Polynômes positifs et sommes de carrés

Pietro Vertechi et Zhiyuan Zhang

Encadrant : Olivier Wittenberg

23 juin 2012

Résumé

Dans cet exposé on résout d'abord le dix-septième problème de Hilbert, c'est-à-dire qu'un polynôme à coefficients réels qui prend toujours des valeurs positives peut s'écrire comme somme de carrés de fonctions rationnelles, mais pas forcément comme somme de carrés de polynômes (ce qui était la conjecture originale de Hilbert). On va passer par le "principe de transfert de Tarski", comme la preuve originale due à Artin, mais on va le montrer de façon plus moderne avec des outils de théorie des modèles. En plus, on va obtenir ces résultats pour les corps réels clos (c'est-à-dire qui se comportent comme $(\mathbf{R}, +, -, \cdot, \leq)$ au premier ordre) dont $\mathbf{R}$ est l'exemple plus important. Ensuite on va aborder une surprenante version sans dénominateurs du même théorème, due à Schmüdgen, qui est valable seulement dans le cas des variétés semi-algébriques compactes pour les corps réels clos archimédiens.

Introduction

En 1880, Hilbert voulut savoir quels polynômes à coefficients réels sont toujours ≥ 0. Évidemment les sommes de carrés de polynômes ne peuvent jamais être négatifs, il est donc naturel de se demander s'il y en a d'autres. Déjà en 1888 Hilbert avait compris que nécessairement il y en avait d'autres [4] , mais il ne connaissait pas d'exemples explicites.

Maintenant on connaît un exemple très facile en deux variables, dû à Motzkin [10] :

$f(x, y) = x^4y^2 + x^2y^4 - 3x^2y^2 + 1$

À cause de l'inégalité entre moyenne arithmétique et moyenne géométrique (c. à. d. $a+b+c \geq 3\sqrt[3]{abc}$ pour tout a, b, c réels positifs), on peut très facilement voir, en posant $a = x^4y^2$, $b = x^2y^4$, $c = 1$, que f n'est jamais négatif.

On peut aussi voir à la main que f n'est pas somme de carrés de polynômes :

Si $f(x, y) = \sum f_i(x, y)^2$ alors les f_i seraient des polynômes de degré au maximum 3, qui ne peuvent pas avoir de termes x^3 ou y^3, ni x^2 ou y^2, ni x ou y, donc

$f(x, y) = \sum(a_i + b_ixy + c_ix^2y + d_ixy^2)^2$

Mais cela entraîne $-3 = \sum b_i^2$, qui est absurde.

À cause de ça, en 1900, Hilbert essaya avec une autre question, le dix-septième problème de Hilbert [3] :

est-ce que un polynôme qui est toujours positif est somme de carrés de fonctions rationnelles ?

On peut s'amuser à vérifier qu'en fait le polynôme de Motzkin n'est pas un contre-exemple à cette nouvelle formulation :

$$f(x, y) = \left[\frac{x^2 - y^2}{x^2 + y^2}\right]^2 + \left[\frac{xy(x^2 + y^2 - 2)}{x^2 + y^2}\right]^2 + \left[\frac{x^2y(x^2 + y^2 - 2)}{x^2 + y^2}\right]^2 + \left[\frac{xy^2(x^2 + y^2 - 2)}{x^2 + y^2}\right]^2$$

La conjecture fut démontrée en 1927 par Artin [1]. Son outil principal était un résultat qui est aujourd'hui connu comme le principe de transfert de Tarski. Déjà à l'époque, il avait compris que le fait de travailler sur les réels n'a aucune importance, mais au contraire la démonstration est valable pour n'importe quel corps réel clos.

La preuve qu'on propose n'est pas celle de Artin, mais une preuve plus moderne qui utilise la théorie des modèles de Tarski. Après on va arriver à des résultats plus récents. D'abord le Positvstellensatz de Krivine [6], qui étudie les polynômes strictement positifs sur des variétés semi-algébriques : des

ensembles définis comme lieu de points où un nombre fini de polynômes fixés $(f_1, \ldots, f_n)$ est plus grand où égal à zéro. Là la situation est différente, parce que il est clair que il n'y a pas seulement les somme de carrés qui sont évidemment positives, mais aussi les somme de carrés fois des produits finis des f_i

Le Positivstellensatz de Krivine est un outil important pour prouver le dernier résultat qu'on obtient dans cet exposé : le Positivstellensatz de Schmüdgen [13]. Il s'agit d'une version sans dénominateurs du problème de Hilbert, sur les variétés semi-algébriques bornées. En fait on va voir que " la variété semi-algébrique associée à $f_1, \ldots, f_n$ est bornée " équivaut à une condition sur les polynômes : " le préordre engendré par $f_1, \ldots, f_n$ est archimédien ".

Le Positivstellensatz de Schmüdgen , à la différence du dix-septième problème de Hilbert et du Positivstellensatz de Krivine, n'est valable sur les corps réel clos en général. On va montrer un exemple de corps réel clos non archimédien, c'est-à-dire où la copie de $\mathbf{N}$ qu'on peut trouver là-dedans est bornée, où il y a des contre-exemples.

1 Ordres et préordres

Définition 1.1. Soit A un anneau commutatif unitaire. Un sous-ensemble $T \subseteq A$ est un préordre si : $T + T \subseteq T$, $T \cdot T \subseteq T$ et $\forall a \in A\ a^2 \in T$. Un préordre T est propre si $-1 \notin T$.

Remarque 1.2. Il existe un plus petit préordre appelé $\sum A^2 = \{a_1^2 + \cdots + a_n^2 \mid n \in \mathbf{N}, a_i \in A\}$. A admet des préordres propres si et seulement si $-1 \notin \sum A^2$.

Proposition 1.3. *Si T est un préordre, $a \in A$ alors $T + aT$ est un préordre. Si T est propre, A est un corps et $-a \notin T$ alors $T + aT$ est propre.*

Démonstration. $(T + aT) + (T + aT) = T + T + a(T + T) \subseteq T + aT$. On procède de la même façon pour les autres propriété. Pour la deuxième partie, si par l'absurde $-1 = s + at$ avec $s, t \in T$ alors $-a = \frac{(1+s)t}{t^2} \in T$ ($t \neq 0$ car sinon $-1 = s \in T$).

□

Définition 1.4. Un ordre est un préordre propre maximal par rapport à l'inclusion.

Remarque 1.5. Grâce au lemme de Zorn, il est clair que tout préordre propre est contenu dans un ordre.

