À propos de la décomposition de fonctions définies en carrés

EMIL ARTIN, Hambourg

Traduction de l'allemand par Claire Lapalle et Matthieu Petit, revue par Michel Coste et Alain Herreman

1 Introduction

Dans sa conférence de Paris sur des problèmes mathématiques[1], Monsieur HILBERT a posé le problème suivant :

Une fonction rationnelle $F(x_1, x_2, \ldots, x_n)$ à n variables est dite définie, si pour aucun système réel de x_i elle ne prend des valeurs négatives.

Soit maintenant $F(x_1, x_2, \ldots, x_n)$ une fonction définie à coefficients rationnels. Peut-elle être décomposée en somme de carrés de fonctions rationnelles à coefficients rationnels ?

Ce problème est aussi mentionné dans le chapitre VII de ses Fondements de la Géométrie[2] consacré aux constructions à la règle et au compas. La preuve du théorème 45 de cette section dépend en particulier de la réponse à cette question.

Monsieur HILBERT a lui-même démontré dans la première édition des Fondements de la Géométrie que ceci était vrai pour $n = 1$.

Pour le cas $n = 2$, il a prouvé ceci[3] : une fonction définie à 2 variables est toujours la somme de carrés des fonctions rationnelles à coefficients réels.

Plus tard E. LANDAU a repris le cas $n = 1$ et a montré qu'une fonction rationnelle entière définie à une variable à coefficients rationnels peut être décomposée en somme de carrés de fonctions toutes rationnelles entières à coefficients rationnels[4]. Il a pu améliorer ce résultat en établissant que pour cette décomposition, 8 carrés suffisent[5].

Nous allons montrer qu'on peut donner une réponse du même genre à la question de HILBERT ainsi qu'à d'autres problèmes semblables en rapport avec elle.

Nous aurons besoin pour cela des définitions et des théorèmes du travail précédent[6]. Nous le désignerons par l'abbréviation A.S.

[1] D. HILBERT, "Mathematische Probleme", Göttinger Nachr. 1900, p. 284, n°17.

[2] D. HILBERT, Grundlagen der Geometrie, Leipzig 1922, p. 106, 107.

[3] D. HILBERT, Über ternäre definite Formen, Acta Math. T. 17, p. 169.

[4] E. LANDAU, Über die Darstellung definiter binärer Formen durch Quadrate, Math. Ann. T. 57, p. 53.

[5] E. LANDAU. Über die Darstellun definiter Funktionen durch Quadrate. Math. Ann. T. 62, p. 272.

[6] E. ARTIN et O. SCHREIER, Algebraische Konstruktion reller Körper.

Dans la première partie nous cherchons à caractériser les éléments d'un corps abstrait qui peuvent s'écrire comme somme de carrés. On réussit ceci facilement par une généralisation naturelle de la notion de "totalement positif". Comme cas particulier, on obtient aisément le théorème de HILBERT et de LANDAU sur la décomposition des nombres algébriques totalement positifs en carrés[7].

Ces résultats ne peuvent pas être appliqués directement au problème de D. HILBERT. La deuxième partie est consacrée à sa preuve et à quelques généralisations de celui-ci.

La troisième partie contient quelques énoncés concernant le cas des fonctions entières définies. Il y est démontré qu'on peut alors choisir les fonctions élevées au carré rationnelles entières en au moins une des variables arbitrairement donnée à l'avance. On ne peut ici en espérer beaucoup plus.

Pour finir, nous traiterons les questions analogues pour des fonctions algébriques à plusieurs variables.

2 Critères généraux

Concernant la question des éléments α d'un corps abstrait $\mathbf{K}$ qui peuvent être décomposés en somme de carrés d'éléments de $\mathbf{K}$, on peut se limiter au cas des corps réels.

Si en effet $\mathbf{K}$ n'est pas réel, alors -1 s'écrit comme somme de carrés :

$$-1 = \xi_1^2 + \xi_2^2 + \ldots + \xi_n^2. \tag{1}$$

Si $\mathbf{K}$ est de caractéristique différente de 2, on en déduit que tout élément α de $\mathbf{K}$ se décompose en $n+1$ carrés :

$$\alpha = \left(\frac{1+\alpha}{2}\right)^2 + \left(\xi_1^2 + \xi_2^2 + \ldots + \xi_n^2\right)\left(\frac{1-\alpha}{2}\right)^2. \tag{2}$$

En particulier, pour des corps de caractéristique $p > 2$, on peut prendre $n = 2$ dans (1).

Mais si $\mathbf{K}$ a pour caractéristique 2, alors le problème se règle par la remarque que chaque somme de carrés est un carré.

Il est clair aussi que la somme et le produit de sommes de carrés reste une somme de carrés. En outre, un quotient $\frac{a}{b}$ de somme de carrés, $a = \sum \alpha_\nu^2$ et $b = \sum \beta_\mu^2$, est encore une somme de carrés car on a :

$$\frac{a}{b} = \frac{a}{b^2} \cdot b = \sum \left(\frac{\alpha_\nu}{b}\right)^2 \cdot \sum \beta_\mu^2.$$

Soit maintenant un corps réel $\mathbf{K}$ et α un de ses éléments qui n'est pas une somme de carrés. Soit Ω une extension algébrique algébriquement close de $\mathbf{K}$. Alors par un raisonnement similaire à la preuve du théorème 7 de A.S., on montre l'existence d'un corps $\mathbf{P}$ compris entre $\mathbf{K}$ et $\boldsymbol{\Omega}$ satisfaisant la propriété suivante : α n'est pas décomposable en somme de carrés dans $\mathbf{P}$, mais l'est dans chaque extension algébrique propre de $\mathbf{P}$.

