Canad. Math. Bull. Vol. **40** (1), 1997 pp. 81–87

UNE CARACTÉRISATION DES CORPS SATISFAISANT LE THÉORÈME DE L'AXE PRINCIPAL

A. MOVAHHEDI ET A. SALINIER

RÉSUMÉ. On caractérise les corps K satisfaisant le théorème de l'axe principal à l'aide de propriétés des formes trace des extensions finies de K. Grâce à la caractérisation de ces mêmes corps due à Waterhouse, on retrouve à partir de là, de façon élémentaire, un résultat de Becker selon lequel un pro-2-groupe qui se réalise comme groupe de Galois absolu d'un tel corps K est engendré par des involutions.

ABSTRACT We characterize general fields K, satisfying the Principal Axis Theorem, by means of properties of trace forms of the finite extensions of K. From this and Waterhouse's characterization of the same fields, we rediscover, in quite an elementary way, a result of Becker according to which a pro-2-group which occurs as the absolute Galois group of such a field K, is generated by involutions.

1**.** **Introduction.** Soit K un corps. Rappelons que K est dit *formellement réel* lorsque -1 n'est pas une somme de carrés de K, et qu'un *corps ordonné maximal* est un corps formellement réel tel que toute extension algébrique formellement réelle de K est triviale. Enfin on dit que K *satisfait le théorème de l'axe principal* si toute matrice symétrique à coefficients dans K est semblable à une matrice diagonale à coefficients dans K. Waterhouse [3] a caractérisé les corps satisfaisant le théorème de l'axe principal comme étant les intersections de corps ordonnés maximaux. L'objet de notre travail est de présenter une autre caractérisation de ces mêmes corps en utilisant les propriétés des formes traces de leurs extensions finies.

Rappelons tout d'abord quelques définitions et notations : si L/K est une extension finie de corps, on note $\mathrm{Tr}_{L/K}$ l'application *trace* de L dans K, c'est-à-dire l'application qui à $x \in L$ associe la trace de l'endomorphisme $\mu_x\colon y \longmapsto xy$ du K-espace vectoriel L. Si K est un corps, un espace quadratique sur K (ou K-espace quadratique) est simplement la donnée d'un espace vectoriel V sur K et d'une forme quadratique $Q\colon V \longrightarrow K$ sur V. Une *base autoduale* (ou *base orthonormale*) de l'espace quadratique (V, Q) (aussi dite base autoduale de V relativement à la forme quadratique Q) est une base (ϵ_j) de V telle que $B(\epsilon_i, \epsilon_j) = \delta_{ij}$ où B désigne la forme bilinéaire symétrique associée à la forme quadratique Q et δ_{ij} est le symbole de Kronecker égal à 1 si $i = j$ et à 0 sinon. Voici maintenant la caractérisation annoncée.

THÉORÈME 1. *Pour un corps K de caractéristique différente de* 2*, les assertions suivantes sont équivalentes :*

(i) K satisfait le théorème de l'axe principal.

Reçu par les éditeurs le 15 mai 1995.
Classification (AMS) par sujet : Primary: 11E10; secondary: 12D15.

(ii) K n'est pas séparablement clos et pour toute extension non triviale finie L de K, et pour tout α dans L, la forme quadratique $Q_{L,\alpha}\colon x \longmapsto \mathrm{Tr}_{L/K}(\alpha x^2)$ n'admet pas de base autoduale.

La démonstration que nous proposons de ce théorème utilise des idées dont certaines sont proches de celles de Waterhouse [3].

En combinant cette caractérisation avec celle due à Waterhouse, nous retrouvons le fait qu'un pro-2-groupe qui se réalise comme groupe de Galois absolu d'un corps pythagoricien K est topologiquement engendré par des involutions (résultat du à Becker [1]). Rappelons qu'un corps K est dit *pythagoricien* lorsque toute somme de carrés de K est un carré dans K.

Remarquons qu'en fait tout corps de caractéristique différente de 2 qui satisfait à la condition (i) du théorème 1 est de caractéristique nulle. En effet, pour tout entier p, le polynôme caractéristique de la matrice carrée d'ordre p dont tous les coefficients sont égaux à 1, est $(-1)^p(X^p - pX^{p-1})$.