Proposition 1.6. *Si T est un ordre, alors $T \cup -T = A$.*

Démonstration. Supposons que $a \notin T$ et $-a \notin T$. Alors $T \subset T + aT$ et $T \subset T - aT$ donc, comme T est maximal, $-1 \in T + aT$ et $-1 \in T - aT$. On peut écrire $-1 = q + ar = s - at$ avec $q, r, s, t \in T$. On a $(s + 1)(q + 1) = -a^2rt \in -T$ donc $1 = sq + s + q + 1 - s - q - qs \in -T$ absurde.

□

Proposition 1.7. *Si T est un ordre, alors $T \cap -T$ est un idéal premier.*

Démonstration. Si $a, b \in T \cap -T$ alors clairement $a + b \in T \cap -T$. Si $a \in T \cap -T$ et $b \in A$, on a $b \in T$ ou $-b \in T$. Dans les deux cas $ab \in T \cap -T$. Donc $T \cap -T$ est un idéal.
Supposons maintenant $ab \in T \cap -T$ mais $a, b \notin T \cap -T$. Sans perte de généralité $a, b \notin T$ (quitte à changer de signe), donc, par maximalité de T il existe $q, r, s, t \in T$ tels que $-1 = aq + r = bs + t$ donc $aqbs = (1 + r)(1 + t) \in -T$ donc $1 \in -T$, absurde.

□

Corollaire 1.8. *Donner un ordre sur un anneau A permet de préordonner l'anneau, c. à. d. définir un symbole de relation binaire qui respecte les axiomes de la section suivante sauf " $a \leq b$ et $b \leq a$*

implique $a = b$ " (anti-symétrie). Pour avoir l'anti-symétrie il faut quotienter par l'idéal premier $T \cap -T$

Exemple 1.9. L'anneau $\mathbf{R}[x]$ avec $f(x) \in T$ ssi pour x suffisamment grand $f(x) \geq 0$ est un anneu avec un ordre, qui est contenu dans son corps de fractions $\mathbf{R}(x)$ toujours avec l'ordre de la comparaison asymptotique.

2 Les corps réels clos

Dans cette section on veut décrire la théorie au premier ordre des corps ordonnés (avec un ordre total) et des corps réels clos.

Le langage des corps ordonnés est le langage des corps (c'est à dire $0, 1, +, -, \cdot, =$) avec en plus le symbole de relation binaire $\leq$ (mais on utilisera aussi $\geq$, qui est défini par : $a \geq b$ ssi $b \leq a$).

Les axiomes sont les axiomes de corps avec en plus, pour tout a,b,c :

$a \leq a$

$a \leq b$ et $b \leq c$ implique $a \leq c$

$a \leq b$ et $b \leq a$ implique $a = b$

$a \leq b$ ou $b \leq a$

si $a, b \geq 0$ alors $ab \geq 0$

si $a \leq b$ alors $a + c \leq b + c$

Remarque 2.1. Un corps ordonné a caractéristique 0, parce que $1 + \cdots + 1 > 0$

Proposition 2.2. *Il y a une bijection entre les modèles de cette théorie et les corps avec un ordre, obtenue en disant que $a \geq b$ ssi $a - b \in T$*

Démonstration. Soit K un corps, T un ordre. On définit : $a \geq b$ si $a - b \in T$. Alors $0 = 0^2 \in T$ donc $a \leq a$. Si $a \leq b$ et $b \leq c$ on a $c - a = (c - b) + (b - a) \in T$ donc $a \leq c$. En outre $a \leq b$ ou $b \leq a$ parce que $T \cup -T = A$, donc $a - b \in T$ ou $b - a \in T$. Si $a \leq b$ et $b \leq a$ alors $a - b \in T \cap -T$ mais $T \cap -T$ est un idéal premier de K, donc il n'y a que zéro. Si a, b sont positifs, alors aussi le produit, comme $T^2 \subseteq T$. Si $a \leq b$ alors $(b + c) - (a + c) = b - a \in T$ donc $a + c \leq b + c$.

Vice versa, soit A un anneau préordonné. On définit $T := A_{\geq 0}$. Si $a, b \geq 0$ alors $ab \geq 0$ et aussi $a \geq 0 \Rightarrow a + b \geq b \geq 0 \Rightarrow a + b \geq 0$ donc $T^2 \subseteq T$ et $T + T \subseteq T$. $a^2 = (-a)^2$ et soit $a \geq 0$ soit $-a \geq 0$, dans les deux cas $a^2 \geq 0$, donc $\sum A^2 \subseteq T$. Si $-1 \in T$ on aurait $-1 \geq 0$, mais $1 = 1^2 \geq 0$, donc $-1 = 0$, absurde. Il est aussi clair que T est maximale : soit S un ordre qui prolonge T. S'il existait $s \in S - T$, comme $T \cup -T = K$, on aurait $s \notin T \Rightarrow \in -T \Rightarrow s \in -S$, donc $s \in S \cap -S$ et $s \neq 0$ (sinon il serait dans T) mais cela n'est pas possible parce qu'on a vu dans la première partie de la preuve que $S \cap -S = \{0\}$ pour tout ordre S. □

On peut maintenant se demander quels corps peuvent être ordonnés et comment. La réponse est

une simple traduction des résultats de la section précédente :

Proposition 2.3. *Un corps K peut être ordonné ssi -1 n'est pas somme de carrés. Si $a \in K$, il existe un ordre où $a > 0$ ssi $-a$ n'est pas somme de carrés.*

Démonstration. Pour la première partie, il suffit d'appliquer la remarque 1.5 avec, comme préordre de départ, $\sum A^2$. Pour la deuxième partie, on peut voir que $\sum A^2 + a\sum A^2$ est un préordre propre par la proposition 1.3 et est donc contenu dans un ordre par la remarque 1.5. □

Définition 2.4. Un corps ordonné est réel clos s'il n'admet pas d'extensions finies de corps ordonnés.

Exemple 2.5. $\mathbb{R}$ est réel clos comme sa seule extension finie de corps est $\mathbb{C}$ qui n'est pas ordonnable.

Maintenant on va montrer quelques propriétés des corps réels clos pour pouvoir en donner une caractérisation avec des énoncés du premier ordre.

Dans la suite K est un corps réel clos.

Proposition 2.6. *Si $a \geq 0$ alors il existe b tel que $a = b^2$*

Démonstration. Supposons le contraire. Soit $F = K[\sqrt{a}]$. $T = \{\sum c_i(d_i\sqrt{a} + e_i)^2 | c_i, d_i, e_i \in K, c_i \geq 0\}$ est un préordre propre. En fait si $-1 = \sum c_i(d_i\sqrt{a} + e_i)^2$ on a $-1 = \sum c_i(d_i^2 a + e_i^2) \geq 0$, absurde. Donc T peut être prolongé à un ordre et on trouve une extension finie de corps ordonnés de K.