[7] E. LANDAU, Über die Zerlegung total positiver Zahlen in Quadrate, Göttinger Nachr. 1919, p. 392.

D'après ce qui a déjà été dit, **P** doit aussi être réel. En outre, l'élément $-\alpha$ est un carré dans **P**. Sinon $\mathbf{P}\left(\sqrt{-\alpha}\right)$ serait une extension algébrique de **P**, et par conséquent α serait dans ce corps une somme de carrés. Posons :

$$\alpha = \sum \left(\xi_\nu \sqrt{-\alpha} + \eta_\nu\right)^2 = -\alpha \sum \xi_\nu^2 + \sum \eta_\nu^2 + 2\sqrt{-\alpha} \sum \left(\xi_\nu \eta_\nu\right),$$

où les ξ_ν et η_ν appartiennent à **P**. La troisième terme à droite disparaît car sinon $\sqrt{-\alpha}$ appartiendrait à **P**. On a dès lors :

$$\alpha \left(1 + \sum \xi_\nu^2\right) = \sum \eta_\nu^2.$$

Comme **P** est un corps réel, on a alors $1 + \sum \xi_\nu^2 \neq 0$ et on aurait :

$$\alpha = \frac{\sum \eta_\nu^2}{1^2 + \sum \xi_\nu^2}.$$

Ainsi α serait un quotient de sommes de carrés, ce qui n'est pas le cas.

Dans une extension algébrique de **P**, α est une somme de carrés et $\frac{\alpha}{-\alpha} = -1$ l'est aussi. Donc aucune extension algébrique de **P** n'est réelle, d'où l'on déduit que **P** est réel clos.

Par le théorème 1 de A.S, **P** peut être ordonné. De là,$-\alpha$ est positif en tant que carré, α est donc négatif. Cet ordre de **P** définit un ordre sur **K** dans lequel α reste négatif. C'est seulement l'existence d'un tel ordre sur **K** qui nous intéresse maintenant.

Ainsi, nous définissons :

Un élément α d'un corps **K** *est dit totalement positif, quand il ne devient négatif dans aucun des ordres possibles de* **K**. *Dans un corps non réel de caractéristique $\neq 2$ (ceci sera toujours supposé dans la suite), chaque élément peut être dit totalement positif.*

Le fait que les sommes de carrés soient totalement positives est évident. En outre, nos raisonnements ont eu comme conséquence la réciproque, en d'autres termes :

Théorème 1. *Les éléments totalement positifs d'un corps* **K**, *et eux seuls, peuvent s'écrire comme somme de carrés d'éléments de* **K**.

D'après le théorème 10 de A.S, pour un corps de nombres algébriques notre définition des nombres totalement positifs coïncide avec le sens habituel. Le théorème 1 implique donc immédiatement le théorème de HILBERT-LANDAU [8].

Suivant l'exemple d'un résultat de E. LANDAU[9], nous voulons maintenant généraliser un peu notre conclusion.

Soit **R** un corps réel fixé muni d'un ordre fixé et **K** un corps contenant **R**.

Nous nous demandons quels sont les éléments α de **K** qui peuvent s'écrire sous la forme

$$\alpha = \sum e_\nu \xi_\nu^2 \tag{3}$$

où les $e_\nu \geq 0$ sont des éléments de **R** mais où les ξ_ν sont des éléments de **K**.

Soit α un élément de **K** ne s'écrivant sous la forme (3). Alors on peut facilement trouver un corps **P** contenant **K**, dans lequel α n'admet pas non plus de décomposition sous la forme (3) (où les $e_\nu \geq 0$ sont des éléments de **R** mais où

[8] voir la note 7.
[9] voir la note 4 en particulier le §3 .

les ξ_ν sont par contre pris dans **P**), tandis que cette décomposition est possible dans chaque extension algébrique.

L'hypothèse selon laquelle un élément $e > 0$ de **R** ne serait pas un carré dans **P**, conduirait à une équation de la forme :

$$\alpha = \sum e_\nu \left(\xi_\nu \sqrt{e} + \eta_\nu\right)^2 = \sum e e_\nu \cdot \xi_\nu^2 + \sum e_\nu \eta_\nu^2 + 2\sqrt{e} \sum e_\nu \xi_\nu \eta_\nu.$$

Le dernier terme de l'expression devrait disparaître. On obtient déjà une contradiction puisque comme $e\, e_\nu \geq 0$, α pourrait être représenté dans le corps **P** sous la forme (3).

Nous savons maintenant que tous les $e_\nu \geq 0$ sont des carrés dans **P**. On peut donc dans **P** se dispenser des coefficients de (3) et dire : α n'est pas une somme de carrés dans **P** mais l'est dans toute extension algébrique de **P**.

De cette manière, nous retrouvons le cas traité dans le théorème 1. **P** est réel clos et α est négatif dans l'ordre naturel de **P**. Comme chaque élement positif de **R** est un carré dans **P**, et donc positif dans **P**, l'ordre de **P** est un prolongement de l'ordre de **R**.

Il y a ainsi un ordre sur **K** qui prolonge l'ordre sur **R** dans lequel α devient négatif.

On définit donc maintenant :

Un élément α d'un corps **K** *est dit totalement positif relativement au sous-corps ordonné* **R**, *quand aucun ordre de* **K** *qui prolonge l'ordre de* **R** *ne rend α négatif.*

Il vient immédiatement :

Théorème 2. *Les éléments α de* **K** *totalement positif relativement à* **R**, *et eux seuls, peuvent se mettre sous la forme :*

$$\alpha = \sum e_\nu \xi_\nu^2,$$

où les éléments $e_\nu \geq 0$ sont des élements de **R** *et les ξ_ν des éléments de* **K**.

