Le XVII$^{\text{e}}$ problème de Hilbert

Dounia Darkaoui et Brian Flanagan

1 Introduction

David Hilbert énonce en 1900 une liste de vingt-trois problèmes mathématiques jusqu'alors non résolus. Parmi eux figure le XVII$^{\text{e}}$ problème de Hilbert : montrer qu'un polynôme positif réel peut s'écrire comme une somme de carrés de fractions rationnelles réelles. Le problème est résolu par l'affirmative par Emil Artin en 1927.
Pour les polynômes en une indéterminée, il est aisé de montrer que tout polynôme positif s'écrit comme une somme de carrés de polynômes réels.

Soit $P \in \mathbb{R}[X]$ positif sur $\mathbb{R}$ et soit $P = \prod_{i=1}^{r} P_k^{\alpha_k}$ sa décomposition en polynômes irréductible (à une constante multiplicative près). Pour tout $k \in [\![1, n]\!]$, il existe un réel x_k tel que $P_k = (X - x_k)$, ou il existe un nombre complexe $z_k = a_k + ib_k \in \mathbb{C}\backslash\mathbb{R}$ tel que $P_k = (X - z_k)(X - \overline{z_k}) = (X - a_k)^2 + b_k^2$.
En outre, puisque P est positif, si P_k est de degré 1, alors α_k est pair. Dès lors, si I est l'ensemble des indices k tels que α_k est impair, on peut se donner $Q \in \mathbb{R}[X]$ tel que :

$$P = Q^2 \prod_{k \in I} ((X - a_k)^2 + b_k^2)$$

Écrit sous une telle forme, P est donc bien une somme de carrés de polynômes réels.

On aurait pu espérer que tout polynôme positif puisse s'écrire comme une somme de carrés de polynômes, plutôt que de fractions rationnelles. C'est le cas pour les polynômes en une indéterminée, mais les fractions rationnelles sont nécessaires pour plus de deux indéterminées, comme l'a démontré Theodore Motzkin en 1966.

Considérons le polynôme en deux indéterminées $P = X^4Y^2 + X^2Y^4 + 1 - 3X^2Y^2$ et montrons dans un premier temps qu'il est bien positif.
Soit $(x, y) \in \mathbb{R}^2$. En appliquant l'inégalité arithmético-géométrique sur $(x^4y^2, x^2y^4, 1)$, on obtient :

$$\frac{x^4y^2 + x^2y^4 + 1}{3} \geqslant \sqrt[3]{x^4y^2 \cdot x^2y^4 \cdot 1} = x^2y^2$$

Ceci nous donne bien que $P(x, y) \geqslant 0$. Supposons maintenant par l'absurde qu'il existe $P_1, \ldots, P_n \in \mathbb{R}[X, Y]$ non nuls tels que : $P = \sum_{i=1}^{n} P_i^2$.
Soit $i \in [\![1, n]\!]$, le polynôme $P_i(X, 1)^2$ est de coefficient dominant strictement positif et est donc de degré au plus 4. Ainsi, $P_i(X, 1)$ est de degré au plus 2, et il en va de même pour $P_i(1, Y)$.
Dès lors, pour tout $i \in [\![1, n]\!]$, il existe $Q_i \in \mathbb{R}_{<3}[X, Y]$ et $R_i \in \mathbb{R}_{<3}[Y]$ tels que :

$$P_i(X, Y) = XQ_i(X, Y) + R_i(Y)$$

En évaluant notre relation en $X = 0$, on obtient : $1 = P(0, Y) = \sum_{i=1}^{n} R_i(Y)^2$ et donc les R_i sont constants.

En évaluant cette fois-ci en $Y = 0$, on a :

$$\begin{aligned} 1 = P(X,0) &= \sum_{i=1}^{n} (XQ_i(X,0) + R_i)^2 \\ &= \sum_{i=1}^{n} (X^2 Q_i(X,0)^2 + 2XR_iQ_i(X,0)) + \sum_{i=1}^{n} R_i^2 \\ &= \sum_{i=1}^{n} (X^2 Q_i(X,0)^2 + 2XR_iQ_i(X,0)) + 1 \end{aligned}$$

Donc : $\sum_{i=1}^{n} X^2 Q_i(X,0)^2 = -2X \sum_{i=1}^{n} R_i Q_i(X,0)$. Soit alors i_0 tel que $d = \deg(Q_{i_0}(X,0))$ est maximal parmi les polynômes $Q_i(X,0)$.
On obtient avec notre relation que : $2d+2 \leqslant d+1$, et donc $d \leqslant -1$. Ainsi, les $Q_i(X,0)$ sont tous nuls, donc on peut se donner des $S_i \in \mathbb{R}_{<2}[X,Y]$ tels que : $Q_i(X,Y) = YS_i(X,Y)$, et donc : $P_i(X,Y) = XYS_i(X,Y) + R_i$.
Dès lors :

$$X^2Y^2(X^2+Y^2-3)+1 = P = X^2Y^2 \sum_{i=1}^{n} S_i(X,Y)^2 + 2XY \sum_{i=1}^{n} R_i S_i(X,Y) + 1$$

On obtient donc que : $X^2Y^2(X^2+Y^2-3-\sum_{i=1}^{n} S_i(X,Y)^2) = 2XY \sum_{i=1}^{n} R_i S_i(X,Y)$ et donc comme les S_i sont de degré au plus 1 : $X^2+Y^2-3 = \sum_{i=1}^{n} S_i(X,Y)^2$

En $(0,0)$, on a $-3 = \sum_{i=1}^{n} S_i(0,0)^2$, contradiction.
Ce polynôme s'écrit cependant bien comme une somme de fractions rationnelles. En effet :

$$\frac{X^2Y^2(X^2+Y^2+1)(X^2+Y^2-2)^2 + (X^2-Y^2)^2}{(X^2+Y^2)^2} = X^4Y^2 + X^2Y^4 - 3X^2Y^2 + 1$$

Pour résoudre le dix-septième problème de Hilbert pour un nombre quelconque d'indéterminées, il faut se donner un cadre d'étude plus général que les simples réels : les corps réels clos, qui permettront de revenir au cas particulier de $\mathbb{R}$.

2 Les corps réels clos : une généralisation de $\mathbb{R}$

2.1 Corps réels

Définition : Corps ordonné

Un corps ordonné est un corps K muni d'une relation d'ordre $\leqslant$ compatible avec la structure de corps i.e. telle que :

(i) $\forall x, y, z \in K, x \leqslant y \Rightarrow x + z \leqslant y + z$

(ii) $\forall x, y \in K, 0 \leqslant x$ et $0 \leqslant y \Rightarrow 0 \leqslant xy$

Exemple.

- Bien évidemment, $\mathbb{R}$ et $\mathbb{Q}$ munis de leur ordre usuel sont des corps ordonnés.

