ACTA ARITHMETICA
XIX (1971)

# Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques

par

Y. POURCHET (Paris)

Dans [7] Landau démontre que tout polynôme défini positif à une indéterminée sur le corps des nombres rationnels est somme des carrés de huit polynômes sur ce corps. Je montre dans ce travail que ce nombre peut être ramené à cinq (corollaire 4 du théorème 2), sans d'ailleurs pouvoir être abaissé davantage (proposition 10).

Ce résultat n'était connu jusqu'à présent que pour un polynôme de degré deux [8] ou quatre [5], [17]. On verra qu'il apparaît comme cas particulier d'un théorème valable pour un corps de nombres algébriques non nécessairement ordonnable (théorème 2 et remarque 1). Dans une publication ultérieure je montrerai, en précisant le théorème 1, que le théorème 2 vaut en fait pour un corps arithmétique global de caractéristique $\neq 2$, moyennant une hypothèse supplémentaire toujours vérifiée en caractéristique zéro.

Une caractérisation des sommes de quatre carrés dans $\boldsymbol{Q}[X]$ est ensuite donnée (proposition 10) et appliquée aux polynômes cyclotomiques (théorème 3): pour chacun d'eux, le nombre minimum des termes d'une représentation en somme de carrés dans $\boldsymbol{Q}[X]$ est déterminé.

Je remercie vivement M. J.-P. Serre qui m'a signalé la proposition 5 et suggéré de nombreuses améliorations dans la rédaction de ce mémoire.

Je remercie également A. Pfister qui, lors du récent congrès de Nice, m'a fait observer que la portée du théorème 2 et de ses corollaires 2 et 3 pouvait être accrue grâce à la proposition 8.

**Notations et définitions.** Dans toute la suite, $K$ désignera, en l'absence de précisions supplémentaires, un corps de caractéristique $\neq 2$. Soient $a, b, c \in K^*$, nous noterons $[a, b]$, et $[a, b, c^*]$ respectivement les formes quadratiques

$$U_1^2 + aU_2^2 + bU_3^2 + abU_4^2 \quad \text{et} \quad U_1^2 + aU_2^2 + bU_3^2 + abU_4^2 + cU_5^2.$$

Pour tout polynôme $f \in K[X_1, \ldots, X_n]$, $\deg(f)$ désignera son degré total, avec la convention $\deg(0) = -\infty$ ([9], p. 118) et, lorsque $n = 1$

et $f \neq 0$, $\operatorname{sgn}(f)$ sera son coefficient directeur. En outre, si $|\ |$ est une valeur absolue sur $K$ et si $f = \sum_i c_i X^i$ est un polynôme $\in K[X]$, nous poserons $|f| = \max_i |c_i|$.

Nous dirons qu'un polynôme $f \in K[X]-\{0\}$ est séparable s'il est premier avec sa dérivée ou, ce qui est équivalent, si pour toute extension $L$ de $K$, les facteurs premiers de $f$ dans $L[X]$ ont pour multiplicité un. Si $K$ est de caractéristique zéro, pour que $f \in K[X]-\{0\}$ soit séparable il faut et il suffit que ses facteurs premiers dans $K[X]$ aient pour multiplicité un.

Lorsque $K$ est un corps ordonné, nous dirons que $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ est défini positif (resp. défini négatif) si, quel que soit $(x_1, \ldots, x_n) \in K^n$, on a $f(x_1, \ldots, x_n) \geqslant 0$ (resp. $\leqslant 0$). De façon analogue, on a la notion de forme algébrique définie positive (ou définie négative) sur un $K$-espace vectoriel.

Enfin par corps de nombres nous entendrons une extension finie du corps $\boldsymbol{Q}$ des rationnels, et nous appellerons corps local un complété d'un corps de nombres pour l'une de ses places ([12], § 11 D). Un corps local archimédien est donc identique à $\boldsymbol{R}$ ou $\boldsymbol{C}$; un corps local ultramétrique est une extension finie d'un corps $p$-adique.

**Préliminaires.**

PROPOSITION 1. *Une forme quadratique régulière sur $K$, qui représente zéro dans ce corps, représente, dans toute $K$-algèbre, tout élément de celle-ci.*

C'est une extension immédiate d'un lemme classique ([12], 42:10).

PROPOSITION 2. *Soit $F(U_1, \ldots, U_n) \in K[U_1, \ldots, U_n]$ un polynôme homogène de degré $>0$ qui ne représente pas zéro dans $K$; alors $F$ ne représente pas non plus zéro dans $K(X)$, et, pour $f_i(X) \in K[X]$ $(1 \leqslant i \leqslant n)$ et $f(X) = F(f_1(X), \ldots, f_n(X))$, on a:*

$$\deg(f(X)) = \deg(F) \cdot \max_{1 \leqslant i \leqslant n} \deg(f_i(X));$$

*en outre, si $f(X) \neq 0$, $F$ représente $\operatorname{sgn}(f(X))$ dans $K$.*

Il suffit évidemment de prouver les deux dernières assertions. Si $f_i(X) = 0$ pour $1 \leqslant i \leqslant n$, les deux membres sont égaux à $-\infty$ puisque $\deg(F) > 0$. Dans le cas contraire, posons $\deg(F) = d$ et $\max_{1 \leqslant i \leqslant n} \deg(f_i) = \delta$; $\delta$ est un entier $\geqslant 0$; soient $f^*(X) = X^{d\delta} f(1/X)$ et $f_i^*(X) = X^{\delta} f_i(1/X)$. On a $f^*(X) = F(f_1^*(X), \ldots, f_n^*(X))$; les $f_i^*(X)$ sont des polynômes et les $f_i^*(0)$ ne sont pas tous nuls, donc $f^*(X)$ est un polynôme et $f^*(0)$ n'est pas nul, par suite $\deg(f(X)) = d\delta$ et $F$ représente $\operatorname{sgn}(f(X)) = f^*(0)$ dans $K$, q.e.d.

PROPOSITION 3. *Soient $a, b \in K^*$ et $f \in K[X]-\{0\}$. Pour que $[a, b]$ représente $f$ dans l'anneau $K[X]$, il faut et il suffit que $[a, b]$ représente $\operatorname{sgn}(f)$ dans $K$, et que pour tout $p$ premier $\in K[X]$, facteur de $F$ avec une multiplicité impaire, $[a, b]$ représente zéro dans l'extension $K[X]/(p)$ de $K$.*



La condition est nécessaire: Par hypothèse il existe des $f_i \in K[X]$ $(1 \leqslant i \leqslant 4)$ tels que $f = f_1^2 + af_2^2 + bf_3^2 + abf_4^2$; d'après les propositions 1 et 2, $[a, b]$ représente $\operatorname{sgn}(f)$ dans $K$. Soit $\Delta$ un p.g.c.d. des $f_i$ et posons $f = \Delta^2 g$, $f_i = \Delta g_i$ $(1 \leqslant i \leqslant 4)$; on a

$$g = g_1^2 + ag_2^2 + bg_3^2 + abg_4^2.$$

Un facteur premier $p$ de $f$, de multiplicité impaire, divise $g$ sans diviser tous les $g_i$, d'où la conclusion en passant au quotient $K[X]/(p)$.

