Représentation des nombres par des formes décomposables I

Par K. GYŐRY (Debrecen)

Dédié au 60ième anniversaire de MM. les Professeurs B. Barna, L. Gyarmathi et B. Gyires

§ 1. Introduction

Soit K un corps algébrique de degré $n \geqq 2$ et soient $1, \alpha_2, \ldots, \alpha_m \in K$ des nombres linéairement indépendants dans le corps rationnel R tels que $K = R(\alpha_2, \ldots, \alpha_m)$. Désignons par N la norme dans le corps K et considérons la forme

$$N(x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m)$$

à coefficients rationnels de degré n. Un problème beaucoup étudié est de déterminer les conditions pour que l'équation

$$N(x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m) = a; \quad a \in R \tag{1}$$

admette un nombre infini de solutions $\mathbf{x} = (x_1, \ldots, x_m)$ en entiers rationnels.

Dans le cas $m = n$, s'il existe une solution entière de l'équation (1) pour une valeur donnée a, alors il y a aussi une infinité de solutions, lesquelles peuvent être caracterisées complètement à l'aide des unités (voir par ex. [1], p. 134—140.)

Le problème est beaucoup plus difficile si $m < n$. Désignons par M le module engendré par $1, \alpha_2, \ldots, \alpha_m$ et soit L l'espace vectoriel sur le corps rationnel R, engendré par M. On appelle le module M dégénéré s'il existe un sous-espace L' de L tel que $\gamma L' = K'$ pour un $\gamma \in K$ et pour un sous-corps K' différent de R et des corps quadratiques imaginaires. Il est connu (voir [1], p. 322.) que si M est dégénéré, alors pour un certain $a \in R$ l'équation (1) a aussi une infinité de solutions en entiers rationnels. Dans la direction opposée, la conjecture suivante est probablement vraie ([1], p. 322.). *Si le module M est non dégénéré, alors l'équation* (1) *n'a qu'un nombre fini de solutions en entiers rationnels.*

Comme il est connu, pour $m = 2$ et pour $m = 3$ la conjecture a été démontrée par A. THUE [8] et par W. M. SCHMIDT [6] respectivement. Pour $m = 4$ et $m = 5$ il y a aussi des résultats nontriviaux [4], [6] et [3] (voir le § 2. et § 3.) Enfin il faut mentionner le résultat général de C. L. SIEGEL [7] qui a prouvé que si n est assez grand par rapport à m et $\alpha_i = \vartheta^{i-1}$ $(i = 1, \ldots, m)$, alors le nombre de solutions de (1) est limité.

Dans ce travail, nous considérons l'équation (1) dans deux cas spéciaux: celui

où K est un corps abélien imaginaire et celui où K est un corps cyclotomique. Entre autres, nous prouvons la conjecture citée pour $m=4$ dans le cas où K est un corps abélien imaginaire de degré n tel que $3\nmid n$ et $4\nmid n$, en appliquant le théorème de Kronecker concernant les unités des corps cyclotomiques.

§ 2. Formes décomposables dans un corps abélien imaginaire

Désignons par E_m l'espace euclidien réel à m dimensions et soient $L^{(1)}(\mathbf{x}), \ldots, L^{(n)}(\mathbf{x})$ les facteurs linéaires de la forme $N(L(\mathbf{x}))$ définie dans l'introduction. Soit r le nombre maximal des formes $L^{(i_1)}, \ldots, L^{(i_r)}$ telles que

$$L^{(i_1)}(\mathbf{a})=0, \ldots, L^{(i_r)}(\mathbf{a})=0 \tag{2}$$

pour un $0\neq\mathbf{a}\in E_m$. Si $m=4$ et $6r<n$, alors l'équation (1) n'a qu'un nombre fini de solutions en entiers rationnels (voir [6] ou [3]). Nous montrerons qu'on peut améliorer ce résultat dans le cas où K est un corps abélien imaginaire.