- Si l'on considère le corps $\mathbb{R}(X)$, il existe un unique ordre tel que X est positif et inférieur à tout réel strictement positif.
  En effet, on peut considérer l'ordre tel que si $P = \sum_{i=k}^{+\infty} a_i X^i \in \mathbb{R}[X]$, avec $a_k \neq 0$, alors $P > 0$ si et seulement si $a_k > 0$. On étend cette définition à $\mathbb{R}(X)$: si $P/Q \in \mathbb{R}(X)$, alors $P/Q > 0$ si et seulement si $PQ > 0$.
  Réciproquement, si pour un ordre $\leqslant$ on a : $\forall a \in \mathbb{R}_+^\times, 0 < X \leqslant a$, alors : $\forall n \in \mathbb{N}, 0 < X^{n+1} < X^n$.
  Dès lors, si $P = \sum_{i=k}^{+\infty} a_i X^i \in \mathbb{R}[X]$, avec $a_k \neq 0$, on a : $P(X) = a_k X^k (1 + \sum_{i=1}^{+\infty} \frac{a_{i+k}}{a_k} X^i)$.
  Or, si $Q \in \mathbb{R}[X], 1 > XQ(X)$, donc : $P > 0 \Leftrightarrow a_k X^k > 0 \Leftrightarrow a_k > 0$.
  Contrairement à $\mathbb{R}$, le corps $\mathbb{R}(X)$ possède plusieurs ordres distincts, donc on notera 0_+ l'ordre que l'on vient d'exhiber.

Définition : Cône

Un cône P d'un corps K est un sous-ensemble de K vérifiant :

(i) $\forall x, y \in P$, $x + y \in P$,

(ii) $\forall x, y \in P$, $xy \in P$,

(iii) $\forall x \in K$, $x^2 \in P$

Le cône P est alors dit propre si $-1 \notin P$

Exemple.

- Dans $\mathbb{R}$, les seuls cônes sont $\mathbb{R}$ et $\mathbb{R}_+$.
- Dans $\mathbb{C}$, tous les éléments sont des carrés, donc le seul cône complexe est $\mathbb{C}$
- Si p est un nombre premier le seul cône de $\mathbb{Z}/p\mathbb{Z}$ est $\mathbb{Z}/p\mathbb{Z}$, puisque 1 est un carré et engendre additivement $\mathbb{Z}/p\mathbb{Z}$.
- Dans $\mathbb{R}(X)$, l'ensemble $\{P/Q \in \mathbb{R}(X) | \forall x \in \mathbb{R}, P(x)Q(x) \geqslant 0\}$ est un cône propre.
- Étant donné un corps K, l'ensemble des sommes de carrés d'éléments de K est un cône, que l'on notera $\sum K^2$.
  Il est en outre à noter que tout cône de K contient $\sum K^2$.

Définition : Le cône positif

Soit $(K, \leqslant)$ un corps ordonné. Le sous-ensemble $P = \{x \in K | x \geqslant 0\}$ est le cône positif de $(K, \geqslant)$.

Propriété : Caractérisation des cônes positifs

Soit $(K, \leqslant)$ un corps ordonné, le cône positif de K est un cône propre satisfaisant :

$$P \cup -P = K$$

Réciproquement, si un cône P vérifie cette relation, alors K peut être ordonné par : $x \leqslant y \Leftrightarrow x - y \in P$.

Exemple. On vérifie bien que dans $\mathbb{R}$, on a : $\mathbb{R} = \mathbb{R}_+ \cup \mathbb{R}_-$.

Lemme des cônes propres

Soit P un cône propre de K.

(i) Si $-a \notin P$, alors $P[a] = \{x + ay | x, y \in P\}$ est un cône propre de K.

(ii) Le cône P est contenu dans un cône positif d'un ordre de K.

Preuve. Démontrons la proposition (ii). Considérons l'ensemble $\mathscr{P}$ des cônes propres de K contenant le cône P. Cet ensemble est clairement inductif pour l'inclusion : en effet, si $(P_i)_{i\in I}$ est une famille totalement ordonnée de X, alors le cône $\bigcup_{i\in I} P_i$ en est un majorant dans $\mathscr{P}$. D'après le lemme de Zorn, il existe donc un cône propre Q contenant P, maximal pour l'inclusion.
Dès lors, si $a \notin Q$, alors par la proposition (i), $Q[-a]$ est un cône propre contenant P et donc $Q = Q[-a]$, et en particulier, $-a \in Q$. Donc : $K = Q \cup -Q$.

✌

Définition-Théorème : Corps réel

Soit K un corps, les assertions suivantes sont équivalentes :

(i) K peut être ordonné.

(ii) Le corps K possède un cône propre.

(iii) $-1 \notin \sum K^2$.

(iv) $\forall x_1, \ldots, x_n \in K, \sum_{i=1}^{n} x_i^2 = 0 \implies x_1 = \ldots = x_n = 0.$

Un corps satisfaisant ces propriétés est alors appelé un corps réel.

Preuve. Les implications (i) $\implies$ (ii) $\implies$ (iii) sont claires.
Montrons l'équivalence (iii) $\Leftrightarrow$ (iv) :

$$\begin{aligned}\exists x_1 \in K^\times, \exists x_2, \ldots, x_n \in K, \sum_{i=1}^{n} x_i^2 = 0 &\Leftrightarrow \exists x_1 \in K^\times, \exists x_2, \ldots, x_n \in K, -1 = \sum_{i=2}^{n} (x_i \cdot x_1^{-1})^2 \\ &\Leftrightarrow \exists x_2, \ldots, x_n \in K, -1 = \sum_{i=2}^{n} x_i^2 \\ &\Leftrightarrow -1 \in \sum K^2\end{aligned}$$

Enfin, si $-1 \notin \sum K^2$, alors $\sum K^2$ est un cône propre et donc par la condition (ii) du lemme précédent, il existe un ordre de K, donc (iii) $\implies$ (i).

✌

Exemple. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{R}(X)$ sont des corps réels, tandis que $\mathbb{C}$ et $\mathbb{F}_6$ ne le sont pas (dans ces corps, $-1 = i^2$ et $-1 = 2^2 + 1^2$ respectivement).
On note en général qu'un corps réel est de caractéristique nulle : si $(K, \leqslant)$ est un corps ordonné de caractéristique non nulle $n \in \mathbb{N}^\times$, alors $0 < 1$, donc : $0 = n = \underbrace{1 + \ldots + 1}_{n \text{ fois}} > 0$, contradiction.

Propriété : Caractérisation des cônes en caractéristique nulle

Soit K un corps contenant $\mathbb{Q}$ (i.e. de caractéristique nulle) et P un cône de K, alors P est l'intersection des cônes positifs des ordres de K qui contiennent P, en convenant que si l'intersection est vide, alors on a $P = K$.