□

Proposition 2.7. *Tout polynôme non constant de degré impair a au moins une racine.*

Démonstration. Raisonnons par l'absurde. Soit f le plus petit contrexemple (donc il est irréductible). Posons $F = K[x]/(f(x))$. $T = \{\sum c_i[g_i]^2(x) | c_i \geq 0\} \subseteq F$ est un préordre propre. En fait si $-1 = \sum c_i[g_i]^2(x)$ (avec, sans perte de généralité $\deg(g_i) < \deg(f)$) on a $-1 + h(x)f(x) = \sum c_i g_i^2(x)$, avec $deg(h)$ impair (les coefficient dominants des $c_i g_i^2(x)$ sont strictement positifs, donc leur somme est non nulle) et $deg(h) < deg(f)$. Soit $p(x)$ un facteur irréductible de degré impair de $h(x)$. Il admet une racine $\alpha \in K$, par minimalité de f, donc $-1 = \sum c_i g_i^2(\alpha) \geq 0$, absurde.

Or, il suffit de prolonger T à un ordre pour trouver une extension finie de corps ordonnés de K, ce qui serait absurde.

□

Théorème 2.8. *Soit K un corps ordonné où les éléments positifs ont une racine carrée et les polynômes de degré impair ont au moins une racine. Alors $K(\sqrt{-1})$ est la seule extension finie de corps de K et est donc algébriquement clos.*

Démonstration. Soit $K \subseteq L$ une extension propre finie de corps. Soit H un 2-Sylow de $Gal\,(L/K)$. Par la correspondance de Galois, il est associé à son corps fixe, E, de degré impair sur K. Soit $\alpha \in E$: α est la racine d'un polynôme irréductible dans K de degré impair (comme $[E : K]$ est impair), donc de degré 1 par la remarque précédente. Comme α était quelconque, on a E=K, donc $H = Gal\,(L/K)$. On sait que les p-groupes sont résolubles et que le seul p-groupe simple est $\mathbf{Z}/p\mathbf{Z}$, donc on peut écrire : $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = H$ où $G_i/G_{i-1} \cong \mathbf{Z}/2\mathbf{Z}$, qui correspond à une tour d'extensions de corps $K = F_k \subseteq \cdots \subseteq F_0 = L$ où chaque extension est de degré 2.
Or $K(\sqrt{-1})$ est la seule extension de degré 2 de K, comme il contient les racines carrées de tous les éléments de K, donc $F_{k-1} = K(\sqrt{-1})$. F_{k-2} devrait donc correspondre à une extension de degré 2 de $K(\sqrt{-1})$, mais ce corps contient les racines carrés de ses éléments :
$a + ib = (a^2 + b^2)(\alpha + i\beta) = \left[\sqrt{a^2 + b^2}\left(\sqrt{\frac{1+\alpha}{2}} + i\sqrt{\frac{1-\alpha}{2}}\right)\right]^2$.
Donc on a que forcément k=1 et $L = K(\sqrt{-1})$ □

Définition 2.9. Un corps ordonné respecte le principe des valeurs intermédiaires si : $\forall p \in K[x]$ s'il existe $a < b \in K$ tel que $p(a) < 0$ e $p(b) > 0$ alors il existe $c \in]a, b[$ tel que $p(c) = 0$

Maintenant on a les outils pour montrer l'équivalence entre différentes notions de "réel clos".

Théorème 2.10. *Soit K un corps ordonné. Les conditions suivantes sont équivalentes :*

-K est réel clos

-les polynômes de degré impair admettent une racine dans K et les éléments positifs de K ont une racine carrée

-$K(\sqrt{-1})$ est algébriquement clos.

-K respecte le principe des valeurs intermédiaires.

Démonstration. On a déjà montré $1 \Rightarrow 2 \Rightarrow 3$

$3 \Rightarrow 4$ il suffit d'écrire un polynôme p comme $\prod(x - a_i)\prod[(x - b_j)^2 + c_j]$ avec $a_i, b_j, c_j \in K$ et $c_j > 0$.
Or, si f change de signe entre a et b, alors il y a forcément un nombre impair de a_i entre a et b, donc

au moins un.

$4 \Rightarrow 2$ si K respecte le principe des valeurs intermédiaires, alors les polynômes de degré impair ont une racine et les éléments positifs ont une racine carrée. En fait si p a degré impair et est unitaire, pour $x << 0$ on a $p(x) < 0$ et pour $x >> 0$ on a $p(x) > 0$ donc il doit s'annuler quelque part. De la même façon $x^2 - a$ si $a > 0$ est négatif en 0 et positif pour x très grand, donc il a une racine.

$3 \Rightarrow 1$ est évident : la seule extension de K est $K(\sqrt{-1})$ qui ne peut pas être ordonnée parce que -1 est un carré. □

Définition 2.11. Soit F un corps ordonné. On dit que $F \subseteq \overline{F}$ est une clôture réelle de F si :

- $F \subseteq \overline{F}$ est une extension algébrique de corps ordonné.

- $\overline{F}$ est réel clos.

Proposition 2.12. *Tout corps ordonné a une clôture réelle.*

Démonstration. Soit F un corps ordonnés et F* une clôture algébrique. Par le lemme de Zorn, on peut trouver, parmi les extensions ordonnés de F (qui prolongent l'ordre de F) contenues dans F*, avec la relation $K \preceq K'$ si $K \subseteq K'$ et l'ordre de K' prolonge l'ordre de K, une, qu'on appelle $\overline{F}$, qui est maximale. Clairement $\overline{F}$ n'admet pas d'extensions finies ordonnées et il est algébrique sur F, étant contenu dans sa clôture algébrique. □

Lemme 2.13. *Soit F un corps ordonné et K, K' deux clôtures réelles. Soit f un polynôme irréductible unitaire à coefficients dans F. Alors le nombre de racines de f dans K est égal au nombre de racines de f dans K'.*