Grâce encore au théorème 10 de AS nous voyons sans peine ce que cet énoncé signifie pour les corps de nombres algébriques.

3 Décomposition des fonctions définies

Nous voyons qu'il nous reste à montrer maintenant que les fonctions définies sont totalement positives.

On peut obtenir cette démonstration en montrant le théorème général suivant :

Théorème 3. *Soit* **R** *un corps de nombres réels dans le sens habituel et* **K** *le corps des fonctions rationnelles à n variables $x_1, x_2, \ldots, x_n$ à coefficients dans* **R**. *On se donne sur* **K** *un ordre quelconque mais fixé qui prolonge l'ordre naturel de* **R**.

Etant donné un système fini de fonctions $\varphi_1(x), \varphi_2(x), \ldots, \varphi_m(x)$ sur **K** *(m quelconque) des variables $x_1, x_2, \ldots, x_n$ (le symbole x représente ici et dans la suite toutes les variables), alors il y a n nombres rationnels $a_1, a_2, \ldots, a_n$ tels que les fonctions $\varphi_\nu(x)$ gardent un sens pour $x_i = a_i$ et que la valeur de la fonction $\varphi_\nu(a)$ a le même signe que $\varphi_\nu(x)$.*

Cette condition sur les signes signifie plus exactement : pour l'ordre donné de $\mathbf{K}$, si $\varphi_\nu(x) > 0$ alors $\varphi_\nu(a) > 0$, si $\varphi_\nu(x) = 0$ on a naturellement $\varphi_\nu(a) = 0$ et si $\varphi_\nu(x) < 0$ on doit aussi avoir $\varphi_\nu(a) < 0$.

Notre théorème est trivial pour $n = 0$, car les fonctions $\varphi_\nu(x)$ sont déjà reduites à des constantes. Supposons le théorème démontré pour le cas à n variables et montrons qu'il reste vérifié pour le cas à $n+1$ variables. En procédant à la démonstration, nous verrons qu'il fallait commencer l'induction par $n = 0$.

Tout d'abord, tirons les conséquences du fait que le théorème est vrai pour n variables. Soit $\mathbf{P}$ un corps réel clos algébrique sur $\mathbf{K}$ dont l'ordre prolonge celui de $\mathbf{K}$. L'existence de $\mathbf{P}$ est garantie par le théorème 8 de A.S.

Nous considérons maintenant des fonctions $f(t, x)$ avec une nouvelle variable t à coefficients dans $\mathbf{K}$, rationnelles entières en t, et convenons de la manière de parler suivante :

Une propriété E d'un système de fonctions $f_1(t, x), f_2(t, x), \ldots, f_k(t, x)$ est dite spécialisable s'il existe un système de fonctions rationnelles $\varphi_1(x), \varphi_2(x), \ldots, \varphi_m(x)$ dépendant seulement de x, satisfaisant la condition suivante. Soient $a_1, a_2, \ldots, a_n$ des nombres rationnels tels que toutes les fonctions $\varphi_\nu(x)$ aient un sens pour $x_i = a_i$ et aient le même signe que leurs valeurs $\varphi_\nu(a)$, alors toutes les fonctions $f_\nu(t, a)$ ont un sens pour $x_i = a_i$ et le système $f_1(t, a), f_2(t, a), \ldots, f_k(t, a)$ a également la propriété E.

Évidemment une conjonction de propriétés spécialisables est encore spécialisable. En outre, d'après l'hypothèse de récurrence, il y a bien des nombres rationnels a_i qui produisent la spécialisation.

Démontrons maintenant les deux lemmes suivants :

Lemme 1. *Pour une fonction $f(t, x)$, le fait d'avoir en tant que fonction de t exactement r racines réelles dans le corps $\mathbf{P}$ est une propriété spécialisable.*

Démonstration : Soit

$$f(t, x) = \psi_0(x)t^s + \psi_1(x)t^{s-1} + \ldots + \psi_s(x)$$

et

$$F(t) = A_0t^s + A_1t^{s-1} + \ldots + A_s$$

l'équation générale de degré s. Puisque, d'après le théorème 6 de A.S, tous les théorèmes de l'algèbre réelle sont valables pour le corps $\mathbf{P}$, on sait qu'il y a une suite d'un nombre fini de fonctions entières $\Phi_\nu(A)$ des A_i à coefficients rationnels telle que, pour des A_i spécialisés dans $\mathbf{P}$, la répartition des signes de la suite $\Phi_\nu(A)$ nous donne le nombre de racines réelles de la fonction $F(t)$ spécialisée en ce A. L'existence d'une telle suite découle directement du théorème de Sturm ou des théorèmes qui conviennent aussi bien ici sur les Bezoutiens.

On prend maintenant pour l'ensemble des fonctions $\varphi(x)$ à construire :

1. tous les coefficients $\psi_i(x)$ de $f(t, x)$, de sorte qu'on obtienne quelque chose qui a un sens par susbtitution de nombres rationnels.
2. les expressions $\Phi_\nu(\psi(x))$, qui sont en nombre fini.

Soit un a_i tel que les $\varphi_\nu(x)$ dans l'ensemble ainsi défini aient toujours le même signe que les $\varphi_\nu(a)$, alors $f(t, a)$ a un sens et a autant de racines réelles que $f(t, x)$ puisque les signes n'ont pas été changés dans la suite correspondante des $\Phi_\nu(\psi(a))$.

Lemme 2. *On considère,pour une suite de fonctions $f_1(t, x), f_2(t, x), \ldots, f_k(t, x)$ donnée, la propriété que $f_\nu(t, x)$ possède une certaine racine réelle α_ν dans $\mathbf{P}$*

et que

$$\alpha_1 < \alpha_2 < \ldots < \alpha_k.$$

Cette propriété de la suite est spécialisable.