La condition est suffisante: Si $[a, b]$ représente zéro dans $K$, cela résulte de la proposition 1; dans le cas contraire, considérons l'algèbre de quaternions $\left(\frac{-a, -b}{K}\right) = K1 \oplus Ki \oplus Kj \oplus Kij$ où $i^2 = -a$, $j^2 = -b$, $ji = -ij$ ([12], § 57 A); la norme réduite d'un élément $u = u_1 1 + u_2 i + u_3 j + u_4 ij$ est $N(u) = u_1^2 + au_2^2 + bu_3^2 + abu_4^2$, et si $u$ et $v$ sont deux éléments de l'algèbre, on a $N(u\bar{v}) = N(u)N(\bar{v}) = N(u)N(v)$. Il existe donc dans $K[U_1, \ldots, U_4; V_1, \ldots, V_4]$ quatre formes bilinéaires $B_i(U, V)$ $(1 \leqslant i \leqslant 4)$, $B_1$ étant la forme polaire de $[a, b]$ et $B_2, B_3, B_4$ des formes alternées, vérifiant:

$$(1) \qquad (U_1^2 + aU_2^2 + bU_3^2 + abU_4^2)(V_1^2 + aV_2^2 + bV_3^2 + abV_4^2) \\ = B_1^2(U, V) + aB_2^2(U, V) + bB_3^2(U, V) + abB_4^2(U, V).$$

Compte tenu de cette identité on peut se borner au cas où $f$ est premier et $\operatorname{sgn}(f) = 1$. Par hypothèse il existe dans $K[X]$ des $r_i$ $(1 \leqslant i \leqslant 4)$ non tous nuls, de degré strictement inférieur à $\deg(f)$, et un polynôme $g$ tels que:

$$fg = r_1^2 + ar_2^2 + br_3^2 + abr_4^2.$$

Parmi les systèmes $(g, r_1, \ldots, r_4)$ possédant ces propriétés, nous en considérons un tel que $\max_{1 \leqslant i \leqslant 4} \deg(r_i)$ soit minimum et nous allons montrer que $\deg(g)$ est alors nul. D'après la proposition 2 on a $\deg(f) + \deg(g) = 2 \max_{1 \leqslant i \leqslant 4} \deg(r_i)$, donc $g \neq 0$ et $\deg(g) < \deg(f)$. Soit $s_i$ le reste de la division euclidienne de $r_i$ par $g$; il existe $h \in K[X]$ vérifiant

$$gh = s_1^2 + as_2^2 + bs_3^2 + abs_4^2.$$

On a (proposition 2) $\deg(g) + \deg(h) = 2 \max_{1 \leqslant i \leqslant 4} \deg(s_i) < 2\deg(g)$, donc $\deg(h) < \deg(g)$, et:

$$fg^2 h = B_1^2(r, s) + aB_2^2(r, s) + bB_3^2(r, s) + abB_4^2(r, s),$$

où l'on a posé: $r = (r_1, \ldots, r_4)$ et $s = (s_1, \ldots, s_4)$. Les congruences $r_j \equiv s_j \pmod{g}$ $(1 \leqslant j \leqslant 4)$ entraînent $B_i(r, s) \equiv B_i(r, r) \pmod{g}$ pour $1 \leqslant i \leqslant 4$;

on a donc $B_i(r, s) \equiv 0 \pmod{g}$ $(1 \leqslant i \leqslant 4)$ car $B_1(r, r) = r_1^2 + ar_2^2 + br_3^2 + abr_4^2$ et $B_i(r, r) = 0$ pour $2 \leqslant i \leqslant 4$. Posons $B_i(r, s) = gt_i$, $t_i \in K[X]$ $(1 \leqslant i \leqslant 4)$; comme $g \neq 0$ on a

$$fh = t_1^2 + at_2^2 + bt_3^2 + abt_4^2,$$

donc $t_1 = \ldots = t_4 = 0$, puisque

$$2\max_{1\leqslant i\leqslant 4}\deg(t_i) = \deg(f) + \deg(h) < 2\max_{1\leqslant i\leqslant 4}\deg(r_i) = \deg(f) + \deg(g);$$

d'où $h = 0$ et par suite (proposition 2) $s_i = 0$ et $g|r_i$ pour $1 \leqslant i \leqslant 4$, donc $g^2|fg$, $g|f$ ce qui, $f$ étant premier et $\deg(g)$ strictement inférieur à $\deg(f)$, implique $\deg(g) = 0$. Cela étant, d'après la proposition 2, la forme $[a, b]$ représente $\operatorname{sgn}(fg) = \operatorname{sgn}(f)\operatorname{sgn}(g) = \operatorname{sgn}(g) = g$ dans $K$, donc représente aussi $g^{-1} = g/g^2$ et par suite $f = g^{-1} \cdot fg$ d'après l'identité (1), q.e.d.

Remarque. Cette démonstration, analogue à celle de Landau dans [7], est la transposition à l'anneau $K[X]$ de la démonstration donnée par Euler du théorème de Fermat–Lagrange établissant qu'un entier rationnel positif est somme des carrés de quatre entiers (cf. e.g. [10], tome 1, art. 153).

La proposition 3 vaut en fait si on remplace $[a, b]$ par une forme de Pfister $(1, a_1) \otimes \ldots \otimes (1, a_k)$ de rang $2^k$. On la démontre alors comme dans [13], Satz 2, lemma en utilisant la propriété multiplicative de cette forme et un théorème récent de J. W. S. Cassels ([2] et [14], Satz 1).

Proposition 4. *Soient $K$ un corps de nombres, $\Omega$ l'ensemble de ses places, et $(K_\mathfrak{p})_{\mathfrak{p}\in\Omega}$ la famille de ses complétés; soient $a, b \in K^*$ et $f \in K[X] - \{0\}$. Les propriétés suivantes sont équivalentes:*

(1) *$[a, b]$ représente $f$ dans $K[X]$,*

(2) *$[a, b]$ représente $f$ dans $K_\mathfrak{p}[X]$ pour toute $\mathfrak{p} \in \Omega$.*

(1) $\Rightarrow$ (2): c'est clair. (2) $\Rightarrow$ (1): soient $p$ premier $\in K[X]$, facteur de $f$ avec une multiplicité impaire et $\prod_{1\leqslant i\leqslant s_\mathfrak{p}} p_{i,\mathfrak{p}}$ une décomposition de $p$ en facteurs premiers dans $K_\mathfrak{p}[X]$. La caractéristique de $K$ étant nulle, le polynôme $p$ est séparable; par suite le facteur premier $p_{i,\mathfrak{p}}$ de $f$ dans $K_\mathfrak{p}[X]$ a même multiplicité que le facteur premier $p$ de $f$ dans $K[X]$, donc (proposition 3) la forme $[a, b]$ représente zéro dans $K_\mathfrak{p}[X]/(p_{i,\mathfrak{p}})$ pour $\mathfrak{p} \in \Omega$ et $1 \leqslant i \leqslant s_\mathfrak{p}$. Ces corps constituent la famille des complétés du corps $K[X]/(p)$ pour l'ensemble de ses places. La forme $[a, b]$ représente donc zéro dans $K[X]/(p)$ d'après le théorème de Minkowski–Hasse ([12], 66: 1). D'autre part $[a, b]$ représente $\operatorname{sgn}(f)$ dans $K_\mathfrak{p}$ pour toute $\mathfrak{p} \in \Omega$; cela résulte de la proposition 1 si $[a, b]$ représente zéro dans $K_\mathfrak{p}$ et de la proposition 2 dans le cas contraire. D'après un corollaire du même théorème ([12], 66: 3), $[a, b]$ représente $\operatorname{sgn}(f)$ dans $K$, d'où la conclusion d'après la proposition 3.



Proposition 5. *Soient $K$ un corps local et $a, b \in K^*$. La forme $[a, b]$ représente zéro dans toute extension de degré pair de $K$, et, si elle ne représente pas zéro dans $K$, seulement dans ces extensions.*

Si $K = \boldsymbol{R}$ ou $\boldsymbol{C}$, c'est clair. Supposons donc que $K$ est ultramétrique. L'algèbre $\left(\frac{-a, -b}{K}\right)$, considérée dans la démonstration de la proposition 3, est centrale simple ([12], 57: 2); son invariant de Hasse est 1/2 ou 0 suivant que c'est, ou non, une algèbre à division; elle est donc neutralisée par toutes les extensions de degré pair de $K$ d'après [15], chapitre XIII, proposition 7, corollaire 1, et, si elle n'est pas neutre, seulement par celles-ci. Nous avons vu, au cours de la démonstration de la proposition 3, que $[a, b]$ représente la norme réduite de cette algèbre dans la base $(1, i, j, ij)$; notre assertion résulte donc de la proposition 57: 9 de [12].