Démonstration. Soit $f(x) = \prod(x-\alpha_t) = \prod_{1\leq t\leq m}(x-\beta_t)\prod_{1\leq s\leq l}(x-\gamma_s)(x-\overline{\gamma}_s)$ avec $\gamma_s = a_s+\sqrt{-1}b_s$ une décomposition de f dans $K(\sqrt{-1})$. f a degré $n = m + 2l$. Définissons la forme quadratique $\rho = \sum_{1\leq t\leq n}\left(\sum_{r=1}^n \alpha_t^{r-1}x_r\right)^2$. Or, étant symétrique dans les α_t, ρ est à coefficients dans F. On a :

$$\sum_{1\leq t\leq n}\left(\sum_{r=1}^n \alpha_t^{r-1}x_r\right)^2 =$$

$$\sum_{1\leq t\leq m}\left(\sum_{r=1}^n \beta_t^{r-1}x_r\right)^2 + \sum_{1\leq s\leq l}\left(\sum_{r=1}^n \gamma_s^{r-1}x_r\right)^2 + \sum_{1\leq s\leq l}\left(\sum_{r=1}^n \overline{\gamma}_s^{r-1}x_r\right)^2 =$$

$$\sum_{1\leq t\leq m}\left(\sum_{r=1}^n \beta_t^{r-1}x_r\right)^2 + \sum_{1\leq s\leq l} 2\left(\sum_{r=1}^n \frac{\gamma_s^{r-1}+\overline{\gamma}_s^{r-1}}{2}x_r\right)^2 + \sum_{1\leq s\leq l} 2\left(\sum_{r=1}^n \frac{\gamma_s^{r-1}-\overline{\gamma}_s^{r-1}}{2}x_r\right)^2 =$$

$$\sum_{1\leq t\leq m} y_t^2 + \sum_{1\leq s\leq l} 2(y_{m+2s-1}^2 - y_{m+2s}^2) =: \rho'$$

où $y_t = \sum_{r=1}^n \beta_t^{r-1}x_r$, $y_{m+2s-1} = \sum_{r=1}^n \frac{\gamma_s^{r-1}+\overline{\gamma}_s^{r-1}}{2}x_r$ et $y_{m+2s} = \sum_{r=1}^n \frac{\gamma_s^{r-1}-\overline{\gamma}_s^{r-1}}{2}x_r$

Donc ρ est conjuguée à ρ' par l'application linéaire qui envoie les x dans les y. ρ n'est pas dégénérée, parce que si on définit $z_t = \sum_{r=1}^{n} \alpha_t^{r-1} x_r$ on a que ρ est la forme quadratique standard dans les z_t. Or, les z_t sont une base parce que la matrice de changement de base est la matrice de Vandermonde des α_t, qui sont dinstincts, donc est inversible.

Donc ρ et ρ' sont inversibles et conjuguées par une application linéaire qui est donc inversible, donc elles ont la même signature (qui est l'indice de positivité moins l'indice de négativité), donc ρ a signature m.

Cela nous dit que m (le nombre de racines de f dans une clôture réelle), ne dépend pas du choix de la clôture réelle, parce que ρ est une forme quadratique à coefficients dans F et donc on peut en calculer la signature sans sortir de F. □

Proposition 2.14. *La clôture réelle est unique, à isomorphisme près.*

Démonstration. Soit F un corps ordonné. Soient K et K' deux clôtures réelles. Soit L et L' deux sous-corps ordonné de K et K' respectivement, et ϕ un isomorphisme entre eux, de façon que tel isomorphisme ne puisse pas être prolongé. On peut trouver L, L', ϕ grâce au lemme de Zorn. Soit p un polynôme à coefficient dans L, irréductible, qui admet au moins une racine dans K. Soit $\alpha \in K$ la plus petite racine de ce polynôme et $\alpha' \in K'$ la plus petite racine de $p' := \phi(p)$. Or, il est clair qu'on peut prolonger ϕ à un isomorphisme $\hat{\phi}$ de $L(\alpha)$ à $L'(\alpha')$. Il reste à vérifier que $\hat{\phi}$ préserve l'ordre.

Supposons que $f(\alpha) > 0$, avec f a coefficients dans L. Alors, par le théorème de l'élément primitif, il existe $\beta \in K$ tel que $\sqrt{f(\alpha)} \in L(\beta)$ est pour tout γ racine de p, $\sqrt{\gamma - \alpha} \in L(\beta)$. Soit f le polynôme minimal de β sur L. Par le lemme 2.13 $\phi(f)$ admet au moins une racine dans K'. On en choisit une au hasard et on l'appelle β'. Soit $\eta : L(\beta) \to L'(\beta')$ l'isomorphisme qui envoie β sur β' et qui prolonge ϕ. $\eta\alpha$ est une racine de $\eta(p) = \phi(p)$ et elle est la plus petite, parce que les autres sont du type $\eta(\gamma) = \eta(\sqrt{\gamma - \alpha})^2 + \eta(\alpha) > \eta(\alpha)$.

Comme η coincide avec $\hat{\phi}$ sur α, il prolonge $\hat{\phi}$. Donc $\hat{\phi} f(\alpha) = \eta(f(\alpha)) = \eta(\sqrt{f(\alpha)})^2 > 0$, donc $\hat{\phi}$ préserve l'ordre.

Comme on avait supposé ϕ maximal on a une absurdité, donc $L = K$ et $L' = K'$ et les deux clôtures sont isomorphes.

□

Corollaire 2.15. *Soit $F \subseteq K$ une extension de corps ordonnés (où l'ordre de K prolonge l'ordre de F) avec K réel clos. Soit $F \subseteq \overline{F}$ une clôture réelle de F. Alors $\overline{F}$ peut être immergé dans K par un morphisme qui fixe F.*

Démonstration. Par le théorème précédent, il suffit de montrer qu'on peut trouver une clôture réelle de F incluse dans K. On considère l'ensemble des éléments de K qui sont algébrique sur F, on l'appelle $\hat{F}$. Or, $\hat{F}$ est un corps, il est ordonné par l'ordre de K et il respecte le principe des valeurs intermédiaires : soit $p \in \hat{F}[x]$, avec $p(a) < 0$, $p(b) > 0$ et $a < b$. Alors il existe $c \in K$ avec $a < c < b$ et $p(c) = 0$, donc c est algébrique sur $\hat{F}$, donc sur F, donc appartient à $\hat{F}$ □

3 Élimination des quantificateurs

Le but de cette section c'est de prouver l'élimination des quantificateurs dans la théorie des corps réels clos, c'est-à-dire la théorie des corps ordonnés avec en plus le principe des valeurs intermédiaires, qui peut être écrit comme un schéma d'énoncés du premier ordre.

