17ème Problème de Hilbert*

PAULO RIBENBOIM

En 1900, à Paris, Hilbert, invité à faire une conférence, expose 23 problèmes ouverts de Mathématiques[10]. La résolution de ces problèmes était difficile; on peut citer, par exemple, les travaux de Montgomery, Zippin et Gleason pour le problème 5, ceux de Julia Robinson et Matijasevich pour le problème 10, et la réponse négative de Nagata au problème 14.

Expliquons maintenant ce qu'était le 17ème de ces problèmes.

Soit $\mathbb{R}$ le corps des réels, $\mathbb{R}[X_1, \ldots, X_n]$ l'anneau des polynômes à n variables et à coefficients dans $\mathbb{R}$, $\mathbb{R}(X_1, \ldots, X_n)$ son corps des fractions, c'est à dire le corps des fractions rationnelles à n variables et à coefficients dans $\mathbb{R}$.

Toute fraction rationnelle $f \in \mathbb{R}(X_1, \ldots, X_n)$ peut s'écrire sous la forme $f = \frac{f_1}{f_2}$ où $f_1, f_2 \in \mathbb{R}[X_1, \ldots, X_n]$. On dit que f est définie en $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ si on peut écrire $f = \frac{f_1}{f_2}$ avec $f_2(x_1, \ldots, x_n) \neq 0$. On dit que f est définie positive si en tout point $x \in \mathbb{R}^n$ où f est définie $f(x) \geq 0$. Il est clair que toute somme de carrés Σf_i^2, où $f_i \in \mathbb{R}(X_1, \ldots, X_n)$, est définie positive. Hilbert a cherché s'il existait d'autres exemples. Dans le cas $n = 0$, $\mathbb{R}(X_1, \ldots, X_n) = \mathbb{R}$ et $f \in \mathbb{R}$ est définie positive si et seulement si f est positif dans $\mathbb{R}$, donc si et seulement si f est un carré.

Dans le cas $n = 1$, $f \in \mathbb{R}(X)$ est définie positive si et seulement si f est somme de deux carrés.

Dans le cas $n = 2$, $f \in \mathbb{R}(X, Y)$ est définie positive si et seulement si f peut s'écrire comme somme de 4 carrés, mais Hilbert n'a pas pu déterminer s'il existait ou non une somme de quatre carrés qui ne soit pas somme de trois carrés.

*Recebido pela SBM em 22 de abril de 1974.

Enonçons alors le 17ème problème de Hilbert dans le cas de n variatles.

Soit $f \in \mathbb{R}(X_1, \ldots, X_n)$ définie positive. f est-elle somme de carrés de fractions rationnelles à coefficients réels, et, si oui, de combien? Notons qu'on peut supposer $f \in \mathbb{R}[X_1, \ldots, X_n]$, positive sur tout $\mathbb{R}^n$ (en multiplicant par le carré du dénominateur) pour étudier ce problème. Une solution qualitative de ce problème a été donnée en 1927 par Artin dans [1].

I. Rappels sur les Notions Intervenant dans l'Etude [15]

Corps ordonné K: c'est un corps muni d'une relation d'ordre total, compatible avec les opérations.

Corps ordonnable K: c'est un corps qui peut être muni d'une relation d'ordre total compatible avec les opérations. Rappelons le théorème d'Artin-Schreier qui caractérise ces corps: un corps K est ordonnable si et seulement si -1 n'est pas une somme de carrés d'éléments de K.

Extension ordonnée d'un corps ordonné K: Soit K un corps ordonné, L une extension de K; L este extension ordonnée de K si L est muni d'un ordre prolongeant celui de K.

Corps ordonné maximal: un corps ordonné K est dit ordonné maximal s'il n'admet aucune extension algébrique ordonnée, distincte de K lui-même.