2**. Quelques lemmes.** Rappelons tout de suite qu'un corps formellement réel est de caractéristique nulle.

Le premier lemme est une caractérisation des corps formellement réels et pythagoriciens par la diagonalisabilité des matrices symétriques 2×2 à coefficients dans K.

LEMME 1. *Pour que toute matrice symétrique* 2×2 *à coefficients dans un corps K se diagonalise dans K, il est nécessaire et suffisant que K soit formellement réel et pythagoricien.*

DÉMONSTRATION. La condition est nécessaire : pour a et b dans K, considérons la matrice symétrique $\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$; puisqu'elle se diagonalise dans K, ses valeurs propres sont éléments de K et donc $a^2 + b^2$ est un carré dans K. Pour montrer que K est formellement réel, il suffit donc de voir que -1 n'est pas un carré dans K. Or, si $-1 = a^2$ pour un élément a de K, la matrice symétrique $\begin{pmatrix} 1 & a \\ a & -1 \end{pmatrix}$ serait nilpotente et non nulle contrairement à l'hypothèse.

La condition est suffisante : en effet le polynôme caractéristique d'une matrice symétrique 2×2 non diagonale à coefficients dans K a dans K deux racines distinctes dès que K est formellement réel (donc de caractéristique nulle) et pythagoricien. ∎

Une deuxième caractérisation des corps formellement réels et pythagoriciens peut s'énoncer en terme d'existence de bases autoduales pour tout sous-espace d'un espace quadratique admettant une base autoduale. Pour simplifier, nous conviendrons d'appeler *standard* tout espace quadratique (V, q) admettant une base autoduale.

LEMME 2. *Pour qu'un corps K soit formellement réel et pythagoricien, il est nécessaire et suffisant que tout sous-espace d'un K-espace quadratique standard soit aussi standard.*

https://doi.org/10.4153/CMB-1997-010-5 Published online by Cambridge University Press

DÉMONSTRATION. La nécessité de la condition résulte de l'existence d'une base orthogonale de tout sous-espace (le fait que le corps K est formellement réel prouvant que tout sous-espace est non dégénéré) et de ce que toute somme de carrés d'éléments non tous nuls du corps pythagoricien et formellement réel K est un carré non nul dans K.

Réciproquement, supposons que tout sous-espace d'un K-espace quadratique standard soit standard. Alors en considérant le K-espace K^2 muni du produit scalaire canonique, on voit que si a et b ne sont pas tous deux nuls, la somme $a^2 + b^2$ est en tant que carré scalaire du vecteur non nul (a, b) un carré non nul dans K, ce qui montre bien que K est pythagoricien et formellement réel. ∎

Le lemme suivant est un cas particulier de [3, Proposition 1]. Nous en proposons une démonstration *ad hoc*.

LEMME 3. *Pour qu'un corps K soit formellement réel, il est nécessaire et suffisant que le polynôme minimal de toute matrice symétrique à coefficients dans K soit sans facteurs carrés.*

DÉMONSTRATION. Montrons d'abord que la condition est nécessaire. Soit donc un corps K formellement réel et une matrice symétrique $n \times n$ M à coefficients dans K. On confère au K-espace vectoriel K^n une structure d'espace quadratique en le munissant du produit scalaire canonique. Interprétons alors M comme la matrice dans la base canonique d'un endomorphisme u autoadjoint de K^n. Soient ϕ le polynôme minimal de M et P un facteur irréductible de ϕ le divisant à la puissance exactement r. Le sous-espace $W := \operatorname{Ker} P(u)^r$ est stable par u et le polynôme minimal de $u|_W$ (la restriction de u à W) est précisément P^r. Si r était plus grand que 1, alors on aurait pour tout x dans W :

$$P(u)^{r-1}(x) \cdot P(u)^{r-1}(x) = P(u)^{r-2}(x) \cdot P(u)^r(x) = 0.$$

Ainsi puisque le corps K est formellement réel on aurait $P(u|_W)^{r-1} = 0$, ce qui contredit le fait que le polynôme minimal de $u|_W$ est P^r. Donc $r = 1$ et la condition est nécessaire.

