THEORIE CONSTRUCTIVE ELEMENTAIRE DES CORPS ORDONNES

Henri LOMBARDI
et
Marie-France ROY

THEORIE CONSTRUCTIVE ELEMENTAIRE DES CORPS ORDONNES

Henri LOMBARDI
Mathématiques
UFR des Sciences et Techniques
Université de Franche-Comté
25 030 Besançon cédex
France

Marie-Françoise ROY
I R M A R
Université de Rennes 1
Campus de Beaulieu
35 042 Rennes cédex
France

Résumé On donne le développement constructif des bases de la théorie des corps ordonnés, jusqu'à la construction de la clôture réelle d'un corps ordonné. L'article peut être lu du point de vue des mathématiques classiques (preuves sans axiome du choix), ou des mathématiques récursives (algorithmes "à oracles" uniformément primitifs récursifs), ou des mathématiques constructives dans le style Bishop (théorie des corps ordonnés discrets).

Mots clés Corps ordonnés, Mathématiques constructives, Preuve par algorithme, Algorithme uniformément primitif récursif, Théorème algébrique des accroissements finis, Algorithme de Hörmander, Algorithme IF (inégalités formelles), Corps ordonné d-clos.

Abstract Classical theory of ordered fields (Artin-Schreier theory) makes an intensive use of non constructive methods, using in particular the axiom of choice. However since Tarski (and even since Sturm and Sylvester) one knows how to compute in the real closure of an ordered field **K** by computations only in **K** . This apparent contradiction is solved in this paper.

We give here a constructive proof of the first results of the theory of ordered fields, including the existence of the real closure.

The proofs can be interpreted in the particular philosophy of each reader. In a classical point of view for example, the effective procedures in the definitions may be interpreted as given by oracles. Hence one gets the existence of the real closure of an arbitrary ordered field without the axiom of choice. In a constructive framework "à la Bishop" one gets the existence of the real closure of a discrete ordered field. From the point of view of recursive theory the proofs give uniformly primitive recursive algorithms.

Key-words Ordered fields, Constructive Mathematics, Uniformly primitive recursive algorithms, Algebraic mean value theorem, Hörmander algorithm, Algorithm IF (formal ineaqualities), d-closed ordered fields.

Théorie constructive élémentaire des corps ordonnés

1) Introduction

La théorie classique élémentaire des corps ordonnés (théorie d'Artin Schreier) fait un usage intensif des méthodes non constructives, notamment par un recours à l'axiome du choix. Par ailleurs, on sait depuis Tarski (d'une certaine manière depuis Sturm et Sylvester) calculer de manière explicite dans la clôture réelle d'un corps ordonné $\mathbf{K}$ en n'effectuant que des calculs dans $\mathbf{K}$. Cette contradiction apparente est levée dans l'article qui suit.

Nous donnons en effet une preuve constructive des premiers résultats de la théorie des corps ordonnés, y compris l'existence de la clôture réelle d'un corps ordonné.

Nous renvoyons à **[MRR]** pour la théorie constructive des corps discrets.

Toutes les preuves peuvent être lues avec des lunettes adaptées à la philosophie ou au cadre de travail de chaque lecteur (lectrice) particulier.

Si on adopte un point de vue "classique" par exemple, les procédures effectives intervenant dans les définitions de départ peuvent être considérées comme données par des oracles. En conséquence, les preuves fournissent une preuve dans le cadre classique, *et sans recours à l'axiome du choix*, de l'existence de la clôture réelle d'un corps ordonné arbitraire.

Si on adopte le point de vue de la théorie classique "récursive", les preuves données fournissent des algorithmes uniformément primitifs récursifs (cf. **[KI]**) sous forme de Machines de Turing à oracles.

Si on adopte le point de vue constructif, on obtient la preuve de l'existence de la clôture réelle d'un corps ordonné discret.

Les outils essentiels pour constructiviser la théorie classique sont les suivants: une version constructive du théorème des accroissements finis pour un polynôme sur un corps ordonné; la notion d'algorithme cohérent d'attribution de signes dans un anneau de polynômes sur un corps ordonné $\mathbf{K}$; la notion de corps ordonné d-clos.
L'utilisation de l'algorithme IF présenté dans **[CR]** permet en outre de donner une présentation particulièrement concrète de la preuve d'existence de la clôture réelle.
Nous donnons dans les paragraphes "commentaires" quelques précisions sur le point de vue constructif "à la Bishop".

A travers le papier "A real root calculus", de H. Zassenhaus [Za], nous avons découvert récemment la thèse de Hollkott [Ho]. Il y développe une problématique assez voisine de celle que nous donnons, mais en restant à un niveau très algorithmique. Ainsi, il n'introduit pas la notion de corps ordonné d-clos. Par ailleurs, il ne dispose pas de la version algébrique du théorème des accroissements finis, et cela le conduit à une acrobatie que nous pouvons interpréter en disant qu'il prouve le théorème de Rolle dans un corps ordonné d-clos pour les polynômes de degré $\leq d+1$, ceci par récurrence sur d. Notre papier peut être considéré comme une présentation moderne, et nous l'espérons, plus claire, des résultats de Hollkott. Merci à L. Gonzalez pour nous avoir communiqué la référence [Za] et à T. Sander pour nous avoir traduits quelques parties décisives de la thèse de Hollkott. Tomas Sander a pour sa part étudié récemment l'indépendance de l'existence de la clôture réelle par rapport à l'axiome du choix, dans le cadre de la théorie ordinaire des ensembles ZF ([Sa]).

Une version anglaise et moins détaillée de ce papier paraît dans les conférences du colloque MEGA 90 (édité chez Birkhaüser).

2) Préliminaires

Corps ordonnés discrets

Définitions

Nous renvoyons à **[MRR]** pour la théorie constructive des corps discrets. Néanmoins, les définitions qui suivent sont formulées de manière à être comprises aussi bien d'un point de vue classique que constructif.

Définitions 1 :

Un ensemble est dit *discret* lorsqu'il est donné dans une présentation où l'égalité de deux éléments de l'ensemble est décidable.

On appelle *corps discret*, un corps **K** donné dans une présentation où il est discret et où les lois de composition $(+ , \times , x \longmapsto -x , x \longmapsto 1/x)$ sont calculables.

On appelle *corps ordonné discret*, un corps ordonné **K** donné dans une présentation où les lois de composition $(+ , \times , x \longmapsto -x , x \longmapsto 1/x)$ sont calculables et où le signe d'un élément est décidable.

Un *intervalle ouvert* est par définition un ensemble $]a,b[$ où a et b sont dans **K** ou égaux à $+\infty$ ou $-\infty$.

Désormais, les corps ordonnés que nous considérons sont tous "ordonnés discrets" et les corps que nous considérons sont tous des "corps discrets".