Clôture réelle d'un corps ordonné K: c'est une extension ordonnée $\tilde{K}$ de K telle que $\tilde{K}$ est extension algébrique de K et $\tilde{K}$ est un corps ordonné maximal. $\tilde{K}$ est unique à un K-isomorphisme près.

caractérisation des corps ordonnés maximaux:
un corps L est ordonné maximal si et seulement si
(i) $L = L^2 \cup (-L^2)$
(ii) pour tout $f \in L[X]$ de degré impair, f a une racine dans L.
Notons qu'un tel corps possède un seul ordre et citons comme exemple le corps $\mathbb{R}$ des réels et le corps des nombres algébriques réels.
Remarquons aussi que (ii) fait penser que les corps ordonnés maximaux sont proches des corps algébriquement clos. En fait, si L est ordonné maximal, alors $L(i)$ est algébriquement clos (ou $i^2 = -1$).

Eléments totalment positifs d'un corps ordonnable:
soit K un corps ordonnable, K est donc susceptible d'admettre plusieurs ordres totaux compatibles avec les opérations. On appellera élément totalement positif de K un élément qui est positif dans chacun de ces ordres. Il existe une caractérisation de ces éléments: $x \in K$ est totalement positif si et seulement si $-x$ est somme de carrés d'éléments de K.

II. Resolution Qualitative du 17ème Probleme de Hilbert

Le corps $\mathbb{R}(X_1, \ldots, X_n)$ est ordonable.

On a vu que toute somme de carrés d'éléments de $\mathbb{R}(X_1, \ldots, X_n)$ était définie positive et on veut étudier la réciproque, donc montrer qu'on a l'implication $f \in \mathbb{R}[X_1, \ldots, X_n]$ définie positive $\longrightarrow$ f est un élément totalement positif de $\mathbb{R}(X_1, \ldots, X_n)$.

La première démonstration de ce théorème, longue et difficile, a été donnée par Artin [1]. On en trouve d'autres présentations dans [15] et [11]. Depuis la résolution d'Artin, d'autres démonstrations utilisant la logique (la Théorie des modèles) ont été écrites; on peut à ce sujet consulter [17], [12] ou [7].

Nous exposerons ici une présentation de ces méthodes logiques. Rappelons d'abord un certain nombre d'éléments de logique.

1. *Rappels de notions de Logique.*

Les énoncés mathématiques s'expriment au moyen d'un langage. Un tel langage est formé de symboles de différents types:

des symboles de constante (comme 0 ou 1)

des symboles logiques (ou: $\vee$; et: $\wedge$; non: $<$; il existe $\bigvee$; pour tout: $\bigwedge$; et d'autres définis à partir de ceux ci, comme, par exemple, l'équivalence logique $\longleftrightarrow$)

des symboles relationnels (comme $\leq$ ou $=$)

des symboles fonctionnels (comme $+$, .)

des variables.

Pour exprimer des énoncés de la théorie des corps commutatifs, on utilisera un langage comprenant 0 et 1 comme symboles de constantes, + et . comme symboles fonctionnels, et = comme symbole relationnel.

Dans ce langage $\mathscr{L}$ on écrit les axiomes de la théorie des corps commutatifs et tout ensemble tel que les axiomes soient des propositions vraies sera un modèle de la théorie des corps commutatifs.

Ici, c'est en fait la théorie des corps commutatifs ordonnés qui nous intéressera. Citons les éléments du langage et énonçons les axiomes de cette théorie. Le langage sera formé par 0 et 1 comme symboles de constantes, + et . comme symboles fonctionnels à deux variables, — comme symbole fonctionnel à une variable et = et > 0 comme symboles relationnels.

Les axiomes de la théorie des corps commutatifs ordonnés s'écriront alors:

$$\wedge x \ \wedge y \ \wedge z \ ((x+y)+z = x+(y+z))$$
$$\wedge x \ \wedge y \ (x+y = y+x)$$
$$\wedge x \ (x+0 = x)$$
$$\wedge x \ (x+(-x) = 0)$$

$$\wedge x \ \wedge y \ \wedge z \ ((x.y).z = x.(y.z))$$
$$\wedge x \ \wedge y \ (x.y = y.x)$$
$$\wedge x \ (x.1 = x)$$
$$\wedge x \ \vee y \ ((x = 0) \vee (x.y = 1))$$
$$\wedge x \ \wedge y \ \wedge z \ (x.(y+z) = x.y + x.z)$$
$$\neg (0 = 1)$$

$$\wedge x \ \wedge y \ ((x > 0) \wedge (y > 0) \longrightarrow x+y > 0)$$
$$\wedge x \ \wedge y \ ((x > 0) \wedge (y > 0) \longrightarrow x.y > 0)$$
$$\wedge x \ (x = 0 \vee x > 0 \vee -x > 0)$$
$$\wedge x \neg ((x > 0) \wedge (-x > 0))$$