Preuve. Il est clair que cette intersection contient P. En outre, si $a \in K \backslash P$, alors P est un cône propre, puisque si $-1 \in P$, alors : $a = \frac{1}{4}((1+a)^2 - (1-a)^2) \in P$. Dès lors, $P[-a]$ est un cône propre d'après la proposition (i) du lemme sur les cônes propres, et il est donc inclus dans un cône positif d'un ordre de K d'après la proposition (ii) de ce même lemme. Ainsi, on a un cône positif contenant $P[-a]$, et donc P et non a.

✌

Corollaire :

Soit K un corps contenant $\mathbb{Q}$, alors $\sum K^2$ est l'intersection des cônes positifs des ordres de K.

Corollaire :

Soit $(K, \leqslant)$ un corps ordonné et K_1 une extension de K.
L'intersection des cônes positifs des ordres de K_1 qui prolongent l'ordre de K est alors exactement l'ensemble Λ des combinaisons linéaires positives sur K de carrés d'éléments de K_1, c'est-à-dire les éléments de la forme $\sum_{i=1}^{n} \lambda_k x_k^2$, où les λ_k sont des éléments positif de K et les x_k des éléments de K_1.
Si K_1 n'admet pas d'ordre prolongeant celui de K, alors $\Lambda = K_1$.

Preuve. L'ensemble Λ est le cône de K_1 engendré par le cône positif de K. En effet, Λ est clairement un cône, et est contenu dans tout cône contenant le cône positif de K. Un ordre de K_1 est donc compatible avec celui de K si et seulement si le cône positif qui lui est associé contient Λ. Dès lors, en appliquant la caractérisation des cônes en caractéristique nulle à Λ, on a bien le résultat souhaité.

✌

2.2 Corps réels clos

Définition : Corps réel clos

Un corps réel clos K est un corps réel qui n'a pas d'extension algébrique réelle K_1 telle que $K_1 \neq K$. On rappelle qu'une extension algébrique d'un corps K est une extension de corps dont tous les éléments soient racines d'un polynôme à valeur dans K.

Exemple. $\mathbb{Q}$ n'est pas clos car $\mathbb{R}_{\text{alg}}$ l'ensemble des nombres algébriques réels est une extension algébrique réelle de $\mathbb{Q}$ et $\mathbb{Q} \subsetneq \mathbb{R}_{\text{alg}}$: on peut considérer $\sqrt{2} \notin \mathbb{Q}$, mais qui est annulé par $X^2 - 2 \in \mathbb{Q}[X]$ et qui appartient donc à $\mathbb{R}_{\text{alg}}$.

Théorème : Caractérisation des corps réels clos

Soit K un corps, les assertions suivantes sont équivalentes :

i. K est réel clos

ii. Il existe un unique ordre de K, le cône positif associé est l'ensemble des carrés de K, et tout polynôme de $K[X]$ de degré impair possède une racine dans K.

iii. L'anneau $K[i] = K[X]/(X^2+1)$ est un corps algébriquement clos.

Exemple. Il est bien connu que $\mathbb{R}$ vérifie les propositions (ii) et (iii). Montrons qu'il est bel et bien réel clos.
Soit L une extension algébrique non triviale de $\mathbb{R}$ et $\alpha \in L\backslash\mathbb{R}$. Soit P le polynôme minimal de α sur $\mathbb{R}$, qui est nécessairement irréductible et donc de degré deux. Soient ainsi β et $\overline{\beta}$ ses deux racines complexes. Le corps $\mathbb{R}[\alpha]$ est isomorphe à $\mathbb{R}[\beta] \simeq \mathbb{C}$ (α et β ont le même polynôme minimal). Or, L est une extension algébrique de $\mathbb{R}[\alpha] \simeq \mathbb{C}$, donc $L = \mathbb{C}$, puisque $\mathbb{C}$ est algébriquement clos.
La seule extension algébrique non triviale de $\mathbb{R}$ est donc $\mathbb{C}$, qui, on l'a vu, n'est pas réel.

Preuve. (i) $\implies$ (ii)
Soit $a \in K$. Si a n'est pas un carré, on définit $K[\sqrt{a}] = K[X]/(X^2-a)$, qui est une extension algébrique non-triviale de K et qui n'est donc pas réelle. Dès lors, par la caractérisation des corps réels, $-1 \in \sum K[\sqrt{a}]^2$ et donc pour $x_1, \dots, x_n, y_1, \dots, y_n \in K$:

$$-1 = \sum_{i=1}^{n} (x_i + \sqrt{a}y_i)^2 = \sum_{i=1}^{n} (x_i^2 + ay_i^2 + 2\sqrt{a}x_iy_i)$$

Puisque $K[\sqrt{a}]$ est un K-espace vectoriel de dimension 2 engendré par 1 et $\sqrt{a}$, on a par identification :

$$-1 = \sum_{i=1}^{n} x_i^2 + a\sum_{i=1}^{n} y_i^2$$

Or, $-1 \notin \sum K^2$, donc $\displaystyle\sum_{i=1}^{n} y_i^2 \neq 0$ et ainsi :

$$-a = \left(\sum_{i=1}^{n} y_i^2\right)^{-1}\left(1 + \sum_{i=1}^{n} x_i^2\right) = \left(\sum_{i=1}^{n}(y_i(\sum_{j=1}^{n} y_j^2)^{-1})^2\right)\left(1 + \sum_{i=1}^{n} x_i^2\right) \in \sum K^2$$

Dès lors, $K = \sum K^2 \cup -\sum K^2$.
Par conséquent, si P est le cône positif d'un certain ordre de K, on a : $P \cup -P = K$ et $\sum K^2 \subset P$, et donc puisque $P \cap -P = \{0\}$, on a : $-P \subset -\sum K^2$. Donc $P = \sum K^2$.
Il existe ainsi un unique ordre de K, donné par $\sum K^2$ et si $a \in K$ n'est pas un carré, il est n'est pas positif pour cet ordre (car $-a \in \sum K^2$), donc les éléments positifs sont exactement les carrés.
On montre que tout polynôme de degré impair de $K[X]$ a une racine dans $K[X]$ en travaillant par récurrence. On utilise alors le fait que si $P \in K[X]$ est un polynôme de degré impair d sans racine dans $K[X]$, alors $K[X]/(P)$ est une extension algébrique non triviale de $K[X]$, et que -1 y est donc une somme de carrés : pour des polynômes $Q_1, \dots, Q_n \in K_{<d}[X], R \in K[X], -1 = \displaystyle\sum_{i=1}^{n} Q_i^2 + PR$ et on applique l'hypothèse de récurrence à R, ce qui permet d'aboutir à un contradiction.