Définition 3.1. Une théorie $\mathcal{T}$ admet l'élimination des quantificateurs si, pour tout $\phi(x_1, \dots, x_n)$ formule du premier ordre, il existe $\psi(x_1, \dots, x_n)$ formule sans quantificateurs, telle que

$\mathcal{T} \vdash \forall x_1, \dots, x_n \ \phi(x_1, \dots, x_n) \Leftrightarrow \psi(x_1, \dots, x_n)$

Pour parvenir à notre but, on rappelle le résultat suivant :

Théorème 3.2. *Soit $\phi(x_1, \dots, x_n)$ une formule du premier ordre. Il existe $\psi(x_1, \dots, x_n)$ formule sans quantificateurs tel que $\mathcal{T} \vdash \forall x_1, \dots, x_n \ \phi(x_1, \dots, x_n) \Leftrightarrow \psi(x_1, \dots, x_n)$ si et seulement si, pour toute paire $\mathfrak{M}, \mathfrak{N}$ de modèles de $\mathcal{T}$ avec une sous-structure $\mathfrak{O}$ en commun, on a $\forall a_0, \dots, a_n \in \mathfrak{O}$ que $\mathfrak{M} \models \phi(a_0, \dots, a_n) \Leftrightarrow \mathfrak{N} \models \phi(a_0, \dots, a_n)$*

Soit $\phi(x_1, \dots, x_n)$ une formule de longueur minimale qui n'est pas équivalente à une formule sans quantificateurs. On a : $\phi(x_1, \dots, x_n) = \exists y \ \hat{\phi}(y, x_1, \dots, x_n)$ ou bien $\neg\phi(x_1, \dots, x_n) = \exists y \ \hat{\phi}(y, x_1, \dots, x_n)$ avec $\hat{\phi}$ une formule plus courte. Quitte à changer ϕ avec sa négation, on peut supposer qu'on est dans le premier cas. Comme $\hat{\phi}$ est plus courte, elle est équivalente à une formule $\tilde{\phi}$ sans quantificateurs, donc ϕ équivaut à $\exists y \ \tilde{\phi}$. Par conséquent il suffit de montrer les hypothèses du théorème pour les formules du type : $\exists y \ \tilde{\phi}(y, x_1, \dots, x_n)$, où $\tilde{\phi}$ est sans quantificateurs.

En plus, comme $\mathfrak{O}$ est une sous-structure d'un corps ordonné, il doit être un anneau intègre, donc il aura, à isomorphisme près, une unique clôture réelle de son corps des fractions, qu'on appelle $\mathfrak{L}$ et qu'on peut considérer comme une sous-structure commune de $\mathfrak{M}$ et de $\mathfrak{N}$.

Donc, en conclusion, il nous suffit de montrer que, si L et M sont deux corps réels clos avec $L \subseteq M$ et $a_1, \dots a_n \in L$ alors $\exists y \in L \ \tilde{\phi}(y, a_1, \dots, a_n)$ ssi $\exists y \in M \ \tilde{\phi}(y, a_1, \dots, a_n)$ (une fois qu'on a fait cela, la formule est vraie dans M ssi elle est vraie dans L ssi elle est vraie dans N et on a terminé).

Cela veut dire, concrètement, que si L est réel clos, et un système d'inégalités à une variable n'admet pas de solution dans L, alors on va pas en trouver dans des extensions de L.

On peut écrire $\tilde{\phi} = \bigvee \tilde{\phi}_r$ où chaque $\tilde{\phi}_r$ est une formule du type $\bigwedge_{i=1}^{k} f_i(y) \geq 0 \wedge \bigwedge_{j=1}^{l} g_j(y) > 0$, où les variables libres $a_0, \dots, a_n$ jouent le rôle des coefficients des f_i et des g_j. Supposons d'avoir prouvé le résultat pour chaque $\tilde{\phi}_r$. Alors, si il existe $y \in M$ tel que $\tilde{\phi}(y, a_1, \dots, a_n)$ on peut trouver r tel que $\exists y \in M \ \tilde{\phi}_r(y, a_1, \dots, a_n)$ donc $\exists y \in L \ \tilde{\phi}_r(y, a_1, \dots, a_n)$ et donc

$\exists y \in L\ \tilde{\phi}(y, a_1, \ldots, a_n)$

Par conséquent, on doit seulement prouver le lemme suivant :

Lemme 3.3. *Soit $L \subseteq M$ deux corps réels clos, $f_i, g_j \in L[y]$*

Si le système suivant admet une solution $\overline{y}$ dans M, alors il admet une solution dans L :

$$\begin{cases} f_1(y) \geq 0 \\ \qquad\vdots \\ f_k(y) \geq 0 \\ g_1(y) > 0 \\ \qquad\vdots \\ g_l(y) > 0 \end{cases}$$

Démonstration. D'abord on peut supposer que les f_i ne sont pas identiquement nuls. Or, soit $z_1 < \cdots < z_n$ l'ensemble des points de L où au moins un parmi ces polynômes vaut zéro. Si $\overline{y} \in \{z_1, \ldots, z_n\}$ on a terminé. Sinon, on a $\overline{y} \in]z_i, z_{i+1}[$ pour quelque i, ou bien $\overline{y} \in]-\infty, z_1[$ ou bien $y \in]z_n, \infty[$. En tout cas, si on prend $x \in L$ qui est dans le même intervalle que $\overline{y}$, il satisfait toutes les inégalités. En fait, les polynomes qu'on considère sont de signe constant dans les intervalles, sinon il y aurait des autres zéros par le principe des valeurs intermédiaires. □

On a donc montré l'élimination des quantificateurs dans la théorie des corps réel clos. Les résultats suivants en découlent immédiatement :

Définition 3.4. Un système d'inégalités larges est un système du type :

$$\begin{cases} f_1(x_1, \ldots, x_n) \geq 0 \\ \qquad\qquad\vdots \\ f_k(x_1, \ldots, x_n) \geq 0 \end{cases}$$

Par contre, en général, un système d'inégalités est un système du type :

$$\begin{cases} f_1(x_1, \ldots, x_n) \geq 0 \\ \qquad\qquad\qquad\qquad \vdots \\ f_k(x_1, \ldots, x_n) \geq 0 \\ g_1(x_1, \ldots, x_n) > 0 \\ \qquad\qquad\qquad\qquad \vdots \\ g_l(x_1, \ldots, x_n) > 0 \end{cases}$$

Théorème 3.5. Principe de transfert de Tarski

Soit $M \subseteq K$ avec M un corps réel clos et K un corps ordonné qui prolonge l'ordre de M. Un système d'inégalités à coefficients dans M admet une solution dans M si et seulement si il admet une solution dans K.

Démonstration. Supposons qu'il y ait une solution dans K. Alors il y a aussi une solution dans la clôture réelle de K, qu'on appelle N. Le fait qu'un système ait une solution s'exprime au premier ordre, donc équivaut à une formule sans quantificateurs qui est vraie dans M si et seulement si elle vraie dans N. □

Théorème 3.6. Principe de transfert de Tarski généralisé

Soit F, K, L trois corps ordonnés. On suppose que K et L sont deux extensions de F (qui prolongent l'ordre) et que L est réel clos. Si un système d'inégalité à coefficients dans F admet une solution dans K, alors il admet une solution dans L.

