arbitraire $\mathbf{K}$ avec un élément spécifié a :

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

ainsi que

$$\begin{gathered}-a \text{ n'est pas une somme de carrés dans } \mathbf{K} \iff \\ \mathbf{K} \text{ peut être ordonné avec } a > 0\end{gathered}$$

La deuxième étape est de nature différente. Si $\mathbf{R}$ est un corps réel clos et $P(x_1, \ldots, x_n)$ un polynome partout positif sur $\mathbf{R}^n$, il faut en déduire qu'il n'existe pas d'ordre rendant P négatif sur le corps de fractions rationnelles $\mathbf{R}(x_1, \ldots, x_n)$. Disons tout de suite que notre clé du mystère ne s'attaque qu'à la première partie de la preuve. Pour la deuxième partie (ou du moins sa traduction), nous utilisons de manière cruciale le principe de transfert de Tarski-Seidenberg, et même une preuve particulièrement élémentaire de ce principe (par l'algorithme de Cohen-Hörmander).

En quelque sorte, c'est la version "théorie des modèles" de la preuve d'Artin-Schreier, telle qu'exposée par exemple dans [1], que nous interprétons comme une preuve constructive cachée. En théorie des modèles, les deux chaînes d'équivalence encadrées ci-dessus se relisent comme suit.

-1 n'est pas une somme de carrés dans $\mathbf{K}$ $\iff$
La théorie formelle des corps réels extensions du corps $\mathbf{K}$ est cohérente $\iff$
La théorie formelle des corps ordonnés extensions du corps $\mathbf{K}$ est cohérente $\iff$
La théorie formelle des corps réels clos extensions du corps $\mathbf{K}$ est cohérente

ainsi que

$-a$ n'est pas une somme de carrés dans $\mathbf{K}$ $\iff$
La théorie formelle des corps ordonnés extensions du corps $\mathbf{K}$, avec $a > 0$ est cohérente

Comme le fait pour une théorie formelle d'être cohérente est de nature infinie négative, nous préférerons les énoncés contrapposés, qui sont de nature finie positive :

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

ainsi que

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

Cependant, maintenant que toutes les affirmations ont un contenu de nature finie et précise, il n'était nullement évident a priori que la théorie d'Artin-Schreier puisse par simple relecture donner la preuve de ces dernières équivalences.

Notez que d'un point de vue constructif, seuls les énoncés en version théorie des modèles ont une chance de pouvoir être prouvés. Les autres semblent relever plutôt de la magie, dans la mesure où il existe des corps réels explicites pour lesquels aucune relation d'ordre récursive ne peut être définie. Notez aussi que pour déduire la première série d'énoncés de la dernière, l'axiome du choix n'est pas requis dans toute sa force. L'axiome du choix équivaut au fait que tout anneau commutatif a un quotient égal à un corps (axiome de l'idéal maximal), tandis que le théorème de complétude de Gödel en théorie des modèles n'utilise que l'axiome de l'idéal premier : tout anneau commutatif a un quotient intègre, c.-à-d. encore peut être envoyé homomorphiquement dans un corps.

Comme nous voulons éviter autant que possible l'utilisation des théorèmes profonds de logique, nous avons préféré la notion "d'évaluation dynamique" (cf. [3], [6], [8], [9], [10]) qui n'utilise pratiquement pas de logique mais qui rend presque les mêmes services que la partie constructive de la théorie des modèles. (C'était aussi, il faut le dire, une condition sine qua non de crédibilité de ce travail). Par exemple l'évaluation dynamique permet de calculer dans la cloture algébrique d'un corps quand bien même celle-ci ne saurait absolument pas être construite. En fait les arbres d'évaluation dynamique dans la cloture algébrique d'un corps *sont* la vraie cloture algébrique constructive de ce corps. La méthode de l'évaluation dynamique nous permet d'échapper à la plupart des dilemmes que posent les preuves classiques au mathématicien constructif. Un mathématicien classique va dire : si le polynome f n'est pas irréductible, je considère un facteur irréductible f_1 de f. Face à cette situation, le mathématicien constructif ressemble à un coq qui a trouvé une petite cuillère, car ses constructions s'arrêtent sur l'obstacle de l'explicitation du facteur irréductible (et je soupçonne qu'il s'agit là de la vraie raison psychologique qui fait que la philosophie constructive n'est pas plus facilement adoptée : personne n'a envie de ressembler à un coq qui a trouvé une petite cuillère). Mais l'évaluation dynamique nous sauve la mise : faisons comme si f était irréductible, tant que ça ne gène pas, et si cela gène, à un moment donné (tel polynome g qui s'annule en un zéro de f est-il bien

multiple de f ?), ouvrons différentes branches pour les calculs à venir, selon le degré du pgcd de f et g, c.-à-d. selon que certains coefficients sous-résultants sont nuls ou inversibles. Objection : vous venez peut être d'ouvrir une branche impossible. Réponse, si une branche meurt, tant pis pour elle, l'important est qu'il en reste toujours au moins une en vie, or l'ouverture d'un tel couple de branches n'est pas problématique à cet égard.

En résumé l'idée, assez simple, est de remplacer les structures algébriques "mirobolantes" "construites" par tiers exclu et axiome du choix en tant que structures figées réellement existantes (ce qui est un peu dur à avaler[1]), par des structures algébriques dynamiques ouvrant un large éventail de possibilités que l'on explore selon les besoins du moment, en ayant montré que chaque ouverture d'un embranchement ne pose pas problème quant à la cohérence générale du tout (le tout ne devient incohérent que si toutes les branches meurent). Signalons que ce point de vue est en fait celui d'une relecture constructive de la théorie du spectre (de Zariski, réel ou autre selon la situation).

Dans l'article présent, nous traitons le 17$^{\text{ème}}$ problème de Hilbert. Nous donnons en parallèle d'une part les énoncés classiques, concernant des structures algébriques classiques figées, avec des preuves qui utilisent l'axiome du choix et le tiers exclu, et d'autre part les énoncés constructifs, concernant des structures algébriques dynamiques, avec des preuves purement algorithmiques.

L'article [2] est la mise en oeuvre des structures algébriques dynamiques pour l'obtention de Nullstellensatz et Positivstellensatz effectifs selon une méthode qui semble assez générale. Cette méthode est plus directe et plus rapide que la traduction pas à pas des preuves classiques, utilisée ici. En particulier, les auteurs obtiennent un nouveau Positivstellensatz effectif pour les corps valués algébriquement clos. Ils développent un peu plus avant la théorie des structures algébriques dynamiques, et la comparent à la théorie des modèles et à la théorie des topos cohérents.

Dans l'article [15] nous utilisons les structures algébriques dynamiques pour donner une interprétation constructive de certains principes "local-global" abstraits en algèbre commutative.

1 Structures algébriques dynamiques

1.1 Premières définitions

Structures algébriques dynamiques

Une *structure algébrique dynamique* est donnée par :

la structure algébrique abstraite d'une part, donnée comme suit

- un langage comportant des constructeurs de termes (les termes sont construits à partir de variables, de paramètres, de constantes et de symboles de fonctions précisés), et des symboles de prédicat (dont au moins l'égalité),
- un système d'axiomes, de nature élémentaire (on va préciser cela), formulés sans utilisation des paramètres[2].

[1] Que celui (celle) qui a réussi à avaler le paradoxe de Banach Tarski, conséquence de l'axiome du choix, lève le doigt : une boule peut être découpée en un nombre fini de morceaux qui, déplacés par des isométries convenables, se réarrangent en deux boules isométriques à la boule initiale.

[2] Dans [2], ce que nous appelons ici une structure algébrique abstraite est appelé une théorie dynamique.

une concrétisation de cette structure algébrique abstraite, encore appelée présentation de la structure algébrique dynamique d'autre part, donnée comme suit

- un ensemble de générateurs, qu'on peut voir comme les paramètres de départ,
- et un système de relations qui sont des prédicats portant sur des termes clos, (c.-à-d. sans variable), qu'on peut voir comme : les faits donnés au départ comme vrais dans la structure. On les appellera les relations de départ.

Étant donnée une structure algébrique dynamique S la structure algébrique abstraite correspondante sera appelé le *type (abstrait)* de S.

Un terme construit sur le langage considéré est appelé un *terme clos* s'il ne fait pas intervenir de variables. Un *fait* concernant cette structure est une affirmation :

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

On pourrait aussi dire que c'est un "fait brut".
L'ensemble des assertions exprimables sous forme de faits dépend de manière critique du langage utilisé. Un langage plus riche permet d'exprimer plus de propriétés sous forme de faits. Si pour la structure d'anneau, on n'introduisait ni la constante -1, ni l'opération $x \mapsto -x$, on serait contraint à des périphrases bien encombrantes.

Les axiomes sont du type général suivant :

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

Les $A_i(\mathbf{x},\mathbf{y}^i)$ et $H(\mathbf{x})$ sont des listes de prédicats portant sur des termes construits avec le langage de départ, sans utilisation des paramètres. Un $\forall\mathbf{x}$ est implicite devant l'axiome. Le E a la signification d'un "il existe".
Un axiome est dit *disjonctif* s'il y a effectivement des "ou", il est dit *existentiel* s'il y a effectivement des variables dans une liste $\mathbf{y}^i$ (c.-à-d. si elles ne sont pas toutes vides).
Un axiome qui n'est ni disjonctif ni existentiel est dit *universel* ou *purement algébrique.*
Une structure abstraite est dite *purement algébrique* si tous ses axiomes sont purement algébriques.

Les axiomes n'ont pas pour signification de donner des énoncés élémentaires vrais, mais d'être utilisés comme règles de déduction, ou plus précisément comme règles de constructions d'évaluations dynamiques.
Quand on utilise légitimement un axiome, on remplace les x_j par des termes clos t_j dont on a établi qu'ils valident l'hypothèse $H(\mathbf{x})$ dans la branche où l'on est. Si l'axiome est disjonctif, on produit un noeud à k branches. Dans la i-ème branche, les prédicats constituant la liste $A_i(\mathbf{t},\mathbf{y}^i)$ sont valides. Si l'axiome est existentiel, on introduit de nouveaux paramètres correspondant aux objets affirmés exister dans l'axiome. Les y^i_j doivent être pris parmi les paramètres non encore utilisés dans la branche où l'on est.
En pratique, nous utiliserons les mêmes lettres pour désigner les variables (présentes uniquement dans les axiomes) et les paramètres (présents dans les faits, mais non dans les axiomes).

Évaluation dynamique d'une structure algébrique dynamique

Une *évaluation dynamique* de la structure est un arbre fini dans lequel sont accumulés des faits, validés en vertu des *hypothèses actives au point considéré* de l'arbre, qui sont d'une part des relations de départ, et d'autre part, les faits introduits lorsque (en suivant le chemin depuis la racine de l'arbre jusqu'au point considéré) on a utilisé légitimement les axiomes. Nous parlerons aussi des *hypothèses présentes en un point de l'arbre* qui sont, les hypothèses actives et toutes

les relations de départ, actives ou non. En fait, si une hypothèse est présente en un point précis de l'arbre d'évaluation dynamique, elle est présente dans toutes les branches au delà de ce point précis de l'arbre. On définirait de même les *paramètres actifs et les paramètres présents* en un point de l'arbre. Les faits considérés en un point de l'arbre ne font intervenir que les paramètres présents en ce point.
Tous les faits dans l'arbre sont validés (chacun dans leur branche) de manière immédiate par les axiomes. Il n'y a pas à proprement parler de logique, en particulier pas de négation ni de formules avec quantificateurs.
On admet que l'ensemble des générateurs puisse être infini, ainsi que l'ensemble des relations de départ. Cependant, dans une évaluation dynamique, on ne manipule jamais qu'un nombre fini de tels générateurs et relations.
D'un point de vue constructif strict on a affaire à des programmes qui tournent sur machine. L'ensemble des relations de départ, s'il est infini, peut alors être imaginé comme testé par un algorithme, ou sinon, à la demande, par un oracle qui donne une des deux réponses : "oui cette relation fait partie des hypothèses de départ", ou "non elle n'en fait pas partie". C.-à-d. encore "oui cette relation est vraie" ou "je ne sais pas si cette relation est vraie". (notez que ceci est très différent de la réponse "cette affirmation est fausse" délivrée par un oracle omniscient).
Si l'ensemble des générateurs et le système de relations de départ sont finis, on dit que la structure dynamique est *de présentation finie.*