(ii) $\implies$ (iii)
Soit $P \in K[X]$ de degré $d = 2^m n$, où n est impair. Montrons par récurrence sur m que P a une racine dans

le corps $K[i]$. Si m est nul, le résultat est clair par hypothèse.
Si le résultat est vrai pour $m-1$, alors soit K_1 une clôture algébrique de K et soient $y_1, \dots, y_d$ les racines de P dans K_1. On pose alors, pour $k \in \mathbb{Z}$:

$$P_k = \prod_{1 \leqslant i < j \leqslant d} (X - X_i - X_j - kX_iX_j) \in K[X][X_1, \dots, X_d]$$

Pour $k \in \mathbb{Z}$ fixé, le polynôme P_k est symétrique en les indéterminées $X_1, \dots, X_n$.
Or, le théorème fondamental des polynômes symétriques (que nous admettrons ici) affirme que si P est un polynôme symétrique en n indéterminées à coefficients dans un anneau A, il existe un unique polynôme T à coefficients dans A tel que : $P(X_1, \dots, X_n) = T(\sigma_1, \dots, \sigma_n)$, où $\sigma_1, \dots, \sigma_n$ sont les polynômes symétriques élémentaires en n variables.
Dès lors, pour $T \in K[X][X_1, \dots, X_d]$, on a $P_k = T(\sigma_1, \dots, \sigma_d)$ et donc :

$$Q_k = P_k(y_1, \dots, y_d) = T(\sigma_1(y_1, \dots, y_d), \dots, \sigma_d(y_1, \dots, y_d)) \in K[X]$$

Car pour $j \in [\![1, d]\!]$, $\sigma_n(y_1, \dots, y_d) \in K$, par les relations coefficients-racines de P. Or, le polynôme Q_k est de degré $\frac{d(d-1)}{2} = 2^{m-1}n(2^m n - 1)$ et donc par hypothèse de récurrence, puisque $n(2^m n - 1)$ est impair, il admet une racine dans $K[i]$.
Il existe donc $1 \leqslant i(k) < j(k) \leqslant d$ tels que $y_{i(k)} + y_{j(k)} + k y_{i(k)} y_{j(k)} \in F[i]$.
Ceci étant vrai pour tout $k \in \mathbb{Z}$, il existe $i, j \in [\![1, d]\!]$ tels que pour $k \neq l$, $i = i(k) = i(l)$ et $j = j(k) = j(l)$. On en déduit donc que $y_i + y_j \in K[i]$ et $y_i y_j \in K[i]$. Dès lors, le polynôme $(X - y_i)(X - y_j) = X^2 - (y_i + y_j)X + y_i y_j$ est à coefficients dans $K[i]$ et a donc ses racines dans $K[i]$ (on travaille comme un polynôme du second degré à coefficients dans $\mathbb{C}$ pour les exhiber). Dès lors, $y_i, y_j \in K[i]$ et le polynôme P a donc au moins une racine dans $K[i]$.
Soit maintenant $P \in K[i][X]$ et $\overline{P}$ le polynôme dont les coefficients sont les conjugués de ceux de P. On a que $P\overline{P} \in K[X]$ (comme dans $\mathbb{C}[X]$) et donc ce polynôme admet une racine x dans $K[i]$.
Dès lors, $P(x) = 0$ ou $P(\overline{x}) = 0$, ce qui montre le résultat.

(iii) $\implies$ (i)

Puisque $K[i] = K[X]/(X^2 + 1)$ est un corps, $X^2 + 1$ est irréductible. Donc -1 n'est pas un carré dans K.
Ainsi, une somme de carrés de K est un carré : si $a, b \in K$, il existe $c, d \in K$ tels que $a + ib = (c + id)^2$ (le polynôme $X^2 - (a + ib)$ est scindé sur $K[i]$).
Donc : $a^2 + b^2 = |a + ib|^2 = |c + id|^4 = (c^2 + d^2)^2$.
Ainsi, K est un corps réel, puisque -1 n'est pas un carré et donc n'est pas une somme de carrés dans K.
On montre enfin de la même manière que pour $\mathbb{R}$ que la seule extension algébrique non triviale de K est le corps $K[i]$.

✌

Exemple. Le corps $\mathbb{R}(X)$ n'est pas un corps réel clos, puisque pour l'ordre 0_+, on a $X > 0$, et ce n'est pas un carré, ce qui contredit la propriété (ii).

Les similarités entre les corps réels clos et $\mathbb{R}$ nous permettent d'énoncer les théorèmes ci-dessous, qui généralisent un certain nombre de résultats sur les fonctions dérivables réelles pour les polynômes à coefficients dans un corps réel clos. Les preuves de ces résultats se basent principalement sur le caractère ordonné du corps, ainsi que le fait qu'on y connaisse les polynômes irréductibles, qui y sont les même que pour $\mathbb{R}$.

Propriété : Un théorème des valeurs intermédiaires polynômial

Soit R un corps réel clos, $P \in R[X]$, et $a, b \in R$ avec $a < b$. Si $P(a)P(b) < 0$, alors il existe $x \in]a, b[$ tel que $P(x) = 0$.

Preuve. Les polynômes irréductibles sur R sont soit de degré 1, soit de la forme $(X-c)^2+d^2$. Dès lors, puisque le polynôme P n'est pas de signe constant sur R, il possède au moins une racine sur R. Il existe donc un facteur irréductible Q de degré 1 de P tel que $Q(a)Q(b)<0$.
Dès lors, si $Q=X-c$, on a $a<c<b$, et donc P possède une racine dans $]a,b[$.

Remarque. L'hypothèse de clôture réelle est essentielle. En effet, si l'on considère $P(Y)=Y^2-X\in\mathbb{R}(X)[Y]$, ce polynôme n'a pas de racine sur $\mathbb{R}(X)$. Or, pour l'ordre 0_+, on a : $P(X)=X^2-X<0$ et $P(1)=1-X>0$. Donc $P(X)P(1)<0$ et pourtant, P ne possède pas de zéro sur $]X,1[$.

Les démonstrations des résultats suivants sont du même acabit.

Propriété : Un théorème de Rolle polynômial

Soit K un corps réel clos, $P\in R[X]$, $a,b\in R$ avec $a<b$ et $f(a)=f(b)=0$.
Alors le polynôme dérivé P' a une racine dans $]a,b[$.

Corollaire : Un théorème des accroissements finis polynômial

Soit R un corps réel clos, $P\in R[X]$, $a,b\in R$ avec $a<b$.
Alors il existe $c\in]a,b[$ tel que : $P(b)-P(a)=(b-a)P'(c)$

Corollaire : Une condition suffisante pour la monotonie

Soit R un corps réel clos, $P\in R[X]$ et $a,b\in R$ avec $a<b$. Si P' est strictement positif (resp. négatif) sur $]a,b[$ alors P est strictement croissante (resp. décroissante).