Démonstration : On ajoute à $\mathbf{K}$ tous les α_i ainsi que toute les racines carrées $\sqrt{\alpha_i - \alpha_j}$, pour tous les couples d'entiers $i > j$. Le corps ainsi obtenu est réel et s'obtient à partir de $\mathbf{K}$ par l'adjonction d'une grandeur réelle ξ. Cette grandeur réelle ξ satisfait l'équation irréductible sur $\mathbf{K}$ $F(t, x) = 0$.

α_i et $\sqrt{\alpha_i - \alpha_j}$ doivent dépendre de ξ, en fait de façon rationnelle entière en ξ, soit :

$$\alpha_i = g_i(\xi, x) \quad ; \quad \sqrt{\alpha_i - \alpha_j} = h_{ij}(\xi, x) \quad (i > j).$$

Nous avons maintenant $f_i(g_i(\xi, x), x) = 0$, et la fonction $f_i(g_i(t, x), x)$ est divisible par $F(t, x)$; on a donc :

$$f_i(g_i(t, x), x) = F(t, x)G_i(t, x). \tag{4}$$

De même l'identité :

$$g_i(\xi, x) - g_j(\xi, x) - (h_{ij}(t, x))^2 = 0 \quad \text{pour } i > j,$$

montre que l'on a :

$$g_i(t, x) - g_j(t, x) - (h_{ij}(t, x))^2 = F(t, x)\Phi_{ij}(t, x) \quad \text{pour} \quad i > j. \tag{5}$$

Enfin $h_{ij}(\xi, x) \neq 0$. De nouveau, son inverse s'exprime de façon rationnelle entière en fonction de ξ, soit :

$$\frac{1}{h_{ij}(\xi, x)} = H_{ij}(\xi, x)$$

Ceci conduit à une équation de la forme :

$$h_{ij}(t, x)H_{ij}(t, x) - 1 = F(t, x)\,\Psi_{ij}(t, x) \quad \text{pour} \quad i > j. \tag{6}$$

Dans l'ensemble de fonctions $\varphi_\nu(x)$ à construire pour la spécialisation, on prend d'abord un système de fonctions qui nous assure que toutes les identités précédentes gardent un sens. On prend précisément tous les coefficients des fonctions des fonctions entières de la variable t suivantes : $f_i(t, x)$, $F(t, x)$, $g_i(t, x)$, $h_{ij}(t, x)$, $G_i(t, x)$, $\varphi(t, x)$, $H_{ij}(t, x)$ et $\Psi_{ij}(t, x)$.

Ensuite l'ensemble de fonctions $\varphi(x)$ dont l'existence a été établie par le lemme 1, qui garantit que $F(t, x)$ a aussi une racine réelle après spécialisation. Ceci suffit.

En effet si les $x_i = a_i$ forment un système de nombres rationnels satisfaisant nos conditions sur les signes, alors l'équation $F(t, a) = 0$ a une racine réelle ξ.

Posons maintenant $\overline{\alpha_i} = g_i(\overline{\xi}, a)$. Si l'on fait $t = \overline{\xi}$ et $x = a$ dans (4), on obtient $f_i(\overline{\alpha_i}, a) = 0$. De (6), on a :

$$h_{ij}(\overline{\xi}, a)H_{ij}(\overline{\xi}, a) = 1 \quad \text{pour} i > j$$

alors en particulier $h_{ij}(\overline{\xi}, a) \neq 0$, ainsi (5) montre que :

$$\overline{\alpha_i} - \overline{\alpha_j} = \left(h_{ij}(\overline{\xi}, a)\right)^2 > 0$$

C'est ce qu'il fallait démontrer.

Après ces préparatifs, on peut facilement terminer la démonstration du thèorème 3.

Nous désignons la $n+1$-ème variable par τ et notons $\mathbf{K}$ le corps des fonctions rationnelles des n variables restantes x_i. On se donne un ordre fixé sur le corps $\mathbf{K}(\tau)$ qui préserve l'ordre de $\mathbf{R}$. Soit $\mathbf{P'}$ la cloture algébrique réelle de $\mathbf{K}(\tau)$ qui préserve cet ordre et $\mathbf{P}$ la cloture réelle de $\mathbf{K}$ contenue dans $\mathbf{P'}$.

Soit maintenant $f_1(\tau, x), f_2(\tau, x), \ldots, f_k(\tau, x)$ des fonctions rationnelles de τ et de x, dont on peut supposer sans perte de généralité qu'aucune n'est identiquement nulle. Il faut montrer que l'on peut remplacer τ et x par des nombres rationnels tels que les signes des valeurs des fonctions soient les mêmes que ceux des fonctions. Pour cela, nous décomposons les fonctions $f_i(\tau, x)$ en fonctions irréductibles de τ. Soit :

$$P_1(\tau, x), P_2(\tau, x), ..., P_m(\tau, x)$$

les fonctions entières irréductibles de τ (avec pour coefficient dominant 1), distinctes deux à deux, qui proviennent des numérateurs et des dénominateurs des $f_i(\tau, x)$ et

$$\psi_1(x), \ldots, \psi_s(x)$$

les facteurs ne dépendant pas de τ, dont on a besoin pour reformer les $f_i(\tau, x)$ à partir des $P_i(\tau, x)$.

Il est clair qu'il suffit de démontrer notre théorème pour le système

$$P_1(\tau, x), ..., P_m(\tau, x), \psi_1(x), \ldots, \psi_s(x).$$

En effet, si on peut spécialiser de façon à ce que tout élément de ce système garde son signe, ceci sera a fortiori vrai pour le système de départ.