Théorème des accroissements finis

Exemple : Pour tout polynôme de degré ≤ 4 on a l'identité:

$$P(a) - P(b) = (a-b)\,(P'(a/6 + 5b/6)/3 + P'(a/3 + 2b/3)/6 + P'(2a/3 + b/3)/6 + P'(5a/6 + b/6)/3)$$

Plus généralement on a les résultats suivants :

Lemme :

Il existe deux suites $(\lambda_{i,j})_{1\leq i\leq j;j=1,2,\ldots,n,\ldots}$ et $(r_{i,j})_{1\leq i\leq j;j=1,2,\ldots,n,\ldots}$ de rationnels $\in]\,0\,,\,1\,[$ telles que, pour tout polynôme $P \in \mathbb{Q}\,[X]$ de degré $\leq n$, on ait :

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

Théorème 1 : (théorème des accroissements finis)

Il existe deux suites $(\lambda_{i,j})_{1\leq i\leq j;j=1,2,\ldots,n,\ldots}$ et $(r_{i,j})_{1\leq i\leq j;j=1,2,\ldots,n,\ldots}$ de rationnels $\in]\,0\,,\,1\,[$ telles que, pour tout corps ordonné **K** et tout polynôme $P \in \mathbf{K}[X]$ de degré $\leq n$, on ait :

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

En particulier,

1) si P' est de signe positif sur un intervalle, la fonction polynôme est croissante sur cet intervalle.

2) sur tout intervalle borné, le taux de variation de P est majoré (la fonction définie par P est lipschitzienne sur tout intervalle borné)

preuve> Le théorème est une conséquence immédiate du lemme: ce dernier fournit en effet des identités algébriques concernant les variables " a, b, et les coefficients du polynôme " qui s'appliquent alors dans tout anneau commutatif qui est une $\mathbb{Q}$-algèbre, et en particulier dans les corps commutatifs de caractéristique nulle.
Démontrons le lemme.
Par changement de variable affine, on se ramène au cas où $a = -1$ et $b = 1$. Considérons le degré n fixé. L'application $P \longmapsto P(1) - P(-1)$ est une forme linéaire ne faisant pas intervenir le coefficient constant. Les formes linéaires ne faisant pas intervenir le coefficient constant forment un espace de dimension n. Pour tout choix de n rationnels $\lambda_{i,n}$, les formes linéaires $P \longmapsto P'(\lambda_{i,n})$ sont indépendantes et ne font pas intervenir le coefficient constant. Il correspond donc à ce choix des rationnels $r_{i,n}$ qui rendent la formule vraie. La difficulté consiste à déterminer des $\lambda_{i,n} \in]\,0\,,\,1\,[$ tels que les $r_{i,n}$ correspondants soient également sur $]\,0\,,\,1\,[$. Les formules de quadrature de Gauss correspondent à un tel choix, mais avec des réels alors que nous voulons des rationnels. Il suffit alors de choisir des $\lambda_{i,n}$ rationnels suffisamment voisins des $\lambda_{i,n}$ de Gauss (zéros des polynômes de Legendre) pour que les $r_{i,n}$ correspondants restent positifs. ❑

Remarques 1 :
1) Une majoration et une minoration explicites de P' peuvent être calculées sur un intervalle borné, donc également un module de Lipschitz pour P.
2) Les identités algébriques énoncées dans le théorème 1 sont encore valables lorsque **K** est un anneau commutatif qui est une $\mathbb{Q}$-algèbre.

Lemme de Thom

Définitions et notations 2 :

On appelle *signe* un élément de $\{-1, 0, +1\}$. Un signe est dit *strict* s'il est $\neq 0$. Si x est un élément d'un corps ordonné et σ un signe, on écrira $x \equiv \sigma$ pour signifier que x a le même signe que σ.

Une partie d'un corps ordonné **K** est dite *convexe* si, chaque fois qu'elle contient deux éléments, elle contient tout élément compris entre ces deux éléments. Elle est dite *ouverte* si elle est réunion d'intervalles ouverts. Une fonction de **K** vers **K** est dite continue si l'image réciproque d'un ouvert est un ouvert.

Une *condition de signe* portant sur un élément x est une relation $x \equiv \sigma$. Une *condition de signe généralisée* (en abrégé csg) portant sur un élément x est une des relations $x < 0$, $x \leqslant 0$, $x = 0$, $x > 0$, $x \geqslant 0$, $x \neq 0$. Quand on remplace une condition de signe $x < 0$ ou $x > 0$ par la condition de signe généralisée associée $x \leqslant 0$ ou $x \geqslant 0$, on dit que la condition de signe a été *relâchée*.

Lemme : Une fonction polynôme est continue.

Théorème 2 : (lemme de Thom, version 1, corps ordonné sans hypothèse de clôture)

Soient un corps ordonné **K**, et P un polynôme de **K**[X], de degré n,
$[\sigma_0, \sigma_1, ..., \sigma_n]$ une liste de signes stricts.
L'ensemble $\{\, x\,;\, P(x) \equiv \sigma_0\,,\, P'(x) \equiv \sigma_1\,,\, ...,\, P^{(i)}(x) \equiv \sigma_i\,,\, ...,\, P^{(n)}(x) \equiv \sigma_n \,\}$ est un

ensemble ouvert convexe .

Si on relâche les conditions de signes, et si l'ensemble était non vide, on rajoute au plus une borne inférieure et/ou une borne supérieure.

Si maintenant, on remplace la première condition de signe par $P(x) = 0$, l'ensemble possède au plus un point. En d'autres termes, deux racines distinctes de P attribuent deux signes distincts à au moins l'une des dérivées de P .

preuve> Le lemme résulte par exemple du fait qu'une fonction polynôme est localement lipschitzienne. Pour le théorème, on raisonne par récurrence sur le degré de P . On sait déjà que l'ensemble défini par les conditions de signes "à la Thom" est ouvert. Par hypothèse de récurrence, on peut supposer qu'on est sur un convexe contenant au moins 1 point, défini par les conditions de signe portant sur P', P'' etc... Sur cet ensemble la fonction P est strictement monotone d'après le théorème des accroissements finis. etc... ❑

Commentaire: D'un point de vue constructif, un ensemble qui possède au plus un point est un ensemble pour lequel il est absurde de supposer qu'il possède deux points distincts. Pour autant, on ne peut pas affirmer que l'ensemble possède forcément 0 ou 1 point. Dans un corps réel clos, on pourra par contre affirmer, dans la dernière phrase du théorème, que l'ensemble défini possède 0 ou 1 point, puisqu'un algorithme permettra de tester dans quel cas on se trouve.

Cônes premiers. Construction d'un corps ordonné par attribution d'un signe à tout élément d'un anneau commutatif

Soit $\mathbf{A}$ un anneau commutatif et α une partie décidable de $\mathbf{A}$. On dit que α est un *cône premier* de $\mathbf{A}$ si on a les quatre propriétés

1) $\forall\ x \in \mathbf{A}, x^2 \in \alpha$,
2) $\alpha + \alpha \subset \alpha$,
3) $\alpha . \alpha \subset \alpha$,
4) $\forall\ x, y \in \mathbf{A} \quad xy \in \alpha \Rightarrow [\ x \in \alpha \ \textbf{ou}\ -y \in \alpha\ ]$

On appelle alors support de α et on note $\mathbf{Supp}(\alpha)$ l'intersection $\alpha \cap -\alpha$. C'est un idéal premier. Le corps de fractions de l'anneau quotient $\mathbf{A/Supp}(\alpha)$ est appelé le corps résiduel de α . On le note $k(\mathbf{Supp}(\alpha))$. C'est de manière naturelle un corps ordonné : les éléments positifs ou nuls de $k(\mathbf{Supp}(\alpha))$ sont les images des éléments de α .