2.3 Clôture réelle d'un corps ordonné

Définition : Séquence de Sturm

Soit R un corps réel clos, $f,g\in R[X]$. La séquence de Sturm de f et g est la séquence de polynômes $(f_0,\dots,f_k)$ défini comme suit :

- $f_0=f$
- $f_1=f'g$
- $f_i=f_{i-1}q_i-f_{i-2}$, avec $-f_i$ le reste de la division euclidienne de f_{i-2} par f_{i-1} pour $i\in[\![2,k]\!]$.

On a alors que f_k est le pgcd de f et $f'g$.

Remarque. Les différents f_i obtenus sont, au signe près, les polynômes que l'on aurait obtenu en appliquant l'algorithme d'Euclide à f et $f'g$.
Par exemple, sur $\mathbb{R}$, si $f=X(X-1)(X+1)=X^3-X$ et $g=X^2$, alors :

- $f_1 = f'g = 3X^4 - X^2$
- $f_2 = -f$
- $f_3 = -2X^2$
- $f_4 = -X$

Notation. Étant donné une suite $(a_0, \dots, a_n) \in R^n$ telle que $a_0 \neq 0$, on définit le nombre de changements de signe de cette suite comme suit : on compte un changement de signe si $a_i a_{i+1} < 0$ pour $0 \leqslant i \leqslant n-1$, ou si $a_i a_j < 0$, pour $1 \leqslant i+1 < j \leqslant n$ et pour tout $i < l < j, a_l = 0$.
Par exemple, la suite $(1, -1, 0, 2, 2, 0, 2, -2)$ comporte 3 changements de signe.
Pour une séquence de Sturm comme définie plus haut, on notera $v(f, g; a)$ le nombre de changements de signe de $(f_0(a), \dots, f_k(a))$

Théorème de Sylvester

Soit R un corps réel clos et $f, g \in R[X]$. Soit $a < b \in R$ qui ne soient pas des racines de f. On a :

$$\text{Card}\{x \in]a, b[\mid f(x) = 0 \text{ et } g(x) \geqslant 0\} - \text{Card}\{x \in]a, b[\mid f(x) = 0 \text{ et } g(x) \leqslant 0\} = v(f, g; a) - v(f, g; b)$$

Exemple.
Considérons la suite de Sturm donnée par $f = X(X-1)(X+1)$ et $g = X^2$ sur l'intervalle $]-2, 2[$.
On a alors : $(f_0(-2), \dots, f_4(-2)) = (-6, 44, 6, -8, 2)$, donc $v(f, g; -2) = 3$
Et : $(f_0(2), \dots, f_4(2)) = (6, 44, -6, -8, -2)$, donc $v(f, g; 2) = 1$
Le polynôme f s'annule en $-1, 0$ et 1 et g est positive en ces trois points, et négative en 0. On a bien l'égalité attendue pour cet exemple.

Corollaire : Théorème de Sturm

Soit R un corps réel clos et $f \in R[X]$. Soient $a < b \in R$ qui ne soient pas des racines de f. Alors

$$\text{Card}\{x \in]a, b[\mid f(x) = 0\} = v(f, 1, a) - v(f, 1, b)$$

Preuve. Il suffit d'appliquer le théorème de Sylvester à f et 1 sur l'intervalle $]a, b[$.

Lemme : Une borne pour les racines

Soit R un corps réel et $P = a_n X^n + \dots + a_0 \in R[X]$ avec $a_n \neq 0$.
En posant $M = 1 + \sum_{i=0}^{n-1} \left| \frac{a_i}{a_n} \right|$, on a :

i. $\forall x > M, a_n P(x) > 0$
ii. $\forall x < -M, (-1)^n a_n P(x) > 0$

Preuve. Soit $x \in R$ tel que $|x| \geqslant M$, on pose $b_i = \frac{a_i}{a_n}$ avec les notations définies comme ci-dessus, $f(x) = a_n x^n(1 + b_{n-1}x^{-1} + \ldots + b_0 x^{-n})$ comme $|x|^{-n} \leqslant |x|^{-1} \leqslant M^{-1} \leqslant 1$ alors $|b_{n-1}x^{-1} + \ldots + b_0 x^{-n}| \leqslant (|b_{n-1}| + \ldots + |b_0|)M^{-1} < 1$, $f(x)$ est du même signe que $a_n x^n$.

Corollaire :

Soit R un corps réel clos, $P, Q \in R[X]$, $(P_0, \ldots, P_n)$ la séquence de Sturm de P et Q.
On note $v(P, Q; +\infty)$ (resp. $v(P, Q; -\infty)$) le nombre de changements de signe dans la suite des coefficients dominants de $(P_0, \ldots, P_n)$ (resp. de $(P_0(-X), \ldots, P_n(-X))$). Alors :

$$\text{Card}\{x \in R \mid P(x) = 0, Q(x) \geqslant 0\} - \text{Card}\{x \in R \mid P(x) = 0, Q(x) \leqslant 0\} = v(P, Q; -\infty) - v(P, Q; +\infty)$$

Preuve. Soit $P, Q \in R[X]$, grâce au lemme précédent on sait qu'il existe $M \in R$ positif tel que toutes les racines de P sont dans $]-M, M[$, et tel que : $v(P, Q; M) = v(P, Q; +\infty)$ et $v(P, Q; -M) = v(P, Q, -\infty)$.
On conclut avec le théorème de Sylvester sur $]-M, M[$.

Exemple. Soit $P = X^2 + 1$, la séquence de Sturm de P et 1 est $P_0 = P, P_1 = P' = 2X, P_2 = -1$.
On a alors : $v(P, 1, -\infty) = 1$ (les changements de signe de $(1, -2, -1)$) et $v(P, 1, +\infty) = 1$ (les changements de signe de $(1, 2, -1)$) donc on retrouve bien que P n'a pas de racine sur R.

Définition : Clôture réelle

Étant donné un corps ordonné $(K, \leqslant)$, une extension algébrique R de K est appelée une clôture réelle de K si elle est réelle close et si son unique ordre prolonge celui de K.

Exemple.

- La seule clôture réelle de $\mathbb{R}$ est... $\mathbb{R}$.
- Une clôture réelle de $\mathbb{Q}$ est $\mathbb{R}_{\text{alg}}$.

Théorème : Existence et unicité de la clôture algébrique

Soit $(K, \leqslant)$ un corps ordonné. Alors $(K, \leqslant)$ admet une clôture réelle R.
De plus, si R et R' sont des clôtures réelles de $(K, \leqslant)$, il existe un unique isomorphisme de $K-$algèbre entre R et R'.

