SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

JEAN-RENÉ JOLY

Polynômes à une variable dont les valeurs aux points entiers sont des carrés, des cubes, des sommes de deux carrés, etc

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 7, p. 1-22

<http://www.numdam.org/item?id=STNG_1974-1975__4__A7_0>

Janvier-Février 1975

Grenoble

POLYNÔMES A UNE VARIABLE DONT LES VALEURS AUX POINTS ENTIERS SONT DES CARRES, DES CUBES, DES SOMMES DE DEUX CARRES, etc...

par Jean-René JOLY

[Les numéros tels que ([1]) renvoient à des notes placées en fin d'exposé, avant la Bibliographie]

1. INTRODUCTION.

Soit $f(X)$ un polynôme à une variable X, et à coefficients dans l'anneau $\mathbb{Z}$ des entiers rationnels. Si $f(X)$ est un carré dans $\mathbb{Z}[X]$, autrement dit, s'il existe $g(X)$ tel que

$$f(X) = [g(X)]^2 , \tag{1.1}$$

alors $f(X)$ possède évidemment la propriété suivante :

(1.2) quel que soit x dans $\mathbb{Z}$, la valeur $f(x)$ prise par $f(X)$ en x est un carré dans $\mathbb{Z}$.

La réciproque est vraie :

THEOREME 1. Si toutes les valeurs $f(x)$, pour x dans $\mathbb{Z}$, sont des carrés dans $\mathbb{Z}$, alors $f(X)$ est lui-même un carré dans $\mathbb{Z}[X]$.

Voici deux démonstrations "naturelles" de ce résultat. (Pour d'autres démonstrations, voir les références ([1]) [5] et [10], citées dans [3]).

Démonstration n° 1 : Si $f(X)$ n'est pas un carré, mais si $f(x)$ est un carré pour tout x dans $\mathbb{Z}$, la fonction $\varphi(x) = \sqrt{f(x)}$ de la variable réelle x est analytique réelle au voisinage de $+\infty$, mais n'appartient pas à $\mathbb{R}[x]$ (noter en effet que $\varphi(x)$ est un entier rationnel pour tout x entier rationnel assez grand ; si donc $\varphi(x)$ était dans $\mathbb{R}[x]$, la formule d'interpolation de Lagrange montrerait que $\varphi(x)$ est en fait dans $\mathbb{Q}[x]$ ([2]) ; mais comme $[\varphi(x)]^2 = f(x)$, et que l'anneau $\mathbb{Z}[x]$ est intégralement clos -il est factoriel-, on voit que $\varphi(x)$ serait même dans $\mathbb{Z}[x]$, et que $f(x)$ serait donc un carré dans $\mathbb{Z}[x]$: contradiction). Cela étant, on peut appliquer à $\varphi(x)$ le théorème de Dörge ([7], p. 147, th. 1) : il existe un entier $B \geq 0$, un entier $m \geq 1$ et un nombre réel $\lambda > 0$ ayant la propriété suivante :

> si $x_0 < x_1 < x_2 < \ldots$ est la suite des valeurs réelles de $x \geq B$ pour lesquelles $\varphi(x)$ est dans $\mathbb{Z}$, alors, pour tout entier $i \geq 0$, on a

$$x_{i+m} - x_i > x_i^{\lambda} \quad . \tag{1}$$

Mais tous les entiers $\geq B$ figurent parmi les x_i ; on a donc d'une part

$$x_i \leq B+i \quad , \tag{2}$$

et d'autre part

$$x_{i+m} \leq x_{i+m} \quad ; \tag{3}$$

portant ces deux inégalités dans (1), on arrive à

$$m > (B+i)^{\lambda} \quad ; \tag{4}$$

il suffit alors de faire tendre i vers l'infini pour aboutir à une contradiction. ∎

Remarque 1 : En utilisant, au lieu du théorème de Dörge, le théorème d'irréductibilité de Hilbert (qui se déduit d'ailleurs lui-même du théorème de Dörge ; voir [7], chap. VIII, §§1-2) on peut donner, de la démonstration n° 1, la variante suivante ([3]), apparemment plus rapide (et plus élégante) :

Si $f(x)$ n'est pas un carré dans $\mathbb{Z}[X]$, il n'est pas non plus un carré dans $\mathbb{Q}[X]$, et le polynôme à deux variables $Y^2 - f(X)$ est irré-

ductible dans $\mathbb{Q}[X,Y]$; d'après le théorème d'irréductibilité de Hilbert ([7], p. 141, et pp. 147-148, coroll.2), il existe alors une infinité de valeurs entières rationnelles x telles que $Y^2 - f(x)$ soit irréductible dans $\mathbb{Q}[Y]$: mais ceci exclut évidemment que $f(x)$ soit un carré pour tout x dans $\mathbb{Z}$.■

Démonstration n° 2 : Etablissons d'abord un lemme (d'ailleurs pratiquement équivalent au th.1 lorsque $f(X)$ est de degré 2) :

LEMME 1. Soit C une conique non décomposée définie par une équation de la forme

$$y^2 = ax^2 + bx + c \ , \tag{5}$$

$a,b,c \in \mathbb{Z}$, $a \neq 0$; et soit I l'ensemble des points de C à coordonnées x , y entières rationnelles. Alors :

- ou bien I est fini (éventuellement vide) ;
- ou bien I est infini ; dans ce cas, si on numérote les éléments (x,y) de I de telle manière que $|x_1| \leq |x_2| \leq \ldots$, il existe deux constantes réelles $\gamma > 0$ et $\mu > 0$ telles que

$$|x_n| \geq \gamma e^{\mu n} \ . \tag{6}$$

Démonstration : Posons $\Delta = b^2 - 4ac$. Par hypothèse, $\Delta \neq 0$. Si $a < 0$, C est une ellipse, et I est évidemment fini. Supposons donc $a > 0$ (C est alors une hyperbole) et distinguons deux cas :

a = un carré dans $\mathbb{Z}$ (ou C hyperbole à asymptotes rationnelles) : si $a = A^2$, A dans $\mathbb{Z}$, l'équation (5) peut s'écrire

$$(2Ay - 2ax - b)(2Ay + 2ax + b) = -\Delta \ ; \tag{7}$$

si I était infini, il existerait (principe de Dirichlet) un diviseur d de Δ et une infinité de couples d'entiers x,y tels que

$$2Ay - 2ax - b = d \ ; \tag{8}$$

l'hyperbole C et la droite d'équation (8) auraient donc une infinité de points communs : contradiction ([4]) ; I est donc toujours fini dans ce premier

cas (et il n'y a rien a prouver).