Soit $\mathbf{K}$ un corps ordonné et $\mathbf{A}$ une $\mathbf{K}$-algèbre. Un cône premier α de $\mathbf{A}$ est dit *compatible avec l'ordre de* $\mathbf{K}$ si on a en outre

5) $\alpha \cap \mathbf{K} = \{\ x \in \mathbf{K} ; x \geqslant 0\ \}$

Le corps $k(\mathbf{Supp}(\alpha))$ est alors une extension ordonnée de $\mathbf{K}$.

Soit $\mathbf{L}$ une extension ordonnée de $\mathbf{K}$ et f un homomorphisme d'anneau de $\mathbf{A}$ dans $\mathbf{L}$. Alors $\mathbf{L}$ est une extension ordonnée de $k(\mathbf{Supp}(\alpha))$ si et seulement si :

$$\mathbf{A} \cap \{\ x \in \mathbf{A} :\ f(x) \geq 0 \text{ dans } \mathbf{L}\ \} = \alpha$$

Si les éléments de $\mathbf{A/Supp}(\alpha)$ sont algébriques sur $\mathbf{K}$, $k(\mathbf{Supp}(\alpha)) = \mathbf{A/Supp}(\alpha)$ et c'est une extension algébrique de $\mathbf{K}$. On dit alors que α est *algébrique sur* $\mathbf{K}$.

Lorsque $\mathbf{A} = \mathbf{K}[X]$ on note X_α l'image de X dans $k(\mathbf{Supp}(\alpha))$. Si de plus α est algébrique sur $\mathbf{K}$, $\mathbf{K}[X_\alpha]$ est le corps ordonné $k(\mathbf{Supp}(\alpha))$ tout entier.

Pour une partie α d'un anneau commutatif $\mathbf{A}$, les propriétés 1), 2), 3) ,4) peuvent être reformulées en considérant les trois parties $\alpha_0 = \alpha \cap -\alpha$, $\alpha_+ = \alpha - \alpha_0$ et $\alpha_- = -\alpha_+$ Les axiomes 1), 2), 3) et 4) se réécrivent alors en

1') $\mathbf{A}$ est réunion disjointe de α_0 , α_+ , α_- , et $\alpha_- = -\alpha_+$

2'a) $\alpha_0 + \alpha \subset \alpha$,
2'b) $\alpha_+ + \alpha_+ \subset \alpha_+$,
3'a) $\alpha_0 . \alpha \subset \alpha_0$,
3'b) $\alpha_+ . \alpha_+ \subset \alpha_+$,

On peut enfin reformuler ces résultats en terme d'un *algorithme d'attribution de signes* dans l'anneau **A** . Construire un cône premier dans **A** revient en effet à attribuer un signe à tout élément de **A** , c.-à-d. à construire une fonction $Sg: \mathbf{A} \longrightarrow \{-1, 0, +1\}$.
On pose alors : $\alpha_0 = \{ x \in \mathbf{A} ; Sg(x) = 0 \}$, $\alpha_+ = \{ x \in \mathbf{A} ; Sg(x) = 1 \}$, $\alpha = \alpha_0 \cup \alpha_+$, $\alpha_- = \{ x \in \mathbf{A} ; Sg(x) = -1 \}$.
La condition 1') peut alors être remplacée par la seule condition:

1") $\alpha_- = -\alpha_+$

Définition 3 : Lorsque les conditions 1"), 2'a), 2'b), 3'a), 3'b), 5) sont vérifiées nous dirons que nous avons un *algorithme cohérent d'attribution de signes dans* **A**.

Remarque 2 : Si l'anneau $\mathbf{A}/\alpha$ est une extension algébrique de **K** , alors c'est un corps (un anneau commutatif discret intègre qui est une extension algébrique d'un corps **K** est nécessairement un corps).

Corps ordonnés d-clos

Corps ordonnés 2-clos et corps réels

Définitions

Définitions 4 :

Un corps est dit *réel* si : " 1 + une somme de carrés = 0 " est absurde.

Un corps ordonné est dit *d-clos* (où $d \geq 1$) si tout polynôme P de degré $\leq d$ qui change de signe entre a et b possède une racine sur l'intervalle d'extrémités a et b .

Remarques 3 : Tout corps ordonné est réel et 1-clos. Tout corps réel est de caractéristique nulle. Dans un corps ordonné d-clos, tout polynôme qui se décompose en facteurs de degrés $\leq$ d possède une racine sur tout intervalle où il change de signe.

Dans le cadre classique, la notion de corps ordonné d-clos ci-dessus est équivalente à la notion de corps réel d-clos donnée dans **[Bou]**.

Commentaire : Dans la définition précédente "posséder une racine" est pris au sens constructif, c.-à-d. "une racine peut être calculée". Nous ne répèterons pas systématiquement ce genre de remarque dans la suite.

Proposition 3 : (Equivalence de deux notions)

Un corps ordonné est 2-clos si et seulement si tout positif est un carré. En particulier dans un corps ordonné est 2-clos, tout carré est une puissance 4 .

Réciproquement, un corps réel où tout carré est une puissance 4 peut être ordonné de manière unique, en prenant pour positifs les carrés, et il est alors ordonné 2-clos.

preuve> La première affirmation est démontrée comme au lycée. La seule non trivialité ensuite est que les carrés permettent d'ordonner un corps réel où tout carré est une puissance 4 . Si a est un élément non nul, on considère b vérifiant $b^4 = a^2$, puis on teste si $a = b^2$ ou $a = -b^2$. Ceci permet d'attribuer un signe à tout élément. Il s'agit ensuite de vérifier que la somme de deux positifs est un positif, c.-à-d. que la somme de deux carrés est un carré. Cela résulte facilement de la réalité de **K** . ❑

La proposition précédente justifie la définition qui suit:

Définition 5 : Un corps réel est dit *2-clos* si tout carré est une puissance 4 (c.-à-d. encore si, pour tout x, x ou $-x$ est un carré). Il est dit *d-clos* ($d \geq 3$) si en outre il est d-clos en tant que corps ordonné.

Construction de la 2-clôture d'un corps ordonné

Définition 6 :

Une extension ordonnée **R** d'un corps ordonné **K** est appelé une *2-clôture ordonnée (ou 2-clôture)* de **K** si c'est un corps ordonné 2-clos et si tout élément de **R** peut être obtenu à partir d'éléments de **K** par répétition des opérations arithmétiques et de l'opération: extraction d'une racine carrée d'un positif.

Nous donnons le théorème qui suit essentiellement à titre de mise en jambe pour la construction de la clôture réelle d'un corps ordonné, qui sera démontrée par une technique analogue.