Pour établir qu'elle est aussi suffisante, donnons-nous un corps K non formellement réel et exhibons une matrice symétrique non nulle de carré nul. Puisque K est supposé non formellement réel, il existe un nombre fini $x_1, x_2, \ldots, x_n$ d'éléments de K tels que $-1 = x_1^2 + x_2^2 + \cdots + x_n^2$. Considérons alors la matrice ligne $X = (x_1, x_2, \ldots, x_n)$. On vérifie facilement que la matrice

$$M = \begin{pmatrix} 1 & X \\ {}^tX & {}^tXX \end{pmatrix}$$

convient, ce qui montre que la condition est suffisante. ∎

Nous terminons ces lemmes par une caractérisation des corps pythagoriciens à l'aide des formes traces de certaines de leurs extensions finies.

https://doi.org/10.4153/CMB-1997-010-5 Published online by Cambridge University Press

LEMME 4. *Pour un corps K de caractéristique différente de* 2, *les assertions suivantes sont équivalentes :*

(1) K est pythagoricien.

(2) Pour toute extension finie L de K contenant une sous-extension quadratique F, la forme quadratique $Q_{L,\alpha}\colon x \longmapsto \mathrm{Tr}_{L/K}(\alpha x^2)$ *n'est standard pour aucun* α *de L.*

DÉMONSTRATION. Montrons d'abord l'implication (1) $\Rightarrow$ (2). Sans restreindre la généralité, on peut supposer K formellement réel car un corps pythagoricien non formellement réel ne possède aucune extension quadratique s'il est de caractéristique différente de 2. En effet, tout élément d'un corps quelconque K de caractéristique différente de 2 est différence de deux carrés de K, donc aussi un carré si K est pythagoricien non formellement réel; or, en caractéristique différente de 2, toute extension quadratique est obtenue par l'adjonction des racines carrées d'un élément de K. Ceci étant, supposons qu'il existe $\alpha \in L$ et une base B du K-espace vectoriel L tels que B soit autoduale pour $Q_{L,\alpha}$. Soit x un élément de F qui n'est pas dans K. La multiplication $\mu_x\colon y \longmapsto xy$ est un K-automorphisme de L autoadjoint par rapport à la forme quadratique $Q_{L,\alpha}$, donc sa restriction à F est autoadjointe par rapport à $Q_{L,\alpha}|_F$. Par le Lemme 2, $Q_{L,\alpha}|_F$ admet une base autoduale dans laquelle $\mu_x|_F$ est représenté par une matrice symétrique 2×2. Donc par le Lemme 1, les valeurs propres de $\mu_x|_F$ sont éléments de K, ce qui est manifestement impossible.

Montrons maintenant l'implication (2) $\Rightarrow$ (1). Supposons K non pythagoricien. Alors il existe $a \in K$ tel que $b := 1 + a^2$ n'est pas carré dans K. Considérons le corps $F := K(\sqrt{b})$ et $\alpha := 2b + 2a\sqrt{b} \in F$. Pour ces choix de F et de α, la forme $Q_{F,\alpha}$ a dans la base $(1, \sqrt{b})$ la matrice

$$\begin{pmatrix} 4b & 4ab \\ 4ab & 4b^2 \end{pmatrix}$$

qui est de déterminant $(4b)^2$. Comme de plus $Q_{F,\alpha}$ représente le carré $4b^2$, on voit que $Q_{F,\alpha}$ est standard [2, Chapitre I, Proposition 5.1]. Le fait que $Q_{F,\alpha}$ est standard aurait aussi pu être obtenu en observant que $(\frac{1}{2\sqrt{b}}, \frac{1}{2} - \frac{a}{2\sqrt{b}})$ est une base de F autoduale relativement à $Q_{F,\alpha}$. ∎