Proposition 6. *Soient $K$ un corps de caractéristique $\neq 2$ et $a, b \in K^*$; les propriétés suivantes sont équivalentes:*

(1) *$[a, b]$ représente zéro dans $K$,*

(2) *$[a, b]$ équivaut linéairement dans $K$ à la forme neutre $U_1U_2 + U_3U_4$,*

(3) *la forme quadratique $aU_2^2 + bU_3^2 + abU_4^2$ représente zéro dans $K$.*

C'est une partie de la proposition 57: 9 de [12].

Proposition 7. *Soient $K$ un corps local et $a, b \in K^*$. La forme $[a, b]$ représente tout élément de $K^*$ sauf si $K = \boldsymbol{R}$ et $a > 0$, $b > 0$ auquel cas elle représente tout élément $> 0$ de $\boldsymbol{R}^*$.*

C'est clair si $K = \boldsymbol{R}$ ou $\boldsymbol{C}$; cela résulte des proposition 42 :11 et 63 : 19 de [12] si $K$ est ultramétrique.

Proposition 8. *Soient $K$ un corps de nombres et $a_1, \ldots, a_5 \in K^*$. Il existe $\varrho, a, b$ et $c \in K^*$ tels que les formes $\varrho(a_1U_1^2 + \ldots + a_5U_5^2)$ et $[a, b, c^*]$ soient linéairement équivalentes sur $K$.*

La forme $a_1U_1^2 + \ldots + a_5U_5^2$, de dimension impaire, représente (Minkowski–Hasse) son discriminant $\delta = a_1 \cdot \ldots \cdot a_5$ dans $K$. Il existe donc une forme quadratique $q(U_1, \ldots, U_4) \in K[U_1, \ldots, U_4]$ dont le discriminant est un carré, telle que

$$a_1U_1^2 + \ldots + a_5U_5^2 \sim q(U_1, \ldots, U_4) + \delta U_5^2,$$

le symbole $\sim$ désignant l'équivalence linéaire sur $K$. Soit $\varrho$ un élément de $K^*$ représenté par $q$ dans $K$; la forme $\varrho q$ représente $\varrho^2$ donc 1 et son discriminant est un carré; par suite, il existe $a, b \in K^*$ tels que $\varrho q \sim [a, b]$. Posons $c = \varrho\delta$; on a

$$\varrho(a_1U_1^2 + \ldots + a_5U_5^2) \sim \varrho q(U_1, \ldots, U_4) + cU_5^2 \sim [a, b, c^*],$$

q.e.d.

Nous pouvons maintenant aborder la démonstration du résultat annoncé dans l'introduction.

**Étude locale.**

THÉORÈME 1. *Soient $K$ un corps local et $a, b, c \in K^*$; soit $f \in K[X]-\{0\}$ séparable et de degré pair $2n$. Lorsque $K = \mathbf{R}$ supposons en outre que*

($\alpha$) *si $a > 0$, $b > 0$, $c > 0$ $f$ est défini positif,*

($\beta$) *si $a > 0$, $b > 0$, $c < 0$ $f$ n'est pas défini négatif et de degré impairement pair (i.e. $n$ impair).*

*Il existe alors cinq polynômes $f_1, \ldots, f_5 \in K[X]$ tels que*

$$f = f_1^2 + af_2^2 + bf_3^2 + abf_4^2 + cf_5^2, \tag{1}$$

$$\deg(f - cf_5^2) = 2n, \tag{2}$$

$$\text{p.g.c.d.}\ (f_1, f_2, f_3, f_4) = 1. \tag{3}$$

I. Supposons d'abord que $K$ est ultramétrique.

1) Si tous les facteurs premiers de $f$ dans $K[X]$ sont de degré pair, soit $p$ l'un d'eux; $[a, b]$ représente zéro dans $K[X]/(p)$ (proposition 5) et $\operatorname{sgn}(f)$ dans $K$ (proposition 7) donc $[a, b]$ représente $f$ dans $K[X]$ (proposition 3). Notre assertion en résulte dans le cas envisagé, car si des $f_i \in K[X]$ $(1 \leqslant i \leqslant 5)$ vérifient (1) et si $f_5 = 0$, alors (2) est trivial et la séparabilité de $f$ implique (3).

2) Si $f$ a un facteur premier de degré impair, on a $n > 0$, et $f$, étant de degré pair $2n$, a un tel facteur de degré $\leqslant n$.

Supposons en premier lieu que $c = -1$. Le théorème résultera, dans ce cas, de l'existence d'un polynôme $g$ de degré $n$, ne divisant pas $f$, tel que la congruence

$$f \equiv au^2 + bv^2 + abw^2 \pmod{g}$$

ait une solution $(u, v, w)$ dans $K[X]$. En effet d'une telle solution on déduit l'existence de polynômes $f_2, f_3, f_4$ non tous nuls, de degré $< n$, et $h$ de degré $n$, tels que $f = af_2^2 + bf_3^2 + abf_4^2 + gh$, ou encore, pour tout $\lambda \in K^*$:

$$f = \left(\frac{\lambda g + \lambda^{-1} h}{2}\right)^2 + af_2^2 + bf_3^2 + abf_4^2 - \left(\frac{\lambda g - \lambda^{-1} h}{2}\right)^2.$$

Les polynômes $f_2, f_3, f_4$ n'ont qu'un nombre fini de facteurs premiers communs; soit $p$ l'un d'eux. Il ne peut diviser à la fois $g$ et $h$ car $p^2$ ne divise pas $f$; on a donc

$$\frac{\lambda g + \lambda^{-1} h}{2} \equiv 0 \pmod{p}$$

pour au plus deux $\lambda \in K^*$. On a de même $\deg\left(\dfrac{\lambda g + \lambda^{-1} h}{2}\right) \neq n$ pour au plus deux $\lambda \in K^*$. Le corps $K$ étant infini, il existe donc $\lambda$ tel que, si on pose $f_1 = \dfrac{\lambda g + \lambda^{-1} h}{2}$, $f_5 = \dfrac{\lambda g - \lambda^{-1} h}{2}$, les $f_i$ $(1 \leqslant i \leqslant 5)$ vérifient les assertions (1), (2), (3) du théorème.



Pour démontrer l'existence de $g$, distinguons trois hypothèses, dont l'une au moins est vérifiée par $f$:

a) $n$ est pair $> 0$; soit $q$ un polynôme premier de degré $n$, ne divisant pas $f$ (il en existe une infinité, définissant par exemple l'extension de $K$ non ramifiée de degré $n$). On peut prendre $g = q$ car la forme $aU^2 + bV^2 + abW^2$ représente zéro dans $K[X]/(q)$ (propositions 5 et 6) donc tout élément de ce corps (proposition 1).

b) $f$ a un facteur de degré $n$; $f$ étant séparable, pour un $\xi \in K^*$ assez voisin de 0, $f - a\xi^2$ a aussi un facteur de degré $n$ (cf. e.g. [1], chap. 6, § 8, exercice 12, c), lequel possède les propriétés requises pour $g$.

c) $n$ est impair et $f$ a un facteur premier $p$ de degré impair $< n$; soit $q \in K[X]$ premier ne divisant pas $f$ et de degré $n - \deg(p)$ pair $> 0$. La congruence $f \equiv au^2 + bv^2 + abw^2$ est soluble $(\operatorname{mod} p)$ trivialement et $(\operatorname{mod} q)$ d'après le même argument qu'en a) donc $(\operatorname{mod} pq)$; on peut prendre $g = pq$, ce qui achève la démonstration lorsque $c = -1$.