Définition 1.1 *Un fait qui ne fait intervenir que les paramètres de départ est dit* vrai dans la structure algébrique dynamique *considérée si on a construit un arbre d'évaluation dynamique de la structure, et que ce fait est prouvé vrai à toutes les feuilles de l'arbre.*

Remarque 1.2 Toute structure algébrique ordinaire S qui satisfait les axiomes d'une structure algébrique dynamique abstraite (lus comme des axiomes ordinaires) fournit un cas particulier de structure algébrique dynamique S' ayant ce même type abstrait, en prenant comme générateurs de départ les éléments de S (ou un système de générateurs de S) et comme relations de départ les faits vrais dans S (ou un ensemble de faits vrais dans S qui impliquent, au sens de l'évaluation dynamique, tous les faits vrais dans S). Les faits vrais (au sens usuel) dans la structure ordinaire S sont alors exactement les faits vrais (au sens de l'évaluation dynamique) dans la structure dynamique S'. Une évaluation dynamique de S' peut alors être comprise comme une exploration de structures "quotients" de S.
Supposons maintenant que nous considérions une structure algébrique dynamique S" ayant pour présentation : comme générateurs, certains éléments de S, et comme relations certains faits vrais dans S. Alors tous les faits vrais dans S" sont vrais (au sens usuel) dans S d'une part, et d'autre part la structure S "correspond" toujours à au moins une branche de toute évaluation dynamique de la structure dynamique S". Explicitons ceci un peu plus en détail. Ici le mot "correspond" signifie que, dans la branche considérée, tous les faits que l'on peut affirmer "en restant dans la branche", c.-à-d. sans faire appel de nouveau à des axiomes disjonctifs ou existentiels, sont vrais dans la structure ordinaire S. En effet, pour chaque axiome avec disjonction, un des embranchements au moins correspond à S puisque S vérifie les axiomes disjonctifs. Et pour chaque axiome avec existence, le paramètre existentiel qu'on introduit de manière formelle pour remplacer la variable existentielle de l'axiome dans l'évaluation dynamique, peut être remplacé par un élément de S qui vérifie l'axiome.

Inversement, une structure algébrique dynamique générale peut être vue comme un projet, non entièrement spécifié, de structure algébrique ordinaire. Le fait de considérer la structure algébrique dynamique comme l'objet mathématique central de l'étude présente l'avantage qu'un

obstacle habituellement offert aux preuves constructives, à savoir l'impossibilité de construire un modèle pour un système d'axiomes cohérent, disparaît de lui-même. Ainsi est donné un certain contenu constructif intuitif à l'adage idéaliste de Hilbert selon lequel en mathématiques l'existence équivaut à la non-contradiction.

Collapsus d'une structure algébrique dynamique

La *structure ponctuelle* est par définition la structure réduite à un point en lequel tous les prédicats sont vrais. Cette structure satisfait toujours les axiomes, ce qui évite radicalement l'usage de la négation. Une branche *meurt*, ou *collapse*, si elle prouve un fait à partir duquel on sait déduire que tous les faits sont vrais (ce qui correspond à la structure ponctuelle précédemment décrite).
Dans le cas de structures qui sont des surstructures de la structure d'anneau, un tel fait est $1 = 0$, (on rajoutera s'il le faut un axiome affirmant, pour chaque nouveau prédicat, qu'il est vrai sous l'hypothèse $1 = 0$). Comme nous ne discuterons dans cet article que des surstructures de la structure d'anneau commutatif, nous ne nous étendrons pas sur ce point[3].

Définition 1.3 *Une structure algébrique dynamique* collapse *si on a construit une évaluation dynamique dans laquelle toutes les branches sont mortes.*

Règles valides dans une structure algébrique dynamique abstraite

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

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

Elle est dite valide (pour la structure dynamique abstraite considérée) si elle peut être prouvée à partir des axiomes. Cette preuve doit être obtenue en donnant une évaluation dynamique "abstraite", démarrant avec l'hypothèse $H(\mathbf{x})$. À l'extrémité de chaque branche doit être prouvée l'une des conclusions $A_i(\mathbf{x},\mathbf{y}^i)$ où les y^i_j sont des termes construits au cours de l'évaluation dynamique abstraite. Il suffit souvent de recopier une preuve classique pour obtenir une telle évaluation dynamique abstraite.
Lorsqu'on a prouvé qu'une règle est valide, son utilisation de la même manière que les axiomes est légitime et elle ne permet pas de démontrer d'autres faits que ceux prouvés à partir des axiomes. En effet le preuve abstraite de la validité de la règle peut être ensuite utilisée concrètement pour transformer les évaluations dynamiques qui utilisent la règle en évaluations dynamiques qui ne l'utilisent pas.
Le lecteur pourra s'entrainer à vérifier ce fonctionnement sur les nombreux exemples de règles valides laissés en exercice dans la suite.

Commentaire : Nous sommes ici à l'intérieur d'un système de démonstrations, les évaluations dynamiques, où les seules choses prouvées sont des faits "bruts", qui peuvent être considérés comme les théorèmes de nature complètement élémentaire. Ce sont alors les règles valides qui jouent le role habituellement tenu par les théorèmes en mathématiques. Mais le statut d'une règle de déduction et celui d'un théorème ne sont pas les mêmes. Paradoxalement, c'est parce que nous introduisons des limitations a priori très contraignantes sur la nature des faits exprimables dans le langage d'une structure algébrique que nous obtenons facilement des preuves simples et constructives de théorèmes réputés difficiles que sont les Nullstellensatz de toutes sortes.

[3] Dans [2] un fait à partir duquel on sait déduire que tous les faits sont vrais est noté $\perp$.

1.2 Exemples de structures algébriques dynamiques

Nous introduisons quelques structures dynamiques abstraites qui nous sont utiles pour la traduction de la théorie d'Artin-Schreier.

Les structures d'anneau (commutatif)

Signalons une fois pour toutes que nous ne cherchons pas des systèmes d'axiomes minimaux. Nous nous intéressons ici à la structure d'anneau commutatif avec le seul prédicat d'égalité et à quelques surstructures obtenues en rajoutant des axiomes universels. La structure d'anneau commutatif est construite avec les constantes 0 et 1 les symboles de fonctions $+$, $-$ et $\times$, et, comme seul prédicat, l'égalité $=$.
Les axiomes sont ceux de l'égalité et ceux des anneaux commutatifs.
On peut, sans changement significatif, prendre tous les éléments de $\mathbb{Z}$ comme constantes, à condition de rajouter les axiomes convenables, par exemple que, pour tout couple (m, n) d'entiers consécutifs $m + 1 - n = 0$. On pourrait aussi prendre tous les éléments de $\mathbb{Z}$ comme constantes, considérer l'égalité à zéro comme seul prédicat, prendre pour axiomes toutes les identités algébriques, et définir l'égalité de deux termes comme l'égalité à zéro de leur différence.
On omettra commutatif dans toute la suite.
Un anneau dynamique de présentation finie peut être pensé comme un anneau de présentation finie ordinaire.
De fait, lorsque les axiomes sont tous universels, l'évaluation dynamique d'une structure algébrique de présentation finie se situe entièrement dans le cadre de la structure ordinaire, de même présentation finie, correspondante. En bref, il s'agit de l'algèbre classique avec axiomes universels, où l'on a automatiquement des structures libres et des structures "universelles" correspondant à une présentation donnée. Par contre, dès qu'il y a disjonction ou existence la notion ordinaire de structure de présentation finie ne fonctionne plus.
Nous donnons dans la suite trois propositions 1.4, 1.5, 1.6 dans le but de mettre en évidence le fait que, tant qu'il ne s'agit que de structures purement algébriques, l'étude des structures algébriques dynamiques n'est rien d'autre que de l'algèbre classique avec axiomes universels.
Étant donnée une présentation d'anneau dynamique, tout terme est égal (au sens de l'évaluation dynamique) à un polynome à coefficients entiers en les générateurs, et toute relation de départ est équivalente (au sens de l'évaluation dynamique) à l'égalité à 0 d'un tel polynome. Dans toute la suite, nous supposerons sans perte de généralité que les relations de départ sont toujours de ce type.

Proposition 1.4 (anneau quotient / collapsus d'un anneau) *Soit un anneau dynamique* $\mathbf{K}$. *Soit* $\mathbb{Z}[\mathbf{g}]$ *l'anneau librement engendré par les générateurs. Soit* I *l'idéal engendré par les polynomes donnés égaux à 0 au départ. Alors :*

a) la structure $\mathbf{K}$ *collapse si et seulement si* 1 *est dans l'idéal* I.

b) un fait $p = 0$ *est vrai dans un anneau dynamique* $\mathbf{K}$ *si et seulement si* p *est dans l'idéal* I.

Preuve (a) est un cas particulier de (b). Dans (b) la partie "si" est claire. Voyons la partie "seulement si". Soit $\mathbf{A}$ l'anneau ordinaire qui a la même présentation que $\mathbf{K}$. Puisque $p = 0$ est vrai dans l'anneau dynamique $\mathbf{K}$, cela implique que $p = 0$ est vrai dans $\mathbf{A}$, c.-à-d. que p est dans l'idéal des relations de départ. □

On sait établir tous les faits vrais dans une structure d'anneau dynamique de présentation finie, c.-à-d. qu'on sait tester si un polynome de $\mathbb{Z}[x_1, \ldots, x_n]$ appartient à un idéal de type fini donné, et en cas de réponse positive, fournir l'appartenance à l'idéal sous forme explicite. Les

faits qui ne sont pas prouvables ne sont ni vrais ni faux dans la structure dynamique. Cependant certains sont moins vrais que d'autres, dans la mesure où ils ont plus de conséquences. Le fait $1 = 0$ est le moins vrai de tous.
Notez que $\mathbb{Q}$ n'est pas un anneau de présentation finie.

La structure d'*anneau réduit*.
On part de la structure d'anneau et on rajoute l'axiome :

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

Proposition 1.5 (radical d'un idéal / collapsus d'un anneau réduit)
Soit un anneau dynamique réduit $\mathbf{K}$. *Soit* $\mathbb{Z}[\mathbf{g}]$ *l'anneau librement engendré par les générateurs. Soit* I *l'idéal engendré par les polynomes donnés égaux à* 0 *au départ et* J *le (nil)radical de* I. *Alors :*

a) la structure $\mathbf{K}$ *collapse si et seulement si* 1 *est dans l'idéal* I.

b) un fait $p = 0$ *est vrai dans l'anneau dynamique réduit* $\mathbf{K}$ *si et seulement si* p *est dans l'idéal* J.

Preuve On vérifie que le radical d'un idéal est bien un idéal, et que l'anneau quotient est réduit. On considère alors l'anneau réduit ordinaire $\mathbf{B}$, quotient de $\mathbb{Z}[\mathbf{g}]$ par le radical de l'idéal des relations de départ de $\mathbf{K}$. On termine comme à la proposition 1.4. □

On sait établir tous les faits vrais dans une structure d'anneau réduit dynamique de présentation finie, c.-à-d. qu'on sait tester si un polynome de $\mathbb{Z}[x_1, \ldots, x_n]$ appartient au radical d'un idéal de type fini donné, et en cas de réponse positive, fournir l'appartenance sous forme explicite.
Notez qu'un anneau dynamique réduit prouve en général plus de faits que l'anneau sous-jacent, mais il ne collapse que si l'anneau sous-jacent collapse.

La structure d'*anneau réel*
Cette structure est obtenue à partir de celle d'anneau en rajoutant les *axiomes de réalité* (un axiome pour chaque entier n :

- $x_1^2 + x_2^2 + \cdots + x_n^2 = 0 \vdash x_1 = 0$

Rappelons que le *radical réel d'un idéal* I dans un anneau A est l'ensemble J défini comme suit :

$$J = \{x \in A;\ \exists n, m \text{ entiers},\ \exists x_1, \ldots, x_n \in A, \text{ tels que } x^{2m} + x_1^2 + \cdots + x_n^2 \in I\}$$

Proposition 1.6 (radical réel d'un idéal / collapsus d'un anneau réel) *Soit un anneau dynamique réel* $\mathbf{K}$. *Soit* $\mathbb{Z}[\mathbf{g}]$ *l'anneau librement engendré par les générateurs. Soit* I *l'idéal engendré par les polynomes donnés égaux à* 0 *au départ et* J *le radical réel de* I. *Alors :*

a) la structure $\mathbf{K}$ *collapse si et seulement si* 1 *est dans l'idéal* J.

b) un fait $p = 0$ *est vrai dans l'anneau dynamique réduit* $\mathbf{K}$ *si et seulement si* p *est dans l'idéal* J.