Pour obtenir les axiomes de la théorie des corps commutatifs ordonnés maximaux, on utilisera le même langage et on ajoutera aux axiomes précédents les axiomes suivants:

$$\wedge x \ \vee y \ ((x = y^2) \vee (-x = y^2))$$

et pour chaque $n \geq 0$, l'axiome

$$\wedge x_1 \ \wedge x_2 \ \ldots \ \wedge x_{2n+1} \ \vee x \ (x^{2n+1} + x_1 \ x^{2n} + \ldots + x_{2n+1} = 0)$$

Nous travaillerons maintenant dans la théorie relative à un corps de base fixé K ordonné maximal. On considère alors le langage $\mathscr{L}'$ obtenu à partir du langage $\mathscr{L}$ précédent en ajoutant aux symboles de constantes des symboles correspondant aux éléments de K.

On considère le système d'axiomes $\mathscr{A}'$ obtenu en ajoutant au système précédent $\mathscr{A}$ tous les énoncés qui lient les constantes (donc les éléments de K).

Les modèles du système $\mathscr{A}'$ sont alors les corps ordonnés maximaux L contenant K. Les corps L sont donc des extensions ordonnées de K, extensions non algébriques en général.

Expliquons maintenant la méthode d'élimination des quantificateurs.

On dit qu'un système d'axiomes $\mathscr{A}$ écrits dans un langage $\mathscr{L}$ permet l'élimination des quantificateurs si pour toute formule F du langage $\mathscr{L}$ il existe une formule F' du même langage et sans quantificateurs, telle que $F \longrightarrow F'$ soit une conséquence de $\mathscr{A}$.

Revenons aux corps commutatifs ordonnés maximaux. Cette théorie permet l'élimination des quantificateurs (voir [12]).

Comme conséquence de ce théorème, si $\mathscr{A}'$ est le système d'axiomes définis ci dessus et écrits dans le langage $\mathscr{L}'$, alors système d'axiomes $\mathscr{A}'$ (de la théorie des corps ordonnés maximaux K) est saturé.

Le mot saturé signifie que si F est une formule du langage $\mathscr{L}'$, alors F ou $\neg F$ est une conséquence de $\mathscr{A}'$. C'est à dire que l'on peut, à partir des axiomes de $\mathscr{A}'$, démontrer F ou on peut démontrer sa négation. Appliquons maintenant ces résultats au 17ème problème de Hilbert.

2. *Résolution par la logique du 17ème problème de Hilbert*

Ecrivons l'hypothèse que $f \in \mathbb{R}[X_1, \ldots, X_n]$ est définie positive. Nous avons la formule (F):

$$\wedge x_1 \ \wedge x_2 \ \ldots \ \wedge x_n \ (f(x_1, \ldots, x_n) \geq 0)$$

Cette formule F est vraie dans $\mathbb{R}$.

Soit $\mathscr{A}'$ l'ensemble d'axiomes précédents avec $K = \mathbb{R}$.

Nous savons que $\mathscr{A}'$ est saturé donc que F ou $\neg F$ peut être démontrée à partir de $\mathscr{A}'$. Puisque F est vraie dans $\mathbb{R}$, c'est que $\neg F$ n'est pas vraie dans $\mathbb{R}$. On ne pourra donc pas démontrer $\neg F$ à partir de $\mathscr{A}'$. C'est donc que F peut être démontrée.

Nous avons donc $\mathscr{A}' \longrightarrow F$. D'oú F est vraie dans tous les modèles de $\mathscr{A}'$.