Démonstration. S'il y a une solution dans K, évidemment il y a aussi une solution dans $\overline{K}$. Le fait qu'il y ait une solution s'exprime comme une formule du premier ordre $\phi(a_0, \ldots, a_n)$ où les a_i sont les coefficients du système d'inégalités. Par l'élimination des quantificateurs, on peut choisir ϕ sans quantificateurs, donc elle est vraie dans $\overline{K}$ ssi elle est vrai dans L. □

Corollaire 3.7. *Soit $M \subseteq A$ avec M un corps réel clos et A un anneau ordonné qui prolonge l'ordre de M. Un système d'inégalités larges à coefficients dans M admet une solution dans M si et seulement si il admet une solution dans A.*

Démonstration. Comme $T \cap -T$ est un idéal premier de A (lemme 1.3) on a que $D := A/T \cap -T$ est un anneau intègre ordonné où 0 est le seul élément positif est négatif à la fois. Soit K le corps de fractions de D. On peut définir un ordre sur K de la façon suivante :

$\frac{a}{b} \geq 0$ ssi $a \geq 0$ et $b > 0$ où $a \leq 0$ et $b < 0$.

Si le système d'inégalités a une solution dans A, alors il a une solution dans D (parce que les inégalités, étant larges, restent vraies après avoir quotienté) donc dans K, donc dans M par le principe de transfert de Tarski. □

4 Le dix-septième problème de Hilbert

Donc on 1900 Hilbert posa le problème suivant, résolu en 1927 par Artin :

Théorème 4.1. Dix-septième problème de Hilbert

Soit $f \in \mathbf{R}[x_1, \ldots, x_n]$ un polynôme tel que $\forall a_1, \ldots, a_n \in \mathbf{R}\ f(a_1, \ldots, a_n) \geq 0$. Alors f peut s'exprimer comme somme de carrés de fonctions rationnelles à coefficients réels.

Démonstration. On va montrer le résultat pour n'importe quel R corps réel clos.
Supposons que f ne s'exprime pas comme somme de carrés de fonctions rationnelles. Alors, par la proposition 2.2, on peut ordonner $R(x_1, \ldots, x_n)$ de façon que $f < 0$ (cet ordre prolonge l'ordre des réels, parce que les éléments de $R_{\geq 0}$ admettent une racine carré). Cela veut dire que f, considéré comme polynôme dans $R(x_1, \ldots, x_n)[t_1, \ldots, t_n]$ prend une valeurs négatives si on lui donne comme arguments le n-uplet $(x_1, \ldots, x_n)$ donc le système à une inégalité $f < 0$ a une solution dans $R(x_1, \ldots, x_n)$, donc aussi dans R, par le principe de transfert de Tarski, donc il existe $a_1, \ldots, a_n \in R$ tel que $f(a_1, \ldots, a_n) < 0$. □

Corollaire 4.2. *Soit $f \in \mathbf{Q}[x_1, \ldots, x_n]$ un polynôme tel que $\forall a_1, \ldots, a_n \in \mathbf{Q}\ f(a_1, \ldots, a_n) \geq 0$. Alors f peut s'exprimer comme somme de carrés de fonctions rationnelles à coefficients rationnels.*

Démonstration. On procède comme dans le théorème précédent : si f ne s'écrivait pas comme somme de carrés, on pourrait trouver un ordre sur $\mathbf{Q}(x_1, \ldots, x_n)$ où $f < 0$, donc il y aurait une solution à $f < 0$ dans $K := \mathbf{Q}(x_1, \ldots, x_n)$. Donc il y a aussi une solution dans n'importe quel corps réel clos qui prolonge F (théorème 3.6), par exemple $\mathbf{R}$. Mais alors, comme f prend des valeurs négatives sur $\mathbf{R}$, il doit prendre des valeurs négatives sur $\mathbf{Q}$ par densité. □

Après avoir prouvé l'existence d'une décomposition comme somme de carrés de fonctions rationnelles, il est intéressant de voir combien de carrés il faut additionner. En général, lorsqu'on choisi un corps K on peut se demander quel est le nombre minimal de carrés nécessaires pour écrire un élément qui peut s'écrire comme somme de carrés. On appelle ce nombre-là le "nombre de Pythagore" et on le note p(K). Nous sommes intéressé à l'étude des $t(n) := p(\mathbf{R}(x_1, \ldots, x_n))$.
Dans l'introduction on a trouvé une écriture du polynôme de Motzkin comme somme de quatre carrés. En fait, on ne peut pas faire mieux : trois carrés ne sont pas suffisants, comme Cassels, Ellison et Pfister ont démontré en 1971 [2]. Par contre, en deux variables quatre carrés suffisent toujours, d'après Hilbert [5] et Landau [8]. Plus en général, Pfister a prouvé que $t(n) \leq 2^n$ [11], mais la valeur

exacte est inconnue, même pour n=3.

Avec les mêmes outils on peut prouver un autre théorème important, qui, historiquement, a été trouvé beaucoup plus tard : le Positivstellensatz.

Définition 4.3. Soit $I = \{f_1, ..., f_k\}$ un sous-ensemble fini de $R[x_1, \ldots, x_n]$ (où R est un corps réel clos). On appelle

$T_I = \{\sum_{J \subset I} g_J^2 \prod_{i \in J} f_i \mid g_J \in R[x_1, \ldots, x_n]\}$ et $W_I = \{(a_1, \ldots, a_n) \mid f_i(a_1, \ldots, a_n) \geq 0 \; \forall i\}$

Il est facile de voir que T_I est le plus petit préordre qui contient I.

Théorème 4.4. Positivstellensatz

Soir R un corps réel clos. Si on a $f \in R[x_1, \ldots, x_n]$ tel que $f(x) > 0 \; \forall x \in W_I$, alors il existe $s, t \in T_I$ tel que $sf = t + 1$

Démonstration. On dénote $T_1 = T - fT$. Si T_1 est un préordre propre, alors il existe un ordre P qui contient T_1. On munit $R[x_1, \ldots, x_n]$ de l'ordre P. On considéré le système suivant :

$$\begin{cases} -f(x) \geq 0 \\ f_1(x) \geq 0 \\ \vdots \\ f_k(x) \geq 0 \end{cases}$$

Il admet une solution dans $R[x_1, \ldots, x_n]$. D'après le corollaire 3.7, il admet un solution dans R. On a une contradiction. Donc il faut que $-1 \in T_1$, cela veut dire qu'il existe $s, t \in T_I$ tel que $sf = t + 1$.

□

5 Préordres archimédiens et le théorème de Schmüdgen

Définition 5.1. Un préordre P de $\mathbf{R}[x_1, \ldots, x_n]$ est appelé archimédien si $\forall f \in R[x_1, \ldots, x_n]$ il existe un entier N tel que $N + f \in P$.

