MÉMOIRES DE LA S. M. F.

JEAN-RENÉ JOLY

Théorème des deux carrés dans un anneau de polynômes

Mémoires de la S. M. F., tome 25 (1971), p. 113-117

<http://www.numdam.org/item?id=MSMF_1971__25__113_0>

Colloque Th. Nombres [1969, Bordeaux]
Bull. Soc. math. France,
Mémoire 25, 1971, p. 113 à 117

THEOREME DES DEUX CARRES DANS UN ANNEAU DE POLYNOMES

par

Jean-René JOLY

-:-:-:-

1. - Introduction. Enoncé de deux théorèmes.

Etant donné un corps commutatif k, on se propose de caractériser les éléments de l'anneau de polynômes $k[T]$ qui sont sommes de deux carrés. On obtient les deux résultats suivants (on suppose naturellement k de caractéristique $\neq 2$) :

THEOREME 1. - *Soit $f \in k[T]$ un polynôme irréductible et unitaire. Les deux propriétés suivantes sont équivalentes :*

(a) *f est somme de deux carrés dans $k[T]$;*

(b) *-1 est un carré dans le corps résiduel $k[T] / (f)$.*

THEOREME 2. - *Soit $g \in k[T]$ un polynôme non nul, de décomposition*

$$g = a\, f_1^{e_1} f_2^{e_2} \dots f_m^{e_m}$$

($a \in k^*$, les f_n irréductibles, unitaires et deux à deux distincts, les $e_j \geq 1$). Les deux propriétés suivantes sont équivalentes :

(a) *g est somme de deux carrés dans $k[T]$;*

(b) *a est somme de deux carrés dans k, et de plus, pour tout indice j tel que f_j ne soit pas somme de deux carrés, l'exposant e_j est pair.*

La situation est donc la même que dans l'anneau $\mathbb{Z}$ des entiers relatifs, les polynômes irréductibles et unitaires f tels que -1 ne soit pas un carré dans $k[T]/(f)$ jouant le même rôle que les nombres premiers $p \equiv 3 \pmod 4$.

Le théorème 1 est démontré au paragraphe 2 : on en propose deux démonstrations, calquées sur deux démonstrations classiques du théorème des deux carrés dans $\mathbb{Z}$. Le théorème 2 est démontré au paragraphe 3. Le paragraphe 4 donne quelques exemples et remarques.

2. - Démonstration du théorème 1.

Si -1 est un carré dans k, le théorème est évident : car (a) est vraie quel que soit f (en vertu de l'identité

$$f = \left(\frac{1+f}{2}\right)^2 - \left(\frac{1-f}{2}\right)^2),$$

et aussi (b) : on supposera donc désormais que -1 n'est pas un carré dans le corps k.

Le fait que (a) implique (b) est également évident : si $f = v^2 + w^2$, la comparaison des termes de plus haut degré dans les deux membres, et le fait que -1 ne soit pas un carré dans k, montrent que $\deg(f) = 2 \sup(\deg(v),\deg(w))$; en particulier, f ne peut diviser ni v, ni w ; si alors $\bar{v}$ et $\bar{w}$ sont les images de v et w dans le corps $k[T]/(f)$, on a $\bar{v} \neq 0$, $\bar{w} \neq 0$ et $\bar{v}^2 + \bar{w}^2 = 0$, donc $-1 = (\bar{v}\bar{w}^{-1})^2 =$ un carré dans $k[T]/(f)$.

Reste à prouver que (b) implique (a). Voici deux méthodes :

Première méthode :

Une démonstration classique du théorème des deux carrés dans $\mathbb{Z}$ s'appuie sur la décomposition des nombres premiers $p \equiv 1 \pmod 4$ dans l'anneau des entiers de Gauss (voir par exemple [3], p. 96). On peut procéder ici de la même manière : adjoignons à k un élément $i = \sqrt{-1}$, et posons

$$A = k[T] , \quad K = k(T) ,$$

$$B = k(i)[T] = k[i,T] = A[i] ,$$

$$L = K(i) = k(i,T) .$$

A et B sont des anneaux principaux, L/K est une extension quadratique, et B est la fermeture intégrale de A dans L.

Prouvons alors que (b) implique (a) ; on a les isomorphismes

$$B/Bf = k[i,T]/fk[i,T] \simeq k[X,T]/(f,X^2+1)$$

$$k_1[X]/(X^2+1) \simeq k_1 \times k_1 ,$$

k_1 désignant le corps $k[T]/(f)$, et le dernier isomorphisme ayant lieu parce que (par hypothèse) -1 est un carré dans k_1. L'idéal premier Af de A est donc décomposé dans B, d'où $Bf = P_1P_2$, P_1 et P_2 étant deux idéaux premiers de B, distincts, permutés par l'unique K-automorphisme non trivial de L, et d'autre part principaux, ce qui permet d'écrire

$$P_1 = B(v+iw) , \quad P_2 = B(v-iw) ,$$

avec $v,w \in A$. De là $Bf = B(v^2+w^2)$, et donc $f = b(v^2+w^2)$, avec $b \in k(i) \cap K = k$; b est d'ailleurs somme de deux carrés dans k, comme on le

voit en comparant les termes de plus haut degré des deux membres : l'identité de Lagrange permet alors de conclure que f est somme de deux carrés dans $A = k[T]$, C.Q.F.D.