Afin d'établir ceci, on considère les fonctions

$$P_1(t, x), P_2(t, x), ..., P_m(t, x)$$

dans $\mathbf{K}$ et $\mathbf{P}$. On ordonne toutes les racines réelles de toutes ces fonctions de la variable t par ordre croissant

$$\alpha_1 < \alpha_2 < ... < \alpha_l,$$

et on suppose α_i racine de $P_{\lambda_i}(t, x)$.

Nous spécialisons maintenant de la façon suivante :

Pour l'ensemble des fonctions $\varphi(x)$ à construire, nous prenons :

1. les fonctions $\psi_1(x), \ldots, \psi_s(x)$.
2. l'ensemble des fonctions $\varphi(x)$ qui servent à montrer que $P_i(t, x)$ a autant de racines réelles que $P_i(t, a)$, dont l'existence est donnée par le lemme 1.
3. l'ensemble de fonctions $\varphi(x)$, donné par le lemme 2 appliqué à la suite $P_{\lambda_1}(t, x), \ldots, P_{\lambda_l}(t, x)$, qui assurent que les $P_{\lambda_i}(t, a)$ ont des racines réelles $\overline{\alpha_i}$ telles que :
$$\overline{\alpha_1} < \overline{\alpha_2} < \ldots < \overline{\alpha_l}.$$

L'existence de tels nombres rationnels a_i est une conséquence de l'hypothèse de récurrence. Puisque nous avons pris les $\psi_\nu(x)$, la conservation du signe de ces fonctions est déjà garantie. Il suffit donc de s'occuper des $P_\nu(t, a)$.

Comme $P_\nu(t,a)$ a exactement le même nombre de racines réelles que $P_\nu(t,x)$, le nombre total des racines réelles de tous les polynômes $P_\nu(t,a)$ est l, de sorte que $\overline{\alpha_1}, \overline{\alpha_2}, \ldots, \overline{\alpha_l}$ sont toutes les racines réelles de nos polynômes. En raison de la troisième condition ci-dessus, la façon dont ces racines sont ordonnées est la même que pour les α_i.

Les fonctions $P_\nu(t,x)$ se décomposent dans le corps $\mathbf{P}'$ en facteurs linéaires et quadratiques, les racines complexes provenant de ces derniers. Il en est de même pour les fonctions $P_\nu(t,a)$. Pour une valeur de t quelconque de $\mathbf{P}'$, les facteurs quadratiques ont une contribution positive au produit, le signe de $P_\nu(t,x)$ ne dépend donc que des facteurs linéaires et donc seulement de l'intervalle entre les racines dans lequel se trouve t.

Supposons l'élément τ dans l'intervalle $\alpha_i < \tau < \alpha_{i+1}$. Comme les racines de $P_\nu(t,a)$ sont ordonnées exactement de la même manière, toutes les fonctions $P_\nu(t,a)$ prendront donc le même signe que $P_\nu(t,x)$ quand on choisit pour t une valeur comprise entre $\overline{\alpha_i}$ et $\overline{\alpha_{i+1}}$. Mais maintenant les $\overline{\alpha_i}$ sont algébriques relativement à $\mathbf{R}$ puisque ce sont les racines des équations $P_\nu(t,a) = 0$. Une extension algébrique d'un corps archimédien $\mathbf{R}$ dont il conserve l'ordre est elle-même archimédienne, puisque d'après le théorème 6 de A.S on peut borner les racines des équations. Il y a forcément un nombre rationnel b entre $\overline{\alpha_i}$ et $\overline{\alpha_{i+1}}$. Posons $t = b$, alors les $P_\nu(b,a)$ ont le même signe que $P_\nu(\tau,x)$ et tout est ainsi démontré. Si l'on est dans le cas $\tau < \overline{\alpha_1}$ ou $\tau > \overline{\alpha_l}$, alors on choisit un nombre rationnel $b < \overline{\alpha_1}$ respectivement $b > \overline{\alpha_l}$.

Avec cette dernière partie, on voit maintenant pourquoi on doit descendre jusqu'au corps $\mathbf{R}$ dans la récurrence. On a besoin pour la preuve de théorèmes sur la séparation des racines qui ne sont valables que pour les corps archimédiens et les corps réels clos.

Soit maintenant $\mathbf{R}$ un corps de nombres réels qui peut être ordonné d'une seule façon. Alors tout ordre sur $\mathbf{K}$ est un prolongement de l'ordre sur $\mathbf{R}$. En outre soit $F(x_i)$ une fonction rationnelle définie sur $\mathbf{K}$, c'est-à-dire une fonction telle que pour tous nombres rationnels a_i tels que $F(x_i)$ a un sens au point $x_i = a_i$, la fonction garde une valeur positive ou nulle : $F(a_i) \geq 0$. Par le théorème 3, $F(x_i)$ n'est négative pour aucun ordre de $\mathbf{K}$ puisqu'elle serait sinon négative pour un certain nombre rationnel. Ainsi, $F(x_i)$ est totalement positive sur $\mathbf{K}$.

D'après le théorème 1, on a ainsi établi :

Théorème 4. *Soit* $\mathbf{R}$ *un corps de nombres réels qui peut être ordonné d'une seule façon, comme par exemple le corps des nombres rationnels ou de tous les nombres algébriques réels ou de tous les nombres réels. Alors chaque fonction rationnelle définie des variables* $x_1, x_2, \ldots, x_n$ *à coefficients dans* $\mathbf{R}$ *est une somme de carrés de fonctions rationnelles à coefficients dans* $\mathbf{R}$.