a non carré dans $\mathbb{Z}$ (ou C hyperbole à asymptotes irrationnelles) : l'équation (5) peut alors s'écrire

$$(9) \qquad (2ax+b)^2 - 4ay^2 = \Delta \quad ,$$

ou encore (avec $u = 2ax+b$, $v = 2y$, et -pour le plaisir de l'œil !- $D = a$)

$$(10) \qquad u^2 - Dv^2 = \Delta \quad ;$$

c'est une équation de Pell ("avec second membre", si l'on peut dire) dont toutes les solutions (entières) sont données par la formule suivante (voir par exemple [15], chap. 2, sect.7)

$$(11) \qquad u + v\sqrt{D} = \pm \varepsilon^z \alpha_j$$

($z \in \mathbb{Z}$, $1 \leq j \leq t$) avec les notations suivantes : ε , unité fondamentale (> 1) de l'ordre quadratique $\mathbb{Z}[\sqrt{D}]$; α_1 , α_2 , ..., α_t ($t \geq 0$, fini) , système maximal d'éléments de $\mathbb{Z}[\sqrt{D}]$ de norme Δ et deux à deux non équivalents (pour la divisibilité). Si $t = 0$, I est vide, donc fini, et il n'y a rien à prouver. Si au contraire $t \geq 1$, (10) admet une infinité de solutions, et si on les numérote de manière que $|u_1| \leq |u_2| \leq \ldots$, il est clair qu'on aura

$$(12) \qquad |u_{4kt+1}| \geq \gamma_1 \varepsilon^k \qquad (^5)$$

pour une constante $\gamma_1 > 0$ convenable et pour tout entier $k \geq 0$, et par conséquent aussi

$$(13) \qquad |u_m| \geq \gamma_2 e^{\lambda m}$$

pour deux constantes $\gamma_2 > 0$, $\lambda > 0$ convenables, et pour tout entier $m \geq 0$. La relation (6) à prouver résulte immédiatement de (13) , et de la formule de changement de variable $u = 2ax + b$. ∎

Cela étant, démontrons (toujours par l'absurde) que (1.2) implique (1.1), et supposons donc que $f(x)$ est un carré pour tout x dans $\mathbb{Z}$, mais que $f(X)$ n'est pas un carré dans $\mathbb{Z}[X]$. On peut alors écrire

$$(14) \qquad f(X) = r(X)\,[g(X)]^2 \quad ,$$

où $r(X)$, partie "quadratfrei" de $f(X)$ dans $\mathbb{Z}[X]$, n'est pas un carré dans $\mathbb{Z}[X]$, mais est tel que $r(x)$ (entier) soit un carré dans $\mathbb{Q}$, donc en fait dans $\mathbb{Z}$ (principal, donc intégralement clos) pour tout x dans $\mathbb{Z}$ (d'où il résulte en particulier que $r(X)$ n'est pas dans $\mathbb{Z}$, donc que $\rho = \deg(r(T)) \geq 1$). Considérons alors la courbe affine, plane, absolument irréductible, de genre $g = [\frac{\rho-1}{2}]$, définie par l'équation

$$y^2 = r(x) \quad ; \tag{15}$$

cette courbe possède évidemment une infinité de points entiers, d'où, par le théorème de Siegel ([7], chap.VII, th.4), $g = 0$, c'est-à-dire en fait $\rho = 1$ ou 2 . Mais l'éventualité $\rho = 1$ est exclue : on aurait alors en effet $r(x) = bx + c$ $(b \neq 0)$, et la progression arithmétique $\{bx+c\}_{x\in\mathbb{Z}}$ ne contiendrait que des carrés, ce qui est absurde pour au moins deux raisons (parce que cette progression contient des termes négatifs ; ou -mieux- parce que cette progression, de densité naturelle $1/|b| > 0$, ne peut être contenue dans l'ensemble des carrés de $\mathbb{Z}$, de densité naturelle nulle) ; l'éventualité $\rho = 2$ est elle aussi exclue : on aurait en effet $r(X) = aX^2 + bX + c$, $a \neq 0$, et comme $r(X)$ n'est pas un carré, on serait dans l'un des deux cas suivants :

1) $r(X) = A(Bx+C)^2$, A non carré dans $\mathbb{Z}$: mais il est alors évidemment exclu que $r(x) = A(Bx+C)^2$ soit un carré pour tout x ;

2) $r(X) = ax^2 + bx + c$ avec $b^2 - 4ac \neq 0$: mais si $r(x)$ est un carré pour tout x , l'ensemble I (lemme 1) est égal à $\mathbb{Z}$ tout entier, ce qui contredit (6) .

Contradiction dans tous les cas, et le th.1 se trouve démontré. ∎

Remarque 2 : On aura noté l'analogie entre le théorème de Dörge et le lemme 1 ; ces deux résultats (de type "archimédien") sont deux aspects du phénomène général suivant : étant donné une courbe plane $h(x,y) = 0$, la première projection de l'ensemble des points entiers de

cette courbe est, soit $\mathbb{Z}$ tout entier, soit un sous-ensemble très "dilué" de $\mathbb{Z}$. On aurait d'ailleurs pu, dans la démonstration n° 2, remplacer le lemme 1 par le lemme 2 ci-dessous, de caractère "non-archimédien" :

LEMME 2. Si le polynôme $aX^2 + bX + c$ n'est pas un carré dans $\mathbb{Z}[X]$, alors

a) ou bien $\Delta = b^2-4ac \neq 0$; ou bien $\Delta = 0$, mais a et c ne sont pas des carrés ;

b) dans les deux cas, il existe un entier x_o et un nombre premier p ayant la propriété suivante : quel que soit $x \equiv x_o \pmod p$, $ax^2 + bx + c$ est un non-carré modulo p , et (a fortiori) n'est pas un carré dans $\mathbb{Z}$.