Preuve On vérifie que le radical réel d'un idéal est bien un idéal, et que l'anneau quotient est réel. On considère alors l'anneau réel ordinaire $\mathbf{C}$, quotient de $\mathbb{Z}[\mathbf{g}]$ par le radical réel de l'idéal des relations de départ de $\mathbf{K}$. On termine comme à la proposition 1.4. □

Quelques axiomes disjonctifs et/ou existentiels

Nous nous en tiendrons ici à quelques exemples toujours sans autres prédicat que celui d'égalité. Nous consacrerons un peu plus loin un paragraphe distinct aux structures de corps.

L'axiome de l'*absence de diviseurs de zéros* est le suivant :

- $xy = 0 \vdash (x = 0 \quad \mathsf{ou} \quad y = 0)$

Cet axiome n'est pas vérifié par le corps des réels en algèbre constructive.

Signalons l'exemple important des *axiomes de cloture algébrique* :

- $\vdash \mathsf{E}\, y\ y^n + x_{n-1}y^{n-1} + \cdots + x_1 y + x_0 = 0$

La structure *anneau réel* $2-clos$ est obtenue à partir de celle d'anneau réel en rajoutant l'*axiome de* $2-$*cloture réelle* :

- $\vdash \mathsf{E}\, y\ x^2 = y^4$

Signalons enfin l'*axiome de Pythagore*, qui définit les *anneaux pythagoriciens*.

- $\vdash \mathsf{E}\, y\ a^2 + b^2 = y^2$

Les structures de corps (discrets)

Nous avons choisi de ne pas introduire le prédicat opposé à l'égalité.

La structure de *corps discret* est obtenue à partir de la structure d'anneau en rajoutant trois axiomes. Le premier, que nous appellerons dans la suite l'*axiome des corps*, est le plus important.

- $\vdash (x = 0 \quad \mathsf{ou} \quad \mathsf{E}\, u\ xu = 1)$

Les deux autres ne sont pas indispensables, puisqu'ils résultent de l'axiome des corps, mais ils sont introduits pour des raisons de commodité (notamment pour pouvoir développer une théorie agréable des extensions algébriques dynamiques).
Ce sont l'axiome des anneaux réduits et celui de l'absence de diviseurs de zéros.

- $x^2 = 0 \vdash x = 0$
- $xy = 0 \vdash (x = 0 \quad \mathsf{ou} \quad y = 0)$

Dans la suite, tous les corps sont discrets, c.-à-d. des surstructures de la structure présentée ici, (sauf mention explicite du contraire), mais nous omettrons désormais le mot discret.

La structure de *corps réel* est obtenue en rajoutant les axiomes de réalité à la structure de corps.

La structure de *corps réel* $2-clos$.
Elle est obtenue à partir de celle de corps en rajoutant les axiomes de réalité et de $2-$cloture réelle.

La structure de *corps algébriquement clos*.
On considère la surstructure de la structure de corps obtenue en rajoutant les axiomes de cloture algébrique

- $\vdash \mathsf{E}\, y\ y^n + x_{n-1}y^{n-1} + \cdots + x_1 y + x_0 = 0$

La version dynamique (et constructive) du théorème (non constructif) selon lequel tout corps possède une cloture algébrique est le théorème suivant (cf. Théorème 1).

"Un corps dynamique qui collapse comme corps algébriquement clos collapse comme corps."

Notez que $\mathbb{Q}$ n'est pas un corps de présentation finie, ou si vous préférez, pour donner $\mathbb{Q}$ de manière entièrement explicite, ou figée, il faut introduire un générateur g_p et une relation $g_p.p = 1$ pour chaque p premier. Par contre $\mathbb{Q}$ est le corps réel de présentation vide.
Un corps sans générateur ni relation s'évalue dynamiquement en branches représentant chacune, soit la structure ponctuelle, soit un ou plusieurs corps premiers finis, soit tous les corps premiers sauf un nombre fini d'entre eux (c'est la branche où tous les faits vrais dans $\mathbb{Q}$ ont été retenus

lors de l'utilisation de l'axiome des corps ou de l'axiome de l'absence des diviseurs de zéro). Voir à ce sujet [7].
Un corps discret ordinaire **K** (cf. [17]) définit une structure algébrique dynamique de corps. On peut qualifier cette structure dynamique de structure *figée* ou *entièrement explicitée*. Cela signifie qu'il n'y a fondamentalement que deux branches possibles dans les évaluations dynamiques de **K**, la branche correspondant à la structure ponctuelle et la branche correspondant à **K**. Tout fait rajouté aux relations de départ est ou bien inutile, ou bien catastrophique (il fait collapser la structure). Par contre, si on regarde un anneau ordinaire comme anneau dynamique, une dichotomie aussi franche ne se produit pas en général (cf. la discussion précédente sur les faits plus ou moins vrais dans un anneau dynamique).
La théorie des évaluations dynamiques d'un anneau comme corps peut être considérée comme une version dynamique constructive de la théorie du spectre de Zariski de l'anneau.

Extensions de structures algébriques dynamiques

On dira qu'une structure dynamique de corps **L** est une *extension* d'un corps ordinaire **K** si les éléments de **K** sont des générateurs de **L** et si les faits $a+b=c,\ ab=c$ vrais dans **K** sont des relations de départ de **L**.

De manière générale, on peut parler d'une *structure algébrique dynamique L extension d'une structure algébrique dynamique K :*
– en ce qui concerne les structures abstraites, le langage de K doit être inclus dans le langage de L, et les axiomes de K doivent être des règles prouvables à partir des axiomes de L
– alors la structure (concrète) L est une extension de K si

- tous les générateurs de K sont exprimés à partir des générateurs de L (c.-à-d. plus précisément qu'à tout générateur de K est associé un terme clos bien précisé de L)
- toutes les relations de départ de K peuvent être prouvées à partir des relations de départ et des axiomes de L (après remplacement des générateurs de K par les termes de L qui les représentent)

La présentation de L est appelée *une extension de la présentation* de K lorsqu'elle est obtenue simplement en rajoutant des générateurs et/ou des relations. Nous utiliserons alors la notation suivante :

$$L = K\oplus \{ \text{ nouveaux générateurs ; nouvelles relations } \}.$$

Par exemple si on étend la présentation d'un corps dynamique K en rajoutant les racines carrées d'éléments a et b, on obtient la présentation $K \oplus \{\alpha, \beta;\ \alpha^2 = a,\ \beta^2 = b\}$. Si K est un corps entièrement explicité, le nouveau corps dynamique obtenu n'est vraiment plus un corps ordinaire, notamment à cause de la théorie de Galois qui est intimement mêlée à la structure dynamique.
Le système D5 développe notamment de manière systématique les évaluations dynamiques de structures de corps du type

$$\mathbb{Q} \oplus \{x_1, \ldots, x_n;\ P_1(x_1) = 0,\ P_2(x_1, x_2) = 0, \ldots,\ P_n(x_1, \ldots, x_n) = 0\}$$

avec chaque P_i unitaire en x_i.

Axiomes avec une relation d'ordre

Commençons par la structure d'*anneau partiellement préordonné*. Cela correspond à la notion de cone. On introduit un nouveau prédicat, qu'on note $x \geq 0$. La notation $x \geq y$, ou encore

$y \leq x$ est une abréviation pour $(x - y) \geq 0$. Les axiomes sont ceux des cones propres (cf. [1]). Plus précisément.

- $(x = y,\ x \geq 0) \vdash y \geq 0$
- $(x \geq 0,\ y \geq 0) \vdash x + y \geq 0$
- $(x \geq 0,\ y \geq 0) \vdash xy \geq 0$
- $\vdash x^2 \geq 0$

On démontre facilement la validité de la règle suivante :

- $1 = 0 \vdash x \geq 0$

La structure d'anneau *partiellement ordonné* s'obtient en rajoutant l'axiome qui dit que le préordre est un ordre :

- $(x \geq 0,\ x \leq 0) \vdash x = 0$

qu'on aurait aussi bien pu écrire sous la forme

- $(x \geq 0,\ y \geq 0,\ x + y = 0) \vdash x = 0$

Nous sommes ici encore dans le cadre de l'algèbre classique avec axiomes universels. Nous sortons de ce cadre avec la structure suivante.

La structure d'*anneau ordonné*.
On rajoute, dans la structure d'anneau partiellement ordonné, l'axiome pour que l'ordre soit total :

- $\vdash (x \geq 0 \quad \mathsf{ou} \quad x \leq 0)$

La structure de *corps ordonné* .
C'est la structure d'anneau ordonné où on a rajouté les axiomes pour les corps. La théorie des évaluations dynamiques d'un anneau comme corps ordonné peut être considérée comme la version dynamique constructive de la théorie du spectre réel de l'anneau.

La structure de *corps ordonné* $2-$*clos* est obtenue en rajoutant l'*axiome de* $2-$*cloture ordonnée* :

- $x \geq 0 \vdash \mathsf{E}\, y\ x = y^2$

Comme en algèbre ordinaire, la structure de corps réel $2-$clos dynamique est équivalente (en un sens naturel que la lectrice pourra préciser, et que nous détaillerons plus loin) à celle de corps ordonné $2-$clos.

La structure de *corps réel clos*.
Nous choisirons la définition suivante pour des raisons de commodité. Le nom qu'il serait logique d'accorder à cette structure est celui de corps ordonné clos.
C'est la structure de corps ordonné, avec les axiomes de la valeur intermédiaire que nous formulerons comme suit :

- $(P(a).P(b) \leq 0,\ a \leq b) \vdash \mathsf{E}\, y\ (a \leq y \leq b,\ P(y) = 0)$

(a, b et les coefficients de P sont des variables, et il y a un axiome pour chaque degré de polynome).
Les corps réels clos sont $2-$clos. Il y a des formulations axiomatiques équivalentes qui ne font pas intervenir le prédicat $x \geq 0$: le corps est réel $2-$clos et tout polynome de degré impair a une racine. C'est cela qui mériterait vraiment le nom de structure de corps réel clos. Comme nous n'avons pas voulu prendre le temps d'expliciter cette équivalence dans le cadre dynamique, nous nous en sommes tenus à une solution moralement boiteuse.
Le théorème (non constructif) disant que tout corps réel peut être plongé dans un corps réel clos admet la version dynamique (et constructive) suivante (cf. Théorème 2) :

"Si un corps réel dynamique collapse en tant que corps réel clos, il collapse en tant que corps réel."

1.3 Compléments

Structures purement algébriques et faits strictement vrais

Rappelons qu'une structure dynamique abstraite est dite *purement algébrique* si tous les axiomes sont purement algébriques (universels). Une évaluation dynamique d'une telle structure ne comporte aucun embranchement, et n'introduit aucun paramètre existentiel. Comme nous l'avons déjà remarqué, on est alors entièrement dans le cadre de l'algèbre classique.

Considérons maintenant une structure algébrique dynamique S et une évaluation dynamique de cette structure. Notons $B_1, \ldots, B_k$ les branches de cette évaluation dynamique (considérées depuis la racine jusqu'à la feuille). Nous disons qu'un fait est démontrable "en restant dans la branche B_i" s'il peut être prouvé en prolongeant l'évaluation dynamique de B_i sans faire appel aux axiomes disjonctifs et/ou existentiels. Notez qu'un tel fait est exprimé au moyen des seuls paramètres présents dans B_i, c.-à-d. les paramètres de départ de S et ceux introduits dans la branche en vertu de l'application des axiomes existentiels.

Chaque branche B_i définit une structure algébrique dynamique S_i de même type abstrait que S et qui est une extension de S, obtenue en rajoutant à S comme paramètres de départ, les paramètres existentiels introduits dans B_i, et comme relations de départ, les faits affirmés dans la branche en vertu de l'usage légitime des axiomes.

Si maintenant un fait est démontré en restant dans la branche B_i il est facile de voir qu'il est démontrable dans la structure algébrique dynamique S_i en utilisant uniquement les axiomes universels.