En outre, soit $\mathbf{R}$ un corps de nombres algébriques quelconque. Une fonction rationnelle à coefficients dans $\mathbf{R}$ est dite totalement définie si elle ne prend que des valeurs totalement positives de $\mathbf{R}$ aux points rationnels pour lesquels elle a un sens. On a de nouveau facilement :

Théorème 5. *Soit* $\mathbf{R}$ *un corps de nombres algébriques, alors toute fonction rationnelle totalement définie à coefficients dans* $\mathbf{R}$ *est une somme de carrés de fonctions rationnelles à coefficients dans* $\mathbf{R}$.

Pour un corps quelconque de nombres réels, il résulte finalement du théorème 3 et du théorème 2 :

Théorème 6. *Soit* $\mathbf{R}$ *un corps quelconque de nombres réels et* $F(x_1, x_2, \ldots, x_n)$

une fonction rationnelle définie à coefficients dans $\mathbf{R}$*. Alors la fonction* $F(x_i)$ *peut se mettre sous la forme :*

$$F(x_i) = \sum_{\nu} e_\nu \cdot (\varphi_\nu(x_i))^2$$

où les e_ν *sont des nombres de* $\mathbf{R}$ *positifs ou nuls et les* $\varphi_\nu(x_i)$ *des fonctions rationnelles à coefficients dans* $\mathbf{R}$*.*

Pour la preuve de nos théorèmes, nous avons fait un usage répété d'un bon ordre. Mais cela est accessoire.

En effet, on note que l'on peut toujours supposer $\mathbf{R}$ dénombrable, puisqu'il suffit de prendre pour $\mathbf{R}$ le corps obtenu à partir du corps des nombres rationnels par l'adjonction des coefficients des fonctions définies considérées. Dès lors, $\mathbf{K} = \mathbf{R}(x_1, x_2, \ldots, x_n)$ est aussi clairement dénombrable, ainsi que le corps des fonctions algébriques sur $\mathbf{K}$.

L'axiome du bon ordre est donc superflu, si l'on a en vue seulement les théorèmes 4, 5 et 6.

En revanche, nos preuves sont indirectes et ne fournissent aucune règle explicite pour la décomposition. Nous pouvons cependant espérer compléter les preuves dans cette direction.

4 La décomposition des fonctions entières définies.

Maintenant, une question naturelle est de savoir si nos résultats peuvent être améliorés d'une manière ou d'une autre pour les fonctions rationnelles entières définies. Comme Monsieur HILBERT[10] l'a montré le premier par la construction d'un exemple extrêmement ingénieux, on ne peut plus espérer, déjà pour des fonctions à deux variables, pouvoir choisir les fonctions élevées au carré rationnelles entières ; et ceci, même si on prend les coefficients dans le corps des nombres réels.

Monsieur LANDAU[11] a le premier montré que ceci peut se faire au moins pour les fonctions d'une variable et que, pour des fonctions de deux variables, on peut toujours choisir les fonctions élevées au carré entières en une des deux variables arbitrairement choisie, si à la base on a pris le corps de tous les nombres réels comme corps de coefficients.

Avec quelques légères modifications, la preuve de E. LANDAU permet de montrer ce fait pour un nombre quelconque de variables et pour un corps arbitraire de coefficients.

Nous voulons montrer que :

Théorème 7. *Soit* $\mathbf{K}$ *un corps réel quelconque et* $\mathbf{K}(x)$ *le corps des fonctions rationnelles d'une variable* x *à coefficients dans* $\mathbf{K}$*. Si la fonction rationnelle entière* $F(x)$ *se décompose en somme de carrés dans* $\mathbf{K}(x)$*, alors il y a aussi une décomposition de* $F(x)$ *en sommes de carrés de fonctions rationnelles entières sur* $\mathbf{K}$ *.*

Démonstration : Le théorème est trivial pour des constantes puisque, dans une représentation d'une constante par une somme de carrés de fonctions rationnelles en x, on peut remplacer x par une valeur qui n'annule aucun des

[10] D. HILBERT, Über die Darstellung definiter Formen als Summe von Formenquadraten. Math Ann. T.32, p.342

[11] cf. en particulier le travail cité dans la note 5.

dénominateurs, et on obtient ainsi une décomposition de la constante en somme de carrés de constantes.

Supposons notre théorème démontré pour les fonctions de degré inférieur à n. Soit maintenant $F(x)$ une fonction de degré n qui est une somme de carrés de fonctions rationnelles.

Nous pouvons supposer que $F(x)$ n'est divisible par aucun carré d'une fonction rationnelle entière $\Phi(x)$ de degré positif. Sinon on peut poser :

$$F(x) = (\Phi(x))^2 \, G(x)$$

où $G(x)$ a un degré plus petit et est aussi une somme de carrés. Alors $G(x)$ peut être représenté comme une somme de carrés de fonctions rationnelles entières, ce qui nous donnerait une représentation pour $F(x)$.

Soit maintenant $\varphi(x)$ le dénominateur commun des fonctions élevées au carré dans la décomposition de $F(x)$. Alors on a une identité de la forme :

$$(\varphi(x))^2 \; F(x) = \sum_{\nu=1}^{N} (g_\nu(x))^2 \qquad \varphi(x) \neq 0, \quad g_\nu(x) \quad \text{entière.} \tag{7}$$

Parmi toutes les égalités de la forme (7) on en choisit une pour laquelle le degré de $\varphi(x)$ est le plus petit possible.