Le cas général s'en déduit: posons $\tilde{f} = (-c^{-1})f$; nous venons de prouver qu'il existe des $\tilde{f}_i \in K[X]$ $(1 \leqslant i \leqslant 5)$ tels que

$$\tilde{f} = \tilde{f}_1^2 + a\tilde{f}_2^2 + b\tilde{f}_3^2 + ab\tilde{f}_4^2 - \tilde{f}_5^2,$$

$$\deg(\tilde{f} + \tilde{f}_5^2) = 2n,$$

$$\text{p.g.c.d.}\ (\tilde{f}_1, \tilde{f}_2, \tilde{f}_3, \tilde{f}_4) = 1.$$

D'autre part il existe aussi (proposition 7) $\gamma = (\gamma_1, \ldots, \gamma_4) \in K^4$ vérifiant $-c = \gamma_1^2 + a\gamma_2^2 + b\gamma_3^2 + ab\gamma_4^2$. Dans l'identité

$$(\gamma_1^2 + a\gamma_2^2 + b\gamma_3^2 + ab\gamma_4^2)(V_1^2 + aV_2^2 + bV_3^2 + abV_4^2) = B_1^2(\gamma, V) + aB_2^2(\gamma, V) + bB_3^2(\gamma, V) + abB_4^2(\gamma, V)$$

la comparaison des discriminants des deux membres, considérés comme formes quadratiques en $V$, montre que, comme $-c \neq 0$, les formes linéaires $B_i(\gamma, V) \in K[V_1, \ldots, V_4]$ sont indépendantes. Elles définissent donc un automorphisme du $K[X]$-module $(K[X])^4$ qui transforme l'élément primitif $f^* = (\tilde{f}_1, \ldots, \tilde{f}_4)$ de ce module en $\big(B_1(\gamma, f^*), \ldots, B_4(\gamma, f^*)\big)$, lequel est donc primitif. Posons $f_i = B_i(\gamma, f^*)$ pour $1 \leqslant i \leqslant 4$ et $f_5 = \tilde{f}_5$; alors les $f_i$ vérifient les assertions (1), (2), (3) du théorème.

II. Supposons maintenant que $K$ est archimédien. Si $[a, b]$ représente zéro dans $K$, cette forme représente $f$ dans $K[X]$ (proposition 1) et on conclut comme en I.1). Supposons donc que $K = \mathbf{R}$ et $a > 0$, $b > 0$; les données vérifient alors l'une au moins des trois hypothèses suivantes:

a) $f$ a un facteur de degré $n$ dans $\boldsymbol{R}[X]$ et $c$ est négatif. Comme $[a, b]$ représente $-c$ (proposition 7) on se ramène, de même qu'en I, au cas où $c = -1$; on peut d'ailleurs, pour cela, remarquer plus simplement que $-c \in \boldsymbol{R}^2$. Le raisonnement fait en I.2)–b), indépendant de l'hypothèse initiale du § 2, vaut alors identiquement ici.

b) $c > 0$; dans ce cas $f$, défini positif et séparable par hypothèse, est un produit de facteurs premiers de degré deux et $\operatorname{sgn}(f)$ est positif. La conclusion résulte de la même argumentation qu'en I.1).

c) $f$ n'a pas de facteur de degré $n$ dans $\boldsymbol{R}[X]$. On voit immédiatement que $n$ est impair et que tous les facteurs premiers de $f$ sont de degré deux. Supposons que $\operatorname{sgn}(f)$ soit négatif; $f$ est alors défini négatif et de degré impairement pair. L'hypothèse (β) entraîne que $c$ est positif et (α) implique alors que $f$ est défini positif d'où une contradiction puisque $f \neq 0$. Donc $\operatorname{sgn}(f) > 0$ et on conclut comme en b) achevant ainsi la démonstration du théorème 1.

Remarque. Les hypothèses (α) et (β) sont nécessaires. Plus précisément, (1) implique (α): c'est clair; (1) et (2) impliquent (β): supposons en effet qu'existent $a > 0$, $b > 0$, $c < 0$ dans $\boldsymbol{R}^*$, $f$ séparable, défini négatif et de degré $2n$ impairement pair, dans $\boldsymbol{R}[X]$, enfin des $f_i \in \boldsymbol{R}[X]$ $(1 \leqslant i \leqslant 5)$ vérifiant (1) et (2). Il existe $a', b', c' \in \boldsymbol{R}^*$ tels que $a = a'^2$, $b = b'^2$, $-c = c'^2$; posons $g_1 = f_1$, $g_2 = a'f_2$, $g_3 = b'f_3$, $g_4 = a'b'f_4$, $g_5 = c'f_5$, on a

$$f = g_1^2+g_2^2+g_3^2+g_4^2-g_5^2 \quad \text{et} \quad \deg(f+g_5^2) = 2n,$$

donc (proposition 2) $\max_{1\leqslant i\leqslant 4}\deg(g_i) = n$, par exemple $\deg(g_1) = n$, et $\deg(g_5) \leqslant n$. L'un au moins des polynômes $g_1 \pm g_5$ est de degré $n$ impair et possède donc une racine réelle $\theta$ qui vérifie

$$f(\theta) = g_2^2(\theta)+g_3^2(\theta)+g_4^2(\theta).$$

Le premier membre est $\leqslant 0$, le second $\geqslant 0$, donc $f(\theta) = 0$; $f$ étant séparable on a $f'(\theta) \neq 0$ et $f$ change de signe en $\theta$ ce qui contredit l'hypothèse que $f$ est défini négatif.

Proposition 9. *Soient $f_1, \ldots, f_5$ satisfaisant aux assertions du théorème 1, et $|\ |$ une valeur absolue définissant la topologie de $K$; il existe alors $\eta > 0$ tel que, pour tout polynôme $g \in K[X]$ vérifiant $\deg(g) \leqslant n$ et $|g-f_5| < \eta$, le polynôme $f-cg^2$ soit de degré $2n$ et soit représenté par $[a, b]$ dans $K[X]$.*

Soient $a_i$ $(1 \leqslant i \leqslant s)$ les racines distinctes du polynôme $f-cf_5^2$ dans une clôture algébrique $\tilde{K}$ de $K$. Le prolongement unique à $\tilde{K}$ de la valeur absolue considérée sur $K$ étant encore noté $|\ |$, soit $\delta = \inf_{1\leqslant i<j\leqslant s} |a_i - a_j|$.



Compte tenu d'un lemme classique sur l'approximation des racines d'un polynôme dans un corps valué algébriquement clos (cf. e.g. [1], chap. 6, § 8, exercice 12, a), il existe $\eta > 0$ tel que les inégalités $\deg(g) \leqslant n$ et $|g-f_5| < \eta$ impliquent $\deg(f-cg^2) = 2n$ et, pour toute racine $\beta$ de $f-cg^2$ dans $\tilde{K}$, l'existence d'un indice $i$ $(1 \leqslant i \leqslant s)$ vérifiant $|\beta - a_i| < \delta$. La caractéristique de $K$ étant nulle, $a_i$ est séparable sur $K$; l'inégalité précédente entraîne donc $K(a_i) \subset K(\beta)$ d'après le lemme de Krasner (cf. ibid. b) qui vaut aussi, trivialement, dans le cas archimédien. Le polynôme minimal de $a_i$ sur $K$ divise $f-cf_5^2$ sans diviser tous les $f_1, \ldots, f_4$ puisque ceux-ci sont premiers entre eux; donc $[a, b]$ représente zéro dans $K(a_i)$ et par suite dans $K(\beta)$ pour toute racine $\beta$ de $f-cg^2$ dans $\tilde{K}$. On peut choisir $\eta > 0$ tel qu'en outre $\operatorname{sgn}(f-cg^2)/\operatorname{sgn}(f-cf_5^2) \in K^{*2}$, donc (propositions 1 et 2) que $[a, b]$ représente $\operatorname{sgn}(f-cg^2)$ dans $K$; $\eta$ répond alors à la question (proposition 3).