Naturellement, il n'est pas exclu que la structure S_i démontre des faits réellement nouveaux, exprimés uniquement avec les paramètres présents dans B_i mais non démontrables "en restant dans B_i". Un tel fait serait prouvé au moyen d'une évaluation dynamique de S_i utilisant les axiomes non universels.

Cette distinction nous paraît suffisamment importante pour que nous introduisions encore un peu de terminologie.

Nous dirons qu'un fait est *strictement vrai dans une branche* B_i d'une évaluation dynamique de S s'il est prouvable dans la branche sans nouvel usage d'axiomes disjonctifs et/ou existentiels. De même nous dirons qu'un fait est *strictement vrai dans la structure* S s'il est prouvable en restant à la racine de S, c.-à-d. sans aucun usage d'axiomes disjonctifs et/ou existentiels. Autrement dit encore, c'est un fait vrai dans la structure algébrique dynamique obtenue à partir de S en supprimant, dans le type abstrait de S les axiomes disjonctifs et/ou existentiels.

On prendra garde cependant à la sensibilité de tels énoncés à la description choisie pour la structure abstraite. Par exemple, si on omettait l'axiome des anneaux réduits dans la description de la structure abstraite de corps dynamique, alors dans le corps dynamique ayant un seul générateur g, avec la seule relation de départ $g^2 = 0$, le fait $g = 0$ serait vrai mais pas strictement vrai.

Donnons deux exemples simples de faits strictement vrais. Disons que deux termes dans une même branche sont strictement égaux dans la branche si leur égalité est un fait strictement vrai dans la branche en question. On a alors facilement les résultats suivants.

Dans un anneau dynamique, tout terme est strictement égal à un polynome de $\mathbb{Z}[g_1, g_2, ..., g_n]$ où les g_i sont des générateurs de l'anneau.

Dans une branche d'une évaluation dynamique d'un corps, tout terme est strictement égal à un polynome de $\mathbb{Z}[g_1, g_2, ..., g_n, v_1, ..., v_k]$ où les g_i sont des générateurs du corps et les v_j sont des paramètres introduits en vertu de l'axiome des corps.

Les Nullstellensatz de toutes sortes affirment, entre autres, pour certaines structures abstraites, que tous les faits vrais sont strictement vrais, c.-à-d. encore vrais pour des raisons particulièrement simples. Notez cependant le caractère subjectif de cette affirmation, qui dépend de la simplicité du système d'axiomes universels considéré. On pourrait en effet à loisir multiplier les axiomes universels dans le but de rendre tous les faits vrais strictement vrais.

Introduction de nouveaux prédicats, existentiels, par définition

Dans le cadre des structures algébriques dynamiques, on peut introduire de nouveaux prédicats et de nouvelles fonctions, avec des axiomes convenables. Une telle "invention" est considérée comme légitime, non nuisible, dès lors qu'elle ne permet pas de prouver plus de faits (s'ils sont exprimés dans l'ancien langage) qu'avant.
Nous nous occuperons ici seulement des prédicats, et plus spécialement du cas où le prédicat est défini comme équivalent à l'existence d'un objet vérifiant un prédicat déjà défini, au moyen des axiomes convenables.
Nous allons nous convaincre rapidement, sur un exemple, que l'introduction du nouveau prédicat, avec ce type d'axiomes est légitime. Ceci est un phénomène de logique pure et est complètement indépendant de la structure abstraite considérée.

Exemple :
Dans les anneaux, le prédicat "être inversible", que nous noterons $Iv(x)$ peut être introduit avec les deux *axiomes de définition* suivants :

- $Iv(x) \vdash \mathsf{E}\, u\ xu = 1$
- $xy = 1 \vdash Iv(x)$

Si maintenant on donne une évaluation dynamique d'un anneau concret en utilisant le prédicat Iv et les deux axiomes qui vont avec, on remarque les deux choses suivantes :
a) Si un fait $Iv(t)$ est affirmé dans une branche, c'est nécessairement en vertu du deuxième axiome, donc on connaît un terme t' qui vérifie $t.t' = 1$ dans la branche considérée.
b) Si le premier axiome est utilisé sous l'hypothèse $Iv(t)$ établie dans la branche, le paramètre existentiel u qui est introduit peut être remplacé partout par le terme t' qui vérifie l'équation convenable. En définitive, on voit que l'usage du prédicat Iv peut être résumé en l'abréviation du terme t' par la lettre u.

Notez que si au lieu d'utiliser un nouveau nom de prédicat, ici $Iv(x)$, on utilisait les conventions syntaxiques usuelles des théories formelles du premier ordre, on écrirait $\exists u\ xu = 1$ au lieu de $Iv(x)$, et le premier axiome de définition de Iv s'écrirait :

- $\exists u\ xu = 1 \vdash \mathsf{E}\, u\ xu = 1$

Ceci n'est pas une mauvaise plaisanterie, précisément parce qu'avec les structures algébriques dynamiques, un axiome n'a pas pour signification d'être une formule vraie, mais sert à construire les arbres d'évaluation dynamique. De sorte que ni le signe " $\vdash$ " ni les signes " E " et " ou " que l'on trouve après le $\vdash$ ne font partie du langage formel de la théorie du premier ordre.
Notez également la validité des règles suivantes (facilement déduite des axiomes de définition) :

- $(x = y,\ Iv(x)) \vdash Iv(y)$
- $1 = 0 \vdash Iv(x)$

2 Préliminaires

Nous développons dans cette section et la suivante la théorie d'Artin-Schreier, en version classique non constructive d'une part, en version dynamique constructive d'autre part.

Nous espérons convaincre le lecteur que dans les démonstrations parallèles que nous donnons, la partie décisive est la partie commune, le reste n'étant qu'un habillage laissé au libre choix du mathématicien selon ses options philosophiques, ou simplement selon les buts poursuivis.

Les démonstrations classiques semblent sensiblement plus courtes, mais il s'agit essentiellement d'un effet de culture. En effet, les prérequis classiques n'ont pas à être explicités pour un lecteur classique. Une phrase comme : "considérons un facteur irréductible R du polynome P et notons $\mathbf{L}$ le corps $\mathbf{K}[X]/R$" semblerait fort mystérieuse à l'hypothétique mathématicienne de la planète Terris gravitant autour de Sirius qui aurait une culture mathématique purement dynamique et constructive, et cela demanderait pour elle plusieurs lemmes d'explicitation, alors que l'analogue dynamique, que nous sommes obligés d'expliciter relativement en détail sur la planète Terre en 1994, serait un acquis du milieu du cursus mathématique sur Terris.

Nous donnons dans cette section des préliminaires pour développer la théorie d'Artin-Schreier. La théorie classique des corps (avec le théorème non constructif d'existence d'une cloture algébrique) et sur des considérations élémentaires qui relient les corps ordonnés 2−clos et les corps réels 2−clos. Nous devons développer les versions dynamiques et constructives de ces préliminaires.

Dans tous les énoncés qui suivent, l'hypothèse "Soit $\mathbf{K}$ un corps" doit être lue, pour l'énoncé dynamique, comme "Soit $\mathbf{K}$ un corps dynamique". Si, dans le cadre dynamique, nous voulons parler d'un corps classique figé, nous dirons "Soit $\mathbf{K}$ un corps entièrement explicité". Quand nous parlons d'une branche d'un corps dynamique, nous signifions une branche dans une évaluation dynamique de ce corps.

2.1 Quelques résultats de base concernant les évaluations dynamiques de corps

Si un corps est engendré par une famille d'éléments, tout élément du corps est une fraction rationnelle, de dénominateur non nul, en les générateurs. Nous aurons besoin de l'analogue dynamique de cette propriété. Comme nous n'avons introduit ni un opérateur de passage à l'inverse, ni le prédicat opposé à l'égalité dans notre définition de la structure de corps dynamique, cela réclame quelques périphrases.

Proposition 2.1 *Soit* $\mathbf{K}$ *un corps.*

(classique)
Si $\mathbf{K}$ *est engendré comme corps par une famille d'éléments, tout élément du corps est une fraction rationnelle, de dénominateur non nul, en les générateurs.*

(dynamique)
Pour tout terme t dans une branche de $\mathbf{K}$*, si $g_1, g_2, ..., g_n$ sont les générateurs de* $\mathbf{K}$ *actifs dans la branche, on peut construire deux polynomes Q et R de $\mathbb{Z}[g_1, g_2, ..., g_n]$, un polynome u de $\mathbb{Z}[g_1, ..., g_n, v_1, ..., v_k]$ où les v_j sont les autres paramètres actifs dans la branche, et un entier m avec les égalités suivantes qui sont strictement vraies dans la branche : $t = u^m.Q$ et $u.R = 1$.*
En outre, les polynomes R et u peuvent être choisis une fois pour toutes tant qu'on reste dans la branche considérée.
En résumé, toute évaluation dynamique de $\mathbf{K}$ *peut être remplacée par une évaluation dynamique*

où le seul usage de l'axiome des corps est fait avec des éléments de l'anneau $\mathbb{Z}[\mathbf{g}]$ *librement engendré par les générateurs.*

Preuve On raisonne par induction sur le nombre k de paramètres existentiels introduits dans la branche. La preuve résulte du "même" calcul que dans le cas d'un corps ordinaire. A priori, dans la branche considérée, le terme t est strictement égal à un polynome :

$$w(g_1, ..., g_n, v_1, ..., v_k) \in \mathbb{Z}[\mathbf{g}, v_1, ..., v_k].$$

On écrit w comme polynome en v_k, avec pour coefficients des polynomes $p_i(\mathbf{g}, v_1, ..., v_{k-1})$.
Le dernier paramètre v_k introduit en application de l'axiome des corps vérifie une équation : $v_k.w_k(\mathbf{g}, v_1, ..., v_{k-1}) = 1$. On applique alors l'hypothèse de récurrence aux polynomes p_i et à w_k. Les détails sont laissés à la lectrice.
Pour la remarque finale, l'évaluation dynamique qui remplace celle donnée au départ permet de démontrer les mêmes faits. Notez qu'elle a aussi la même structure arborescente. □

Remarque 2.2 On pourra utiliser, en application de la proposition précédente, la notation Q/R^m pour le terme t, en ayant conscience qu'il s'agit d'un léger abus de notation.

Terminologie Désormais, l'expression "*soit un élément a d'un corps dynamique* $\mathbf{K}$" signifiera que a est un polynome à coefficients entiers en les générateurs, tandis que l'expression "*soit un élément a dans une branche d'un corps dynamique* $\mathbf{K}$" signifiera que a est une fraction rationnelle à coefficients entiers en les générateurs, le sens de cette expression étant explicité par la proposition précédente.

Définition 2.3 (extensions algébriques finies)
(classique) *Étant donné un corps* $\mathbf{K}$*, nous appellerons* extension algébrique simple *de* $\mathbf{K}$ *un surcorps* $\mathbf{L}$ *de* $\mathbf{K}$ *engendré par un élément* α *vérifiant une relation de dépendance algébrique* $\alpha^n + x_{n-1}\alpha^{n-1} + \cdots + x_1\alpha + x_0 = 0$*, où les* x_i *sont des éléments de* $\mathbf{K}$*. Nous noterons* $\mathbf{K} -_{as} \mathbf{L}$*.*

(dynamique) *Étant donné un corps dynamique* $\mathbf{K}$*, nous appellerons* extension algébrique simple *de* $\mathbf{K}$ *un corps dynamique* $\mathbf{L} = \mathbf{K} \oplus \{\alpha;\ \alpha^n + x_{n-1}\alpha^{n-1} + \cdots + x_1\alpha + x_0 = 0\}$*, où les* x_i *sont des éléments de* $\mathbf{K}$*. Nous noterons* $\mathbf{K} -_{as} \mathbf{L}$*.*

(classique ou dynamique) *De même, nous appellerons* extension algébrique finie *de* $\mathbf{K}$ *un corps* $\mathbf{L}$ *donné avec une chaîne d'extensions algébriques simples :*

$$\mathbf{K} = \mathbf{L}_0 -_{as} \mathbf{L}_1 -_{as} \ldots -_{as} \mathbf{L}_{k-1} -_{as} \mathbf{L}_k = \mathbf{L}$$

Nous noterons alors $\mathbf{K} -_{af} \mathbf{L}$ *ou simplement* $\mathbf{K} - \mathbf{L}$ *.*

Nous commençons par l'explicitation d'un fait classique assez banal en termes d'évaluation dynamique.