Dès lors, les $g_\nu(x)$ ne peuvent pas être tous divisibles par $F(x)$. Car on pourrait alors poser $g_\nu(x) = F(x) q_\nu(x)$ et obtenir :

$$(\varphi(x))^2 = F(x) \sum_{\nu=1}^{N} (q_\nu(x))^2 \, .$$

Comme $F(x)$ est sans facteurs carrés, $\varphi(x)$ doit être divisible par $F(x)$. En divisant alors l'équation (7) par $(F(x))^2$, on obtient :

$$\left(\frac{\varphi(x)}{F(x)} \right)^2 \cdot F(x) = \sum_{\nu=1}^{N} (q_\nu(x))^2 \ ,$$

ce qui est impossible puisque $\frac{\varphi(x)}{F(x)}$ a un degré inférieur à celui de $\varphi(x)$.

Ainsi quand on pose $g_\nu(x) = q_\nu(x) \, F(x) + h_\nu(x)$, où le degré de $h_\nu(x)$ est au plus égal à $n-1$, les $h_\nu(x)$ ne sont pas tous nuls. Si on utilise cette égalité dans (7), on obtient alors en passant tous les termes divisibles par $F(x)$ du côté gauche :

$$f(x) \, F(x) = \sum_{\nu=1}^{N} (h_\nu(x))^2 \neq 0 \, . \tag{8}$$

Le degré du membre de droite est au plus $2n-2$, donc celui de $f(x)$ est au plus $n-2$.

Parmi toutes les identités de la forme (8) on en choisit une telle que le degré de $f(x)$ soit le plus petit possible. Puisque ce degré sera sûrement plus petit que n, nous savons que $f(x)$ (comme il est aussi somme de carrés en tant que quotient de sommes de carrés) s'écrit comme une somme de carrés de fonctions rationnelles entières. Si $f(x)$ est constante, il en est de même pour $\frac{1}{f(x)}$ et on obtient immédiatement la décompsition recherchée de $F(x)$.

Soit alors $f(x)$ non constante de degré m. Alors on a deux cas possibles :

1. Toutes les $h_\nu(x)$ sont divisibles par $f(x)$ (posons $h_\nu(x) = f(x)\, q_\nu(x)$). Alors on a d'après (8) :

$$F(x) = f(x) \cdot \sum_{\nu=1}^{N} (q_\nu(x))^2$$

Mais comme $f(x)$ est décomposable en fonctions rationnelles entières, on obtient la décomposition recherchée pour $F(x)$.

2. On a $h_\nu(x) = q_\nu(x)\, f(x) + r_\nu(x)$ où les $r_\nu(x)$ ont un degré au plus $m-1$ et ne sont pas tous nuls. Comme $r_\nu(x) \equiv h_\nu(x) \pmod{f(x)}$, on a donc :

$$\sum_{\nu=1}^{N} (r_\nu(x))^2 \equiv \sum_{\nu=1}^{N} (h_\nu(x))^2 = f(x)\, F(x) \equiv 0 \pmod{f(x)}.$$

Alors on peut poser

$$\sum_{\nu=1}^{N} (r_\nu(x))^2 = f(x)\, f_1(x) \neq 0\,, \tag{9}$$

où $f_1(x) \neq 0$ et a un degré plus petit que $f(x)$, précisément au plus $m-2$. On utilise maintenant l'identité connue en rapport avec l'inégalité de Schwarz :

$$\begin{aligned} &\sum_{\nu=1}^{N} (h_\nu(x))^2 \cdot \sum_{\nu=1}^{N} (r_\nu(x))^2 \\ &= \left(\sum_{\nu=1}^{N} h_\nu(x)\, r_\nu(x) \right)^2 + \sum_{1 \geq \nu < \mu \geq N} (h_\nu(x)\, r_\mu(x) - h_\mu(x)\, r_\nu(x))^2 \,. \end{aligned} \tag{10}$$

D'après (8) et (9) on a à gauche la fonction $F(x)\ (f(x))^2\ f_1(x \neq 0$. Le membre de droite de l'égalité est une somme de carrés.

Puisque

$$\sum_{\nu=1}^{N} h_\nu(x)\, r_\nu(x) \equiv \sum_{\nu=1}^{N} (h_\nu(x))^2 = f(x)\, F(x) \equiv 0 \pmod{f(x)}$$

et

$$h_\nu(x)\, r_\mu(x) - h_\mu(x)\, r_\nu(x) \equiv h_\nu(x)\, h_\mu(x) - h_\mu(x)\, h_\nu(x) \equiv 0 \pmod{f(x)}\,,$$

toutes les fonctions élevées au carré du terme de droite de l'équation (10) sont divisibles par $f(x)$, donc sont de la forme $f(x) \cdot \Phi_i(x)$.

De (10) on obtient ainsi :

$$\begin{aligned} F(x)\ (f(x))^2\ f_1(x) &= \sum (f(x)\, \Phi_i(x))^2 \neq 0 \quad \text{ou} \\ F(x)\, f_1(x) &= \sum (\Phi_i(x))^2 \neq 0 \end{aligned}$$

On a maintenant une contradiction, car ceci est une identité de la forme (8) et $f_1(x)$ a un degré infèrieur à celui de $f(x)$.

D'autre part, on a aussi le théorème général :

Théorème 8. *Soit* $\mathbf{R}$ *un sous-corps réel de* $\mathbf{K}$ *muni d'un ordre fixé. Si une fonction rationnelle entière* $F(x)$ *dans* $\mathbf{K}(x)$ *se décompose sous la forme :*

$$F(x) = \sum e_\nu \ ((\varphi_\nu(x))^2 \ ,$$

où les $e_\nu \geq 0$ *appartiennent à* $\mathbf{R}$ *et les* $\varphi_\nu(x)$ *sont rationnelles, alors on a aussi une décomposition de cette forme avec les* $\varphi_\nu(x)$ *rationnelles et entières.*