Deuxième méthode :

On peut également démontrer le théorème des deux carrés dans $\mathbb{Z}$ en utilisant un théorème d'approximation des nombres réels par des nombres rationnels (voir par exemple [1], p.III.4). Cette méthode se laisse de même adapter à $A = k[T]$. D'abord, un lemme élémentaire :

LEMME 1. - *Si E est un sous-espace vectoriel de dimension finie de l'anneau de polynômes $k[T]$, E admet une base formée de polynômes de degrés tous différents.*

Ce lemme se démontre par récurrence sur $\dim(E)$. Prouvons alors que, dans le théorème 1, (b) implique (a). Comme $k[T]/(f)$ contient par hypothèse $k(i)$, quadratique sur k, le degré de f est pair, soit $\deg(f) = 2r$. D'autre part, comme -1 est un carré modulo f, il existe $g \in k[T]$ tel que f divise $1+g^2$. Enfin :

LEMME 2. - *Il existe u et $v \in k[T]$ tels que $v \neq 0$ et*

$$\deg(vg-uf) \leq r \quad \text{et} \quad \deg(v) \leq r \ .$$

Prouvons ce lemme : soit E_r le sous-espace vectoriel de $k[T]$ formé des polynômes de degré $\leq r$, et pour tout $v \in E_r$, soit $\rho(v)$ le reste de division de vg par f ; ρ est une application linéaire injective de E_r dans $k[T]$, d'où $\dim(\rho(E_r)) = r+1$; de plus, tout élément de $\rho(E_r)$ est de degré $\leq 2r-1$. Le lemme 1 montre alors que $\rho(E_r)$ contient un polynôme non nul de degré au plus égal à

$$(2r-1) - (r+1) + 1 = r-1 \leq r \ ,$$

assertion qui équivaut au lemme 2.

Posons alors $w = vg - uf$, u et v satisfaisant aux conditions du lemme 2. On a

$$v^2 + w^2 = v^2(1+g^2) - 2uvfg + u^2f^2 \ ,$$

ce qui, compte tenu du choix de g, montre que f divise $v^2 + w^2$; d'autre part,

$$\deg(v^2+w^2) \leq 2r = \deg(f) \ ;$$

enfin, -1 n'étant pas un carré dans k, v^2+w^2 n'est pas nul. Ainsi, f et v^2+w^2 sont associés dans $k[T]$, il existe $a \in k^*$ tel que

$$f = a(v^2+w^2) \ ;$$

on vérifie que a est somme de deux carrés dans k, et on conclut par l'identité de Lagrange, comme dans la première méthode.

3. - Démonstration du théorème 2.

Le fait que (b) implique (a) est encore une conséquence immédiate de l'identité de Lagrange. Prouvonx la réciproque, et écrivons donc

$$g = v^2 + w^2 = a\, f_1^{e_1} f_2^{e_2} \dots f_m^{e_m} .$$

La comparaison des termes de plus haut degré prouve d'abord que a est somme de deux carrés dans k. Reste à prouver que si, pour j donné, f_j n'est pas somme de deux carrés, alors e_j est pair ; ce qui, compte tenu du théorème 1, équivaut à prouver ceci (qui est vrai d'ailleurs dans n'importe quel anneau principal) :

LEMME 3. - Soit $f \in k[T]$ un polynôme irréductible et unitaire. Si -1 n'est pas un carré dans g, et si f divise g, alors la plus haute puissance de f qui divise g est paire.

Soit en effet u un plus grand commun diviseur de v et w, et écrivons

$$v = uv_1 \quad , \quad w = uw_1 \quad ,$$
$$g = u^2(v_1^2 + w_1^2) \quad ;$$

f ne peut diviser $v_1^2 + w_1^2$: cela impliquerait $\bar{v}_1^2 + \bar{w}_1^2 = 0$ dans $k[T]/(f)$, où -1 n'est pas un carré ; on aurait donc $\bar{v}_1 = \bar{w}_1 = 0$, f diviserait v_1 et w_1, et u ne serait par p.g.c.d. de v et w. Ainsi, f divise g par l'intermédiaire du facteur u^2, ce qui prouve le lemme.

Le théorème 2 est ainsi démontré.

4. - Exemples et remarques.

(1) Si $k = \mathbb{R}$, le théorème 2 redonne ce résultat bien connu : $g \in \mathbb{R}[T]$ est somme de deux carrés si (et seulement si) il est défini positif.

(2) Si $k = \mathbb{F}_q$, corps fini à q éléments ($q = p^n$, $p \neq 2$), et si $q \equiv 1 \pmod 4$, alors -1 est un carré dans k, et tout élément de $k[T]$ est somme de deux carrés. Si au contraire $q \equiv 3 \pmod 4$ (c'est-à-dire si $p \equiv 3 \pmod 4$ et si n est impair), on voit sans peine que le théorème 2 donne ceci :
$g = a\, f_1^{e_1} f_2^{e_2} \dots f_m^{e_m} \in \mathbb{F}_q[T]$ est somme de deux carrés si (et seulement si) pour tout j tel que f_j soit de degré impair, l'exposant e_j est pair.

Ce résultat est dû à W. Leahey (voir [2]).

(3) La caractérisation (b) des sommes de deux carrés donnée dans le théorème 2 n'est pas valable dans un anneau principal quelconque, même euclidien : ainsi, dans l'anneau des entiers de Gauss, l'élément $g = -4 - 4i = i^2 + (2-i)^2$ est somme de deux carrés, mais sa décomposition en facteurs irréductibles $g = (1+i)^5$ fait apparaître $1+i$ (qui n'est pas somme de deux carrés) avec l'exposant impair 5 .

-:-:-:-

BIBLIOGRAPHIE

[1] K. CHANDRASEKHARAN. - Einführung in die analytische Zahlentheorie. Springer.

[2] W. LEAHEY. - Sums of squares of polynomials with coefficients in a finite field. Amer. Math. Monthly. 74 (1967).

[3] P. SAMUEL. - Théorie algébrique des nombres. Hermann.

-:-:-:-

Faculté des Sciences de Grenoble
Département de Mathématiques
Boîte Postale n° 116
38 - Saint-Martin-d'Hères (France)