Démonstration : a) est évident (voir d'ailleurs la fin de la démonstration n° 2). Pour prouver b), séparons les deux cas $\Delta = 0$ et $\Delta \neq 0$.

Si $\Delta = 0$, c n'est pas un carré ; il suffit alors de prendre $x_o = 0$ et p premier quelconque tel que $(\frac{c}{p}) = -1$ (c'est-à-dire p ne divisant pas c , et inerte dans le corps quadratique $\mathbb{Q}(\sqrt{c})$).

Si $\Delta \neq 0$, soit p premier impair, ne divisant pas a , et tel que $(\frac{\Delta}{p}) = +1$ (si Δ est un carré dans $\mathbb{Z}$, tout p ne divisant pas Δ convient ; sinon, se limiter aux p ne divisant pas Δ et décomposés dans le corps quadratique $\mathbb{Q}(\sqrt{\Delta})$) . L'image $\bar{f}(X)$ du polynôme $f(X) = aX^2+bX+c$ dans $\mathbb{F}_p[X]$ est de la forme $\alpha(X-\beta)(X-\gamma)$, $\alpha \neq 0$, $\beta \neq \gamma$; lorsque ξ décrit $\mathbb{F}_p$, les valeurs de $\bar{f}(\xi)$, modulo les carrés ([6]) , sont les mêmes que celles de la fonction homographique

$$\varphi(\xi) = \alpha \frac{\xi-\beta}{\xi-\gamma} \quad ; \tag{16}$$

cette fonction prend toute valeur dans $\mathbb{F}_p$, à l'exception de α ; par ailleurs, $\mathbb{F}_p$ contient $\frac{p-1}{2}$ non-carrés ; si donc on impose $p \geq 5$, il existera certainement un $\xi_o \in \mathbb{F}_p$ tel que $\varphi(\xi_o)$ et par suite $\bar{f}(\xi_o)$ ne soit pas un carré dans $\mathbb{F}_p$; il suffit donc finalement de prendre $p \geq 5$, ne divisant pas a ,

et tel que $(\frac{\Delta}{p}) = +1$, puis $x_o \in \mathbb{Z}$ tel que $\bar{x}_o = \xi_o$. ■

Si d'ailleurs on combine ce lemme avec la démonstration n° 2 du théorème 1, on voit que le lemme 2 est vrai pour n'importe quel polynôme f(X) (et pas seulement pour un polynôme du second degré). D'où le résultat suivant, qui renforce le théorème 1, et qui est un aspect particulier d'un phénomène qu'on va étudier en détail dans ce qui suit :

THEOREME 1 bis. Soit f(X) un élément de $\mathbb{Z}[X]$, et soit I l'ensemble des entiers x tels que f(x) soit un carré. Supposons que l'ensemble I rencontre toute progression arithmétique. Alors, f(X) est un carré dans $\mathbb{Z}[X]$.

*

Quoi qu'il en soit, le théorème 1 se trouve démontré. On peut essayer de le renforcer ou de le généraliser de plusieurs manières :

- soit en modifiant la condition (1.1), ce, en exigeant par exemple que f(T) soit un cube, une puissance quatrième, etc..., dans $\mathbb{Z}[T]$; ou encore une somme de deux carrés, de trois carrés, etc..., dans $\mathbb{Z}[T]$;
- soit en modifiant (plus précisément, en affaiblissant) la condition (1.2), ce, en remplaçant la contrainte universelle : "quel que soit x dans $\mathbb{Z}$" par une contrainte plus faible, telle que celle figurant dans le théorème 1 bis ;
- soit enfin en modifiant simultanément (et "parallèlement") les conditions (1.1) et (1.2) comme il vient d'être dit.

Le but de l'exposé est de décrire une "bonne" manière d'affaiblir la condition (1.2) (voir §2 ci-dessous), puis de donner (§§3-4) une liste de résultats analogues au théorème 1, valables avec une propriété (1.1) modifiée, et sous une condition (1.2) modifiée et "affaiblir comme au §2". ([7])

2. ENSEMBLES EXCELLENTS.

La définition suivante ("à usage interne") est justifiée, si l'on veut, par le théorème 1 bis :

DEFINITION 1. Un sous-ensemble E de $\mathbb{Z}$ est dit excellent s'il rencontre toute progression arithmétique, ou encore, si toute progression arithmétique contient au moins un élément de E.

Remarques :

a) Si E est excellent, toute progression arithmétique contient en fait une infinité d'éléments de E : car toute progression arithmétique contient une infinité de sous-progressions deux à deux disjointes ([8]) dont chacune contient par hypothèse au moins un élément de E.

b) Dans la définition 1, on aurait pu remplacer "toute progression arithmétique" par "toute progression de raison puissance d'un nombre premier" (appliquer le théorème chinois). On voit d'ailleurs ainsi qu'un ensemble E est excellent s'il est p-adiquement dense dans $\mathbb{Z}$ pour tout p premier, ou -ce qui revient au même- s'il est dense dans $\mathbb{Z}_p$ pour tout p premier.

c) En revanche, un ensemble excellent peut être extrêmement "dilué" du point de vue archimédien : si par exemple on se donne une suite $\{a_n\}_{n\geq 0}$ d'entiers strictement positifs, et si on pose $e_n = n!a_n + n$, alors l'ensemble E des valeurs de la suite $\{e_n\}_{n\geq 0}$ est évidemment excellent : la progression arithmétique $\{b+kN\}_{k\geq 0}$ contient tous les e_n tels que $n \geq N$ et $n \equiv b \pmod N$ mais il est clair que E peut être rendu arbitrairement "dilué" par choix d'une suite $\{a_n\}$ tendant arbitrairement vite vers l'infini.