Preuve. On admet le théorème de Steinitz, qui affirme que tout corps admet une clôture algébrique. On se donne donc une clôture algébrique $\overline{K}$ de K, et $\mathscr{E}$ l'ensemble des sous-extensions $(L, \leqslant)$ de K qui préservent l'ordre de $(K, \leqslant)$. Cet ensemble est ordonné, pour l'ordre $\prec$:

$$\forall (L, \leqslant_L), (L', \leqslant_{L'}) \in \mathscr{E}, (L, \leqslant_L) \prec (L', \leqslant_{L'}) \Leftrightarrow (L \subset L' \text{ et } \forall x, y \in L, x \leqslant_L y \Leftrightarrow x \leqslant_{L'} y)$$

Par le lemme de Zorn, $\mathscr{E}$ possède un élément maximal $(R, \leqslant)$. Montrons que ce corps est réel clos.
Soit $a \in R$ positif. Supposons par l'absurde que ce n'est pas un carré de R. Alors si $R(\sqrt{a})$ est le plus petit sous-corps de $\overline{K}$ contenant $\sqrt{a}$ et R :

$$P = \left\{ \sum_{k=1}^{n} b_k (c_k + d_k \sqrt{a})^2 \in R(\sqrt{a}) | \forall\ 1 \leqslant k \leqslant n, b_k, c_k, d_k \in R \text{ et } b_k \geqslant 0 \right\}$$

est un cône propre de R, car si P contient -1, par identification, on peut écrire : $-1 = \sum_{k=1}^{n} b_k (c_k^2 + a d_k^2) \geqslant 0$.
Par le lemme des cônes propres, P est contenu dans le cône positif d'un ordre de $R(\sqrt{a})$, maximal parmi les cônes propres contenant P. L'ordre ainsi obtenu est cohérent avec l'ordre de $(R, \leqslant)$, puisque P contient le cône positif de $(R, \leqslant)$. Par hypothèse sur a, on a $R \subsetneq R(\sqrt{a}) \subset \overline{K}$, ce qui contredit la maximalité de R. Les éléments positif de $(R, \leqslant)$ sont donc exactement les carrés, et R possède donc un unique ordre. Si maintenant $R \subset L \subset F$ est un corps réel, alors tout ordre sur L prolonge l'ordre de R, et donc celui de K. Ainsi, $L = R$ par maximalité de R. Le corps R est donc bien réel clos.

Soit maintenant une clôture réelle R de $(K, \leqslant)$ et R' un corps réel clos contenant $(K, \leqslant)$ et dont l'ordre est prolonge celui de K. On se donne $\mathscr{F}$ l'ensemble des morphismes de K-algèbre de L dans R', où $K \subset L \subset R$ et φ préserve l'ordre de L. On définit alors la relation d'ordre sur $\mathscr{F}$:

$$\forall \varphi_1 : L_1 \to R', \varphi_2 : L_2 \to R', \varphi_1 \prec \varphi_2 \Leftrightarrow L_1 \subset L_2 \text{ et } \forall x \in L_1, \varphi_1(x) = \varphi_2(x)$$

De nouveau, par le lemme de Zorn, on peut se donner un élément maximal $\psi : L \to R'$ de $\mathscr{F}$. Supposons par l'absurde que $L \subsetneq R$. Alors si $x \in R \backslash L$, on peut se donner $P = \sum_{k=0}^{n} a_k X^k \in L[X]$ son polynôme minimal sur L.
Le polynôme P est irréductible sur L, et donc, puisque L est de caractéristique nulle, P et P' sont premiers entre eux sur L, et ils le sont aussi sur la clôture algébrique de L (par le théorème de Bézout). Par conséquent, le polynôme P n'a pas de racine multiple dans R et on peut se donner ses racines $x_1 < \ldots < x_m$ dans R. La séquence de Sturm associée à P et à 1 est constituée de polynômes de $L[X]$ et donc si $P_\psi = \sum_{k=0}^{n} \psi(a_k) X^k$, puisque ψ conserve l'ordre, on a :

$$v(P, 1; -\infty) - v(P, 1; +\infty) = v(P_\psi, 1; -\infty) - v(P_\psi, 1; +\infty)$$

Dès lors, le polynôme P_ψ a lui aussi m racines $y_1 < \ldots < y_m$ dans R' (il est lui aussi à racines simples dans la clôture algébrique de R', la relation de Bézout passe par mrophisme d'algèbre). On dispose donc d'un morphisme de K-algèbre $\rho : L(x) \to R'$ prolongeant ψ, défini par $\rho(x) = b_j$, où l'entier $1 \leqslant j \leqslant m$ est tel que $x = x_j$.
Soit L_1 une extension de degré fini de L contenue dans R. L'extension L_1 est finie et séparable, c'est-à-dire qu'elle est algébrique (car contenue dans R) et que le polynôme minimal sur L de tout élément de L_1 est à racines simples (car L est de caractéristique nulle), donc d'après le théorème de l'élément primitif (que nous admettons ici), L_1 est une extension simple. Il existe donc un élément $\alpha \in L$ tel que $L_1 = L(\alpha)$. D'après ce que l'on vient de faire, on peut donc se donner un morphisme de K-algèbre $\rho_1 : L_1 \to R'$ prolongeant ψ.
Montrons alors que le morphisme ρ préserve l'ordre.
Soit $z \geqslant 0 \in L(x)$ et $\xi_1, \ldots, \xi_{m-1}, z \in R$ tels que : $\xi_k^2 = x_{k+1} - x_k$ et $\zeta^2 = z$. D'après ce que l'on vient de montrer, si $L_1 = L(x_1, \ldots, x_m, z, \xi_1, \ldots, \xi_{m-1}, \zeta)$, on dispose de $\rho_1 : L_1 \to R'$.
Puisque ρ_1 prolonge ψ, les $\rho_1(x_i)$ sont des racines de P_ψ. Or, $\rho_1(x_{k+1}) - \rho_1(x_k) = \rho_1(\xi_k)^2 > 0$, donc on a

que $\rho_1(x_k) = y_k$, et en particulier $\rho_1(x) = y_j$.
Dès lors, $\rho_{1|L(a)} = \rho$ et donc : $\rho(z) = \rho_1(z) = \rho_1(\zeta)^2 \geqslant 0$. Le morphisme ρ préserve donc l'ordre, ce qui contredit la maximalité de ψ. Ansi, $L = R$ et ψ est un morphisme de K-algèbres de R dans R'. Il est de plus unique, car il conserve l'ordre des racines des polynômes minimaux des éléments de R sur K. C'est de plus un isomorphisme si l'on suppose que R' est une clôture algébrique de K : par symétrie des rôles, on dispose d'un unique morphisme $\psi' : R' \to R$, qui est par unicité des endomorphismes de R et de R', tel que $\psi' \circ \psi = \mathrm{Id}_R$ et $\psi \circ \psi' = \mathrm{Id}_{R'}$.