Théorème 4 :

Tout corps ordonné **K** possède une 2-clôture, unique à un **K**-isomorphisme croissant unique près.

preuve> Si a est un élément positif de **K**, on constate facilement qu'il existe une extension ordonnée de **K** obtenue en "rajoutant" une racine carrée positive de a : sans préjuger du fait que **K** possédait déjà ou non une telle racine carrée positive, on peut attribuer sans ambiguïté un signe à toute expression $x + y\sqrt{a}$, où x et y sont dans **K** (on procède comme au lycée), donc également à toute expression $Q(\sqrt{a})$ où $Q \in \mathbf{K}[X]$, en considérant le reste de la division de $Q(X)$ par $X^2 - a$; il reste alors à vérifier que l'on a ainsi un algorithme cohérent d'attribution des signes dans $\mathbf{K}[X]$, qui est derechef noté $\mathbf{K}[\sqrt{a}]$.
Cette extension ordonnée est unique à un **K**-isomorphisme croissant unique près, parce qu'il n'y a pas d'ambiguïté possible dans l'attribution d'un signe à $x + y\sqrt{a}$: plus précisément, on a le résultat suivant : si **L** est une extension ordonnée de **K** où a possède une racine carrée positive λ, alors il existe un **K**-isomorphisme croissant unique de $\mathbf{K}[\sqrt{a}]$ vers $\mathbf{K}[\lambda]$ (sous corps de **L** engendré par **K** et λ). D'où on déduit le :

Lemme : Supposons a et $b > 0$ dans un corps ordonné **K**, alors il existe un unique **K**-isomorphisme croissant de $\mathbf{K}[\sqrt{a}][\sqrt{b}]$ vers $\mathbf{K}[\sqrt{b}][\sqrt{a}]$.

En itérant cette construction, on va voir qu'on obtient une extension algébrique ordonnée **R** de **K** où tous les positifs sont des carrés.
Concrètement, tout élément de **R** apparaît comme construit en un nombre fini d'étapes h : il est alors de la forme $x_h + y_h\sqrt{a_h}$ où x_h, y_h, a_h sont 3 éléments d'une extension $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_{h-1}}]$ construite à l'étape $h-1$, avec a_h positif.
Considérons maintenant l'union disjointe de toutes les extensions $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$ possibles. La 2-clôture cherchée sera un quotient de cette union.
Soient :

$\mathbf{K}_1 = \mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$ (avec $a_{h\,(h=1,...,i)}$ positif dans $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_{h-1}}]$)
et $\mathbf{K}_2 = \mathbf{K}[\sqrt{b_1}][\sqrt{b_2}]...[\sqrt{b_j}]$ (avec $b_{h\,(h=1,...,j)}$ positif dans $\mathbf{K}[\sqrt{b_1}][\sqrt{b_2}]...[\sqrt{b_{h-1}}]$).
Définissons $\mathbf{K}' = \mathbf{K}_1[\sqrt{b_1}][\sqrt{b_2}]...[\sqrt{b_j}]$ et $\mathbf{K}'' = \mathbf{K}_2[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$.

Ces définitions sont possibles parce que, par exemple, le fait que a_h est positif dans $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_{h-1}}]$ peut être testé par des calculs dans $\mathbf{K}$ qui sont a fortiori valable dans $\mathbf{K}_2$.
En utilisant plusieurs fois le lemme on construit un $\mathbf{K}$-isomorphisme croissant de $\mathbf{K}'$ vers $\mathbf{K}''$, et cet isomorphisme est manifestement unique.
Par définition, des éléments de $\mathbf{K}_1$ et de $\mathbf{K}_2$ sont équivalents si ils sont "égaux" via cet isomorphisme. Il faut vérifier que cette relation est bien une relation d'équivalence compatible avec la structure de corps ordonné: la réflexivité et la symétrie sont immédiates. La transitivité s'obtient en considérant les isomorphismes uniques liant des extensions composées obtenues à partir des trois extensions en cause.
La 2-clôture cherchée est alors le quotient de l'union disjointe des $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$ pour cette relation d'équivalence. ❑

Commentaire: Il est impossible de démontrer constructivement que tout corps réel peut être ordonné, ou plus prosaïquement qu'on puisse, dans un corps réel, soit rajouter une racine carrée de a, soit rajouter une racine carrée de $-a$, et obtenir une extension réelle : il faudrait pour cela être capable d'affirmer que a ou $-a$ n'est pas une somme de carrés. Ceci impliquerait manifestement le "très petit principe d'omniscience" (LLPO), qui n'est pas admissible constructivement (cf. [MRR] chap. 1 à ce sujet). On trouvera un exemple de corps réel récursivement présenté mais non récursivement ordonnable dans [MN].

Corps ordonnés d-clos

Introduction

Théorème 5 :

Dans un corps ordonné d-clos $\mathbf{K}$, la liste ordonnée $[\alpha_1, ..., \alpha_i]$ des racines d'un polynôme P de degré $\leq d$ peut être calculée.

En outre, si $\alpha_0 = -\infty$, $\alpha_{i+1} = +\infty$, le polynôme P est de signe strict constant sur chaque intervalle $]\alpha_j, \alpha_{j+1}[$ $(0 \leq j \leq i)$ dans n'importe quelle extension ordonnée de $\mathbf{K}$.

NB : $i = 0$ si P ne possède pas de racine dans $\mathbf{K}$.

preuve> On raisonne par récurrence sur le degré de P. On suppose donc qu'on a calculé les racines de P'. Ceci permet déjà d'expliciter les racines communes à P et P'. Si maintenant a et b sont deux racines consécutives de P', le polynôme P' a même signe sur tout l'intervalle $]a,b[$ qu'en $(a+b)/2$. Donc P est strictement monotone sur cet intervalle et s'annule au plus une fois. Il s'annule si et seulement si $P(a).P(b) < 0$, auquel cas la racine peut être calculée dans $\mathbf{K}$ (d'après la définition d'un corps d-clos). Même raisonnement avec le ou les deux intervalles d'extrémité du tableau de variation de P, en remplaçant $+\infty$ ou $-\infty$ par un élément au delà duquel le polynôme est de signe connu. ❑

Commentaires: 1) Une formulation constructive plus "provocante" du théorème ci-dessus est la suivante : Dans un corps ordonné d-clos, les racines d'un polynôme de degré $\leq d$ forment un ensemble fini, et le polynôme n'admet pas d'autre racine dans une extension ordonnée de $\mathbf{K}$.
2) La mise à plat de la preuve par récurrence du théorème 5 conduirait à appliquer la méthode de Hörmander à la liste [P] pour déterminer les racines de P (cf. §4).

Algorithmes de Sturm et de Sturm-Sylvester

Rappelons tout d'abord comment est construite la suite de Sturm pour les polynômes P et Q :

$\mathbf{Stu}_0(P,Q) := P$, $\mathbf{Stu}_1(P,Q) := \mathbf{Rst}(P'Q,P)$,

$\mathbf{Stu}_{i+1}(P,Q) := -\mathbf{Rst}(\mathbf{Stu}_i(P,Q),\mathbf{Stu}_{i-1}(P,Q)$ (on s'arrête au dernier reste non nul).

La suite de Sturm de P est obtenue en prenant Q = 1 . On note $V_{St}(P,Q;a)$ le nombre de variations de signes dans la suite des $\mathbf{Stu}_i(P,Q)(a)$ (sans tenir compte des 0) , et $V_{St}(P,Q;a,b)$ la différence $V_{St}(P,Q;a) - V_{St}(P,Q;b)$.
Le théorème de Sturm-Sylvester affirme que, dans le cas d'un corps réel clos, si $a < b$ sont non racines de P , le nombre $V_{St}(P,Q;a,b)$ est égal au nombre de racines de P sur]a,b[rendant $Q > 0$ moins le nombre de racines de P sur]a,b[rendant $Q < 0$.