3. LISTE DE THEOREMES.

Avec la définition 1, le théorème 1 bis signifie que le théorème 1 reste vrai quand on y remplace la condition "pour tout x dans $\mathbb{Z}$ ..." par la même condition affaiblie en "pour tout x dans un sous-ensemble excellent (fixé) de $\mathbb{Z}$ ..." ; si d'autre part on y remplace "carré" par "puissance k-ième"

($k \geq 2$ fixé), ce théorème demeure toujours valable. D'où au total l'énoncé suivant :

THEOREME 2. Soient $f(X)$ un élément de $\mathbb{Z}[X]$, et $k \geq 2$ un exposant entier. Si l'ensemble des x pour lesquels $f(x)$ est une puissance k-ième est excellent, alors $f(X)$ est lui-même une puissance k-ième dans $\mathbb{Z}[X]$.

Ce théorème 2 est d'ailleurs un cas particulier (avec $h(X,Y) = f(X) - Y^k$) du théorème suivant :

THEOREME 3. (Davenport, Lewis, Schinzel [3]). Soit $h(X,Y)$ un polynôme à deux variables et à coefficients entiers rationnels. Soit I l'ensemble des x tels que l'équation à une inconnue Y : $h(x,Y) = 0$, admet une solution entière y. Alors, si I est excellent, il existe un polynôme $g(X)$ à coefficients rationnels ([9]) tel qu'on ait ("identiquement")

$$h(X,g(X)) = 0 . \tag{17}$$

Revenons au théorème 1 bis ; si on y remplace "carré" par "somme de deux carrés", il reste encore vrai ([10]) :

THEOREME 4. Soit $f(X)$ un élément de $\mathbb{Z}[X]$, et soit I l'ensemble des x tels que $f(x)$, soit somme de deux carrés dans $\mathbb{Z}$. Alors, si I est excellent, il existe $u(X)$ et $v(X)$ dans $\mathbb{Z}[X]$ tels que

$$f(X) = [u(X)]^2 + [v(X)]^2 , \tag{18}$$

autrement dit, $f(X)$ est lui-même somme de deux carrés dans $\mathbb{Z}[X]$.

Ce théorème est conséquence du résultat plus général ci-dessous :

THEOREME 5. (Davenport, Lewis, Schinzel [3]). Soit $f(X)$ un polynôme à coefficients rationnels (non nécessairement entiers). Soit d'autre part K une extension galoisienne de degré fini n de $\mathbb{Q}$, et soit $\omega_1, \omega_2, \ldots, \omega_n$ une base d'entiers pour $K/\mathbb{Q}$. Soit enfin I l'ensemble

des entiers rationnels x tels qu'il existe u_1 , u_2 , ... , u_n , eux-mêmes entiers rationnels, avec

(19) $$f(x) = N_{K/Q}(u_1\omega_1 + \ldots + u_n\omega_n)$$ ([11])

Si I est excellent, et si $K/\mathbb{Q}$ vérifie l'une des hypothèses suivantes :

(H_1) $K/\mathbb{Q}$ est cyclique ;

(H_2) le degré $n = [K:\mathbb{Q}]$ est premier avec la multiplicité de chacun des zéros de $f(X)$ (disons, dans $\mathbb{C}$) ; ([12])

alors il existe n polynômes $u_1(X)$, $u_2(X)$, ... , $u_n(X)$, à coefficients rationnels, tels qu'on ait, dans l'anneau de polynômes $\mathbb{Q}[X]$:

(20) $$f(X) = N_{K/Q}(u_1(X)\omega_1 + \ldots + u_n(X)\omega_n) .$$

Signalons que ce théorème devient faux en général si, $f(X)$ étant à coefficients entiers, on essaie d'imposer aux $u_i(X)$ d'être eux-mêmes à coefficients entiers. Prenons en effet ([3], p.116)

$$K = \mathbb{Q}(\sqrt{-23}) \quad \text{(cyclique sur } \mathbb{Q}) ;$$

$$(\omega_1, \omega_2) = (1, \frac{-1+\sqrt{-23}}{2}) ;$$

$$N(u_1, u_2) = N_{K/Q}(u_1\omega_1 + u_2\omega_2) = u_1^2 + u_1u_2 + 6u_2^2 ;$$

$$f(X) = 2X^2(X+1)^2 + 3X(X+1) + 4 .$$

Un calcul immédiat montre que si on pose $t = t(X) = \frac{1}{2}X(X+1)$, on a

$$f(X) = N(t+2, t) ;$$

$f(X)$ vérifie donc à la fois les hypothèses et la conclusion du théorème 5 ; mais, bien que $f(X)$ soit dans $\mathbb{Z}[X]$, il est impossible de trouver $u_1(X)$ et $u_2(X)$ dans $\mathbb{Z}[X]$ et tels que

(21) $$f(X) = N(u_1(X), u_2(X)) ;$$

car l'égalité (21) mènerait, en identifiant les coefficients dominants des deux membres, à une égalité $2 = a^2+ab+6b^2$: absurde, 2 n'étant pas norme d'entiers dans $\mathbb{Q}(\sqrt{-23})/\mathbb{Q}$.