Proposition 2.4 *Soit* $\mathbf{K} - \mathbf{L}$ *une extension algébrique finie de corps, obtenue en rajoutant des éléments* α_i*.*

(classique) *Le corps* $\mathbf{L}$ *est aussi égal à la* $\mathbf{K}$*-algèbre* $\mathbf{K}[(\alpha_i)]$*.*

(dynamique) *Toute évaluation dynamique de* $\mathbf{L}$ *peut être remplacée par une évaluation dynamique où l'axiome des corps n'est utilisé qu'avec des éléments de* $\mathbf{K}$*.*
Dans une telle évaluation dynamique, tout terme est strictement égal à un polynome en les nouveaux générateurs α_i*, polynome dont les coefficients sont des éléments de* $\mathbf{K}$ *dans la branche correspondante.*

Plus précisément, le remplacement se fait à chaque noeud où est appliqué l'axiome des corps, en partant depuis la racine. Chaque embranchement est remplacé par une arborescence, et à chaque feuille de cette arborescence est prouvée l'une des alternatives de l'embranchement. De sorte que la nouvelle évaluation dynamique est capable de prouver tous les faits prouvés par l'ancienne.
En outre, on peut supposer que l'usage de l'axiome des corps avec les éléments de $\mathbf{K}$ *est effectué avant tout autre usage des axiomes.*

Preuve
(classique)
Il suffit de considérer le cas d'une extension algébrique simple. Soit $P(X)$ le polynome unitaire qui annule α par hypothèse. On considère P_1, un diviseur unitaire de P, de degré minimum, qui annule α. Alors P_1 est irréductible dans $\mathbf{K}[X]$. Soit maintenant $R(\alpha)$ un élément non nul de $\mathbf{K}[\alpha]$. Nous devons montrer que $R(\alpha)$ est inversible dans $\mathbf{K}[\alpha]$. Comme $R(X)$ n'est pas multiple de $P_1(X)$ et que P_1 est irréductible, P_1 et R sont premiers entre eux et il y a une relation de Bezout dans $\mathbf{K}[X]$:

$$A(X)P_1(X) + B(X)R(X) = 1$$

Et donc $B(\alpha)R(\alpha) = 1$.
(dynamique)
La dernière remarque résulte de la première affirmation, puisque l'axiome des corps est le seul qui introduise de nouveaux paramètres, et qu'il ne réclame la vérification d'aucune hypothèse préalable pour être appliqué. Démontrons la première affirmation.
Il suffit de montrer comment on peut effectuer le remplacement dans le cas du premier usage de l'axiome des corps dans $\mathbf{L} = \mathbf{K} \oplus \{\alpha;\ P(\alpha) = 0\}$ avec P unitaire.
On considère un polynome $R(\alpha)$ dont les coefficients sont des éléments de $\mathbf{K}$ définis là où on se trouve. On a un embranchement, avec $R(\alpha) = 0$ dans la première branche, et $u.R(\alpha) = 1$ dans la deuxième, où u est un nouveau paramètre existentiel. C'est cet embranchement que nous allons remplacer par une arborescence dans laquelle l'axiome des corps ne sera appliqué qu'à des éléments de $\mathbf{K}$. D'après la proposition 2.1, on pourra même n'appliquer l'axiome des corps qu'avec des éléments de $\mathbb{Z}[\mathbf{g}]$ (où les g_i sont les générateurs de $\mathbf{K}$).
On commence par se ramener au cas où le degré formel de R en α est strictement inférieur à celui de P puisque la division par P correspond à une égalité strictement vraie. Si, après cette division, $R(\alpha)$ ne mentionne pas explicitement α, c.-à-d. est de degré 0 en α, on peut appliquer l'axiome des corps avec cet élément de $\mathbf{K}$.
Sinon, on ouvre une première arborescence qui nous permet de "fixer" le degré de R en procédant comme suit. Nous notons r_j le coefficient de degré j dans R et m le degré de R. Nous allons ouvrir des branches et sous-branches de manière qu'à chaque extrémité, le degré de R soit assuré (R est identiquement nul ou bien un coefficient de R est connu inversible, et les coefficients de degrés supérieurs sont connus nuls). Cela se fait comme suit.
On ouvre l'embranchement $r_m = 0$ ou r_m inversible.
Dans la branche $r_m = 0$ on ouvre l'embranchement $r_{m-1} = 0$ ou r_{m-1} inversible.
. . . . . .
Dans la branche $r_1 = 0$ on ouvre l'embranchement $r_0 = 0$ ou r_0 inversible.
À ces deux dernières feuilles, on a respectivement $R(\alpha) = 0$ et $R(\alpha)$ inversible, de sorte qu'on est satisfait. Pour ce qui concerne les autres feuilles, on peut multiplier R par l'inverse du coefficient dominant, ce qui nous ramène au cas où R est unitaire de degré strictement positif et inférieur au degré de P. On effectue alors la division de P par R et on obtient un reste S. De nouveau,

on peut ouvrir une arborescence aux feuilles de laquelle, ou bien $S(\alpha)$ est identiquement nul, ou bien il est de degré connu, son coefficient dominant étant inversible. À la feuille où $S(\alpha)$ est identiquement nul, on a explicité $R(X)$ comme diviseur de $P(X)$. À la feuille où $S(\alpha)$ est de degré 0 et inversible, on a explicité une relation de Bezout $P(X) - R(X)B(X) = a$ élément inversible de $\mathbf{K}$, de sorte qu'on a aussi $R(\alpha)B(\alpha) = -a$ et donc $R(\alpha)$ inversible. En poursuivant de la sorte, on exécute en entier (toutes les possibilités de) l'algorithme d'Euclide démarrant avec P et R. À chaque feuille de l'arborescence complète, on n'a utilisé l'axiome des corps qu'avec des éléments de $\mathbf{K}$, et un pgcd G de P et R a été explicité avec une relation de Bezout et des relations de divisibilité :

$$A(X)P(X) + B(X)R(X) = G(X), \quad G(X)P_1(X) = P(X), \quad G(X)R_1(X) = R(X)$$

en outre le polynome G est non identiquement nul, son coefficient dominant est connu inversible, et le coefficient dominant de P_1 est lui aussi connu inversible.
Aux feuilles où G est de degré 0 on a établi une relation $R(\alpha)B(\alpha) = a$ inversible, donc $R(\alpha)$ inversible, de sorte qu'on est satisfait.
Aux feuilles où G est de degré strictement positif, on a :

$$G(\alpha)P_1(\alpha) = P(\alpha) = 0, \quad G(\alpha)R_1(\alpha) = R(\alpha)$$

On ouvre donc, en utilisant l'axiome de l'absence de diviseurs de zéro (avec des éléments de $\mathbf{K}[\alpha]$), un embranchement. Dans la première branche $G(\alpha) = 0$ et donc aussi $R(\alpha) = 0$. Dans la deuxième branche $P_1(\alpha) = 0$, avec le coefficient dominant de P_1 connu inversible. Si a est l'inverse de ce coefficient, on est ramené à la situation initiale, aP_1 remplaçant P, mais avec le degré de aP_1 strictement inférieur à celui de P. De sorte que tout est maintenant clair par induction sur le degré de P. □

Remarques 2.5
1) Cela peut sembler bien lourd. Mais c'est le prix à payer lorsque l'on n'a pas le moyen de décomposer un polynome en facteurs irréductibles. D'ailleurs en pratique, même lorsqu'un algorithme de factorisation existe, cela peut s'avérer plus coûteux de travailler sur des structures de corps figées, où chaque nouvelle extension algébrique donne lieu à un calcul de plus en plus laborieux, plutôt que sur une structure algébrique dynamique, où la seule difficulté algorithmique est l'explosion de l'arbre des disjonctions. C'est en tout cas le pari du système d'évaluation dynamique D5. En pratique, on peut d'ailleurs alléger considérablement l'arborescence en utilisant la théorie des polynomes sous-résultants. Il y a en outre des cas où le corps dynamique $\mathbf{K}$ est relativement bien explicité, ce qui fait que certains embranchements peuvent être évités parce qu'on sait que tel ou tel élément soumis à l'axiome des corps est en fait nul, ou inversible dans $\mathbf{K}$. Comme on raisonne par induction sur le nombre des α_i introduits, si on démarre avec un corps entièrement explicité mais sans algorithme de factorisation des polynomes, on aura nécessairement à gérer une structure dynamique plutôt qu'une collection finie de corps figés extensions algébriques de $\mathbf{K}$.
2) Dans la théorie d'Artin-Schreier, nous utiliserons la proposition 2.4 uniquement pour les extensions $\mathbf{L} = \mathbf{K} \oplus \{\alpha;\ \alpha^2 = a\}$. La lectrice pourra s'entrainer à écrire la preuve dans ce cas, qui est beaucoup plus simple.
Nous utiliserons aussi le fait suivant, contenu dans la preuve de la proposition 2.4 :
"on peut exécuter dynamiquement l'algorithme d'Euclide pour le pgcd de deux polynomes"
c.-à-d. encore : si $P(X)$ et $R(X)$ sont deux polynomes à coefficients dans un corps dynamique $\mathbf{K}$, avec P unitaire et de degré ≥ 2, alors on peut construire une évaluation dynamique de $\mathbf{K}$ telle qu'à chaque feuille soit explicité un pgcd unitaire de P et R, de degré ≥ 0.

Le théorème suivant ne nous est pas utile pour la théorie d'Artin-Schreier, mais il est intéressant en soi.

Théorème 1 (existence d'extensions algébriques et de clotures algébriques)
(classique)
a) Soit $\mathbf{K}$ *un corps et* $(P_i)_{i=1,\dots,n}$ *des polynomes à coefficients dans* $\mathbf{K}$*, chaque* P_i *étant unitaire et de degré* > 0 *en une nouvelle variable* X_i*. Alors il existe une extension algébrique* $\mathbf{L}$ *de* $\mathbf{K}$ *engendrée par des* α_i *vérifiant les équations* $P_i(\alpha_1, \dots \alpha_i) = 0$*.*
b) Tout corps $\mathbf{K}$ *peut être plongé dans un corps algébriquement clos.*
(dynamique)
a) Soit $\mathbf{K} - \mathbf{L}$ *une extension algébrique finie de corps dynamiques. Si un fait ne concernant que des éléments de* $\mathbf{K}$ *est établi dans* $\mathbf{L}$*, il peut également être établi dans* $\mathbf{K}$*. En particulier, le corps* $\mathbf{L}$ *collapse si et seulement si le corps* $\mathbf{K}$ *collapse.*
b) Un corps dynamique $\mathbf{K}$ *collapse comme corps algébriquement clos dynamique si et seulement si il collapse comme corps dynamique.*

Preuve
(classique) Pour le (a), il suffit de traiter le cas d'un seul polynome $P(X)$. Alors, par omniscience classique, "il existe" un diviseur $P_1(X)$ de degré minimum du polynome P, ce diviseur est irréductible et l'anneau $\mathbf{K}[X]/(P(X))$ est un corps.
Le (b) résulte du (a) par le lemme de Zorn, ou plus modestement par une utilisation judicieuse de l'axiome de l'idéal premier.