3. **Démonstration du Théorème 1.** Montrons d'abord l'implication (i) $\Rightarrow$ (ii). On observe qu'en vertu du Lemme 1, le corps K est formellement réel donc ne peut être algébriquement clos, ni séparablement clos puisque sa caractéristique est nulle. Soit par ailleurs L une extension de K et supposons qu'il existe $\alpha \in L$ tel que la forme quadratique $Q_{L,\alpha}$ admette une base autoduale. Pour tout x dans L, la multiplication $\mu_x\colon y \longmapsto xy$ est un K-endomorphisme de L autoadjoint par rapport à la forme $Q_{L,\alpha}$ donc représenté par une matrice symétrique dans une base $Q_{L,\alpha}$-autoduale. Par ailleurs les valeurs propres de μ_x sont exactement les conjugués de x, donc $x \in K$ en vertu de (i) et l'extension L/K est triviale.

Montrons maintenant l'implication (ii) $\Rightarrow$ (i). Par le Lemme 4, on sait que le corps K est pythagoricien. Si K n'était pas formellement réel, tout élément de K serait donc un carré dans K et par conséquent tout K-espace quadratique non dégénéré admettrait une base autoduale, ce qui est incompatible avec l'hypothèse (ii). Donc, le corps K est formellement réel et pythagoricien.

Introduisons maintenant pour une extension L de K et pour $x \in L$ le K-espace vectoriel $E_{L,x}$ des formes quadratiques $L \longrightarrow K$ par rapport auxquelles la multiplication $\mu_x\colon y \longmapsto xy$ est un endomorphisme autoadjoint de L. Montrons d'abord que
$E_{L,x} = \{Q_{L,\alpha} : \alpha \in L\}$ si x est primitif dans l'extension L/K. Puisque K est de caractéristique nulle, l'extension L/K est séparable et donc les formes $Q_{L,\alpha}$ sont non dégénérées pour $\alpha \neq 0$. On voit ainsi que l'application K-linéaire $\alpha \longmapsto Q_{L,\alpha}$ de L dans $E_{L,x}$ est injective. Il nous suffit donc d'établir que la dimension du K-espace vectoriel $E_{L,x}$ est au plus égale au degré n de l'extension L/K :

$$\dim_K E_{L,x} \leq n.$$

Notons B la forme bilinéaire symétrique associée à une forme quadratique $Q \in E_{L,x}$. Puisque x est supposé primitif dans L/K, on peut exprimer $B(x^i, x^j)$ comme combinaison K-linéaire des $B(1, x^k)$ où k varie de 0 à $n-1$. D'où l'inégalité désirée.

Ceci étant, soit M une matrice symétrique à coefficients dans K et montrons qu'elle est diagonalisable sur K. Pour cela, il suffit de montrer que son polynôme minimal ϕ est produit de facteurs linéaires deux à deux premiers entre eux. Nous savons déjà par le Lemme 3 que ϕ est produit de facteurs irréductibles deux à deux premiers entre eux. Il ne nous reste plus qu'à montrer que tout facteur irréductible de ϕ est linéaire. Soit donc P un facteur irréductible de ϕ. Interprétons M comme matrice dans la base canonique d'un endomorphisme u autoadjoint de K^n muni du produit scalaire canonique. Fixons un vecteur non nul y dans le noyau de $P(u)$. Regardons K^n comme un $K[X]$-module pour l'action définie par $X \cdot z = u(z)$ pour tout élement z de K^n. Alors l'application

$$\begin{aligned} K[X] &\longrightarrow K^n \\ Q &\longmapsto Q(u)(y) \end{aligned}$$

est un homomorphisme non nul de $K[X]$-modules. Comme P est irréductible dans $K[X]$ cet homomorphisme a exactement pour noyau l'idéal engendré par P, d'où un isomorphisme de $K[X]$-modules entre $L := K[X]/(P)$ et un sous-espace W de K^n stable par u. Par transport de structure cet isomorphisme permet de définir sur L une forme quadratique qui en vertu du Lemme 2 admet une base autoduale, et par rapport à laquelle la multiplication par la classe de X est autoadjointe. Cette forme quadratique est, d'après l'étude de $E_{L,x}$ ci-dessus, nécessairement une des formes quadratiques $Q_{L,\alpha}$. Ainsi l'hypothèse (ii) entraîne que l'extension L/K est triviale et P est linéaire, ce qui achève la démonstration. ∎