En particulier, F est vraie dans $\mathscr{R}$, clôture réelle de $\mathbb{R}(X_1, \ldots, X_n)$ muni d'un ordre arbitraire. Choisissons alors comme éléments de $\mathscr{R}$: $x_1 = X_1, \ldots, x_n = X_n$. D'après F, nous en déduisons $f(X_1, \ldots, X_n) \geq 0$ dans $\mathscr{R}$ donc aussi dans $\mathbb{R}(X_1, \ldots, X_n)$. Ceci étant vrai pour tout ordre de $\mathbb{R}(X_1, \ldots, X_n)$, $f(X_1, \ldots, X_n)$ est totalement positif dans $\mathbb{R}(X_1, \ldots, X_n)$ donc f est une somme de carrés d'éléments de $\mathbb{R}(X_1, \ldots, X_n)$.

III. Etude Quantitative du 17ème Problème de Hilbert

Nous avons donc le résultat que $f \in \mathbb{R}(X_1, \ldots, X_n)$ définie positive est somme d'un nombre fini m de carrés d'éléments de $\mathbb{R}(X_1, \ldots, X_n)$, ce m dépendant de f et de n. Est-il possible de trouver $m(n)$ borne supérieure des $m(n, f)$ pour toutes les fonctions définies positives f de $\mathbb{R}(X_1, \ldots, X_n)$.

Examinons les cas des premières valeurs de n.
Si $n = 0$, on a $m(0) = 1$.
Si $n = 1$, on a $m(1) = 2$.
Si $n = 2$, on a $m(2) \leq 4$.

Un travail non publié de Ax en 1968 a montré que $m(3) \leq 8$, mais Pfister a démontré indépendamment que pour tout n on a $m(n) \leq 2^n$. [13]

Appelons donc constante de Pfister, et notons $Pf(K)$, le plus petit entier m (s'il existe) tel que toute somme de carrés d'éléments de K soit somme d'au plus m carrés; si un tel entier n'existe pas, posons $Pf(K) = \infty$. Avec cette notation, le résultat précédent de Pfister devient $Pf(\mathbb{R}(X_1, \ldots, X_n)) \leq 2^n$.

D'autre part, Cassels a établi le résultat suivant: $n + 1 \leq Pf(K(X_1, \ldots, X_n))$ quel que soit le corps K [2].

On en déduit que si $n = 2$, $3 \leq Pf(\mathbb{R}(X_1, X_2)) \leq 4$.
Mais dans un article, [3], Cassels, Ellison et Pfister ont démontré qu'un certain polynôme de $\mathbb{R}[X, Y]$ défini positif donc somme de 4 carrés n'était pas somme de 3 carrés, ainsi $Pf(\mathbb{R}(X_1, X_2)) = 4$.

Pour $n \geq 3$, le problème reste ouvert et on sait seulement que $n + 1 \leq Pf(\mathbb{R}(X_1, \ldots, X_n) \leq 2^n$.

Notons qu'on peut considérer ces questions sur d'autres corps que $\mathbb{R}$ et que Pourchet [14] a démontré récemment que $Pf(\mathbb{Q}(X)) = 5$. On ne connaissait jusque là que le résultat de Landau $Pf(\mathbb{R}(X)) \leq 8$. Nous remarquons donc que la constante de Pfister d'un corps n'est pas toujours une puissance de 2.

Le paragraphe qui suit est consacré à l'étude des notions intervenant dans la démonstration du très joli résultat de Pfister.

Sommes de carrés – Niveau et Dimension diophantienne d'un corps.

Rappelons d'abord l'identité classique:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

Nous avons ensuite l'identité de Lagrange:
le produit de deux sommes de quatre carrés est une somme de quatre carrés.

On peut démontrer cette identité en utilisant la norme multiplicative sur les quaternions définie par la somme des carrés des quatre composantes. Puis nous avons l'identité de Cayley:

Le produit de deux sommes de huit carrés est une somme de huit carrés, qui se démontre en utilisant l'algèbre, non associative et non commutative, de Cayley. Là encore, nous aurons une norme multiplicative définie par la somme des carrés des huit composantes.

Dans chacun de ces trois cas, les composantes du produit sont des formes bilinéaires des composantes des sommes données. Mais Hurwitz a montré que ceci n'était possible que pour des produits de sommes de 1, 2, 4 ou 8 carrés.