Exemple. Examinons le cas de $\mathbb{R}(X)$.
On introduit l'ensemble des séries de Puiseux $K[X]^\wedge$ sur un corps K de manière informelle comme l'ensemble des séries de la forme :

$$\sum_{i=k}^{+\infty} a_i X^{i/q}, \text{ où } k \in \mathbb{Z}, q \in \mathbb{N}^\times, (a_i)_{i \geqslant k} \in K^{\mathbb{N}}$$

On admet que $\mathbb{C}[X]^\wedge = \mathbb{R}(X)^\wedge[i]$ est algébriquement clos, et par conséquent, $\mathbb{R}(X)^\wedge$ est un corps réel clos. De même que pour les fractions rationnelles, si $(K, \leqslant)$ est un corps ordonné et si $(a_k)_{i \geqslant k} \in K^{\mathbb{N}}$ avec $a_k \neq 0$, on muni $K(X)^\wedge$ d'un ordre par la relation :

$$\sum_{i=k}^{+\infty} a_i X^{i/q} > 0 \Leftrightarrow a_k > 0$$

Le corps $\mathbb{R}(X)$ est un sous-corps des séries de Puiseux réelles et dans $\mathbb{R}(X)^\wedge$, on a :

$$X = (X^{1/2})^2 > 0 \text{ et } \forall a \in \mathbb{R}_+^\times, (a - X) = a\left(1 + \sum_{k=1}^{+\infty} \frac{(-1)^k}{2^k} \frac{(2k)!}{k!^2} a^{-k} X^k\right)^2 > 0$$

(on obtient cette dernière formule par le développement en série entière de $x \mapsto \sqrt{a - x}$), donc l'ordre induit sur $\mathbb{R}(X)$ est l'ordre 0_+.
La clôture réelle de $(\mathbb{R}(X), 0_+)$ est l'ensemble des séries de Puiseux algébriques sur $\mathbb{R}(X)$: $\mathbb{R}(X)^\wedge{}_{\mathrm{alg}} \supsetneq \mathbb{R}(X)$ (par exemple, $X^{1/2}$ est algébrique sur $\mathbb{R}(X)$, de polynôme minimal $Y^2 - X$, mais n'est pas une fraction rationnelle).

On a exploré les corps réel clos et les similarités particulières qu'ils partagent avec $\mathbb{R}$, et montré que l'on dispose d'une opération primordiale sur les corps ordonné permettant de les étudier de ce point de vue : la clôture réelle. On peut désormais s'atteler à la résolution du dix-septième problème de Hilbert à proprement parler.

3 Le XVII$^{\mathrm{e}}$ problème de Hilbert

3.1 Le principe de Tarski-Seidenberg et ses conséquences

Principe de Tarski-Seidenberg

Soit $(f_i(X,Y))_{1\leqslant i\leqslant s} \in \mathbb{Z}[X,Y]^s$, où $Y=(Y_1,\dots,Y_n)$, et ε une fonction de $\{1,\dots,s\}$ dans $\{0,\pm 1\}$.
Alors il existe un ensemble booléen (c'est-à-dire une composition de disjonctions, conjonctions et négations) $\mathscr{B}(Y)$ d'égalités et d'inégalités polynomiales en Y à coefficients entiers, telle que si R est un corps réel clos et $y\in R^n$, le système :

$$\begin{cases} \text{signe}(f_1(X,y)) = \varepsilon(1) \\ \vdots \\ \text{signe}(f_s(X,y)) = \varepsilon(s) \end{cases}$$

admet une solution $x\in R$ si et seulement si $\mathscr{B}(y)$ est vrai dans R.

Remarque.

- On convient que $\text{signe}(0)=0$
- En d'autres termes, le principe de Tarski-Seidenberg permet, sur un corps réel clos, de traduire un système d'équations et d'inéquations sur $n+1$ variables en un système sur les n dernières variables.

Corollaire :

Soit K un corps réel, et $(f_1(X,Y),\dots,f_s(X,Y)) \in K[X,Y]^s$, où $Y=(Y_1,\dots,Y_n)$, et ε une fonction de $\{1,\dots,s\}$ dans $\{0,\pm 1\}$.
Alors il existe un ensemble booléen $\mathscr{B}(Y)$ d'égalités et d'inégalités polynomiales en Y à coefficients dans K, telle que si R est un corps réel clos contenant F et $y\in R^n$, le système :

$$\begin{cases} \text{signe}(f_1(X,y)) = \varepsilon(1) \\ \vdots \\ \text{signe}(f_s(X,y)) = \varepsilon(s) \end{cases}$$

admet une solution $x\in R$ si et seulement si $\mathscr{B}(y)$ est vrai dans R.

Preuve. Soit p tel que pour tout $1\leqslant i\leqslant s$, on peut écrire : $f_i(X,Y) = \sum_{\alpha\in\mathbb{N}^{n+1},|\alpha|\leqslant p} a_{i,\alpha}(X,Y)^\alpha$.
Dès lors, si $Z=(Z_{(i,\alpha)})_{1\leqslant i\leqslant s,|\alpha|\leqslant p}$ est une variable à multi-indices, on peut écrire :

$$f_i(X,Y) = G(X,Y,(\delta_{i,j}a_{i,\alpha})_{|\alpha|\leqslant p})$$

Où :

$$G = \sum_{|\alpha|\leqslant p} Z_{(i,\alpha)}(X,Y)^\alpha \in \mathbb{Z}[X,Y,Z]$$

Donc en appliquant le principe de Tarski-Seidenberg aux polynômes G_i en (y,a) sur R, où $a=(a_{i,\alpha})_{i,\alpha}$, on dispose d'un système booléen $\mathscr{C}(Y,Z)$ qui traduit le système étudié, et donc d'un système $\mathscr{B}(Y)=\mathscr{C}(Y,a)$ comme on le souhaitait.

✌

Proposition : Une conséquence du principe de Tarski-Seidenberg

Soit R un corps réel clos et R_1 une extension réelle close de R.
Soit $\mathscr{B}(X)$ un ensemble booléen d'égalités et d'inégalités polynomiales en $X = (X_1, \dots, X_n)$ à coefficients dans R. Si $\mathscr{B}(y)$ est vrai pour un certain $y \in R_1^n$, alors $\mathscr{B}(x)$ est vrai pour un certain $x \in R^n$.

Preuve. Travaillons par récurrence sur n.
Si $n = 0$, il n'y a rien à prouver.
Soit $n \geqslant 1$, on suppose le résultat vrai au rang $n-1$. Alors par le corollaire du principe de Tarski-Seidenberg, il existe un ensemble booléen $\mathscr{C}(X')$ d'égalités et d'inégalités polynomiales en $X' = (X_1, \dots, X_{n-1})$ à coefficients dans R tel que pour toute corps réel clos R_2 contenant R, et pour tout $x' \in R_2^{n-1}$, $\mathscr{B}(x', X_n)$ a une solution dans R_2 si et seulement si $\mathscr{C}(x')$ est vrai.
Dès lors, si $(y_1, \dots, y_n)$ est une solution de $\mathscr{B}(X)$ dans R_1^n, alors $y' = (y_1, \dots, y_{n-1})$ est solution de $\mathscr{C}(X')$.
Par hypothèse de récurrence, $\mathscr{C}(X')$ admet une solution $x' \in R^{n-1}$.
Ainsi, il existe $x_n \in R$ tel que $(x', x_n) \in R^n$ est une solution de $\mathscr{B}(X)$

3.2 Résolution du XVII$^{\text{e}}$ problème de Hilbert

Théorème du morphisme d'Artin-Lang

Soit R un corps réel clos et A une R-algèbre de type fini.
S'il existe un morphisme de R-algèbre $\varphi : A \to R_1$ dans une extension réelle close R_1 de R, alors il existe un morphisme de R-algèbre $\psi : A \to R$.