Signalons également le résultat suivant :

THEOREME 6. (Davenport, Lewis, Schinzel [4]). Soient T une indéterminée et $a(T)$, $b(T)$ des polynômes de T à coefficients entiers rationnels. Soit I l'ensemble des entiers t tels que l'équation

$$a(t)x^2 + b(t)y^2 = z^2 \tag{22}$$

admette une solution entière non triviale (x,y,z) . Alors, si I est excellent, il existe trois polynômes $x(T)$, $y(T)$ et $z(T)$ à coefficients entiers, non identiquement nuls, et tels que

$$a(T)\,[x(T)]^2 + b(T)\,[y(T)]^2 = [z(T)]^2 \ . \tag{23}$$

*

Le §4 donne une démonstration du théorème 3 (et la manière d'en déduire le théorème 2) , ainsi qu'une démonstration du théorème 4. Pour des démonstrations des théorème 5 et 6 , voir [3] et [4] (la démonstration du théorème 5 sous l'hypothèse (H_1) est analogue à celle du théorème 4 ; cette démonstration sous l'hypothèse (H_2) est nettement plus pénible ; la démonstration du théorème 6 est tout à fait élémentaire à partir du moment où on sait prouver le théorème 4). Les démonstrations utilisent essentiellement le théorème d'irréductibilité de Hilbert, et les résultats classiques sur les idéaux premiers de $\mathbb{Q}$ décomposés dans une extension finie donnée $K/\mathbb{Q}$.

*

Indiquons pour conclure que le théorème 1, qui reste vrai (th.4) si on y remplace "carré" par "somme de deux carrés", devient au contraire faux pour "somme de trois carrés" et pour "somme de quatre carrés". Posons en effet

$$f(X) = 112X^2 + 1 \tag{24}$$

($112 = 7.16 = 4^2.7$). Alors :

a) quel que soit x entier, $f(x)$ est somme de trois carrés d'entiers ;

b) $f(X)$ n'est pas somme de trois carrés dans $\mathbb{Z}[X]$;

c) $f(X)$ n'est même pas somme de quatre carrés dans $\mathbb{Z}[X]$.

Démonstration : a) est immédiat : en effet, $116 \equiv 0 \pmod 8$, et $f(x) \equiv 1 \pmod 8$ pour tout x entier. Il en résulte que $f(x)$ est toujours impair, mais n'est jamais de la forme $8m + 7$: $f(x)$ est donc toujours somme de trois carrés (voir par exemple [12], pp.79-80) .

b) est non moins immédiat : si $f(X)$ était somme de trois carrés dans $\mathbb{Z}[X]$, il s'agirait obligatoirement de carrés de binômes du 1er degré (au plus) ; on pourrait écrire

$$f(X) = (a_1X + b_1)^2 + (a_2X + b_2)^2 + (a_3X + b_3)^2 \quad , \tag{25}$$

et on aurait $112 = 4^2.7 = a_1^2 + a_2^2 + a_3^2$; absurde, puisque 112, de la forme $4a(8m+7)$, n'est pas somme de trois carrés dans $\mathbb{Z}$.

c) est plus difficile. En fait, on peut prouver que $f(X)$ n'est pas somme de quatre carrés dans $\mathbb{Q}[X]$ en utilisant un critère dû à Pourchet ([14], p. 100, prop.10) . Comme $f(X)$ est défini positif et irréductible sur $\mathbb{Q}$, il s'agit de vérifier que -1 n'est pas somme de deux carrés dans le corps des racines de $f(X)$. Mais ce corps est $\mathbb{Q}(\sqrt{-7})$, qu'on peut plonger dans $\mathbb{Q}_2$ (corps des nombres 2-adiques), et il est bien connu que dans $\mathbb{Q}_2$, -1 est somme de quatre carrés, mais non de deux (se ramener au même énoncé pour $\mathbb{Z}_2$, puis pour $\mathbb{Z}/8\mathbb{Z} \simeq \mathbb{Z}_2/2^3\mathbb{Z}_2$, et faire alors la vérification "à la main".) ∎

4. DEMONSTRATIONS.

Démonstration du théorème 3. On ne diminue évidemment pas la généralité en supposant

(4.1) que $h(X,Y)$ est sans facteur carré dans $\mathbb{Q}[X,Y]$, soit

(26) $h(X,Y) = h_1(X,Y)\ldots h_m(X,Y)$,

$m \geq 1$, les $h_i(X,Y)$ irréductibles sur $\mathbb{Q}$ et deux à deux distincts ;

(4.2) que pour chaque i $(1 \leq i \leq m)$, il existe une infinité de x tels que l'équation

(27) $h_i(x,Y) = 0$

admette une solution entière y .

Mais alors

LEMME 3. L'un au moins des polynômes $h_i(X,Y)$ est de degré 1 par rapport à Y .

Prouvons ce lemme par l'absurde, en supposant que $n_i = \deg_Y h_i \geq 2$ pour $i = 1,\ldots,m$. Utilisant l'hypothèse (4.1) et le théorème d'irréductibilité de Hilbert ([7], chap. VIII, §§1-2), on voit qu'il existe un <u>entier</u> x_o tel que chaque polynôme $h_i(x_o,Y)$ (à coefficients entiers et à <u>une</u> variable) soit irréductible et de degré n_i (en Y). Soit (pour chaque i) η_i une racine du polynôme $h_i(x_o,Y)$, et posons $K_i = \mathbb{Q}(\eta_i)$. Comme $[K_i : \mathbb{Q}] = n_i \geq 2$, la densité de $\mathrm{Spl}^1(K_i)$ est <u>strictement inférieure à</u> 1 (voir l'exposé [6] , ou encore [1] , chap. VIII, et p. 361, exercice 6 (^{13})) : on peut donc (pour chaque i) trouver un nombre premier (en fait, une infinité) assez grand, q_i , n'admettant dans K_i <u>aucun</u> facteur premier (idéal) de degré 1 , et donc tel (théorème de Kummer : [1], pp. 92-93) que la congruence

(28) $h_i(x_o,Y) \equiv 0 \pmod{q_i}$

<u>n'admette pas</u> de solution entière y . Mais soit $q = q_1 q_2 \ldots q_m$: par hypothèse (I excellent), il existe $x \equiv x_o \pmod{q}$ et y (entier) tels que

(29) $h(x,y) = h_1(x,y) \ldots h_m(x,y) = 0$.

Pour un indice i au moins, on a donc $h_i(x,y) = 0$, et a fortiori $h_i(x_o,y) \equiv 0 \pmod{q}$, donc $h_i(x_o,y) \equiv 0 \pmod{q_i}$: contradiction.