**Étude globale.**

Théorème 2. *Soient $K$ un corps de nombres et $a, b, c \in K^*$; soit $f \in K[X]-\{0\}$ de degré pair $2n$. Pour toute relation d'ordre sur $K$ supposons que*

*(α) si $a > 0$, $b > 0$, $c > 0$, $f$ est défini positif,*

*(β) si $a > 0$, $b > 0$, $c < 0$, $f$ n'est pas défini négatif et de degré impairement pair.*

*Il existe alors cinq polynômes $f_1, \ldots, f_5 \in K[X]$ tels que*

$$f = f_1^2+af_2^2+bf_3^2+abf_4^2+cf_5^2, \tag{1}$$

$$\deg(f-cf_5^2) = 2n. \tag{2}$$

Il suffit évidemment de démontrer le théorème lorsque $f$ est séparable. Soient $\Omega$ l'ensemble des places de $K$ et $T$ l'ensemble fini des $\mathfrak{p} \in \Omega$ telles que $[a, b]$ ne représente pas zéro dans $K_\mathfrak{p}$. Si $T$ est vide, $[a, b]$ représente zéro dans $K$ (Minkowski–Hasse) donc (proposition 1) représente $f$ dans $K[X]$, d'où le résultat avec $f_5 = 0$. Si $T$ n'est pas vide, soient, pour toute $\mathfrak{p} \in T$, $f_{i,\mathfrak{p}} \in K_\mathfrak{p}[X]$ $(1 \leqslant i \leqslant 5)$ vérifiant les assertions (1), (2) et (3) du théorème 1, $|\ |_\mathfrak{p}$ une valeur absolue définissant la topologie de $K_\mathfrak{p}$, enfin $\eta_\mathfrak{p} > 0$ ayant la propriété énoncée dans la proposition 9. Comme $\deg(f_{5,\mathfrak{p}}) \leqslant n$ d'après (2), le théorème d'approximation faible ([12], 11 : 8) entraîne l'existence de $f_5 \in K[X]$ tel que $\deg(f_5) \leqslant n$ et $|f_5-f_{5,\mathfrak{p}}|_\mathfrak{p} < \eta_\mathfrak{p}$ pour toute $\mathfrak{p} \in T$. Le polynôme $f-cf_5^2$ est donc de degré $2n$ puisque $T \neq \emptyset$ et il est représenté par $[a, b]$ dans $K_\mathfrak{p}[X]$ pour toute $\mathfrak{p} \in T$, donc pour toute $\mathfrak{p} \in \Omega$ (proposition 1). D'après la proposition 4, $f-cf_5^2$ est donc représenté par $[a, b]$ dans $K[X]$, q.e.d.

Remarques. 1) Lorsque la forme $[a, b, c^*]$ représente zéro dans $K$, ce qui est toujours le cas (Minkowski–Hasse) si $K$ n'est pas formellement réel, la propriété (2) constitue, compte tenu de la proposition 1, l'essentiel du théorème.

2) Lorsque $[a, b, c^*]$ ne représente pas zéro, (1) implique $\max_{1\leqslant i\leqslant 5}\deg(f_i) = n$ (proposition 2).

3) Lorsque $[a, b]$ ne représente pas zéro, (2) équivaut à $\max_{1\leqslant i\leqslant 4}\deg(f_i) = n$ (proposition 2) et implique $\max_{1\leqslant i\leqslant 5}\deg(f_i) = n$.

4) Lorsque $[a, b]$ représente zéro, il existe en fait des $f_i \in K[X]$ $(1\leqslant i\leqslant 4)$ vérifiant

$$(1') \qquad f = f_1^2+af_2^2+bf_3^2+abf_4^2,$$

$$(2') \qquad \max_{1\leqslant i\leqslant 4}\deg(f_i) = n.$$

En effet, d'après la proposition 6, il existe quatre formes linéaires $L_1(U), \ldots, L_4(U) \in K[U_1, \ldots, U_4]$ telles que

$$L_1^2(U)+aL_2^2(U)+bL_3^2(U)+abL_4^2(U) = U_1U_2+U_3U_4.$$

Soient $g_1 \in K[X]$ un polynôme arbitraire de degré $n$, et $g_2$, $g_3$ respectivement le quotient et le reste de la division euclidienne de $f$ par $g_1$; on a $\deg(g_3) < n$ et $\deg(g_2) = n$. Posons $f_i = L_i(g_1, g_2, g_3, 1)$ pour $1\leqslant i\leqslant 4$; les $f_i$ vérifient (1') et l'inégalité $\max_{1\leqslant i\leqslant 4}\deg(f_i)\leqslant n$, donc aussi (2'), q.e.d.

Corollaire 1. *Soient $K$ un corps de nombres et $a_1, \ldots, a_5 \in K^*$; soit $f\in K[X]-\{0\}$ de degré pair $2n$. Pour toute relation d'ordre $\omega$ sur $K$, désignons par $\nu_\omega$ le nombre des $a_i$ $(1\leqslant i\leqslant 5)$ qui sont négatifs et supposons que*

*(α) si $\nu_\omega = 0$ (resp. $\nu_\omega = 5$), $f$ est défini positif (resp. défini négatif),*

*(β) si $\nu_\omega = 1$ (resp. $\nu_\omega = 4$), $f$ n'est pas défini négatif (resp. défini positif) et de degré impairement pair.*

*Il existe alors cinq polynômes $f_1, \ldots, f_5 \in K[X]$ tels que*

$$(1) \qquad f = a_1f_1^2+a_2f_2^2+a_3f_3^2+a_4f_4^2+a_5f_5^2,$$

$$(2) \qquad \max_{1\leqslant i\leqslant 5}\deg(f_i) = n.$$

D'après la proposition 8 il existe $\varrho, a, b, c \in K^*$ et cinq formes linéaires $L_1(U), \ldots, L_5(U) \in K[U_1, \ldots, U_5]$ vérifiant

$$\varrho\big(a_1L_1^2(U)+\ldots+a_5L_5^2(U)\big) = U_1^2+aU_2^2+bU_3^2+abU_4^2+cU_5^2.$$

On voit aisément, à l'aide de la loi d'inertie de Sylvester, que les éléments $a, b, c \in K^*$ et le polynôme $g = \varrho f$ satisfont aux hypothèses (α) et (β) du théorème 2. Compte tenu des remarques 3) et 4), il existe donc $g_1, \ldots, g_5 \in K[X]$ tels que $g = g_1^2+ag_2^2+bg_3^2+abg_4^2+cg_5^2$ et $\max_{1\leqslant i\leqslant 5}\deg(g_i) = n$. Posons $f_i = L_i(g_1, \ldots, g_5)$ pour $1\leqslant i\leqslant 5$; les $f_i$ vérifient (1) et l'inégalité $\max_{1\leqslant i\leqslant 5}\deg(f_i)\leqslant n$, donc aussi (2).



Corollaire 2. *Soient $K$ un corps de nombres et $a_1, \ldots, a_5 \in K^*$; soit $F$ une forme algébrique non nulle, de degré pair $2n$, sur un $K$-espace vectoriel $E$ de dimension 2. Pour toute relation d'ordre $\omega$ sur $K$ designons par $\nu_\omega$ le nombre des $a_i$ $(1\leqslant i\leqslant 5)$ qui sont négatifs et supposons que*

*(α) si $\nu_\omega = 0$ (resp. $\nu_\omega = 5$), $F$ est définie positive (resp. définie négative),*

*(β) si $\nu_\omega = 1$ (resp. $\nu_\omega = 4$), $F$ n'est pas définie négative (resp. définie positive) et de degré impairement pair.*

*Il existe alors cinq formes algébriques $F_1, \ldots, F_5$ sur $E$ telles que*

$$(1) \qquad F = a_1F_1^2+a_2F_2^2+a_3F_3^2+a_4F_4^2+a_5F_5^2,$$

$$(2) \qquad \deg(F_i) = n \quad \text{ou } F_i = 0 \quad \text{pour} \quad 1\leqslant i\leqslant 5.$$

$F$ n'étant pas nulle, est représentée dans une base convenable de $E$ par un polynôme homogène, de degré $2n$, $f(X, Y)\in K[X, Y]$ tel que $f(1, 0)\neq 0$. Le polynôme $g(X) = f(X, 1)$, de degré $2n$, vérifie les hypothèses du corollaire 1; il existe donc, dans $K[X]$, des polynômes $g_i(X)$ $(1\leqslant i\leqslant 5)$ tels que $g = a_1g_1^2+a_2g_2^2+a_3g_3^2+a_4g_4^2+a_5g_5^2$ et $\max_{1\leqslant i\leqslant 5}\deg(g_i) = n$. Posons $f_i(X, Y) = Y^n g_i(X/Y)$ pour $1\leqslant i\leqslant 5$; les $f_i$ sont des polynômes homogènes nuls ou de degré $n$, qui définissent dans la base considérée des formes $F_i$ $(1\leqslant i\leqslant 5)$ vérifiant (1) et (2).