Toutefois, Pfister a réussi à démontrer que lorsqu'on considère des sommes de carrés d'éléments de corps (et non seulement d'algèbres), le produit de deux sommes de 2^n carrés est une somme de 2^n carrés d'éléments du corps. De plus, le résultat n'est pas susceptible d'amélioration en ce sens que si on considère un q tel que, dans tout corps, le produit de deux sommes de q carrés est une somme de q carrés, alors nécessairement q est une puissance de deux.

Ce théorème est utilisé dans l'étude des niveaux des corps.

Rappelons ce qu'est le niveau d'un corps K: si K est ordonnable, alors -1 ne peut être une somme de carrés d'éléments de K et on posera pour le niveau de K: $v(K) = \infty$.

Si K n'est pas ordonnable, alors -1 est une somme de carrés d'éléments de K et on appellera *niveau* de K le plus petit entier m tel que -1 soit une somme de m carrés dans K. Le résultat sur les sommes de carrés a permis à Pfister de démontrer que si K n'est pas ordonnable, alors $v(K)$ est une puissance de 2. De plus, réciproquement, pour toute puissance de 2, on peut trouver un corps K qui ait pour niveau cette puissance de 2.

Par exemple dans le cas où K est fini, tout élément est somme de deux carrés, donc $v(K)$ est 1 ou 2. Au moyen du symbole de Legendre, on sait quand $v(K) = 1$.

Il est plus intéressant de chercher quel est le niveau des corps de nombres algébriques non ordonnables c'est à dire totalement imaginaires. Pour ce faire, on utilise le principe du local – global sous la forme du théorème de Hasse-Minkowski qui permet de réduire le problème au cas du corps des complexes (trivial) et des extensions algébriques finies des corps p-adiques.

La question est alors résolue par un théorème de Hasse qui énonce que *toute forme quadratique à cinq variables et à coefficients dans un corps extension algébrique finie d'un corps p-adique, a un zéro non trivial.*

Donc, localement, -1 est somme de 4 carrés et ceci est aussi vrai globalement. En conclusion, le niveau de tout corps de nombres totalement imaginaire est 1, 2 ou 4. Un article de Connell [5] permet de décider quel est le niveau du corps dans chaque cas.

Ces questions conduisent aux problèmes d'existence de zéro non trivial pour des polynômes homogènes. Ceci est en fait la détermination de la dimension diophantienne des corps. Si K est un corps donné, on cherche à savoir quelles conditions sur le nombre des variables et sur le degré des polynômes homogènes entraîneront qu'un tel polynôme aura zéro non trivial. Sur ce sujet, on peut consulter [15].

IV. Quelques Developpements Recents du 17ème Probleme de Hilbert

Nous parlerons tout d'abord d'un théorème de Dubois dont la démonstration utilise le résultat de Artin sur le 17ème problème de Hilbert et qui est l'analogue du théorème des zéros de Hilbert. [6]

Puis nous exposerons quelques résultats sur des problèmes semblables au 17ème problème de Hilbert d'abord pour des variétés réelles [8], ensuite pour des matrices symétriques [9], considérés dernièrement par Danielle Gondard et moi même.

1. *Théorème de Dubois*

Commençons par rappeler le théorème des zéros de Hilbert.

Si K est un corps et $S \subseteq K[X_1, \ldots, X_n]$, $n \geq 1$, on associe à S l'ensemble

$$V(S) = \{x = (x_1, \ldots, x_n) \in K^n \mid f(x_1, \ldots, x_n) = 0 \quad \forall\ f \in S\}.$$

On dit que $V(S)$ est le K-ensemble algébrique associé à S.

Réciproquement, soit $T \subseteq K^n$; définissons

$$Id(T) = \{f \in K[X_1, \ldots, X_n] \mid f(x_1, \ldots, x_n) = 0, \quad \forall \times \in I\}$$

$Id(T)$ est un idéal de $K[X_1, \ldots, X_n]$.

Notons quelques propriétés:

(i) *Soit* I *l'idéal engendré par* S. *Alors* $V(I) = V(S)$.