REMARQUE. On peut rapprocher la construction de l'isomorphisme de $K[X]$-modules entre une extension de K et un sous-espace de K^n utilisée dans la démonstration précédente de la description des "paires indécomposables" figurant dans [3, paragraphe

https://doi.org/10.4153/CMB-1997-010-5 Published online by Cambridge University Press

précédant le Théorème 2, p. 238]. Plus précisément dans notre construction W est le plus petit sous-espace de K^n contenant y et stable par u. Donc, en notant B_W la restriction du produit scalaire canonique de K^n à W, la paire $(u|_W, B_W)$ est une paire indécomposable au sens de [3]. Par conséquent, W s'identifie à une extension finie L de K et dans cette identification u correspond à la multiplication par un élément primitif de l'extension L/K; de plus B_W s'identifie à la forme bilinéaire associée à une forme quadratique $Q_{L,\alpha}$.

EXEMPLE. Soit K la clôture pythagoricienne d'un sous-corps M de $\mathbb{R}$ maximal pour l'exclusion de $\sqrt{2}$. Alors on voit facilement que toute extension finie de K contient une sous-extension quadratique; le Lemme 4 et le Théorème 1 impliquent donc que le corps K satisfait le théorème de l'axe principal. Cet exemple illustre un fait général que nous étudions dans la section suivante.

4. **Une application.** Comme application, nous allons retrouver le résultat suivant du à Becker [1].

THÉORÈME 2. *Soit K un corps de caractéristique différente de* 2 *dont le groupe de Galois absolu G_K est un pro-*2*-groupe. Alors K est pythagoricien si et seulement si G_K est topologiquement engendré par des involutions.*

DÉMONSTRATION. Sans restreindre la généralité, on peut supposer que K n'est pas séparablement clos. Puisque G_K est un pro-2-groupe, toute extension finie non triviale de K contient une sous-extension quadratique.

Supposons K pythagoricien. En vertu du Lemme 4, on constate que pour toute extension finie non triviale L de K, la forme quadratique $Q_{L,\alpha}\colon x \longmapsto \mathrm{Tr}_{L/K}(\alpha x^2)$ n'est standard pour aucun α de L, ce qui, d'après le Théorème 1, signifie que K satisfait le théorème de l'axe principal. Par la caractérisation de ces corps due à Waterhouse [3], on en déduit que K est une intersection de corps ordonnés maximaux, autrement dit G_K est topologiquement engendré par des involutions, puisqu'on sait qu'un corps ordonné maximal est d'indice 2 dans sa clôture algébrique.

Réciproquement, si G_K est topologiquement engendré par des involutions, alors K est intersection de corps laissés fixes par des involutions de G_K. Comme on sait par la théorie d'Artin-Schreier qu'un corps d'indice fini dans sa clôture algébrique est un corps ordonné maximal, on voit que le corps K est, en tant qu'intersection de corps ordonnés maximaux, un corps pythagoricien. ∎

REMERCIEMENTS. Nous remercions le professeur William C. Waterhouse dont les remarques nous ont permis d'améliorer une version préliminaire de ce travail et qui nous a en particulier signalé le résultat de Becker.

REFERENCES

1. Eberhard Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II., J. Reine Angew. Math. **268/269**(1974), 41–52.

2. Tsit Yuen Lam, *The Algebraic Theory of Quadratic Forms*, Math. Lecture Note Ser., W. A. Benjamin, Inc., Reading, Massachusetts, 1973.

3. William C. Waterhouse, *Self-adjoint operators and formally real fields*, Duke Math. J. (2) **43**(1976), 237–243.

LACO (URA 1586 CNRS)
Département de Mathématiques
Faculté des Sciences
123, avenue Albert Thomas
87060 Limoges Cedex
France

https://doi.org/10.4153/CMB-1997-010-5 Published online by Cambridge University Press