(dynamique) Le (b) résulte clairement du (a). Il suffit de montrer le (a) pour une extension algébrique simple $\mathbf{L} = \mathbf{K} \oplus \{\alpha;\ P(\alpha) = 0\}$ avec P unitaire.
Ceci est "moralement" clair, par l'argument que, à partir du moment où, par la proposition précédente, l'axiome des corps n'est utilisé qu'avec des éléments de $\mathbf{K}$, tous les calculs se passent en fait dans $\mathbf{K}$.
Nous devons expliciter cet argument moral en une preuve convaincante.
Nous nous reportons à la preuve de 2.4 et nous voyons que nous avons en fait plus de détails que ceux affirmés dans l'énoncé. Précisément, regardons, dans un arbre d'évaluation dynamique de $\mathbf{L}$ transformé selon la méthode 2.4, quelles sont les hypothèses $V(\alpha) = 0$, rajoutées en vertu de l'axiome de l'absence des diviseurs de zéro, actives dans une branche donnée.
On voit que ce sont des hypothèses $G_1(\alpha) = 0$, ..., $G_r(\alpha) = 0$ introduites les unes après les autres, avec les faits suivants validés au fur et à mesure $G_1(X)$ divise $P(X)$, $G_2(X)$ divise $G_1(X)$, etc... En conséquence, tout fait $R(\alpha) = 0$ à une feuille quelconque de l'arbre d'évaluation dynamique obtenu est établi à cet endroit en vertu d'une égalité de polynomes $R(X) = G_r(X).T(X)$ dans une branche où a été introduite l'hypothèse $G_r(\alpha) = 0$, avec G_r un diviseur explicite de P, de degré strictement positif. En effet, c'est le cas lorsqu'on remplace l'usage de l'axiome des corps avec un polynome $R(\alpha)$ par l'usage de l'axiome de l'absence des diviseurs de zéro avec un polynome diviseur de P, et cela se maintient lorsqu'on prouve $R(\alpha) = 0$ par de pures manipulations algébriques (c.-à-d. lorsqu'on utilise les axiomes des anneaux commutatifs). En particulier pour tout élément r de $\mathbf{K}$ (c.-à-d. pour tout élément de $\mathbb{Z}[\mathbf{g}]$), si on a établi $r = 0$ en un point d'une évaluation dynamique de $\mathbf{L}$, alors après la transformation de l'arbre proposée en 2.4, le fait $r = 0$ résulte d'une égalité de polynomes $r = G(X)T(X)$, en tenant compte de l'hypothèse supplémentaire $G(\alpha) = 0$, introduite dans l'arbre par l'usage de l'axiome de l'absence des diviseurs de zéro dans $\mathbf{L}$. Mais cette égalité $r = G(X)T(X)$ est quant à elle établie uniquement par des calculs dans $\mathbf{K}$, et comme à cet endroit de l'arbre, le coefficient dominant de G est inversible, cela implique aussi facilement que $r = 0$ sans avoir à

utiliser l'hypothèse $G(\alpha) = 0$ (on voit de proche en proche que tous les coefficients de T sont nécessairement nuls à cet endroit de l'arbre).
En conclusion, si un fait $r = 0$ est établi à toutes les feuilles d'une évaluation dynamique de $\mathbf{L}$, après les transformations de cet arbre selon la proposition 1.6, on obtient une évaluation dynamique de $\mathbf{K}$ qui établit $r = 0$ à toutes ses feuilles. □

Remarques 2.6
1) La lectrice aura pris plaisir, nous l'espérons, à la surprise procurée par l'interprétation dynamique des énoncés classiques élémentaires de la théorie des extensions algébriques. Que ce soit là la vraie signification des énoncés classiques lui semblera sans doute une affirmation téméraire, et en tout cas bien encombrante. Quant à nous, n'ayant jamais réussi auparavant à trouver une *signification* claire pour la théorie classique, nous nous contenterons de celle livrée ci-dessus, la seule que nous ayons trouvé pour le moment[4].

2) Le théorème 1 dynamique (b) possède une preuve quasiment instantanée "par Nullstellensatz". On vérifie tout d'abord qu'on ne change pas les conditions de collapsus lorsqu'on rajoute aux axiomes des anneaux l'axiome des corps (la preuve recopie ce qu'on a l'habitude d'appeler le truc de Rabinovitch). On vérifie ensuite qu'on ne change pas les conditions de collapsus lorsqu'on rajoute aux axiomes des corps les axiomes de cloture algébrique (compte tenu de la forme particulièrement simple du collapsus d'un anneau, la preuve est essentiellement une division euclidienne). Cependant, dans l'article présent, nous ne sommes pas intéressés par les preuves télégraphiques, mais par la traduction pas à pas des preuves classiques.

2.2 Quelques résultats élémentaires concernant les corps ordonnés dynamiques

Dans cette section, on se contente de laisser le lecteur vérifier que les preuves usuelles classiques sont suffisamment élémentaires pour pouvoir être immédiatement traduites en preuves constructives concernant les structures algébriques dynamiques correspondantes. On démontre d'abord quelques règles valides dans un corps ordonné.

- les axiomes de réalité
- $x + y \geq 0 \vdash (x \geq 0 \quad \text{ou} \quad y \geq 0)$
- $xy \leq 0 \vdash (x \leq 0 \quad \text{ou} \quad y \leq 0)$

On démontre ensuite :
a) Dans un anneau réel pythagoricien, le prédicat existentiel $Sq(x)$ défini comme signifiant "x est un carré" vérifie les axiomes du prédicat $x \geq 0$ dans un anneau partiellement ordonné.
b) Un corps réel 2−clos vérifie l'axiome de Pythagore. Avec le prédicat $x \geq 0$ pris comme une autre notation pour le prédicat défini $Sq(x)$ on obtient alors un corps ordonné 2−clos.
c) Un corps ordonné 2−clos est réel 2−clos, et dans un corps ordonné 2−clos, le prédicat ≥ 0 est équivalent au prédicat défini $Sq(x)$.
d) Dans un corps ordonné 2−clos, est valide la règle de simplification suivante

- $(x \geq 0,\ (1 + x)y \geq 0) \vdash y \geq 0$

En conséquence de (a), (b) et (c), il y a équivalence entre les notions de corps ordonné 2−clos et de corps réel 2−clos. En particulier, une évaluation dynamique de corps comme corps ordonné 2−clos peut être transformée en une évaluation dynamique comme corps réel 2−clos, qui prouve les mêmes faits dès qu'ils ne font pas appel au prédicat $x \geq 0$.

[4] et au diable des accords du participe passé.

3 La théorie d'Artin-Schreier

Nous avons besoin dans la théorie d'Artin-Schreier de parler de sommes de carrés. Nous pourrions pour cela introduire un prédicat $Ssq(x)$ avec les axiomes suivants :

- $\vdash Ssq(x^2)$
- $(Ssq(x),\ Ssq(y)) \vdash Ssq(x+y)$
- $(Ssq(x),\ Ssq(y)) \vdash Ssq(xy)$

Dans la nouvelle structure algébrique dynamique obtenue, il n'est pas difficile de voir qu'un fait $Ssq(t)$ établi dans une branche d'une évaluation dynamique peut toujours être "confirmé" par un fait $t =$ une somme de carrés, établi au même endroit.
D'autre part, vus les axiomes, qui ne permettent jamais de tirer la moindre conséquence en matière d'égalité ou de relation d'ordre, à partir de faits $Ssq(t_i)$, l'introduction du prédicat Ssq(x) avec les axiomes donnés ci-dessus ne modifie pas les faits établis en matière d'égalité ou de relation d'ordre.
En pratique, nous nous passerons de ce prédicat, et, quitte à nous écarter un tout petit peu des conventions de l'évaluation dynamique concernant les faits, nous nous contenterons de dire qu'une évaluation dynamique prouve qu'un terme t (défini à la racine) est une somme de carrés si à chaque feuille de l'arbre, un fait $t =$ une somme de carrés, est établi.

Dans les preuves "dynamiques" nous utiliserons librement les résultats concernant les extensions algébriques établis à la section précédente.
Nous utiliserons aussi implicitement le résultat suivant, qui se démontre aisément en prenant le "produit cartésien" de deux évaluations dynamiques. Si une structure algébrique dynamique prouve séparément deux faits, elle prouve également leur conjonction, c.-à-d. qu'on peut construire une évaluation dynamique de cette structure telle que, à la fin de chaque branche, les deux faits soient établis en vertu de l'utilisation légitime des axiomes.

Dans tous les énoncés qui suivent, l'hypothèse "Soit **K** un corps" doit être lue, pour l'énoncé dynamique, comme "Soit **K** un corps dynamique". Si, dans le cadre dynamique, nous voulons parler d'un corps classique figé, nous dirons "Soit **K** un corps entièrement explicité".

Proposition 3.1 *Soit* **K** *un corps.*

(classique)
K *est réel si et seulement si* -1 *n'est pas une somme de carrés*

(dynamique)
K *collapse comme corps réel dynamique si et seulement si, comme corps dynamique, il prouve que* -1 *est une somme de carrés*

Preuve *(classique)*
Si -1 est une somme de carrés **K** ne peut être réel car cela impliquerait $1 = 0$. Si -1 n'est pas une somme de carrés et si $a_1^2 + \cdots + a_n^2 = 0$, montrons que $a_1 = 0$. Si ce n'était pas le cas, on multiplierait par l'inverse de a_1^2 et on exprimerait -1 comme somme de carrés.

(dynamique)
Supposons tout d'abord qu'une évaluation dynamique de **K** en tant que corps prouve que -1 est une somme de carrés. Dans chacune des branches, on peut continuer l'évaluation dynamique de **K** en tant que corps réel en utilisant l'axiome de réalité, ce qui permet d'établir le fait $1 = 0$. Ainsi toutes les branches meurent, et **K** collapse comme corps réel. Inversement, supposons que **K** collapse comme corps réel, et considérons l'évaluation dynamique correspondante. Nous

allons à partir de cela construire une évaluation dynamique de $\mathbf{K}$ comme corps, de la manière suivante. On considère toutes les utilisations de l'axiome de réalité, en commençant par les plus proches des feuilles et en remontant l'arbre jusqu'à la racine. Chaque fois que l'axiome de réalité est utilisé pour établir un fait $a_1 = 0$ à partir d'un fait $a_1^2 + a_2^2 + ... + a_n^2 = 0$ nous supprimons cette utilisation de l'axiome de réalité et, en remplacement nous ouvrons deux branches $a_1 = 0$ et $a_1 v = 1$, où v est un paramètre non encore utilisé, en application de l'axiome des corps. Dans la première branche, on se retrouve dans la situation précédente où on avait utilisé l'axiome de réalité, et on poursuit avec l'ancienne branche correspondante. Dans la deuxième branche, on obtient après multiplication par v^2 le fait $1 + (va_2)^2 + \cdots + (va_n)^2 = 0$. Donc -1 est une somme de carrés et on arrête la branche à cet endroit. En fin de compte, on obtient une évaluation dynamique de corps pour laquelle toutes les branches se terminent par un fait "-1 est une somme de carrés" (le fait $1 = 0$ qui termine les branches qui meurent peut être suivi par $-1 = 0^2$) □

Dans l'énoncé suivant, on parle d'un élément inversible d'un corps $\mathbf{K}$. Pour l'interprétation dynamique, cela signifie que a est défini à la racine, c.-à-d. est un polynome à coefficients entiers en les générateurs du corps dynamique $\mathbf{K}$ et que pour un autre élément a' du même type, l'égalité $a.a' = 1$ est vraie dans $\mathbf{K}$.

Proposition 3.2 *Soit* $\mathbf{K}$ *un corps et* a *un élément inversible de* $\mathbf{K}$.

(classique)
Supposons $\mathbf{K}$ *réel, alors* $\mathbf{K}$ *possède une extension réelle où* a *est un carré si et seulement si* $-a$ *n'est pas une somme de carrés dans* $\mathbf{K}$

(dynamique)
$\mathbf{K} \oplus \{\alpha;\ \alpha^2 = a\}$ *collapse comme corps réel dynamique si et seulement si comme corps réel dynamique,* $\mathbf{K}$ *prouve que* $-a$ *est une somme de carrés*

Preuve *(classique)*
Si a est un carré α^2 dans une extension réelle $\mathbf{L}$ de $\mathbf{K}$, $-a$ n'est pas une somme de carrés dans $\mathbf{K}$ parce que sinon, comme $\mathbf{L}$ est réel, α est nul, et donc a aussi, ce qui est absurde. Supposons maintenant que $-a$ n'est pas une somme de carrés dans $\mathbf{K}$. Si a est un carré α^2 dans $\mathbf{K}$, le corps $\mathbf{K}$ convient. Si a n'est pas un carré dans $\mathbf{K}$, soit $\mathbf{L} = \mathbf{K}[X]/(X^2 - a)$ et α la classe de X dans $\mathbf{L}$. Il suffit de montrer que $\mathbf{L}$ est réel. Si ce n'était pas le cas, on aurait, avec les u_i et v_i dans $\mathbf{K}$:

$$1 + \sum_i (u_i + \alpha v_i)^2 = 0 \qquad (\text{dans } \mathbf{L})$$

D'où

$$1 + \sum_i u_i^2 + a \sum_i v_i^2 = 0 \qquad (\text{dans } \mathbf{K})$$

Comme $1 + \sum_i u_i^2$ est non nul, il en va de même pour $v = \sum_i v_i^2$ et donc

$$-a = (1/v)^2 (1 + \sum_i u_i^2)(\sum_i v_i^2)$$

contrairement à l'hypothèse.