Corollaire 3. *Soient $K$ un corps de nombres et $a_1, \ldots, a_5 \in K^*$; soit $f\in K[X]-\{0\}$ de degré impair $2n+1$. Supposons que $a_1, \ldots, a_5$ ne sont tous de même signe pour aucune relation d'ordre sur $K$. Il existe alors cinq polynômes $f_1, \ldots, f_5 \in K[X]$ tels que*

$$(1) \qquad f = a_1f_1^2+a_2f_2^2+a_3f_3^2+a_4f_4^2+a_5f_5^2,$$

$$(2) \qquad \max_{1\leqslant i\leqslant 5}\deg(f_i) = n+1.$$

Quelle que soit la relation d'ordre sur $K$, le polynôme homogène non nul $g(X, Y) = Y^{2n+2}f(X/Y)$, de degré pair $2n+2$, n'est ni défini positif, ni défini négatif, puisque le polynôme $g(X, 1) = f(X)$, étant de degré impair, change de signe dans $K$.

Le corollaire 2, interprété dans la base canonique de $K^2$, entraîne l'existence de cinq polynômes homogènes $g_1, \ldots, g_5 \in K[X, Y]$ tels que

$$g(X, Y) = a_1g_1^2+\ldots+a_5g_5^2$$

et

$$\deg(g_i) = n+1 \quad \text{ou} \quad g_i = 0 \quad \text{pour } 1\leqslant i\leqslant 5.$$

Posons $f_i(X) = g_i(X, 1)$; les $f_i$ vérifient (1) ainsi que les inégalités $\deg f_i(X)\leqslant \deg g_i(X, Y)\leqslant n+1$; ils vérifient donc aussi (2) puisque (1) implique

$$2\max_{1\leqslant i\leqslant 5}\deg(f_i)\geqslant \deg(f).$$

Remarque. L'hypothèse concernant $a_1, \ldots, a_5$ équivaut (Minkowski-Hasse) au fait que $a_1 U_1^2 + \ldots + a_5 U_5^2$ représente zéro dans $K$; l'intérêt du corollaire réside donc (proposition 1) dans la propriété (2). Cette hypothèse est nécessaire; en effet, si $a_1 U_1^2 + \ldots + a_5 U_5^2$ ne représente pas zéro dans $K$, (1) implique (proposition 2) que $\deg(f) = 2 \max_{1 \leqslant i \leqslant 5} \deg(f_i)$ qui est pair.

Corollaire 4. *Pour tout polynôme $f \in \boldsymbol{Q}[X]$ défini positif, il existe cinq polynômes $f_1, \ldots, f_5 \in \boldsymbol{Q}[X]$ tels que*

$$f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2.$$

Si $f = 0$ c'est clair; dans le cas contraire $f$ est nécessairement de degré pair, et il suffit d'appliquer le théorème 2 avec $K = \boldsymbol{Q}$ et $a = b = c = 1$.

On ne peut abaisser le nombre des carrés dans cet énoncé; ainsi pour que $f = c_2 X^2 + c_1 X + c_0 \in \boldsymbol{Q}[X] - \{0\}$ soit somme de quatre carrés dans $\boldsymbol{Q}[X]$, il faut et il suffit que $4c_0 c_2 - c_1^2$ soit somme de trois carrés dans $\boldsymbol{Q}$ et que $\operatorname{sgn}(f) > 0$ [11]. Plus généralement:

Proposition 10. *Soit*

$$f \in \boldsymbol{Q}[X] - \{0\};$$

*les propriétés suivantes sont équivalentes:*

(1) *$f$ est somme de quatre carrés dans $\boldsymbol{Q}[X]$.*

(2) $\operatorname{sgn}(f) > 0$ *et, pour tout facteur premier $p$ de $f$ de multiplicité impaire, $-1$ est somme de deux carrés dans le corps $\boldsymbol{Q}[X]/(p)$.*

(3) *$f$ est défini positif et, dans $\boldsymbol{Q}_2[X]$, ses facteurs premiers de multiplicité impaire sont de degré pair.*

L'équivalence de (1) et (2) résulte des propositions 3 et 6 et du fait que tout nombre rationnel $> 0$ est somme de quatre carrés.

(1) $\Rightarrow$ (3) d'après les propositions 3 et 5 puisque $[1, 1]$ ne représente pas zéro dans $\boldsymbol{Q}_2$.

(3) $\Rightarrow$ (1): en effet, $f$ est alors (propositions 3, 5 et 7) somme de quatre carrés dans $\boldsymbol{R}[X]$ et dans $\boldsymbol{Q}_2[X]$, donc (proposition 1) dans $\boldsymbol{Q}_p[X]$ pour tout $p \in \{2, 3, 5, \ldots, \infty\}$ puisque $[1, 1]$ représente zéro dans $\boldsymbol{Q}_p$ lorsque $p$ est fini et $\neq 2$; par suite (proposition 4) $f$ est somme de quatre carrés dans $\boldsymbol{Q}[X]$.

En ce qui concerne les sommes de deux carrés nous avons la

Proposition 11. *Soient $a \in K^*$ et $f \in K[X] - \{0\}$. Pour que la forme $U_1^2 + aU_2^2$ représente $f$ dans $K[X]$, il faut et il suffit qu'elle représente* $\operatorname{sgn}(f)$ *dans $K$, et que pour tout $p$ premier $\in K[X]$, facteur de $f$ avec une multiplicité impaire, l'extension $K[X]/(p)$ de $K$ contienne $K(\sqrt{-a})$.*



Cette proposition, analogue à la proposition 3, peut se démontrer de la même façon à l'aide de l'identité

$$(U_1^2 + aU_2^2)(V_1^2 + aV_2^2) = (U_1V_1 + aU_2V_2)^2 + a(U_1V_2 - U_2V_1)^2.$$

Pour prouver que $f$ premier $\in K[X]$, tel que $\operatorname{sgn}(f) = 1$ et que $E = K[X]/(f) \supset F = K(\sqrt{-a})$, est représenté par $U_1^2 + aU_2^2$ dans $K[X]$, on peut aussi, en se bornant (proposition 1) au cas où cette forme ne représente pas zéro dans $K$, remarquer plus simplement que, si $\theta$ désigne l'image de $X$ dans $E = K[X]/(f)$, on a

$$f(X) = N_{E(X)/K(X)}(X - \theta) = N_{F(X)/K(X)}\big(N_{E(X)/F(X)}(X - \theta)\big)$$

cf. [4], lemme 2.

**Application aux polynômes cyclotomiques.** Nous allons étudier, à l'aide des propositions 10 et 11, la représentation des polynômes cyclotomiques en somme de carrés dans $\boldsymbol{Q}[X]$. Nous noterons $\Phi_n(X)$ le $n$-ième polynôme cyclotomique.

Soient $A$ un anneau et $m$ un entier $> 0$; nous écrirons pour abréger, comme A. Pfister, que $a = \boxed{m}$ ou bien que $a$ est $\boxed{m}$ (resp. $a \neq \boxed{m}$ ou $a$ n'est pas $\boxed{m}$) dans $A$, si $a \in A$ est (resp. n'est pas) somme des carrés de $m$ éléments de $A$.