On peut donc ne considérer que des idéaux de $K[X_1, \ldots, X_n]$.

(ii) $Id(V(I)) \supseteq I$.
(iii) $V(Id(T)) \supseteq T$.
(iv) $V(Id(V(I))) = V(I)$.

Une question importante est la détermination de $Id(V(I))$ et des idéaux tels que $Id(V(I)) = I$.

Dans le cas où K est un corps algébriquement clos, le problème est résolu par le théorème des zéros de Hilbert.

THÉORÈME DES ZÉROS DE HILBERT. *Soit K un corps algébriquement clos, I un idéal de $K[X_1, \ldots, X_n]$ alors*

$$Id(V(I)) = \sqrt{I} \quad \text{(le radical de } I\text{)}$$

defini par

$$\sqrt{I} = \{f \in K[X_1, \ldots, X_n] \mid \exists\, m \geq 1 \quad f^m \in I\}.$$

Alors, nous avons une correspondance biunivoque entre les idéaux radicaux qui sont tels que $I = \sqrt{I}$ et les K-ensembles algébriques.

De plus, les idéaux radicaux I sont caractérisés par le fait que I est intersection d'idéaux premiers et même d'un nombre fini d'idéaux premiers. $V(I)$ est alors la réunion d'un nombre fini de K-ensembles algébriques correspondant à ces idéaux premiers. Ces K-ensembles algébriques irréductibles sont alors appelés variétés de K^n.

L'étude de ces variétés est alors équivalente à celle des idéaux premiers P de $K[X_1, \ldots, X_n]$. Chaque idéal premier P est associé bijectivement à l'anneau des coordonnés de $V(P)$ c'est à dire à

$$K[X_1, \ldots, X_n]/P = K[\xi_1, \ldots, \xi_n]$$

Cet anneau est une K-algèbre intègre de type fini et toute telle algèbre peut s'obtenir à partir d'un idéal premier.

Le théorème des zéros de Hilbert permet donc de ramener l'étude géométrique des variétés à celle, algébrique, des K-algèbres intègres de type fini.

Dans le cas où K n'est pas algébriquement clos, il n'y a plus de théorème. Cependant, les corps ordonnés maximaux étant très proches des corps algébriquement clos, on peut espérer avoir dans ce cas un théorème analogue. C'est le théorème de Dubois, d'ailleurs découvert sous une forme légèrement distincte par Risler [16].

THÉORÈME DE DUBOIS. *Soit K un corps ordonné maximal, I un idéal de $K[X_1, \ldots, X_n]$. Alors $Id(V(I)) = \sqrt[R]{I}$ (le radical réel de I), défini par*

$$\sqrt[R]{I} = \{f \in K[X_1, \ldots, X_n] \mid \exists\, m \geq 1, \exists\, u_1 \ldots \exists u_r \in K(X_1, \ldots, X_n), \; f^m(1 + \sum u_i^2) \in I\}.$$

Il est clair que $\sqrt[R]{I} \supseteq \sqrt{I}$, mais il est possible que ces idéaux soient distincts; par exemple, si I est un idéal principal de $\mathbb{R}[X]$ engendré par $1 + X^2$, alors $\sqrt{I} = I$ alors que $\sqrt[R]{I}$, contenant 1, est $\mathbb{R}[X]$.

Un idéal tel que $I = \sqrt[R]{I}$ sera appelé idéal réel. Les idéaux premiers réels de $K[X_1, \ldots, X_n]$ sont alors en bijection avec les variétés irréductibles de K^n (K étant naturellement ordonné maximal) et également en bijection avec les K-algèbres intègres de type fini de la forme $K[X_1, \ldots, X_n]/P$ où $P = \sqrt[R]{P}$ est un idéal réel premier. De telles K-algèbres sont caractérisées par le fait que leur corps des fractions L est ordonnable. Les anneaux de coordonnées des variétés irréductibles de K^n ont donc la propriété que leur corps des fractions est ordonnable.