Théorème 6 : (polynôme de degré $\leq d$ dans un corps ordonné d-clos)
Soit **K** un corps ordonné sous corps d'un corps ordonné d-clos **L** . Les algorithmes de Sturm (pour le nombre de racines de P sur un intervalle donné, dans **L**) et de Sturm-Sylvester (pour le nombre de racines de P rendant $Q > 0$ sur un intervalle donné, dans **L**) donnent un résultat correct si P est de degré $\leq d$.

preuve> la preuve classique fonctionne sans problème, vu le théorème précédent (cf. par exemple **[GLRR]** pour la preuve classique) ❑

Remarque 4 : Il y a des exemples de corps ordonnés avec des polynômes P de signe constant sur un intervalle, mais avec un nombre de racines > 0 prescrit par l'algorithme de Sturm: rajouter à $\mathbb{Q}$ un infiniment petit positif ε , considérer le polynôme $P = (X^2 - \varepsilon^3).(X^3 - \varepsilon^4)$ et l'intervalle $[\varepsilon^2,\varepsilon]$.

Proposition 7 : (polynôme de degré d+1 dans un corps ordonné d-clos)
On suppose que P est un polynôme de degré d+1 à coefficients dans un corps ordonné d-clos **K** . On considère un intervalle I du corps **K** , P ne s'annulant pas aux extrémités de l'intervalle.
Si P est sans facteur carré, l'algorithme de Sturm (pour le nombre de racines de P sur l'intervalle I) compte le nombre de changements de signes de P sur l'intervalle . En particulier, le nombre de racines de P dans **K** sur l'intervalle est au plus égal à celui, positif ou nul, prévu par l'algorithme de Sturm.
Si P est décomposable dans **K**[X] , en particulier s'il possède un facteur carré, l'algorithme de Sturm compte le nombre racines de P dans **K** sur l'intervalle.

preuve> Si P est sans facteur carré, on répète la preuve classique en omettant les racines de P dans le tableau de toutes les racines des polynômes de la suite de Sturm (sauf celles qui sont déjà racines de l'un des autres polynômes). Si P est décomposable on peut répéter la preuve donnée dans **[GLRR]**[1] parce que P possède une racine sur tout intervalle où il change de signe, de même que les autres polynômes de la suite de Sturm (qui sont de degré $\leq d$). ❑

Le lemme de Thom

Théorème 8 : (lemme de Thom, version 2, corps ordonné d-clos)
Soient un corps ordonné d-clos **K** , P un polynôme de **K**[X], de degré $n \leqslant d$, et $[\sigma_0, \sigma_1, ..., \sigma_n]$ une liste de signes stricts.
L'ensemble $\{ x ; P(x) \equiv \sigma_0 , P'(x) \equiv \sigma_1 , ..., P^{(i)}(x) \equiv \sigma_i , ..., P^{(n)}(x) \equiv \sigma_n \}$ est ou bien vide, ou bien un intervalle ouvert ayant pour chaque extrémité $+\infty$, $-\infty$, ou une racine de l'un des polynômes P , P' , P" etc... .

---

[1] Dans le cas où le Pgcd de P et P'Q est $\neq 1$, la preuve, plus subtile que la preuve ordinaire, est basée sur la considération de la suite des restes signés démarrant avec $P_1 = P/\text{Pgcd}(P,P')$ et $P_2 = P'/\text{Pgcd}(P,P')$.

Si on relâche les conditions de signes, et si l'ouvert était un intervalle non vide, on obtient l'intervalle fermé correspondant.

Si maintenant, on remplace la première condition de signe par $P(x) = 0$, l'ensemble possède zéro ou un point.

NB: Ce théorème doit être lu d'un point de vue constructif. La première affirmation signifie que les extrémités de l'intervalle sont calculables à partir des données; la dernière signifie qu'il y a un algorithme pour décider si l'ensemble possède zéro ou un point, et dans ce dernier cas, l'algorithme fournit le point.

preuve> Preuve par récurrence sur le degré du polynôme. Quand on coupe un intervalle bien précisé en deux, en un endroit bien précisé, chaque moitié est un intervalle bien précisé. ❑

Définition 7 :

Soit **K** un corps ordonné possédant une d-clôture **R** . Un élément ξ de **R** est dit *codé à la Thom* (dans **K**) s'il est présenté comme racine d'un polynôme P , de degré $\leq d$, de $\mathbf{K}[X]$, en précisant les signes stricts de $P'(\xi)$, $P''(\xi)$, etc...

Un intervalle ouvert non borné de **R** est dit *codé à la Thom* (dans **K**) s'il est présenté comme l'ensemble des éléments ζ qui attribuent des signes stricts précisés à une liste de polynômes [P , P' , P'' , etc...] avec $\deg(P) \leq d$) l'extrémité finie α de l'intervalle étant obtenue pour $P(\alpha) = 0$.

Un intervalle ouvert borné de **R** est dit *codé à la Thom* (dans **K**) s'il est présenté comme l'ensemble des éléments ζ qui attribuent des signes stricts précisés à deux listes de polynômes [P , P' , P'' , etc...] et [Q , Q' , Q'' , etc...]) avec $\deg(P)$ et $\deg(Q) \leq d$, les extrémités α et β de l'intervalle étant obtenues pour $P(\alpha) = 0$ et $Q(\beta) = 0$.

L'algorithme IF

Nous rappelons brièvement dans ce paragraphe l'algorithme IF ("inégalités formelles simultanées") proposé dans [**CR**] en vue de calculer avec des nombres réels algébriques présentés via des systèmes d'équations emboîtées, dont les racines sont spécifiées "à la Thom" pour chaque nouvelle équation introduite (cf. également [**BKR**]) . Vus les théorèmes 6 et 8 déjà établis pour les corps ordonnés d-clos, l'algorithme pourra s'appliquer pour tout corps ordonné **K** qui possède une extension ordonnée d-close **R** .

Petit préliminaire

Un *système d'équations algébriques emboîtées sur le corps* **K** (ou encore *système triangulaire d'équations algébriques sur le corps* **K**) est donné par une liste de polynômes $\mathbf{P} := [P_1,P_2,...,P_k]$ avec

$$P_1 \in \mathbf{K}[X_1] \text{ , } P_2 \in \mathbf{K}[X_1,X_2] \text{ , ... , } P_k \in \mathbf{K}[X_1,X_2,...,X_k]$$

chaque P_j étant unitaire de degré d_j en tant que polynôme en X_j

Le système est dit *normalisé* si les conditions suivantes sur les degrés sont réalisées

$$d_j \geq 2 \text{ pour tout } j \text{ et } d_{X_h}(P_j) < d_h \text{ pour tout } h < j$$

Une *solution réelle du système défini par la liste* **P** est un k-uple $\xi = [\xi_1,\xi_2,...,\xi_k]$ dans une extension ordonnée de **K** , avec :

$$P_1(\xi_1) = 0 \text{ , } P_2(\xi_1,\xi_2) = 0 \text{ , ... , } P_k(\xi_1,\xi_2,...,\xi_k) = 0 \text{ .}$$

On est alors amené naturellement à travailler dans le corps $\mathbf{K}[\xi_1,\xi_2,...,\xi_k]$.