Le lemme 3 permet de supposer (par exemple) $\deg_Y h_1 = 1$,

c'est-à-dire

(30) $$h_1(X,Y) = a(X)Y - b(X) \quad ,$$

avec (irréductibilité sur $\mathbb{Q}$) $a(X)$ et $b(X)$ premiers entre eux dans $\mathbb{Q}[X]$; il existe alors d entier non nul (^{14}) et $u(X)$, $v(X)$ dans $\mathbb{Z}[X]$ tels que

(31) $$a(X)u(X) + b(X)v(X) = d \quad .$$

Utilisant maintenant l'hypothèse (4.2), on voit qu'il existe une infinité de x entiers tels que $a(x)Y - b(x) = 0$ ait une solution entière y ; laissant de côté les x en nombre fini tel que $a(x) = 0$, on voit ainsi qu'il existe une infinité de x tels que $a(x)$ divise $b(x)$, donc (par (31)) que $a(x)$ divise d : mais ceci signifie que $a(X)$ est une constante non nulle, et il suffit pour vérifier le théorème 3 de prendre

$$g(X) = a^{-1}b(X) \in \mathbb{Q}[X] \quad . \quad \blacksquare$$

*

Démonstration du théorème 2. Le théorème 3, appliqué à $h(X,Y) = f(X) - Y^k$, montre que si $f(x)$ est une puissance k-ième pour tout x dans un ensemble excellent, alors $f(X) = [g(X)]^k$ pour $g(X) \in \mathbb{Q}[X]$. Mais $g(X)$ est alors (dans le corps $\mathbb{Q}(X)$) entier sur l'anneau $\mathbb{Z}[X]$, lequel est factoriel et donc intégralement clos : $g(X)$ est donc en fait dans $\mathbb{Z}[X]$, comme annoncé. ■

(Naturellement, le même raisonnement s'applique, dans le théorème 3, lorsque $h(X,g) = 0$ est une équation de dépendance intégrale pour g sur l'anneau $\mathbb{Z}[X]$.)

*

Démonstration du théorème 5. On sait que dans $\mathbb{Q}$, tout entier qui est somme de deux carrés est, en fait, somme de deux carrés d'entiers (voir par exemple [12], p. 80, "lemme de Davenport-Cassels" ; la même propriété est d'ailleurs vraie, mutatis mutandis, dans $\mathbb{Q}(X)$: voir [16]). Ceci

permet de supposer $f(X)$ sans facteur carré dans $\mathbb{Q}[X]$ et d'écrire

$$f(X) = cf_1(X) \dots f_m(X) \quad , \tag{32}$$

$m \geq 1$, les $f_i(X)$ irréductibles dans $\mathbb{Z}[X]$ et deux à deux distincts, c dans $\mathbb{Z}$.

On a alors les trois lemmes suivants :

LEMME 4. Pour chaque i $(1 \leq i \leq m)$, soit $q = q_i$ un nombre premier assez grand ayant un facteur premier (idéal) de degré 1 dans $K_i = \mathbb{Q}(\eta_i)$, où η_i désigne une racine du polynôme $f_i(X)$ ([15]) . Alors :

a) la congruence $f_i(X) \equiv 0 \pmod{q}$ admet une solution entière x ;

b) le nombre premier q est décomposé dans le corps quadratique $\mathbb{Q}(\sqrt{-1})$.

Prouvons ce lemme : a) est conséquence du théorème de Kummer déjà cité ([1], pp. 92-93). Passons à b) : $f(X)$ a évidemment toutes ses racines distinctes, d'où $(f(X), f'(X)) = 1$ dans $\mathbb{Q}[X]$, et (comme en (31)) une "identité de Bezout"

$$f(X)u(X) + f'(X)v(X) = d \quad , \tag{33}$$

$u(X)$, $v(X) \in \mathbb{Z}[X]$, $d \in \mathbb{Z}$, $d \neq 0$. Par choix de q , et en utilisant a) , on peut supposer $q > |d|$, et on peut trouver x_o entier tel que $f_i(x_o) \equiv 0 \pmod{q}$: (33) implique alors que $f'(x_o) \not\equiv 0 \pmod{q}$. Mais la formule de Taylor, écrite

$$f(x_o+q) = f(x_o) + qf'(x_o) + q^2 e \quad ,$$

$e \in \mathbb{Z}$, montre alors que l'un (soit x_1) des deux entiers x_o et x_o+q vérifie

$$f_i(x_1) \equiv 0 \pmod{q} \ , \quad f(x_1) \not\equiv 0 \pmod{q^2} \ ,$$

c'est-à-dire

$$f_i(x_1) \equiv 0 \pmod{q} \ , \ f_i(x_1) \not\equiv 0 \pmod{q^2} \ \text{ et } \ f_j(x_1) \not\equiv 0 \pmod{q} \tag{34}$$
pour $j \neq i$, $1 \leq j \leq m$.

Par hypothèse (I excellent), il existe d'autre part $x_2 \equiv x_1 \pmod{q^2}$ tel que

$$f(x_2) = a^2+b^2 \quad , \quad a,b \in \mathbb{Z} \ . \tag{35}$$

Les congruences ou non-congruences (34) restent évidemment vraies si on y remplace x_1 par x_2 : compte tenu de (35) , elles montrent alors que $q \mid (a^2+b^2)$, mais que $q^2 \nmid (a^2+b^2)$, ce qui, combiné avec le théorème des deux carrés ([16]) , implique bien $q \equiv 1 \pmod 4$, donc q décomposé dans le corps quadratique $\mathbb{Q}(\sqrt{-1})$, comme annoncé.