Soient $p$ et $q \in \boldsymbol{Z}$ premiers entre eux et soit $f \in \boldsymbol{N}$; nous dirons que $q$ est d'ordre $f \pmod p$ si l'image de $q$ dans le groupe $(\boldsymbol{Z}/(p))^*$ est d'ordre $f$.

Théorème 3. 1) *Si $n = 1$ ou 2, $\Phi_n(X)$ n'est pas somme de carrés dans $\boldsymbol{Q}[X]$.*

2) *Si $n > 2$, $\Phi_n(X)$ est $\boxed{5}$ et n'est pas $\boxed{1}$ dans $\boldsymbol{Q}[X]$.*

3) *Pour que $\Phi_n(X)$ soit $\boxed{2}$ dans $\boldsymbol{Q}[X]$, il faut et il suffit que $4|n$.*

4) *Si $4 \nmid n$, $\Phi_n(X)$ n'est pas $\boxed{3}$ dans $\boldsymbol{Q}[X]$, et pour qu'il soit $\boxed{4}$ dans cet anneau, il faut et il suffit que $n$ ait un facteur premier $p \neq 2$ tel que 2 soit d'ordre pair* $(\bmod p)$.

1) C'est clair puisque $\Phi_1(X) = X - 1$ et $\Phi_2(X) = X + 1$ sont de degré impair.

2) Si $n > 2$, le corps $\boldsymbol{Q}[X]/(\Phi_n(X))$, qui contient les racines $n$-ièmes de l'unité, n'est pas ordonnable; donc $\Phi_n(X)$ n'a aucune racine réelle et il est par suite défini positif puisque $\operatorname{sgn}(\Phi_n(X)) = 1 > 0$. D'après le corollaire 4 du théorème 2, $\Phi_n(X)$ est donc $\boxed{5}$ dans $\boldsymbol{Q}[X]$. D'autre part, il n'est pas $\boxed{1}$ dans cet anneau puisqu'il est séparable (en fait premier dans $\boldsymbol{Q}[X]$).

3) Compte tenu de $\operatorname{sgn}(\Phi_n(X)) = 1$, pour que $\Phi_n(X)$ soit $\boxed{2}$ dans $\boldsymbol{Q}[X]$, il faut et il suffit (proposition 11) que $\boldsymbol{Q}[X]/(\Phi_n(X))$ contienne $\boldsymbol{Q}(\sqrt{-1}) = \boldsymbol{Q}[X]/(\Phi_4(X))$ ce qui, comme on le voit aisément, équivaut à $4|n$.

4) Supposons enfin que $4\nmid n$. Si $\nu$ est un entier impair, on a $\Phi_{2\nu}(X) = \Phi_\nu(-X)$ (cf. e.g. [9], p. 206); il suffit donc de démontrer 4) lorsque $n$ est impair $>1$. Soit alors

$$n = \prod_{1\leqslant i\leqslant s} p_i^{a_i} \qquad (a_1, \ldots, a_s \geqslant 1)$$

la décomposition de $n$ en facteurs premiers.

Posons $q = \prod_{1\leqslant i\leqslant s} p_i$ et démontrons d'abord que $\Phi_q(2) \neq \boxed{3}$ dans $\boldsymbol{Q}$. Soit $\boldsymbol{Z}_2 \subset \boldsymbol{Q}$ le localisé de $\boldsymbol{Z}$ pour l'idéal $2\boldsymbol{Z}$, et soit $U_2 = \boldsymbol{Z}_2^*$. Pour tout diviseur $d$ de $q$ on a $2^d-1 \in U_2$; si $d \neq 1$, on a en outre $2^d-1 \equiv -1$ dans le groupe $U_2$ modulo le sous-groupe $1+8\boldsymbol{Z}_2$, car $d \geqslant 3$ puisque $q$ est impair. Compte tenu des égalités $\sum_{d|q,d>1} \mu(q|d) = -\mu(q)$ et $\mu(q) = \pm 1$, où $\mu$ désigne la fonction de Möbius, on obtient, dans $U_2$ modulo $1+8\boldsymbol{Z}_2$,

$$\Phi_q(2) = \prod_{d|q} (2^d-1)^{\mu(q|d)} \equiv (-1)^{-\mu(q)}(1)^{\mu(q)} = -1,$$

et par suite, dans l'anneau $\boldsymbol{Z}$, $\Phi_q(2) \equiv -1 \pmod 8$; donc $\Phi_q(2) \neq \boxed{3}$ dans $\boldsymbol{Q}$.

D'après [16], $\Phi_q(2)$ n'est pas non plus $\boxed{3}$ dans l'extension $\boldsymbol{Q}(\theta)$ de $\boldsymbol{Q}$ définie par $\theta^{n/q} = 2$, puisque $[\boldsymbol{Q}(\theta):\boldsymbol{Q}] = n/q$ ([9], p. 221, th. 16) est impair. La première assertion de 4) en résulte car d'une part on a ([9], p. 206, formule 2)

$$\Phi_n(\theta) = \Phi_q(\theta^{n/q}) = \Phi_q(2) \neq \boxed{3} \quad \text{dans} \quad \boldsymbol{Q}(\theta)$$

et d'autre part une relation $\Phi_n(X) = f_1^2(X)+f_2^2(X)+f_3^2(X)$ où $f_i(X) \in \boldsymbol{Q}[X]$ $(1 \leqslant i \leqslant 3)$ impliquerait

$$\Phi_n(\theta) = f_1^2(\theta)+f_2^2(\theta)+f_3^2(\theta) = \boxed{3} \quad \text{dans } \boldsymbol{Q}(\theta).$$

Soit maintenant $f$ l'ordre de $2 \pmod n$; les facteurs premiers de $\Phi_n(X)$ dans $\boldsymbol{Q}_2[X]$ sont de degré $f$ ([3], p. 87, lemme 4) et de multiplicité 1. Soit $f_i$ $(1 \leqslant i \leqslant s)$ l'ordre de $2 \pmod{p_i^{a_i}}$; on a

$$(\boldsymbol{Z}/(n))^* = \prod_{1\leqslant i\leqslant s} (\boldsymbol{Z}/(p_i^{a_i}))^*,$$

donc $f = \text{p.p.c.m.}\ (f_i)_{1\leqslant i\leqslant s}$; d'autre part, comme $p_i \neq 2$, $f_i$ est le produit de l'ordre de $2 \pmod{p_i}$ et d'une puissance de $p_i$. La deuxième assertion de 4) résulte alors de la proposition 10 et le théorème 3 est démontré.

Soit $K_n = \boldsymbol{Q}[X]/(\Phi_n(X))$ le corps des racines $n$-ièmes de l'unité sur $\boldsymbol{Q}$; soit $S_n$ le plus petit des entiers $m \in \boldsymbol{N}$ tels que $-1 = \boxed{m}$ dans $K_n$, s'il existe de tels entiers, et posons $S_n = \infty$ dans le cas contraire; $S_n$ est l'index de Pfister de $K_n$ (cf. [14]). On a (Minkowski–Hasse) $S_n = \infty$ ou $S_n \leqslant 4$, donc $S_n = 1, 2, 4$ ou $\infty$. Les résultats précédents nous permettent



de déterminer $S_n$ pour tout $n$ [1]. En effet, du théorème 3 et des propositions 3 et 11, on déduit immédiatement la

PROPOSITION 12. 1) *Si* $n = 1$ *ou* 2, *on a* $S_n = \infty$.

2) *Si* $n > 2$, *on a* $S_n = 1, 2$ *ou* 4.

3) *Pour que* $S_n = 1$, *il faut et il suffit que* $4 | n$.

4) *Pour que* $S_n = 2$, *il faut et il suffit que* $4 \nmid n$ *et que* $n$ *ait un facteur premier* $p \neq 2$ *tel que* 2 *soit d'ordre pair* $(\operatorname{mod} p)$.

Cette proposition peut d'ailleurs être obtenue plus directement à l'aide du théorème de Minkowski–Hasse et de la proposition 5.