Si **K** possède une extension ordonnée d-close **R** , et si tous les d_i sont inférieurs ou égaux à d , les solutions réelles dans **R** du système emboîté peuvent être caractérisées "à la Thom", à l'étage i , par la liste des signes des dérivées de $P_i(\xi_1,\xi_2,...,\xi_{i-1},X)$ en $X = \xi_i$.

L'algorithme IF proprement dit

Soient $P, Q_1, Q_2, \ldots, Q_n$ des polynômes de $\mathbf{K}[X]$ avec $\deg(P) \leqslant d$, $[\sigma_1, \sigma_2, \ldots, \sigma_n]$ une liste de signes stricts. Supposons que $\mathbf{K}$ possède une extension ordonnée d-close $\mathbf{R}$. On peut déterminer le nombre de racines de P (dans $\mathbf{R}$) qui attribuent les signes $\sigma_1, \sigma_2, \ldots, \sigma_n$ aux polynômes $Q_1, Q_2, \ldots, Q_n$ en calculant le nombre de racines de P rendant R_i positif, le nombre de racines de P rendant R_i négatif et le nombre de racines de P rendant R_i nul, où R_i parcourt les 3^n produits de Q_j pris à la puissance 0, 1 ou 2. (en fait on peut se ramener à un calcul nettement plus court, cf. **[BKR]**). Ceci donne en particulier un test dans $\mathbf{K}$ pour savoir s'il existe une racine de P dans $\mathbf{R}$ vérifiant un codage à la Thom particulier, puis pour calculer le signe de $Q(\xi)$ si ξ est une racine de P dans $\mathbf{R}$ codée à la Thom dans $\mathbf{K}$. Autrement dit cela permet de ramener tous les calculs dans $\mathbf{K}[\xi]$ à des calculs dans $\mathbf{K}$.
Si maintenant, on considère un système d'équations emboîtées, toutes de degré $\leqslant d$, on pourra appliquer l'algorithme précédent de manière itérative (par rapport au nombre de variables) et déterminer, par des calculs dans $\mathbf{K}$ tous les codages à la Thom des solutions $(\xi_1,\xi_2,\ldots,\xi_k)$ dans $\mathbf{R}^k$ du système considéré.
Pour une de ces solutions, soit $(\xi_1,\xi_2,\ldots,\xi_k)$, l'algorithme IF permet alors de calculer le signe de $Q(\xi_1,\xi_2,\ldots,\xi_k)$ où $Q \in \mathbf{K}[X_1,X_2,\ldots,X_k]$.
Autrement dit les calculs dans $\mathbf{K}[\xi_1,\xi_2,\ldots,\xi_k]$ sont ramenés à des calculs dans $\mathbf{K}$. D'où le :

Théorème 9 : Si un corps ordonné $\mathbf{K}$ possède une extension ordonnée d-close $\mathbf{R}$, on peut, uniquement par des calculs dans le corps ordonné $\mathbf{K}$, expliciter la structure de corps ordonné de toute extension $\mathbf{K}[\xi_1,\xi_2,\ldots,\xi_k]$ contenue dans $\mathbf{R}$ et définie par un système d'équations emboîtées, où chaque ξ_i est spécifié "à la Thom" comme racine d'un polynôme de degré $\leq d$ et à coefficients dans l'extension précédente $\mathbf{K}[\xi_1,\xi_2,\ldots,\xi_{i-1}]$.
L'existence, à chaque étage, d'une racine dans $\mathbf{R}$ répondant à la spécification "à la Thom" choisie, se vérifie également par des calculs dans le corps ordonné $\mathbf{K}$.

Remarques 5 : On entend par "calculs dans le corps ordonné $\mathbf{K}$ " des calculs qui font intervenir exclusivement la structure de corps ordonné de $\mathbf{K}$. On notera que le théorème 9 implique que, si elle existe, la d-clôture de $\mathbf{K}$ est essentiellement unique.

Corps réels clos

Définition 8 : Un corps $\mathbf{K}$ est dit *réel clos* s'il est ordonné et d-clos pour tout entier d, c.-à-d. encore s'il possède un ordre unique défini par ses carrés et si tout polynôme qui change de signe sur un intervalle possède une racine sur l'intervalle.

Théorème 10 : Soit $\mathbf{K}$ un corps. Les propriétés suivantes sont équivalentes

a) $\mathbf{K}$ est ordonné, tout positif est un carré, tout polynôme de degré impair possède une racine

a') $\mathbf{K}$ est réel, tout carré est une puissance 4, tout polynôme de degré impair possède une racine

b) $\mathbf{K}$ est ordonné et tout polynôme possède le nombre de racines que lui prescrit l'algorithme de Sturm (ceci sous entend que le nombre prescrit est toujours positif ou nul)

c) $\mathbf{K}$ est réel et tout polynôme est décomposable en facteurs de degré un ou deux

d) -1 n'est pas un carré et $\mathbf{K}[\sqrt{-1}]$ est algébriquement clos

e) $\mathbf{K}$ est réel clos

preuve> e) $\Rightarrow$ a) $\Rightarrow$ a') immédiat. a') $\Rightarrow$ a) cf. proposition 3
a) $\Rightarrow$ d)la preuve classique fonctionne ([**BCR**] p 9) . On peut également répéter la preuve donnée dans [**MRR**] p 189-191 pour les nombres algébriques complexes.
d) $\Rightarrow$ c)Il est clair que tout polynôme se décompose en facteurs de degré 1 ou 2 . Ensuite, pour tout a dans $\mathbf{K}$, a ou $-a$ est un carré : il suffit de décomposer le polynôme $T^4 - a$ en un produit de 2 polynômes unitaires de degré 2 et d'identifier. Enfin, la somme de deux carrés est un carré : on écrit $a + b\sqrt{-1} = (c + d\sqrt{-1})^2$, d'où : $a^2 + b^2 = (c^2 + d^2)^2$
c) $\Rightarrow$ e)Pour tout a , a ou $-a$ est un carré (comme ci-dessus); donc $\mathbf{K}$ est ordonné 2-clos; on construit ensuite facilement le tableau des signes d'un polynôme arbitraire, et il est alors clair qu'il s'annule sur tout intervalle où il change de signe (les facteurs irréductibles de degré 2 n'influent pas sur le tableau de signes).
e) $\Rightarrow$ b) résulte d'un théorème déjà démontré dans le cadre des corps ordonnés d-clos
b) $\Rightarrow$ e)$\mathbf{K}$ est 2-clos parce que l'algorithme de Sturm prescrit 2 racines à un polynôme $X^2 - a$ si $a > 0$; puis par récurrence sur d on prouve que $\mathbf{K}$ est ordonné d-clos, en utilisant la proposition 7 pour passer de d à d+1 . ❑

3) Construction de la clôture réelle d'un corps ordonné

Rajout d'une racine à un polynôme de degré d+1 dans un corps ordonné d-clos

Théorème 11 : Soit $\mathbf{K}$ un corps ordonné d-clos, P un polynôme de degré d+1 , $a < b$ deux éléments de $\mathbf{K}$. On suppose $P(a).P(b) < 0$ et P' de signe constant sur]a,b[(ce qui est décidable).

Il est possible d'attribuer un signe à tout élément de $\mathbf{K}[X]$ de manière à obtenir une extension ordonnée, notée $\mathbf{K}[X_\alpha]$ (X_α est la classe d'équivalence de X), de $\mathbf{K}$, où X_α est racine de P sur l'intervalle]a,b[.