LEMME 5. Soit $g(X)$ un polynôme à coefficients entiers, irréductible sur $\mathbb{Q}$, et soit θ une racine de $g(X)$ (dans une clôture algébrique donnée de $\mathbb{Q}$). Posons $L = \mathbb{Q}(\theta)$, et soit K un corps intermédiaire entre $\mathbb{Q}$ et L . Il existe alors $g_K(X) \in K[X]$, de degré $[L:K]$, et $a \in \mathbb{Z}$, tels que

$$g(X) = aN_{K/Q}(g_K(X)) \ . \tag{36}$$

Prouvons ce lemme : Posons $M = [K:\mathbb{Q}]$, soit ω un élément primitif de K , et soient $\omega_1 = \omega , \omega_2, \ldots, \omega_M$ les conjugués de ω sur $\mathbb{Q}$. Comme $K \subset L = \mathbb{Q}(\theta)$, on peut écrire $\omega = h(\theta)$, avec $h(X) \in \mathbb{Q}[X]$. Posons alors

$$k(X) = \prod_{\mu=1}^{M} [h(X)-\omega_\mu] \ ; \tag{37}$$

$k(X)$ est dans $\mathbb{Q}[X]$ et vérifie $k(\theta) = 0$ (puisque $h(\theta) = \omega = \omega_1$) ; $k(X)$ et $g(X)$ ont donc un facteur commun dans $L[X]$, et aussi dans $\mathbb{Q}[X]$; mais $g(X)$ a été supposé irréductible sur $\mathbb{Q}$: $g(X)$ divise donc $k(X)$. Soit alors $k_\mu(X)$ le p.g.c.d. (dans $K[X]$) de $g(X)$ et $h(X)-\omega_\mu$; les $k_\mu(X)$ divisent $g(X)$, sont premiers entre eux deux à deux ([17]) et forment une famille de conjugués sur $\mathbb{Q}$; leur produit divise donc $g(X)$ et on a

$$g(X) = \ell(X)\ N_{K/Q}(k_1(X)) \ , \tag{38}$$

les deux facteurs de droite étant dans $\mathbb{Q}[X]$; $g(X)$ étant irréductible sur $\mathbb{Q}$, et le second facteur non constant, on a sûrement $\ell(X)$ = un polynôme constant a : d'où le lemme 5 , avec $g_K(X) = k_1(X)$.

LEMME 6. Soient K et L deux extensions algébriques de degré fini de $\mathbb{Q}$, contenue dans une même clôture algébrique de $\mathbb{Q}$. Faisons les deux hypothèses suivantes :

(H_1) $K/\mathbb{Q}$ est galoisienne ;

(H_2) tout p premier assez grand ayant un facteur premier (idéal) de degré 1 dans L, admet aussi un facteur premier (idéal) de degré 1 dans K.

Alors K est un sous-corps de L.

Ce lemme n'est autre que le "théorème de Bauer" : voir (pour une démonstration) [6], ou [1], chap. VIII et exercice 6.1, p. 362 (^{18}).

Cela étant, prouvons le théorème 5 : le lemme 4, b), et le lemme 6, avec $L = K_i$, et $K = \mathbb{Q}(\sqrt{-1})$, montrent que $K \subset K_i$ pour $i = 1,\ldots,m$. Le lemme 5 permet alors d'écrire (faire $g(X) = f_i(X)$)

$$f_i(X) = a_i N_{K/Q}(g_{i,K}(X)) \tag{39}$$

pour $i = 1,\ldots,m$, et K désignant toujours $\mathbb{Q}(\sqrt{-1})$. Par multiplication, (32) et (39) donnent

$$f(X) = a N_{K/Q}(g(X)) , \tag{40}$$

avec $a = ca_1a_2\ldots a_m$ = un entier rationnel, et $g(X) = g_{1,K}(X)\ldots g_{m,K}(X) \in K[X]$. En donnant à X une valeur x telle que $f(x)$ soit une somme de deux carrés, donc une norme dans $K/\mathbb{Q}$, on voit que a est lui-même une norme dans $K/\mathbb{Q}$. (40) peut ainsi s'écrire (multiplicativité de la norme, fait que $K = \mathbb{Q}(\sqrt{-1})$, et changement de notation évident)

$$f(X) = [u_1(X)]^2 + [v_1(X)]^2 , \tag{41}$$

avec $u_1(X)$, $v_1(X) \in \mathbb{Q}[X]$.

Reste à prouver que (quitte à modifier leur choix), on peut supposer ces deux polynômes dans $\mathbb{Z}[X]$. Dans l'anneau <u>factoriel</u> $\mathbb{Z}[\sqrt{-1},X]$, écrivons

$$u_1(X) + \sqrt{-1}.v_1(X) = \alpha w(X) , \tag{42}$$

avec $w(X)$ primitif. On a alors (voir (41))

$$f(X) = \alpha\bar{\alpha}\, w(X)\,\bar{w}(X) \quad ,$$

$w(X)\bar{w}(X)$ étant primitif (lemme de Gauss !) et $f(X)$ à coefficients entiers (par hypothèse) : mais alors $\alpha\bar{\alpha}$ est entier rationnel et norme (de α) dans $K/\mathbb{Q}$, donc somme de deux carrés dans $\mathbb{Z}$ ("lemme de Davenport-Cassels" déjà cité). Il suffit alors de poser $\alpha = a^2+b^2$, puis

$$\alpha = a+b\sqrt{-1} \quad ,$$

$$u(X) + \sqrt{-1}.v(X) = (a+b\sqrt{-1})w(X)$$

$(a,b \in \mathbb{Z})$, pour avoir $u(X)$, $v(X) \in \mathbb{Z}[X]$ et naturellement

$$f(X) = [u(X)]^2 + [v(X)]^2 \quad ,$$

c.q.f.d. ■

Notes "de pied" (comme dirait Delange)

(1) L'auteur avoue n'avoir pas vu la référence [5]. Signalons par ailleurs qu'une partie de ce qui suit reste valable si on y remplace "carré" par "puissance k-ième", et que la démonstration n° 2 est donnée pour son caractère "instructif", mais non pour sa simplicité !

(2) Dans ces quelques lignes, x désigne exceptionnellement une variable réelle (donc un élément transcendant sur $\mathbf{R}$) et non une valeur entière de X.