Nous compléterons le théorème 3 et la proposition 12 par la

PROPOSITION 13. *Soit* $p$ *un nombre premier. Si* $p \equiv -1 \pmod 8$, 2 *est d'ordre impair* $(\operatorname{mod} p)$; *si* $p \equiv \pm 3 \pmod 8$, 2 *est d'ordre pair. Quant aux* $p \equiv 1 \pmod 8$, *il en existe une infinité tels que* 2 *soit d'ordre pair* $(\operatorname{mod} p)$ *et aussi une infinité tels que* 2 *soit d'ordre impair; ces deux ensembles de nombres premiers ont chacun une densité, égale respectivement à* $5/24$ *et* $1/24$.

Les deux premières assertions résultent immédiatement de la congruence

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod p, \qquad p \neq 2.$$

La dernière, due à Hasse, est une conséquence du

LEMME (Hasse [6]). *Soit* $t$ *un entier* $\geqslant 3$. *Les nombres premiers* $p$ *tels que* $2^t \| p-1$ *et que* 2 *soit d'ordre impair* $(\operatorname{mod} p)$, *ont une densité qui est* $1/2^{2t-1}$.

On en déduit en effet que la densité inférieure [2] des $p \equiv 1 \pmod 8$ tels que 2 soit d'ordre impair $(\operatorname{mod} p)$ est

$$\geqslant \sum_{t=3}^{\infty} \frac{1}{2^{2t-1}} = \frac{1}{24}.$$

D'autre part, les $p$ tels que $2^t \| p-1$ ont une densité qui est

$$\frac{1}{\varphi(2^{t+1})} = \frac{1}{2^t};$$

par suite, la densité inférieure des $p \equiv 1 \pmod 8$ tels que 2 soit d'ordre pair $(\operatorname{mod} p)$, est

$$\geqslant \sum_{t=3}^{\infty} \left(\frac{1}{2^t} - \frac{1}{2^{2t-1}}\right) = \frac{1}{4} - \frac{1}{24} = \frac{5}{24}.$$

(1) Des résultats partiels ont été obtenus par P. et S. Chowla dans deux notes parues au J. of Number Theory (1(1969), p. 208–210; 2(1970), p. 271–272).

(2) i.e. $\varliminf_{x\to\infty} P(x)\log x/x$, où $P$ désigne la fonction énumératrice de l'ensemble de nombres premiers considérés.

Comme 1/4 est la densité des $p \equiv 1 \pmod 8$, on voit que les $p \equiv 1 \pmod 8$ tels que 2 soit $(\bmod p)$ d'ordre impair (resp. pair) ont une densité qui est 1/24 (resp. 5/24), q.e.d.

### Bibliographie


[1] N. Bourbaki, *Algèbre commutative*; chap. 5–6, Paris 1964.
[2] J. W. S. Cassels, *On the representation of rational functions as sums of squares*, Acta Arith. 9 (1964), p. 79–82.
[3] — and A. Fröhlich (editors), *Algebraic Number Theory*, Academic Press 1967.
[4] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), p. 107–116.
[5] A. Fleck, *Zur Darstellung definiter binärer Formen als Summen von Quadraten ganzer rationalzahliger Formen*, Archiv für Math. und Physik (3) 10 (1906), p. 23–38 et (3) 16 (1910), p. 275–276.
[6] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a ≠ 0 von gerader bzw. ungerader Ordnung mod p ist*, Math. Ann. 166 (1966), p. 19–23.
[7] E. Landau, *Über die Darstellung definiter Funktionen durch Quadrate*, Math. Ann. 62 (1906), p. 272–285.
[8] — *Über die Zerlegung definiter Funktionen in Quadrate*, Archiv für Math. und Physik (3) 7 (1904), p. 271–277.
[9] S. Lang, *Algebra*, Addison-Wesley, 1969.
[10] A. M. Legendre, *Théorie des nombres*, Paris 1798; rééd. Blanchard, 1955.
[11] L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Zeitschr. 35 (1932), p. 1–15.
[12] O. T. O'Meara, *Introduction to quadratic forms*, Berlin 1963.
[13] A. Pfister, *Zur Darstellung definiter Funktionen als Summe von Quadraten*, Inventiones math. 4 (1967), p. 229–237.
[14] — *Multiplikative quadratische Formen*, Arch. Math. 16 (1965), p. 363–370.
[15] J.-P. Serre, *Corps locaux*, Paris 1962.
[16] T. Springer, *Sur les formes quadratiques d'indice zéro*, C. R. Acad. Sci. Paris 234 (1952), p. 1517–1519.
[17] W. Wolff, *Neuer Beweis für die Darstellbarkeit definiter biquadratischer Funktionen als Summen von fünf Quadraten*, Vierteljahrsschrift Naturf. Gesell. Zürich, 56 (1911), p. 110–124.


*Reçu le 9. 7. 1970* (101)

ACTA ARITHMETICA
XIX (1971)

## ERRATA

| Page, line | For | Read |
|---|---|---|
| | | [illegible] |

## BOOKS PUBLISHED BY THE INSTITUTE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES

. Janiszewski, Oeuvres choisies, 1962, 320 pp., $ 6.00.
. Marcinkiewicz, Collected papers, 1964, 673 pp., $ 12.00.
. Banach, Oeuvres, vol. I, 1967, 381 pp., $ 12.00.
. Mazurkiewicz, Travaux de topologie et ses applications, 1969, 380 pp., $ 7.20.

## MONOGRAFIE MATEMATYCZNE

0. S. Saks i A. Zygmund, Funkcje analityczne, 3rd ed., 1959, VIII+431 pp., $ 5.00.
0. C. Kuratowski, Topologie I, 4th ed., 1958, XII+494 pp., $ 10.00.
7. K. Kuratowski i A. Mostowski, Teoria mnogości, 2nd ed., enlarged and revised, 1966, 376 pp., $ 6.00.
8. S. Saks and A. Zygmund, Analytic functions, 2nd ed., enlarged, 1965, X+510 pp., $ 12.00.
0. J. Mikusiński, Rachunek operatorów, 2nd ed., 1957, 375 pp., $ 5.00.
1. W. Ślebodziński, Formes extérieures et leurs applications I, 1954, VI+154 pp., $ 6.00.
4. W. Sierpiński, Cardinal and ordinal numbers, 2nd ed., revised, 1965, 492 pp., $ 13.00.
7. R. Sikorski, Funkcje rzeczywiste II, 1959, 261 pp., $ 5.00.
8. W. Sierpiński, Teoria liczb II, 1959, 487 pp., $ 7.00.
9. J. Aczél und S. Gołąb, Funktionalgleichungen der Theorie der geometrischen Objekte, 1960, 172 pp., $ 8.00.
0. W. Ślebodziński, Formes extérieures et leurs applications II, 1963, 271 pp., $ 10.00.
2. W. Sierpiński, Elementary theory of numbers, 1964, 480 pp., $ 13.00.
3. J. Szarski, Differential inequalities, 2nd ed., 1967, 256 pp., $ 12.00.
4. K. Borsuk, Theory of retracts, 1967, 251 pp., $ 12.00.
6. M. Kuczma, Functional equations in a single variable, 1968, 383 pp., $ 10.00.
7. D. Przeworska-Rolewicz and S. Rolewicz, Equations in linear spaces, 1968, 380 pp., $ 15.00.
8. K. Maurin, General eigenfunction expansions and unitary representations of topological groups, 1968, 368 pp., $ 15.00.
9. A. Alexiewicz, Analiza funkcjonalna, 1969, 535 pp., $ 8.00.
0. K. Borsuk, Multidimensional analytic geometry, 1969, 443 pp., $ 15.00.
1. R. Sikorski, Advanced calculus. Functions of several variables, 1969, 460 pp., $ 15.00.
2. W. Ślebodziński, Exterior forms and their applications, 1970, 427 pp., $ 15.00.
3. M. Krzyżański, Partial differential equations of second order, vol. I, 1971, 562 pp., $ 15.00.
4. M. Krzyżański, Partial differential equations of second order, vol. II, 1971, 406 pp., $ 10.00.