On a l'équivalence suivante :

Proposition 5.2. *W_I est borné ssi T_I est archimédien.*

Démonstration. D'abord on suppose que T_I soit archimédien. Alors il existe un entier N tel que $h = N - \sum_{i=1\ldots n} x_i^2 \in T_I$. Alors $\forall a \in W_I$ on a $h(a) \geq 0$, donc W_I est borné.

Supposons maintenant que W_I soit borné. Alors il existe un entier N tel que $h = N - \sum_{i=1\ldots n} x_i^2$ est toujours positif sur W_I. D'après le Positivstellensatz, il existe $s, t \in T_I$ tel que $sh = 1 + t$.
On peut construire un préordre $T_1 = T + hT$. On a :

Lemme 5.3. *Si Q est un préordre qui contient $N - \sum_{i=1\ldots n} x_i^2$ pour un entier N, alors Q est un préordre archimédien.*

Démonstration. On a $N + \frac{1}{4} \pm x_i = (N - \sum_{j=1\ldots n} x_j^2) + (x_i \pm \frac{1}{2})^2 + \sum_{j \neq i} x_j^2$, donc $N + 1 - x_i \in Q$.
Si pour f_1, f_2, il existe des entiers N_1, N_2 tel que $N_i \pm f_i \in Q$. Alors on a $(N_1 + N_2) \pm (f_1 + f_2) \in Q$.

$N_1N_2 + f_1f_2 = \frac{1}{2}((N_1 + f_1)(N_2 + f_2) + (N_1 - f_1)(N_2 - f_2)) \in Q$ et
$N_1N_2 - f_1f_2 = \frac{1}{2}((N_1 - f_1)(N_2 + f_2) + (N_1 + f_1)(N_2 - f_2)) \in Q$

En raisonnant par récurrence sur la complexité du polynôme, on peut montrer que Q est un préordre archimédien.

□

D'après le lemme ci-dessus, T_1 est un préordre archimédien. Alors il existe un entier m tel que $m - t \in T_1$, c'est-à-dire il existe $u, v \in T$, tel que $(m - t) = u + vh$.
Alors on a $(m - t)(1 + t) = (u + vh)(1 + t) = u + ut + vsh^2 \in T_I$, mais
$(m - t)(1 + t) = m - t + mt - t^2 = m - t + \frac{m^2}{4} - (\frac{m}{2} - t)^2$, donc $m + \frac{m^2}{4} - t \in T_I$, donc pour tout entier $c > m + \frac{m^2}{4}$ on a $c - t \in T_I$. De la même façon, il existe l tel que $l + h \in T_1$, c'est-à-dire, il existe p, q, tel que $l + h = p + qh$, alors on a $(l + h)(1 + t) = (p + qh)(1 + t) = p(1 + t) + qsh^2 \in T_I$, donc $l + h + t(l + h) = l + h + (l + N)t - t\sum_{i=1\ldots n} x_i^2 \in T_I$ donc $l + h + (l + N)(t - c + c) \in T_I$ donc $l + h + (l + N)c \in T$.
D'après le lemme ci-dessus, on en déduit que T_I est archimédien.

□

Maintenant on peut montrer un théorème très important :

Théorème 5.4 (Schmüdgen)**.** *On suppose que W_I est borné. Si $f \in \mathbf{R}[x_1, \ldots, x_n]$ est strictement positif sur W_I, alors $f \in T_I$*

Démonstration. Comme W_I est borne, d'après la proposition ci-dessus, T_I est un préordre archimédien. Comme f est strictement positif sur W_I, d'après le Positivstellensatz, il existe $s, t \in T_I$ tel que $sf = t + 1$.

Si on prend k suffisamment grand, on a $2k - 1 - s^2 f \in T_I$ et $2k - s \in T_I$. Il existe un entier r tel que $f + r \in T_I$. Si $r < 0$, on a $f \in T_I$. Donc on peut supposer que $r \geq 0$. Alors

$k^2 f + k^2 r - 1 = (k-s)^2(f+r) + 2ks(f+r) - s^2(f+r) - 1$

$= (k-s)^2(f+r) + 2k(sf-1) + 2k(1+sr) - s^2(f+r) - 1$

$= (k-s)^2(f+r) + 2k(sf-1) + rs(2k-s) + (2k - 1 - s^2 f) \in T_I$ (*)

donc $f + r - \frac{1}{k^2} \in T_I$. k ne dépend que de s. Si $r - \frac{1}{k^2} \geq 0$, on peut remplacer r par $r - \frac{1}{k^2}$ dans (*) : $k^2 f + k^2 r - 2 = (k-s)^2(f + r - \frac{1}{k^2}) + 2k(sf-1) + (r - \frac{1}{k^2})s(2k-s) + (2k - 1 - s^2 f)$ comme $r - \frac{1}{k^2} \geq 0$ et $f + r - \frac{1}{k^2} \in T_I$, on a encore une fois que $f + r - \frac{2}{k^2} \in T_I$. il existe un entier a, tel que $r - \frac{a-1}{k^2} \geq 0$, mais $r - \frac{a}{k^2} < 0$, alors par récurrence, on peut montrer que $f + r - \frac{a}{k^2} \in T_I$, donc $f \in T_I$

□

Remarque 5.5. Il est facile de voir que la même conclusion est vraie et toute la preuve marche sans rien changer si on remplace $\mathbf{R}$ par un corps F réel clos archimédien, c'est-à-dire, pour $\forall a \in F$, il existe un entier N tel que $N \geq a$.

Remarque 5.6. Il est nécessaire que f soit strictement positif, sinon on peut prendre $f(x,y,z) = x^4y^2 + x^2y^4 - 3x^2y^2z^2 + z^6$ (l'homogénéisé du polynôme de Motzkin) sur $\mathbf{R}^3$. Soit $I = \{1 - x^2 - y^2 - z^2\}$. Si l'on avait $f(x,y,z) = \sum f_i^2 (+(1 - x^2 - y^2 - z^2) \sum g_j^2 = \sum f_i^2 + \sum (g_j \sqrt{1 - x^2 - y^2 - z^2})^2$ alors on aurait $f(x,y,z) = \sum appr(f_i)^2 + \sum appr(g_j \sqrt{1 - x^2 - y^2 - z^2})^2$ où $appr(p(x,y,z))$ est l'approximation au troisième ordre pour $x, y, z \to 0$. En fait, en général, si on a $f = \sum h_i^2$ avec les h_i des fonctions C^∞ et f un polynôme homogène de degré 6, on a, pour $x, y, z \to 0$, que $\limsup \frac{|h_i|}{x^2+y^2+z^2} \leq \sqrt{\limsup \frac{h_i^2}{(x^2+y^2+z^2)^2}} \leq \limsup \frac{f}{(x^2+y^2+z^2)^2} = 0$. Donc les h_i sont 0 à l'ordre constant, premier et deuxième, donc le terme d'ordre six de $\sum h_i^2$ est la somme des carrés des termes d'ordre trois.