(3) Voir d'ailleurs les démonstrations des th.3 et 4 .

(4) On a supposé C non décomposée.

(5) Ceci parce que les solutions de (10) se groupent "4t par 4t", avec

$$u+v\sqrt{D} = \pm\varepsilon^{\pm k}\alpha_j \quad (1 \le j \le t) .$$

(6) Multiplicativement, bien entendu. On laisse de côté le petit ennui correspondant à $\xi = \gamma$.

(7) Bibliographie : [10], [5], [8], [3], [4], [2], [9], [13], [11] .

(8) Petit exercice laissé au lecteur.

(9) Il n'y a aucune raison en général pour que les coefficients soient entiers (exemple : $h(X,Y) = X(X+1) - 2Y$).

(10) Bien qu'on ne connaisse pas de contre-exemples, il semble peu probable que le théorème 4 reste vrai pour "deux cubes", "deux puissances quatrièmes", etc...

(11) Ce qui signifie simplement que $f(x)$ est une norme d'entier dans $K/\mathbb{Q}$.

(12) Au prix de pénibles contorsions, on peut d'ailleurs étendre le théorème 5 à des extensions K de $\mathbb{Q}$ non galoisiennes, mais satisfaisant à des conditions assez particulières. Voir [9] et [13].

(13) Si K est une extension finie (galoisienne ou non) de $\mathbb{Q}$, $Spl^1(K)$ désigne l'ensemble des p premiers ayant dans K au moins un facteur premier (idéal) de degré 1. La densité dont il est question est la densité (analytique, ou naturelle) dans l'ensemble des nombres premiers. Voir [6] ou [1].

.../...

(^{14}) $\mathbb{Q}[X]$ est principal, mais non $\mathbb{Z}[X]$; a(X) et b(X) peuvent avoir un facteur commun entier (non trivial) dans $\mathbb{Z}[X]$: dans l'identité de Bezout (31), d n'est donc pas forcément égal à 1 .

(^{15}) Dans l'énoncé et la démonstration du lemme 4, i est fixé, et on écrit q au lieu de q_i pour alléger l'écriture. Ce choix de q est possible parce que la densité de $Spl^1(K_i)$ (voir Note (^{13})) est au moins égale à $1/n_i$, $n_i = [K_i:\mathbb{Q}]$.

(^{16}) Voir n'importe quel "First Course in Number Theory", ou encore le "p'tit Samuel", p. 96, proposition 2. Comme on suppose q "assez grand", donc impair, on a en fait équivalence entre "$q \equiv 1 \pmod 4$", "q somme de deux carrés", "q décomposé dans $\mathbb{Q}(\sqrt{-1})$" et "il existe un entier N somme de deux carrés (ici, $N = f(x_2)$) tel que l'exposant de q dans N soit impair (ici, égal à 1)".

(^{17}) Parce que les $h(X) - \omega_\mu$ sont déjà premiers entre eux deux à deux, leurs différences deux à deux étant du type $\omega_\mu - \omega_\lambda$ = des constantes non nulles.

(^{18}) Indiquons quand même le principe de la démonstration. Avec la notation Spl^1 (voir notes (^{13}) et (^{15})) et en ignorant pour simplifier les nombres premiers ramifiés dans KL , on a $Spl^1(KL) = Spl^1(K) \cap Spl^1(L) = Spl^1(L)$ (la première égalité valable en général, la seconde valable parce que (H_2) équivaut à $Spl^1(L) \subset Spl^1(K)$) . Soit alors ν le degré de l'extension galoisienne KL/L , $Spl^1(KL) = Spl^1(L)$ implique que la densité (analytique) des idéaux premiers de degré 1 de L complètement décomposés dans KL est égale à 1 ; cette densité est d'autre part égale à $1/\nu$ (théorème d'Artin-Tchebotarev pour la classe de conjugaison de l'élément neutre : voir les exposés [6] et [17] , ou [1], chap. 8). On a donc $\nu = 1$, d'où $KL = L$ et $K \subset L$, c.q.f.d.

BIBLIOGRAPHIE

[1] CASSELS + FRÖHLICH - Algebraic Number Theory, Academic Press (1967).

[2] CHOWLA - Some problems of elementary number theory, J. Crelle, 222 (1966), 71-74.

[3] DAVENPORT, LEWIS, SCHINZEL - Polynomials of certain special types, Acta arithm., 9 (1964), 107-116.

[4] DAVENPORT, LEWIS, SCHINZEL - Quadratic diophantine equations with a parameter, Acta arithm., 11 (1966), 353-358.

[5] FRIED + SURANYI - Neuer Beweis eines Zahlentheoretisches Satzes über Polynome, Matematikai Lapok, 11, (1960), 75-84.

[6] GAUTHIER - Ensembles de nombres premiers..., chap. I, séminaire de Théorie des Nombres, Grenoble, 1974-1975.

[7] LANG - Diophantine Geometry, Interscience (1962).

[8] LEVEQUE - On the equation $y^m = f(x)$, Acta arithm., 9 (1964), 209-219.

[9] LEWIS, SCHINZEL, ZASSENHAUS - An extension of the theorem of Bauer, and Polynomial of certain special types, Acta arithm., 11 (1966), 345-352.

[10] POLYA + SZEGÖ - Aufgaben und lehrsätze aus der Analysis, II ter Band, Springer (1954).

[11] RIBENBOIM - Polynomial whose values are powers, J. Crelle, 22 (197), 34-40.

[12] SERRE - Cours d'arithmétique, P.U.F. (1970).

[13] SCHINZEL - On a theorem of Bauer and some of its applications, I, Acta arithm., 11 (1966), 333-344 ; II, ibid., 22 (1973), 221-231.

[14] POURCHET - Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques, Acta arithm. 19 (1971), 89-104.

.../...

[15] BOREVICH + SHAFAREVICH - Number Theory. Academic Press (1966).

[16] CASSELS - On the representation of rational functions as sums of squares, Acta arithm., 9 (1964), 79-82 .

-:-:-:-