Comme la démonstration est mot à mot celle du théorème 7, nous la laissons au soin du lecteur. A la place de l'identité (10) on a besoin ici de :

$$\sum_{\nu=1}^{N} e_\nu \ (h_\nu(x))^2 \cdot \sum_{\nu=1}^{N} e_\nu \ (r_\nu(x))^2$$

$$= \left(\sum_{\nu=1}^{N} e_\nu \, h_\nu(x) \, r_\nu(x) \right)^2 + \sum_{1 \geq \nu < \mu \geq N} e_\nu \, e_\mu \ (h_\nu(x) \, r_\mu(x) - h_\mu(x) \, r_\nu(x))^2 \, .$$

De ces deux theorèmes, on déduit que :

Théorème 9. *Les décompositions établies dans les théorèmes 4, 5 et 6 peuvent, dans le cas des fonctions rationnelles entières, être arrangées de façon que toutes les fonctions élevées au carré qui y figurent soient rationnelles entières en une variable arbitrairement donnée à l'avance.*

5 La décomposition des fonctions algébriques

Il est possible aussi briévement d'examiner la décomposabilité des fonctions algébriques de plusieurs variables en carrés.

Soit $\mathbf{R}$ le corps de tous les nombres réels (on pourrait aussi ici partir d'un corps de coefficients quelconque) et $\mathbf{K}$ le corps des fonctions rationnelles réelles à n variables x_i.

Soit $\mathbf{K}(\xi)$ une extension algébrique réelle de $\mathbf{K}$. Que signifie cette réalité ? Si $F(t, x) = 0$ est l'équation irréductible sur $\mathbf{K}$ pour ξ, alors celle-ci a pour un ordre approprié de $\mathbf{K}$ l'élément ξ comme racine réelle. Par le lemme 1, il suit que l'on peut trouver pour x une valeur rationnelle telle que pour $x = a$ notre équation $F(t, a) = 0$ a une racine réelle dans le sens habituel. D'après les arguments développés dans le lemme 1, ceci doit encore être le cas dans un petit voisinage de a, puisque dans un voisinage suffisamment petit on n'a aucun changement de signe pour l'ensemble de fonctions $\varphi(x)$ considéré.

Ainsi ξ a une branche réelle au voisinage d'un point a_i. Réciproquement, supposons que ceci soit le cas. Alors -1 ne s'écrit sûrement pas comme somme de carrés dans $\mathbf{K}(\xi)$, car sinon on pourrait trouver dans ce voisinage un point où toutes les spécialisations nécessaires garderaient un sens et ainsi on aurait -1 représenté comme somme de carrés dans $\mathbf{R}$, ce qui ne va pas. Nous obtenons ainsi :

Théorème 10. *La réalité du corps* $\mathbf{K}(\xi)$ *signifie que la fonction algébrique* ξ *possède une branche réelle dans un voisinage suffisamment petit d'un point a convenable et qu'ainsi* ξ *est une fonction algébrique réelle au sens habituel.*

Quels éléments $\alpha = \varphi(\xi, x)$ de $\mathbf{K}(\xi)$ sont alors totalement positifs dans ce corps ? On considère seulement les points pour lesquels $F(t, x) = 0$ n'admet que des racines finies et le dénominateur de $\varphi(\xi, x)$ ne s'annule pas. Les points exclus sont alors sur des variétés algébriques de dimension inférieure à n. Si $\varphi(\xi, x)$ est totalement positif, et donc somme de carrés, alors, en chaque point où aucun des dénominateurs qui apparaissent ne s'annule, il doit devenir positif pour chaque valeur réelle existante de ξ. Réciproquement, si ceci est le cas, alors $\varphi(\xi, x)$ doit être totalement positif. Précisément, supposons qu'il existe un ordre de $\mathbf{K}(\xi)$ où $\varphi(\xi, x)$ devient négatif.

Alors construisons le corps réel $\mathbf{K}\left(\xi, \sqrt{-\varphi(\xi, x)}\right) = \mathbf{K}(\eta)$. Soit

$$\xi = f(\eta, x), \quad \sqrt{-\varphi(\xi, x)} = \psi(\eta, x) \qquad \text{et} \quad \Phi(t, x) = 0$$

l'équation pour η. Alors on a $F\left(f(t, x), x\right) = 0$, et donc

$$F\left(f(t, x), x\right) = \Phi(t, x)\, G(t, x) \ .$$

De même

$$-\varphi\left(f(t, x), x\right) - \left(\psi(t, x)\right)^2 = \Phi(t, x)\, H(t, x) \ .$$

On spécialise maintenant de telle façon que $\Phi(t, a) = 0$ a une racine réelle $\overline{\eta}$ et que les deux identités gardent un sens. Ceci a lieu dans un voisinage suffisamment petit d'un point. Nos formules donnent, si l'on pose $\overline{\xi} = f(\overline{\eta}, a)$:

$$F(\overline{\xi}, a) = 0 \ ; \qquad -\varphi(\overline{\xi}, a) = \left(\phi(\overline{\eta}, a)\right)^2 \ .$$

Si l'on prend soin aussi que $\phi(\overline{\eta}, a) \neq 0$, ce que l'on peut obtenir en raisonnant comme dans la preuve du lemme 2, alors on voit que $F(t, a) = 0$ a une racine réelle $\overline{\xi}$ pour laquelle $\varphi(\overline{\xi}, a) < 0$, et même dans tout un voisinage. Ceci contredit nos hypothèses. On trouve ainsi :

Théorème 11. *Dans le corps $\mathbf{K}(\xi)$ un élément $\alpha = \varphi(\xi, x)$ est totalement positif, et donc somme de carrés, quand, en tout point a_i, il devient positif pour chaque branche réelle de ξ existant là. Des exceptions sont autorisées sur des variétés de dimension inférieure.*

Hambourg, Séminaire de Mathématiques, Juin 1926.