Mais maintenant, si on pose $z = 1$ dans $f(x,y,z) = \sum appr(f_i)^2 + \sum appr(g_j \sqrt{1 - x^2 - y^2 - z^2})^2$

on trouve un absurde, parce qu'on avait prouvé que le polynôme de Motzkin n'est pas somme de carrés de polynômes.

Remarque 5.7 (un autre contre-exemple). On peut prendre $f(x) = (1-x)^3$ et $h(x) = (1-x^2)^5$, alors $W_{\{}h\} = [-1, 1]$. Si on a $f = \sum f_i^2 + (1-x^2)^5 \sum g_j^2$, alors on a $f_i(1) = 0$ pour tout i. On considéré l'ordre en $x = 1$: on a ordre 3 à gauche, mais à droite on a ordre pair ou au moins de 5. C'est une contradiction.

Remarque 5.8. Dans cette section, les théorèmes qu'on a montrés pour $\mathbf{R}$ ne sont pas valable pour un corps réel clos quelconque, qui a priori n'est pas archimédien. Pour trouver un contre-exemple on peut prendre N, le corps des réels non-standard, c. à. d. une extension de $\mathbf{R}$ qui respecte la théorie de $\mathbf{R}$ au premier ordre et sur laquelle on peut définir la partie standard : à tout élément fini (c. à. d. plus petit en valeur absolue que au moins un entier) $s \in N$ on peut associer un réel, qu'on note $std(s)$ tel que $s - std(s)$ est infinitésimal.

Soit f le contrexemple de la remarque 5.6. Soit ϵ un infinitésimal > 0. $f + \epsilon$ est strictement positif. Donc on devrait avoir

$f + \epsilon = \sum f_i^2 + (1 - x^2 - y^2 - z^2) \sum g_j^2$ avec les f_i et les g_j à coefficients dans N.

Mais tous les f_i et les g_j sont finis pour tout (x,y,z) tels que $x^2 + y^2 + z^2 \leq \frac{1}{2}$. Or si un polynome $p(t)$ à coefficient dans N est fini pour infini valeurs réels distincts de t, alors les coéfficient sont finis. Il suffit de choisir $n + 1$ parmi ces valeurs : $a_0, \ldots, a_n$, où n est le degré, et écrire $p(t) = \sum \lambda_i q_i(t)$ où $q_i(t) = \prod_{j \neq i}(x - a_j)$. Il est clair que les λ_i sont finis et donc aussi les coefficients de p.

Si on applique ce fait trois fois on peut prouver que les coefficients des f_i et des g_j sont finis.

Donc, si on prend la partie standard, on obtient : $f = \sum std(f_i)^2 + (1 - x^2 - y^2 - z^2) \sum std(g_j)^2$ qui est une contradiction.

Remarque 5.9 (un autre contre-exemple). Notons F la clôture réelle de $\mathbf{R}((t))$. D'après le théorème de Puiseux, on a $F = \bigcup_n \mathbf{R}((t^{\frac{1}{n}}))$. Encore une fois, on considère $f = (1-x)^3 + t$ et $h = (1-x^2)^5$. Alors, on a $W_h = \{x : h(x) \geq 0\}$. Si on note $x = \sum_{j \geq n_0} c_j t^{\frac{j}{N}}$ avec $c_{n_0} \neq 0$ pour $x \in W_h$, alors on a $1 \geq x^2$. C'est équivalent à $n_0 = 0$ et $|c_0| \leq 1$, ou $n_0 > 0$. Alors W_h est borné.

Si on a $f = \sum_i f_i^2 + (1-x^2)^5 \sum_j g_j^2$, si on écrire f_i comme $\sum_{k \geq n_0} a_k^{(i)} t^{\frac{k}{N}}$, où $a_k^{(i)} \in \mathbf{R}[x]$, et g_i comme $\sum_{k \geq n_0} b_k^{(i)} t^{\frac{k}{N}}$,où $b_k^{(i)} \in \mathbf{R}[x]$. On peut supposer que au moins un des $a_{n_0}^{(i)}$, $b_{n_0}^{(j)}$ est non-nul. Alors en comparant le term de degré plus bas, on aurait $\sum_i (a_{n_0}^{(i)})^2 + (1-x^2)^5 \sum_j (b_{n_0}(j))^2 = 0$ ou $(1-x)^3$. Tous les deux sont impossible.

Références

[1] E. Artin, Uber die Zerlegung definiter Funktionenin Quadrate, Abh. Math. Sem. Univ. Hamburg, 5 (1927), 85-99.

[2] J.W.S. Cassels, W.J. Ellison, and A. Pfister, On sums of squares and on elliptic curves over function fields, J. Number Theory 3 (1971) 125-149.

[3] D. Hilbert, "Mathematical Problems"., Bulletin of the American Mathematical Society, vol. 8, no. 10 (1902), pp. 437-479. Earlier publications (in the original German) appeared in Göttinger Nachrichten, 1900, pp. 253-297, and Archiv der Mathematik und Physik, 3dser., vol. 1 (1901), pp. 44-63, 213-237.

[4] D. Hilbert, Uber die Darstellung definiter Formen als Summe von Formenquadraten. Math. Ann. 32, 342–350 (1888).

[5] D. Hilbert, Über ternäre definite Formen, Acta Math. 17 (1893), 169-197 ; voir Ges. Abh. 2, 345-366, Springer, Berlin, 1933

[6] J.-L. Krivine, Anneaux préordonnés, J. Analyse Math. 12 (1964), 307–326.

[7] T.Y. Lam, An introduction to real algebra, Ordered fileds and real algebraic geometry (Boulder, Colorado, 1983), Rocky Mountain J.Math. 14 (1984), no.4, 767-814.

[8] E. Landau, Uber die Darstellung definiter Funktionen durch Quadrate, Math. Ann. 62 (1906), 272-285.

[9] M. Marshall, Positive polynomials and sums of squares, Mathematical Surveys and Monographs, Volume 14, AMS, 2008.

[10] T. S. Motzkin, The arithmetic-geometric inequality. 1967 Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965) pp. 205–224.

[11] A. Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. Invent. Math. 4 (1967), 229–237.

[12] A. Prestel, C. Delzell, Positive polynomials, From Hilbert's 17th problem to real algebra, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2001.

[13] K. Schmüdgen, The K-moment problem for compact semi-algebraic sets. Math. Ann. 289 (1991), no. 2, 203-206.