La démonstration du théorème de Dubois fait usage du théorème d'Artin. Ceci laisse croire que Hilbert, ayantes, théorème des zéros sur les complexes, voulait avoir un théorème analogue sur les réels et pressentait que la démonstration exigerait la réponse préalable à son 17ème problème.

2. *17ème problème de Hilbert pour les variétés réelles*

Soit K un corps ordonné maximal, P un idéal premier réel et $V = V(P)$. Soit $K(V)$ le corps des fractions de

$$K[X_1, \ldots, X_n]/P = K[\xi_1, \ldots, \xi_n].$$

Tout élément de $K(V)$ s'écrit $\frac{f_1}{f_2}$ où f_1 et $f_2 \in K[\xi_1, \ldots, \xi_n]$. Tout élément $f \in K[\xi_1, \ldots, \xi_n]$ peut être considéré comme une application de V dans K

ou comme la restriction à $V \subseteq K^n$ d'une fonction polynômiale $F \in K[X_1, \ldots, X_n]$.

On dira que $f \in K(V)$ est définie en $x = (x_1, \ldots, x_n) \in K$ si f peut s'écrire $f = \frac{f_1}{f_2}$ où f_1 et $f_2 \in K[\xi_1, \ldots, \xi_n]$ et que f_2 est non nulle en x.

De même, on dira que $f \in K(V)$ est définie positive sur un ensemble si elle est positive en tout point de cet ensemble où elle est définie.

On peut alors se poser la question de savoir si $f \in K(V)$ définie positive sur V est une somme de carrés dans $K(V)$.

On peut montrer qu'il existe des fonctions $f \in K[\xi_1, \ldots, \xi_n]$ définies positives sur V qui ne sont pas la restriction à V d'une fonction polynôme $F \in K[X_1, \ldots, X_n]$ définie positive sur K^n. La réponse à la question ne peut donc pas être une simple application du théorème d'Artin. Par contre, en utilisant une méthode de logique analogue à celle exposée ci-dessus, on peut démontrer que le problème admet une réponse affirmative: une fonction $f \in K(V)$ définie positive est somme de carrés dans $K(V)$.

Nous nous sommes alors intéressés au problème quantitatif correspondant.

En utilisant un lemme de Pfister, on peut montrer que $Pf(K(V)) \leq 2^d$ où d est la dimension de la variété.

D'autre part, nous faisons la conjecture que

$$d + 1 \leq Pf(K(V))$$

Cette conjecture est démontrée dans beaucoup de cas, par exemple, lorsque $d = 1$, lorsque V est une variété rationnelle donc que $K(V) = K(\eta_1, \ldots, \eta_d)$, lorsque $K(V) = K[\eta_1, \ldots, \eta_d](\alpha)$ avec $[K(V) : K(\eta_1, \ldots, \eta_d)]$ impair, ou encore lorsque V est une sphère réelle de l'espace $\mathbb{R}^3$.

3. 17*ème problème de Hilbert pour les matrices symétriques*

Précisons d'abord quelques définitions.

Soit K un corps ordonné et R une clôture réelle de K; soit $A = (A_{ij})$ une matrice symétrique d'ordre n à coefficients dans K; on dit que A est positive lorsque la forme quadratique associée à A sur $\mathbb{R}$ est positive, c'est à dire lorsque

$$\forall u = (u_1, \ldots, u_n) \in \mathbb{R}^n \qquad \sum A_{ij} u_i u_j \geq 0.$$

Cette définition est indépendante du choix de la clôture réelle $\mathbb{R}$ de K et permet de définir une relation d'ordre sur le groupe additif des matrices symétriques d'ordre n à coefficients dans K. Cet ordre sera appelé extension naturelle de l'ordre de K.

Soit maintenant K un corps quelconque. Une matrice symétrique A d'ordre n à coefficients dans K sera dite naturellement positive si A est positive pour tout ordre extension naturelle d'un ordre de K.

Nous avons d'abord obtenu la généralisation d'un résultat de Ciampi [4] qui peut alors s'exprimer grâce aux définitions ci dessus de la manière suivante:

Soit K un corps de caractéristique différente de 2. Une matrice symétrique à coefficients dans K est naturellement positive si et seulement si elle est somme de carrés de matrices symétriques à coefficients dans K. (résultat trivial si K est non ordonnable).