(dynamique)
Si une évaluation dynamique de $\mathbf{K}$ comme corps réel prouve que $-a$ est une somme de carrés, alors la même évaluation dynamique, pour la présentation $\mathbf{K} \oplus \{\alpha;\ \alpha^2 = a\}$, se poursuit (dans chaque branche) en prouvant $\alpha = 0$, puis $a = 0$ puis $1 = 0$ puisque $a.a' = 1$ est vraie dans $\mathbf{K}$.

Supposons maintenant que $\mathbf{L} = \mathbf{K} \oplus \{\alpha;\ \alpha^2 = a\}$ collapse comme corps réel dynamique. Par la proposition 3.1, une évaluation dynamique de $\mathbf{L}$ comme corps prouve que -1 est une somme de carrés. Cette évaluation dynamique de $\mathbf{L}$ peut être remplacée par une évaluation dynamique où le seul usage de l'axiome des corps est fait avec des éléments de $\mathbf{K}$.
Considérons une branche arbitraire de cette évaluation dynamique, depuis la racine jusqu'à la feuille. Elle se termine par

$$1 + \sum_i v_i^2 = 0 \qquad (1)$$

Les termes v_i sont strictement égaux à des termes $u_i + \alpha v_i$ où u_i et v_i sont des éléments (dans cette branche) de $\mathbf{K}$. On obtient donc :

$$\left(1 + \sum_i u_i^2 + a \sum_i v_i^2\right) = -2\alpha \sum_i u_i v_i \quad (2)$$

On ouvre alors deux sous branches, en utilisant l'axiome des corps, en disant que $-2 \sum_i u_i v_i$ est inversible ou nul.
Dans la première sous-branche, on introduit w avec $(-2 \sum_i u_i v_i)\, w = 1$, on a comme conséquence de (2) : $\alpha = w(1 + \sum_i u_i^2 + a \sum_i v_i^2)$.
L'équation $1 + \sum_i v_i^2 = 0$ donne alors

$$-1 = \sum_i \left(u_i + w \left(1 + \sum_i u_i^2 + a \sum_i v_i^2\right) v_i\right)^2$$

et -1 est une somme de carrés dans cette branche de $\mathbf{K}$. Cette branche meurt pour le corps réel dynamique $\mathbf{K}$, et a fortiori, $-a$ est nul donc égal à une somme de carrés.
Dans la deuxième sous-branche, $-2 \sum_i u_i v_i = 0$, donc (2) donne $-1 = \sum_i u_i^2 + a \sum_i v_i^2$.
On ouvre maintenant deux sous-sous-branches selon que $v = \sum_i v_i^2$ est inversible ou nul.
Dans la première $-a$ est une somme de carrés dans $\mathbf{K}$: $-a = (1/v)^2(1 + \sum_i u_i^2)(\sum_i v_i^2)$.
Dans la deuxième -1 est une somme de carrés dans $\mathbf{K}$. □

Remarque 3.3 On a établi un résultat technique un peu plus précis que celui annoncé. Si $\mathbf{L}$ collapse comme corps réel dynamique, alors une évaluation dynamique de $\mathbf{K}$ comme corps "tout court" prouve dans chacune de ses branches que $-a$ ou -1 est une somme de carrés.

Une extension d'un corps est dite 2−algébrique, si elle est algébrique et si tout élément de l'extension peut être obtenu à l'intérieur d'une tour de sous-extensions, chaque étage de la tour étant de degré 2.

Proposition 3.4 *Soit* $\mathbf{K}$ *un corps.*

(classique)
si $\mathbf{K}$ *est réel il peut être plongé dans une extension* 2−*algébrique qui est un corps réel* 2−*clos.*

(dynamique)
si $\mathbf{K}$ *collapse comme corps réel* 2−*clos dynamique, alors il collapse comme corps réel.*

Preuve *(classique)*
Par Zorn, on sait qu'il existe une extension réelle 2−algébrique maximale de $\mathbf{K}$. On utilise la proposition 3.2 pour montrer que cette extension est réelle 2−close. En effet, dans un corps réel, si pour un élément a, a et $-a$ sont des sommes de carrés, a est nul, et sinon on peut introduire

(si elle n'existait pas encore) la racine carrée de $-a$ ou celle de a sans perdre le caractère de réalité, ni celui de 2-extension algébrique.

(dynamique)
Il suffit de montrer que si une utilisation de l'axiome de 2−cloture fournit un collapsus d'un corps réel dynamique, on peut aussi obtenir le collapsus sans cela. Supposons qu'on a introduit α vérifiant $\alpha^4 = a^2$ c.-à-d. $(a - \alpha^2).(a + \alpha^2) = 0$. On va prouver qu'il y a collapsus sans l'usage de cet axiome. Ouvrons une branche avec $a = 0$ et une autre avec a inversible. La branche avec $a = 0$ collapse : on remplace partout a et α par 0 dans le collapsus avec $\alpha^4 = a^2$.
En ce qui concerne la branche "a inversible" on fait la remarque suivante.
On peut à partir de là dédoubler l'arbre. Dans le premier arbre on remplace $\alpha^4 = a^2$ par $a = \alpha^2$, dans le second, par $-a = \alpha^2$. Puisqu'il y avait collapsus avec $\alpha^4 = a^2$, il y a collapsus dans chacun des deux arbres. Par la proposition 3.2 le premier arbre peut être remplacé par un arbre qui prouve, sans l'hypothèse $a = \alpha^2$, que $-a$ est une somme de carrés, et le second peut être remplacé par un arbre qui prouve, sans l'hypothèse $-a = \alpha^2$, que a est une somme de carrés. Bref, sans l'usage de l'axiome de 2−cloture, le corps réel dynamique prouve, dans la branche "a inversible", que a et $-a$ sont des sommes de carrés. On déduit alors, par l'axiome de réalité que a est nul, ce qui fournit le collapsus de cette branche. □

Proposition 3.5 *Soit* $\mathbf{K}$ *un corps,* a *et* b *deux éléments de* $\mathbf{K}$*,* $P(X)$ *un polynome de* $\mathbf{K}[X]$*.*
(classique)
si $\mathbf{K}$ *est réel* 2−*clos et* $P(a).P(b) \leq 0$ *alors il existe une extension réelle* 2−*close de* $\mathbf{K}$ *dans laquelle* P *admet un zéro.*

(dynamique)
si $\mathbf{K} \oplus \{\alpha;\ P(\alpha) = 0\}$ *collapse comme corps réel* 2−*clos, alors* $\mathbf{K} \oplus \{\ ;\ P(a).P(b) \leq 0\}$ *collapse comme corps réel* 2−*clos.*

Preuve
(classique)
On procède par récurrence sur le degré de P. (le corps $\mathbf{K}$ n'est pas fixé dans l'hypothèse de récurrence). Il suffit de montrer l'existence d'un corps réel $\mathbf{L}$ dans lequel P admet un zéro.
Si P est une constante, c'est la constante nulle puisque $P^2 \leq 0$, et le corps $\mathbf{K}$ convient.
Si P est de degré 1, le corps $\mathbf{K}$ convient.
Soit maintenant P de degré ≥ 2.
— Si P n'est pas irréductible dans $\mathbf{K}[X]$, il y a un facteur irréductible R de P dans $\mathbf{K}[X]$ pour lequel $R(a).R(b) \leq 0$. Par hypothèse de récurrence R admet un zéro dans une extension ordonnée $\mathbf{L}$ de $\mathbf{K}$, donc P aussi.
— Si P est irréductible dans $\mathbf{K}[X]$, soit $\mathbf{L}$ le corps $\mathbf{K}[X]/P(X)$. On va montrer par l'absurde que $\mathbf{L}$ est réel. Supposons que $\mathbf{L}$ ne soit pas réel.
Écrivons dans $\mathbf{L}$: 1+ une somme de carrés = 0. Remontons dans $\mathbf{K}[X]$, cela donne

$$1 + \sum_i A_i(X)^2 = P(X)S(X)$$

Réduisons les A_i modulo P. Il vient :

$$1 + \sum_i B_i(X)^2 = P(X)T(X)$$

Avec maintenant $\deg(T) \leq \deg(P) - 2$. En outre, vue l'égalité précédente, $P(a).T(a) > 0$ et $P(b).T(b) > 0$, donc $T(a).T(b) \leq 0$. Par hypothèse de récurrence, soit $\mathbf{L}'$ une extension

ordonnée de $\mathbf{K}$ où T admet un zéro α. Alors dans $\mathbf{L}'$ on obtient $1+\sum_i B_i(\alpha)^2=0$, ce qui est bien absurde.

(dynamique)

Nous raisonnons par induction sur le degré formel de P.

Les cas des degrés 0 et 1 sont faciles. On suppose maintenant $\deg(P)=p\geq 2$.

Si $\mathbf{K}\oplus\{\alpha;\ P(\alpha)=0\}$ collapse comme corps réel 2−clos dynamique, il collapse également comme corps réel. Notre but est de montrer que $\mathbf{K}\oplus\{\ ;\ P(a).P(b)\leq 0\}$ collapse comme corps réel 2−clos.

Par utilisations successives de l'axiome des corps, nous ouvrons des branches où le degré de P est connu (un coefficient connu inversible et ceux de degrés supérieurs connus nuls). Par hypothèse de récurrence, nous n'examinons que la branche où le degré de P est égal à p, et sans perte de généralité, nous supposons P unitaire.

Puisque $\mathbf{K}\oplus\{\alpha;\ P(\alpha)=0\}$ collapse comme corps réel, il prouve comme corps que -1 est une somme de carrés. Écrivons cela, en exprimant les éléments de ce corps comme des polynomes en α, de degrés $<\deg(P)$.

Cela donne :

$$1+\sum_i A_i(\alpha)^2=0$$

Par ailleurs la division formelle de $1+\sum_i A_i(X)^2$ par $P(X)$ donne :

$$1+\sum_i A_i(X)^2=P(X)S(X)+R(X)$$

avec $\deg(R)<\deg(P)$ et $\deg(S)<\deg(P)-2$. On a donc le fait $R(\alpha)=0$, vrai dans le corps dynamique $\mathbf{K}\oplus\{\alpha;\ P(\alpha)=0\}$.

En calculant dynamiquement le pgcd des polynomes P et R, on peut ouvrir une arborescence pour le corps dynamique $\mathbf{K}$ du type suivant. A chaque extrémité de l'arborescence, on est dans une structure algébrique dynamique de corps $\mathbf{K}_j$ dans lequel un pgcd unitaire G_j de degré d_j $(1\leq d_j\leq p)$ pour les polynomes $R(X)$ et $P(X)$ est explicité.

Regardons d'abord ce qui se passe dans une branche $\mathbf{K}_j$ où le polynome $R(X)$ est nul, c.-à-d. lorsque $d_j=p$.

On a $1+\sum_i A_i(X)^2=P(X)S(X)$. Donc $\mathbf{K}_j\oplus\{\beta\ ;\ S(\beta)=0\}$ collapse comme corps réel.

Donc, par hypothèse de récurrence $\mathbf{K}_j\oplus\{\ ;\ S(a).S(b)\leq 0\}$ collapse comme corps réel 2−clos.

On a aussi $1+\sum_i A_i(a)^2=P(a)S(a)$ donc $P(a).S(a)>0$ et de même $P(b).S(b)>0$. Donc $\mathbf{K}_j\oplus\{\ ;\ P(a).P(b)\leq 0\}$ prouve $S(a).S(b)\leq 0$, et donc il collapse comme corps réel 2−clos.

Voyons maintenant le cas d'une branche $\mathbf{K}_j$ avec $d_j<p$.

On a dans cette branche $P=G_jQ_j$ avec G_j et Q_j de degrés $<p$. Puisque $\mathbf{K}_j\oplus\{\alpha;\ P(\alpha)=0\}$ collapse comme corps réel 2−clos, il en va de même pour $\mathbf{K}_j\oplus\{\alpha;\ G_j(\alpha)=0\}$ et $\mathbf{K}_j\oplus\{\alpha;\ Q_j(\alpha)=0\}$.