En outre cette extension est unique à $\mathbf{K}$-isomorphisme croissant unique près, c.-à-d. : pour toute extension ordonnée $\mathbf{L}$ de $\mathbf{K}$ qui possède un élément ξ racine de P sur]a,b[, il existe un unique $\mathbf{K}$-isomorphisme croissant de $\mathbf{K}[X_\alpha]$ vers $\mathbf{K}[\xi]$

preuve> Supposons par exemple que P' soit positif sur l'intervalle.
Soit Q un polynôme de $\mathbf{K}[X]$, imaginons qu'il ait une racine ξ sur l'intervalle]a,b[dans une extension ordonnée de $\mathbf{K}$ et cherchons à attribuer un signe à $Q(\xi)$.
Soit Q_1 le reste de la division de Q par P . Si Q_1 est nul, (cas 1), on doit poser $Sg(Q) := 0$.
Sinon, calculons les racines de Q_1 situées sur l'intervalle]a,b[, d'où la liste ordonnée $[a=u_0, u_1, ..., u_n=b]$. Les valeurs successives de P sont en ordre strictement croissant. Si $P(u_i) = 0$ pour un certain i , (cas 2), on pose $Sg(Q) := 0$. Sinon, (cas 3), P passe du signe $-$ au signe $+$ sur un et un seul des sous intervalles $[u_i, u_{i+1}]$, et Q_1 est de signe constant connu σ sur l'intervalle $]u_i, u_{i+1}[$. On pose alors $Sg(Q) := \sigma$.

Comme nous n'avions pas la liberté de faire une autre affectation de signe dans le cadre d'une extension ordonnée de **K** où P admet une racine ξ sur l'intervalle]a,b[, cela montre l'unicité de l'extension à **K**-isomorphisme croissant unique près. Et on a aussi établi :

Lemme: Si P possède une racine c dans **K** ou dans une extension ordonnée de **K** sur l'intervalle]a,b[, l'affectation de signe définie ci-dessus vérifie : Sg(Q) = Signe de (Q(c)), et donc c'est une affectation de signe cohérente.

Nous allons voir que nous avons dans tous les cas une affectation cohérente de signes dans **K**[X] . Les conditions 1") et 5) sont trivialement vérifiées. Avant de passer aux autres conditions, faisons une remarque préliminaire: si au cours de la démonstration, nous sommes amenés à affecter 0 à un R(α) avec deg(R) $\leqslant$ d , cela signifie que P(c) = 0 pour une racine c de R sur]a,b[, donc c dans **K** , nous pouvons alors court-circuiter la démonstration en faisant appel au lemme précédent (notez que nous ne faisons pas pour autant l'hypothèse non constructive selon laquelle P admet ou n'admet pas de racine dans **K** sur l'intervalle]a,b[ ). Nous pouvons supposer en particulier que nous ne sommes jamais dans le cas 2) où P admet une racine dans **K** sur l'intervalle considéré.

2'a) et 3'a) : supposons Q dans α_0 , et S dans α_0 ou α_+ ; comme nous évitons le cas 2), Q est multiple de P, donc QR également, et par ailleurs Q + S et S ont le même reste modulo P .

2'b) : $\alpha_+ + \alpha_+ \subset \alpha_+$: Sg(S) = + 1 , Sg(Q) = + 1 , le reste de la division de Q+S par P est Q_1+S_1 . Notons $[u_0, u_1, ..., u_n]$, $[v_0, v_1, ..., v_m]$ et $[w_0, w_1, ..., w_p]$ les subdivisions introduites avec les racines de S_1 , Q_1 et Q_1+S_1 respectivement. On peut les fusionner en une seule subdivision, les 2 polynômes S_1 et Q_1 ont le signe + sur l'intervalle ouvert où P change de signe (ce sont des sous-intervalles des intervalles considérés séparément pour S_1 et Q_1) donc également Q_1+S_1 , et cet intervalle est un sous-intervalle de celui qui doit être considéré pour l'attribution d'un signe à Q+S via Q_1+S_1 .

3'b) : $\alpha_+ \times \alpha_+ \subset \alpha_+$: le reste de la division de Q.S par P est égal au reste R de la division de $Q_1.S_1$ par P , ce qui donne $Q_1.S_1 = A.P + R$, avec deg(A) < d . Si A_1 est nul, nous raisonnons comme au cas précédent. Sinon, nous fusionnons les subdivisions associées aux polynômes R , A , Q_1 et S_1 . Sur l'intervalle ouvert minimum ( ]c,d[ ) de la subdivision où P change de signe, on sait déjà que Q_1 et S_1 ont le signe + 1 . Soit σ le signe de A sur cet intervalle. Le polynôme P a le signe $-\sigma$ en l'une des extrémités c, d, et également, vue la continuité de la fonction P, en un point c' intérieur à]c,d[. On a :

$$R(c') = (-A.P + Q_1.S_1)(c') > 0 .$$ ❑

Commentaire : Notons que si **K** est une partie détachable de $\mathbf{K}[X_\alpha]$, alors on est capable de dire si P admet ou non une racine dans **K** sur l'intervalle. Inversement, si on est capable de calculer un facteur irréductible (dans **K**[X]) de P , changeant de signe sur l'intervalle, alors **K** est une partie détachable de $\mathbf{K}[X_\alpha]$. Fort heureusement, la construction de $\mathbf{K}[X_\alpha]$ est indépendante de telles hypothèses, qui ne sont en général pas vérifiées d'un point de vue constructif.

Une preuve "abstraite"

Définitions 9 :

On appelle clôture réelle d'un corps ordonné **K** une extension ordonnée algébrique de **K** qui est un corps réel-clos.

Une extension ordonnée **R** d'un corps ordonné **K** est appelé une *d-clôture (ordonnée)* de **K** si c'est un corps ordonné d-clos et si tout élément de **R** peut être obtenu à partir

d'éléments de **K** par répétition des opérations arithmétiques et de l'opération: calcul d'une racine d'un polynôme de degré $\leq d$.

Théorème 12 : Tout corps ordonné **K** possède une clôture réelle, unique à **K**-isomorphisme croissant unique près.

preuve> Nous raisonnons par récurrence sur d pour montrer que:

H(d) : Pour tout corps ordonné **K**, on peut construire une d-clôture ordonnée $\mathbf{K}^{(d)}$ de **K**. En outre, pour toute extension ordonnée d-close **L** de **K**, il existe un unique **K**-homomorphisme croissant de $\mathbf{K}^{(d)}$ vers **L**.