Preuve. On écrit A sous la forme $R[X_1, \dots, X_n]/I$, où I est un idéal de $R[X_1, \dots, X_n]$ engendré par les polynômes $P_1, \dots, P_m$. Soit alors b_i l'image de la classe de X_i par φ, pour tout $i \in [\![1, n]\!]$.
Le n-uplet $(b_1, \dots, b_n)$ est alors solution du système d'équations $P_1 = \dots = P_m = 0$ dans R_1^n. D'après la proposition précédente, ce système d'équations admet une solution $(a_1, \dots, a_n)$ dans R^n.
Soit alors $\overline{\psi}$ le morphisme de $R[X_1, \dots, X_n]$ dans R défini par : $\overline{\psi}(X_i) = a_i$.
Puisque $\overline{\psi}$ est surjectif et $I \subset \mathrm{Ker}(\overline{\psi})$, donc par le théorème de factorisation, il induit bien un morphisme de R-algèbre $\psi : A \to R$.

Théorème : Solution au XVII$^{\text{e}}$ problème de Hilbert

Soit R un corps réel clos et $P \in R[X_1, \dots, X_n]$. Si P est positif sur R^n, alors P s'écrit comme une somme de carrés dans le corps des fractions rationnelles $R(X_1, \dots, X_n)$.

Preuve. Puisque $L = R(X_1, \dots, X_n)$ contient $\mathbb{Q}$ (à isomorphisme près), d'après le premier corollaire de la caractérisation des cônes en caractéristique nulle, $\sum L^2$ est l'intersection des cônes positifs donnés par les ordres de L. Donc si P ne s'écrit pas comme une somme de carrés dans $R(X_1, \dots, X_n)$, alors il existe

un ordre $R(X_1,\dots,X_n)$ tel que P est négatif.
Soit alors K la clôture réelle de $R(X_1,\dots,X_n)$, muni de cet ordre. Dès lors, $-P$ a une racine carrée non nulle dans K (car $K[T]/\langle T^2+P\rangle$ est une extension algébrique réelle de K), et donc il existe un morphisme de R-algèbre $\varphi : R[X_1,\dots,X_n][T]/\langle PT^2+1\rangle \to K$ (on peut considérer l'unique morphisme de R-algèbre qui envoie l'image de T dans le quotient $R[X_1,\dots,X_n][T]/\langle PT^2+1\rangle$ sur $\sqrt{-P}^{-1}$)
D'après le théorème de morphisme d'Artin-Lang, il existe un morphisme de R-algèbre :

$$\psi : R[X_1,\dots,X_n][T]/\langle PT^2+1\rangle \to R$$

Par construction, le polynôme $P(Y_1,\dots,Y_n)Z^2+1$ admet une racine dans $\big(R[X_1,\dots,X_n][T]/\langle PT^2+1\rangle\big)^{n+1}$, que l'on note $(y_1,\dots,y_n,z)$.
Donc si $x := (\psi(y_1),\dots,\psi(y_n))$ et $t := \psi(z)$, alors :

$$P(x)t^2+1 = P(\psi(y_1),\dots,\psi(y_n))\psi(z)+1 = \psi(f(y_1,\dots,y_n))z+1) = \psi(0) = 0$$

Ainsi, puisque $t \neq 0$ (car $1 \neq 0$), on a : $P(x) = -t^{-2} < 0$. Il existe donc un élément $x \in R^n$ tel que $P(x) < 0$, ce qui, par contraposée, démontre le théorème.

Exemple. L'hypothèse de clôture sur R est primordiale. En effet, si $K = \mathbb{R}(t)$ muni de l'ordre 0_+, qui n'est pas réel clos (sa clôture réelle est $R = \mathbb{R}(X)^{\wedge}{}_{\text{alg}}$) et si $f(X) = (X^2-t)^2 - t^3 = X^4 - 2tX^2 + t^2 - t^3 \in K[X]$, alors :
Si $P \in \mathbb{R}(t)$, si l'on écrit P comme une série formelle (en développant son dénominateur en série entière), alors si son premier terme est une constante non nulle, le premier terme de $f(P(t))$ est positif strictement, et sinon, son premier terme est t^2. Donc f est positive sur K.
En outre, si I est l'intervalle de R suivant : $\left]\sqrt{t(1-\sqrt{t})}, \sqrt{t(1+\sqrt{t})}\right[$, on a :

$$f(\pm\sqrt{t(1\pm\sqrt{t})}) = (t(1\pm\sqrt{t})-t)^2 - t^3 = (t\sqrt{t})^2 - t^3 = 0$$

Donc f est négative sur $I \cup -I$ (son coefficient dominant est positif), et ne peut donc pas s'écrire comme d'éléments de $R(X)$, et donc en particulier comme somme d'éléments de $K(X)$.

Il existe cependant une généralisation du dix-septième problème de Hilbert pour les corps ordonnés.

Théorème :

Soit $(K,\leqslant)$ un corps ordonné et R sa clôture réelle. Soit $P \in K[X_1,\dots,X_n]$, alors si P est positif sur R^n, on peut écrire P comme une combinaison linéaire sur K de carrés d'éléments de $K(X_1,\dots,X_n)$.

Preuve. Par contraposée, si P ne s'écrit pas : $\sum_{i=1}^{n} \lambda_k Q_k^2$, avec pour $1 \leqslant k \leqslant n$ les λ_k des éléments positifs de K et les Q_k dans $K(X_1,\dots,X_n)$, alors d'après le second corollaire de la caractérisation des cônes en caractéristique nulle, il existe un ordre de $K(X_1,\dots,X_n)$ prolongeant celui de K pour lequel P est négatif. On se donne L la clôture algébrique de $K(X_1,\dots,X_n)$ pour cet ordre.
Le corps L contient R, puisque $K(X_1,\dots,X_n)$ contient K. On a donc un morphisme de R-algèbre de $R[X_1,\dots,X_n][T]/(PT^2+1)$ dans L et on conclue à l'existence d'un élément $x \in R$ tel que $P(x) < 0$ comme dans la résolution du dix-septième problème de Hilbert.