On en déduit par hypothèse de récurrence que les corps $\mathbf{K}_j\oplus\{\ ;\ G_j(a).G_j(b)\leq 0\}$ et $\mathbf{K}_j\oplus\{\ ;\ Q_j(a).Q_j(b)\leq 0\}$ collapsent comme corps réels 2−clos. D'où enfin le collapsus de la branche $\mathbf{K}_j\oplus\{\ ;\ P(a).P(b)\leq 0\}$ puisque la règle

$$uv\leq 0\ \vdash\ (u\leq 0\quad \mathsf{ou}\quad v\leq 0)$$

est valide dans les corps réels 2−clos. □

Remarque 3.6 La version classique de la proposition précédente admet également une preuve constructive, un peu plus délicate, cf. [16].

Corollaire 3.7 *Soit* $\mathbf{K}$ *un corps,* a, b *deux éléments de* $\mathbf{K}$, $P(X)$ *un polynome de* $\mathbf{K}[X]$.
(classique)
si $\mathbf{K}$ *est réel* $2-$*clos,* $a \leq b$ *et* $P(a).P(b) \leq 0$ *alors il existe une extension réelle* $2-$*close de* $\mathbf{K}$ *dans laquelle* P *admet un zéro sur l'intervalle* $[a, b]$
(dynamique)
si $\mathbf{K} \oplus \{\alpha;\ P(\alpha) = 0,\ a \leq \alpha \leq b\}$ *collapse comme corps réel* $2-$*clos, alors* $\mathbf{K} \oplus \{\ ;\ P(a).P(b) \leq 0,\ a \leq b\}$ *collapse comme corps réel* $2-$*clos*

Preuves laissées à la lectrice □

Théorème 2 *Soit* $\mathbf{K}$ *un corps.*
(classique)
si $\mathbf{K}$ *est réel il peut être plongé dans un corps réel clos*
(dynamique)
si $\mathbf{K}$ *collapse comme corps réel clos dynamique, alors il collapse comme corps réel*

Preuve
(classique)
Par Zorn, on considère une extension réelle algébrique maximale $\mathbf{L}$ de $\mathbf{K}$. D'après la proposition 3.4, c'est un corps réel $2-$clos, donc ordonné $2-$clos. D'après le corollaire 3.7, $\mathbf{L}$ vérifie l'axiome des corps réels clos.

(dynamique)
Supposons que $\mathbf{K}$ collapse comme corps réel clos dynamique. Par induction sur le nombre de fois qu'est utilisé l'axiome des corps réels clos, on voit, en utilisant le corollaire 3.7, que $\mathbf{K}$ collapse comme corps réel $2-$clos. Mais alors, par la proposition 3.4, il collapse comme corps réel. □

Théorème 3 ($17^{\text{ème}}$ problème de Hilbert)
Soit $\mathbf{K}$ *un corps réel* $2-$*clos entièrement explicité,* $\mathbf{R}$ *sa cloture réelle,* $P(x_1, \ldots, x_n)$ *un polynome de* $\mathbf{K}[x_1, \ldots, x_n]$ *partout* ≥ 0 *sur* $\mathbf{R}^n$
(classique et non constructif) P *une somme de carrés dans* $\mathbf{K}(x_1, \ldots, x_n)$
(dynamique et constructif) P *une somme de carrés dans* $\mathbf{K}(x_1, \ldots, x_n)$

Preuve
(classique)
On peut supposer P non identiquement nul. Soit $\mathbf{L}$ le corps $\mathbf{K}(x_1, \ldots, x_n)$. C'est un corps réel puisque $\mathbf{K}$ est réel. Supposons que P ne soit pas une somme de carrés dans $\mathbf{L}$. Considérons alors une relation d'ordre sur $\mathbf{L}$ qui rende $P < 0$. Elle prolonge celle sur $\mathbf{K}$ puisque $\mathbf{K}$ est réel $2-$clos. Soit $\mathbf{S}$ la cloture réelle de $\mathbf{L}$ muni de cette relation d'ordre. La preuve par l'algorithme de Cohen-Hörmander que P est partout ≥ 0 sur $\mathbf{R}^n$ n'utilise que des calculs dans $\mathbf{K}$ (en tant que corps ordonné) et prouve donc également que P est partout ≥ 0 sur $\mathbf{S}^n$. En particulier la valeur de P en $(x_1, \ldots, x_n)$ est P lui-même, et donc P est ≥ 0 dans $\mathbf{L}$. Contradiction.

(dynamique)
Soit $\mathbf{L}$ le corps dynamique $\mathbf{K}(x_1, \ldots, x_n)$ entièrement explicté. Soit le corps dynamique $\mathbf{L}' = \mathbf{K} \oplus \{x_1, \ldots, x_n, v, w;\ v.P = 1,\ -P(x_1, \ldots, x_n) = w^2\}$. La preuve par l'algorithme de Cohen-Hörmander que P est partout ≥ 0 sur $\mathbf{R}^n$ donne une évaluation dynamique de $\mathbf{L}'$ comme corps réel clos dynamique qui prouve $P \geq 0$ et donc qui collapse.
Par le théorème 2, $\mathbf{L}'$ collapse également comme corps réel.

Par la proposition 3.2, $\mathbf{L}'' = \mathbf{K} \oplus \{x_1, \ldots, x_n, v;\ v.P = 1\}$ possède une évaluation dynamique comme corps réel qui prouve que P est une somme de carrés. Une branche de cette évaluation dynamique (qu'il est facile de repérer) ne prouve que des faits vrais dans le corps réel entièrement explicité $\mathbf{L}$. On a donc, dans cette branche, explicité P comme somme de carrés dans $\mathbf{L}$. □

Remarques 3.8

1) L'affirmation, dans la preuve dynamique, selon laquelle l'algorithme de Cohen-Hörmander fournit une évaluation dynamique de corps réel-clos, repose sur l'inspection détaillée de cet algorithme (cf. [1] ou [2]). Le seul point qui n'est pas immédiat est comment faire avec le théorème des accroissements finis pour les polynomes dans un corps ordonné. On pourrait reproduire la preuve habituelle de ce théorème dans le cas des corps réels clos telle qu'elle est donnée par exemple dans [1], ce qui donne la validité de la règle correspondante pour la structure algébrique dynamique abstraite de corps réel clos. Il est nettement plus économique d'utiliser le théorème algébrique des accroissements finis donné dans [16] ou les formules de Taylor généralisées données dans [14].

2) Bien que nous ayons parlé dans l'énoncé du théorème 3 de "la cloture réelle d'un corps réel 2−clos totalement explicité", une théorie constructive de cette cloture réelle (comme donnée dans [16] par exemple) n'est pas vraiment nécessaire à la solution constructive du 17$^{\text{ème}}$ problème de Hilbert, mais l'énoncé nécessiterait alors quelques reformulations. Cf. le Nullstellensatz de Hilbert dans [2]. Par ailleurs, la preuve constructive du théorème 2 (dynamique) peut fournir comme sous-produit une preuve constructive de l'existence de la cloture réelle d'un corps réel 2−clos : puisque la cloture réelle, si elle existe, est unique à isomorphisme unique près, il suffit de montrer que les calculs dans un projet de cloture réelle ne conduisent jamais à contradiction, pour que ce projet constitue du coup une vraie cloture réelle. Or précisément le théorème 2 nous dit ce que nous désirons. (nous avons fait une remarque analogue dans [12] au sujet de la preuve constructive du Positivstellensatz, qui implique l'existence constructive de la cloture réelle d'un corps ordonné).

3) La preuve du théorème peut être maintenue si on affaiblit légèrement l'hypothèse en remplaçant la 2−cloture par le fait suivant : pour tous x dans $\mathbf{K}$, x ou $-x$ est une somme de carrés.

4) La preuve constructive présentée ici conduit à un algorithme construisant la somme de carrés qui pourrait s'avérer assez proche de l'une des constructions suggérées par Kreisel dans [11], avec les différences que Kreisel s'appuyait sur l'algorithme d'élimination des quantificateurs de Tarski, moins élémentaire que l'algorithme de Cohen-Hörmander, et qu'il n'utilisait pas les formules de Taylor généralisées pour rendre compte du théorème des accroissements finis. Pour plus de détails historiques, voir [5], [13] et l'étude magistrale [4].

5) A la fin de la preuve, on a établi qu'une évaluation dynamique de

$$\mathbf{L}'' = \mathbf{K} \oplus \{x_1, \ldots, x_n, v;\ v.P = 1\}$$

comme corps réel prouve que P est une somme de carrés. Nous avons ensuite extrait de cette évaluation dynamique une branche qui correspond au corps $\mathbf{L}$, le corps des fractions rationnelles en $x_1, \ldots, x_n$. Ce faisant, nous avons perdu une partie de l'information rendue disponible par notre preuve. En fait comme on l'a remarqué après la proposition 3.2, une évaluation dynamique de $\mathbf{L}''$ comme corps prouve, à chacune de ses feuilles, que -1 ou P est une somme de carrés. En regardant un peu plus en détail ce qui se passe avec l'arbre tout entier, on pourrait voir qu'il est possible de "recoller" les sommes de carrés aux différentes feuilles de manière à obtenir

que P est une somme de carrés de fractions rationnelles dont les dénominateurs ne s'annulent qu'aux zéros de P, amélioration apportée par Stengle à la solution du $17^{\text{ème}}$ problème de Hilbert par Artin-Schreier. Cependant, pour obtenir constructivement ce résultat, il est plus simple de démontrer le Positivstellensatz de Stengle [18] selon la méthode donnée dans l'article [2].

Remerciements : Je remercie vivement Marie-Françoise Roy et Michel Coste pour les nombreuses discussions que nous avons eu sur cet article, lesquelles m'ont permis d'en améliorer grandement la présentation.

Références

[1] Bochnak, Coste M., Roy M.-F. : *Géometrie Algébrique réelle.* Springer-Verlag. Ergeb. M. n°11. 1987. 3, 13, 28

[2] Coste M., Lombardi H., Roy M.-F. : *Dynamical method in algebra : Effective Nullstellensätze* preprint 1996. 5, 8, 28, 29

[3] Della Dora J., Dicrescenzo C., Duval D. : *About a new method for computing in algebraic number fields* Proceedings Eurocal'85. Lecture Notes in Computer Science 204, (1985) 289–290. (Springer) 4

[4] Delzell C.N. : Kreisel's unwinding of Artin's proof, 113–245 in *Kreiseliana : : About and Around Georg Kreisel*, ed. P. Odifreddi, A K Peters, Ltd.(1996). 28

[5] Delzell C.N., González-Vega L., Lombardi H. : *A continuous and rational solution to Hilbert's 17–th problem and several cases of the Positivstellensatz.* 61–76 in Computational Algebraic Geometry. Ed. Eyssette F., Galligo A.. Birkhaüser (1993) Progress in Math. n°109. (Compte-rendus du colloque MEGA 92, avril 92 à Nice) 28

[6] Dicrescenzo C., Duval D. : *Algebraic extensions and algebraic closure in Scratchpad.* Symbolic and algebraic computation (ISSAC 88). Lecture Notes in Computer Science 358, (1989), 440–446. (Springer). 4

[7] Duval, D. : *Simultaneous computations in fields of arbitrary characteristic* Computers and Mathematics, Eds Kaltofen E. and Watt S. M., (1989), 321–326. Springer. 12

[8] Duval D., Gonzalez-Vega L. : *Dynamic evaluation and real closure.* Proceedings IMACS'93. (1993) 4

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

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

[11] Kreisel G. : *Sums of squares.* Summaries of Talks Presented at the Summer Institute in Symbolic Logic in 1957 at Cornell Univ., Institute Defense Analyses, Princeton, (1960) 313–320. 28

[12] Lombardi H. : *Effective real Nullstellensatz and variants.* Effective Methods in Algebraic Geometry. Editors T. Mora and C. Traverso. Progress in Mathematics, volume 94, 263–288, Birkhauser (1991).
Version française détaillée : *Théorème effectif des zéros réel et variantes.* Publications Mathématiques Besançon, Théorie des Nombres, 1988-1989. 3, 28

[13] Lombardi H. : *Une étude historique sur les problèmes d'effectivité en algèbre réelle.* Mémoire d'habilitation (1990). 3, 28

[14] H. Lombardi : *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) 3, 28

[15] 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, 1995-1996. 5

[16] 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. 26, 28

[17] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, 1988. 12

[18] Stengle, G. : *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry.* Math. Ann. 207, 87-97 (1974) 3, 29