Pour d=1, il n'y a rien à prouver.
Supposons l'hypothèse vraie pour d. Si **K** est un corps ordonné, si P est un polynôme unitaire de degré d+1 dans $\mathbf{K}^{(d)}[X]$, et si a et b sont deux racines consécutives de P' vérifiant $P(a).P(b) < 0$, nous noterons :

α := le cône construit comme au théorème 11 à partir de (P,a,b),

et donc, conformément aux notations précédemment définies :

$\mathbf{K}^{(d)}[X_\alpha]$ l'extension de $\mathbf{K}^{(d)}$ définie à partir de α

$\mathbf{K}^{(d)}[X_\alpha]^{(d)}$ la d-clôture du corps $\mathbf{K}^{(d)}[X_\alpha]$

Nous avons une construction analogue pour le premier, le dernier ou l'unique intervalle du tableau de variation de P, c.-à-d. que nous pouvons prendre $a = -\infty$ et b = la première racine de P' etc...
Cette dirons que "$\mathbf{K}^{(d)}[X_\alpha]$ est bien défini" pour signifier que les conditions requises pour P, a, b sont bien vérifiées.
Nous itérons maintenant cette construction et utilisons la notation :

$$\mathbf{K}^{(d)}[X_{\alpha 1}]^{(d)}[X_{\alpha 2}]^{(d)}...[X_{\alpha i}]^{(d)} .$$

Pour obtenir $\mathbf{K}^{(d+1)}$ nous allons "recoller" entre elles toutes ces extensions: ce qui revient à introduire une bonne relation d'"égalité" sur leur réunion disjointe.
Nous établissons tout d'abord un lemme (sous l'hypothèse de récurrence H(d)).

Lemme : Si **L** est une extension ordonnée d-close de **K** et si $\mathbf{K}^{(d)}[X_\alpha]$ est bien défini, alors $\mathbf{L}[X_\alpha]$ est bien défini, et il existe un unique **K**-homomorphisme croissant de $\mathbf{K}^{(d)}[X_\alpha]^{(d)}$ vers $\mathbf{L}[X_\alpha]^{(d)}$.

Supposons $\alpha = (P,a,b)$. Comme il y a un unique **K**-homomorphisme croissant de $\mathbf{K}^{(d)}$ vers **L**, les points a et b et le polynôme P sont définis sans ambiguïté dans **L**, qui peut être vue comme une extension ordonnée de $\mathbf{K}^{(d)}$. En outre, comme P' est de degré d, ses racines dans $\mathbf{K}^{(d)}$ sont ses seules racines dans **L** (cf. théorème 5). Donc a et b sont bien deux racines consécutives de P' dans **L** (raisonnement analogue dans les cas avec ∞). On applique ensuite le théorème 11 et H(d) pour obtenir l'existence et l'unicité du **K**-homomorphisme croissant de $\mathbf{K}^{(d)}[X_\alpha]^{(d)}$ vers $\mathbf{L}[X_\alpha]^{(d)}$. ❑

Nous pouvons maintenant recoller nos extensions :
si $\mathbf{K}_1 = \mathbf{K}^{(d)}[X_{\alpha 1}]^{(d)}[X_{\alpha 2}]^{(d)}...[X_{\alpha i}]^{(d)}$ et $\mathbf{K}_2 = \mathbf{K}^{(d)}[X_{\beta 1}]^{(d)}[X_{\beta 2}]^{(d)}...[X_{\beta j}]^{(d)}$ sont deux extensions construites sur le modèle précédent, les deux extensions "composées"

$$\mathbf{K'} = \mathbf{K}_1[X_{\beta 1}]^{(d)}[X_{\beta 2}]^{(d)}...[X_{\beta j}]^{(d)} \text{ et } \mathbf{K''} = \mathbf{K}_2[X_{\alpha 1}]^{(d)}[X_{\alpha 2}]^{(d)}...[X_{\alpha i}]^{(d)}$$

sont bien définies, par application répétée du lemme. De même, il existe un unique **K**-homomorphisme croissant de **K'** vers **K"**, et un autre de **K"** vers **K'**, qui par composition ne peuvent donner que l'identité. D'où un isomorphisme canonique de **K'** vers **K"**.
Un élément x de l'extension $\mathbf{K}_1$ devra donc être considéré comme égal (dans $\mathbf{K}^{(d+1)}$) à un élément y de l'extension $\mathbf{K}_2$, si et seulement si x a pour image y par l'isomorphisme

canonique de **K'** vers **K"** . Il faut vérifier que cette relation ("être considéré comme égal à") est bien une relation d'équivalence : la réflexivité et la symétrie sont immédiates. La transitivité s'obtient en considérant les isomorphismes uniques liant des extensions composées obtenues à partir des 3 extensions en cause.

Il est clair que l'on obtient, avec le recollement de toutes les extensions du type initial, une extension (d+1)-close et qu'elle est unique à **K**-isomorphisme croissant unique près. ❑

On notera que l'unicité d'une d-clôture résulte également du théorème 9 .
Il serait intéressant de fournir une preuve plus directe du corollaire suivant du théorème 12 .

Corollaire : Dans tout corps ordonné, les algorithmes de Sturm et de Sturm-Sylvester prescrivent des nombres de racines positifs ou nuls.

Explicitation de l'algorithme sous-jacent, une preuve plus concrète

Examen de la preuve

Si nous examinons les calculs impliqués récursivement dans la preuve "abstraite" donnée au paragraphe précédent, nous voyons que tout élément de la clôture réelle est présenté comme élément $Q(\xi_1,\xi_2,...,\xi_k)$ d'une "extension emboîtée normalisée réellement spécifiée", avec $Q \in \mathbf{K}[X_1,X_2,...,X_k]$: une extension emboîtée réellement spécifiée est définie par un système d'équations emboîtées et une spécification de la racine réelle considérée à chaque étage (dans cette preuve, elle est spécifiée comme unique racine sur un intervalle où P change de signe et où P' est de signe constant).

Le théorème 11 nous dit que, si $d_k = d+1$, l'attribution d'un signe à $Q(\xi_1,\xi_2,...,\xi_k)$ peut être faite par un algorithme où n'interviennent que des calculs dans une d-clôture réelle $\mathbf{L}_{k-1}$ de $\mathbf{K}[\xi_1,\xi_2,...,\xi_{k-1}]$, (la spécification réelle de ξ_k est elle-même explicitée et vérifiable dans $\mathbf{L}_{k-1}$). Le théorème 11 nous dit aussi que, dès qu'une d-clôture réelle existe belle et bien, l'algorithme d'attribution de signes est cohérent (c.-à-d. fournit bien une nouvelle extension ordonnée) et unique. Mais en fait, la d-clôture réelle n'est jamais manipulée en entier (pas plus que **K** lui-même).

Si nous appliquons le théorème 11 à chacun des calculs de signe impliqués dans l'attribution du signe à un polynôme particulier, nous sommes amenés à introduire des systèmes d'équations emboîtées (réellement spécifiées) *plus gros* que $[P_1,P_2,...,P_{k-1}]$ mais où les polynômes qui sont rajoutés (comme par exemple la dérivée de P_k , dont il faut expliciter les racines) sont tous de degré $\leq d$ (en les nouvelles variables introduites). En fait, tout nouveau polynôme introduit par l'algorithme d'attribution de signe est ou bien la dérivée d'un polynôme précédemment introduit, ou bien le reste de la division de 2 polynômes déjà introduits[2].

La récurrence sous-jacente

Ceci nous suggère une recopie plus évidemment algorithmique de la preuve "abstraite" :
– examinons d'abord l'assertion suivante :

---

2 a) un pseudo-reste ferait aussi bien l'affaire, ce qui évite alors toute division dans les extensions considérées
b) mis à plat, l'algorithme d'attribution de signe dans $\mathbf{K}[\xi_1,\xi_2,...,\xi_k]$ par utilisation récursive du théorème 11 n'est autre que l'algorithme de Hörmander (cf. § 4)