Considérons alors des matrices symétriques $F = (F_{ij})$ avec $F_{ij} \in K(X_1, \ldots, X_m)$ où K est ordonné maximal. On dit que F est définie au point $x = (x_1, \ldots, x_m) \in K^m$ lorsqu'on peut écrire pour tout i et tout j

$$F_{ij} = \frac{G_{ij}}{H_{ij}}, G_{ij}, H_{ij} \in K[X_1, \ldots, X_m] \quad \text{et} \quad H_{ij}(x_1, \ldots, x_m) \neq 0.$$

On dit que F est définie positive sur K^m si la matrice $F(x) = (F_{ij}(x))$ est positive en tout point x où elle est définie.

Toujours en utilisant une méthode de logique analogue à celle exposée précédemment, nous prouvons qu'une matrice symétrique à coefficients dans $K(X_1, \ldots, X_m)$ (K ordonné maximal) est définie positive si et seulement elle est somme de carrés de matrices à coefficients dans $K(X_1, \ldots, X_m)$. Dans le cas $n = 1$, on retrouve le théorème d'Artin.

On peut alors considérer les questions quantitatives correspondantes et définir une constante de Pfister $Pf(n,m)$ pour les matrices symétriques d'ordre n à coefficients dans un corps $K(X_1, \ldots, X_m)$, K étant ordonné maximal.

Il est possible de démontrer le résultat suivant $m + 1 \leq Pf(n,m) \leq 2^m$, la minoration étant obtenue assez facilement, la majoration étant plus difficile et utilisant les résultats du §2 de cette partie.

BIBLIOGRAPHIE

[1] E. ARTIN, *Uber die Zerlegung definiter Funktionen in Quadrate*, Abh. Math. Sem. Hamburg **5** (1927), 110-115.

[2] J. W. S. CASSELS, *On the representation of rational functions as sums of squares*, Acta Arithmetica **IX** (1964), 79-82.

[3] J. W. S. CASSELS, W. J. ELLISON, A. PFISTER, *On sums of squares and on elliptic curves over function fields*, Journal of Number Theory.

[4] J. R. CIAMPI, *Characterization of a class of matrices as sums of squares*, Linear Algebra and its Applications **3**. (1970), 45-50.

[5] J. G. CONNELL, *The Stufe of Number Fields*, Math. Z. **124** (1972), 20-22.

[6] D. W. DUBOIS, G. EFROYMSON, *Algebraic theory of real varieties*, Studies and Essays presented to Yu-Why-Chen on his Sixtieth Birthday. 1970.

[7] D. GONDARD, *Sur le 17ème problème de Hilbert*, thèse (3ème cycle) – 1973 – Orsay.

[8] D. GONDARD, P. RIBENBOIM, *Fonctions définies positives sur les variétés réelles*, Bulletin Sc. Math. (1974).

[9] D. GONDARD, P. RIBENBOIM, *17ème problème de Hilbert pour les matrices*, Bull. Sc. Math. (1974).

[10] D. HILBERT, *Mathematische Probleme*, Göttinger Nach. (1900), 284-285.

[11] N. JACOBSON, Abstract Algebra, vol. III, Van Nostrand, Princeton, 1964.

[12] G. KREISEL et J.L. KRIVINE, Eléments de logique mathématique – Théorie des modèles, Dunod, Paris, 1967

[13] A. PFISTER, *Zur Darstellung definiter Funktionen als Summe von Quadraten*, Invent. Math. **16** (1965), 363-370.

[14] Y. POURCHET, *Sur les représentations en sommes de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arithmetica **19** (1971), 89-104.

[15] P. RIBENBOIM, L'Arithmétique des Corps, Hermann, Paris, 1972.

[16] J. J. RISLER, *Une caractérisation des idéaux des variétés algébriques réelles*, C.R.A.S., Paris, 271(1930), 1171-73.

[17] A. ROBINSON, Introduction to model theory and the matemathematics of algebra, North Holland, Amsterdam, 1966.

Queen's University
Ringston — Ontario
Canada