Théorème 1. *Soit K un corps abélien imaginaire de degré n et soient $1, \alpha_2, \alpha_3, \alpha_4$ des nombres linéairement indépendants tels que $K=R(\alpha_2, \alpha_3, \alpha_4)$. Alors, pour aucun $a\in R$, l'équation (1) n'admet un nombre infini de solutions en entiers rationnels, en supposant qu'on a $3r<n$.*

On peut démontrer de manière analogue le théorème suivant en utilisant un résultat d'approximation récent de W. M. Schmidt ([9], théorème 5.)

Théorème 2. *Soit K un corps abélien imaginaire de degré n et soient $1, \alpha_2, \alpha_3$ α_4, α_5 des nombres linéairement indépendants tels que $K=R(\alpha_2, \alpha_3, \alpha_4, \alpha_5)$. Alors, pour aucun $a\in R$, l'équation (1) n'admet un nombre infini de solutions en entiers rationnels, en supposant qu'on a $6r<n$.*

Nous observons que si $\vartheta\in K$ est un élément primitif et spécialement $\alpha_i=\vartheta^{i-1}$ $(i=1, \ldots, 5)$, alors pour $m=4$ on a $r=2$, c'est-à-dire dans ce cas le théorème 1 est vrai déjà pour $n>6$; de même, pour $m=5$ on a $r\leqq 4$, c'est-à-dire le théorème 2 est vrai déjà pour $n>24$. En même temps nous notons que les théorèmes 1, 2 et 3 ne sont pas contenus dans les résultats de B. G. Mojshezon [4], mentionnés dans l'introduction.

Nous aurons besoin du lemme suivant

Lemme. *Soient $1, \beta_2, \beta_3, \beta_4$ des nombres algébriques non tous réels et linéairement indépendants dans R, et soient $c>0$, $\varepsilon>0$ des constantes arbitraires. Alors l'inégalité*

$$|L(\mathbf{x})| = |x_1+\beta_2 x_2+\beta_3 x_3+\beta_4 x_4|<c|\mathbf{x}|^{-2-\varepsilon}; \qquad |\mathbf{x}| = \max_i (|x_i|) \tag{3}$$

n'admet qu'un nombre fini de solutions $\mathbf{x}=(x_1, \ldots, x_4)$ en entiers rationnels.

Démonstration. Supposons le contraire de la proposition et soit

$$\beta_k = \gamma_k + i\delta_k \qquad k=1, 2, 3, 4,$$

où $\beta_1 = 1$ et γ_k, δ_k sont des nombres réels algébriques. Alors d'après (3) on a simultanément

$$|x_1 + \gamma_2 x_2 + \gamma_3 x_3 + \gamma_4 x_4| < c\,|\mathbf{x}|^{-2-\varepsilon} \tag{4}$$

et

$$|\delta_2 x_2 + \delta_3 x_3 + \delta_4 x_4| < c\,|\mathbf{x}|^{-2-\varepsilon} \tag{5}$$

pour une infinité de solutions $\mathbf{x} = (x_1, x_2, x_3, x_4)$. Maintenant il existe une transformation non singulière $Y = A \cdot X$ à coefficients entiers telle que pour une infinité de solutions $\mathbf{y} = (y_1, y_2, y_3, y_4)$ en entiers rationnels on déduit de (4) et (5)

$$|y_1 + \gamma_2' y_2 + \gamma_3' y_3 + \gamma_4' y_4| < c_1\,|\mathbf{y}|^{-2-\varepsilon} \tag{6}$$

et

$$|\mathbf{y}| = \max_i (|y_i|)$$

$$|\delta_2' y_2 + \delta_3' y_3 + \delta_4' y_4| < c_1\,|\mathbf{y}|^{-2-\varepsilon} \tag{7}$$

où les éléments différents de zéro parmi $\delta_2', \delta_3', \delta_4'$ sont déjà linéairement indépendants dans R (d'après l'hypothèse on a par exemple $\delta_4' \neq 0$). Ainsi d'après Schmidt ([9], théorème 2) (7) n'a qu'un nombre fini de solutions en y_2, y_3, y_4 et la forme $\delta_2' y_2 + \delta_3' y_3 + \delta_4' y_4$ est zéro sauf pour un nombre fini de solutions $\mathbf{y} = (y_1, y_2, y_3, y_4)$, vu que $|\mathbf{y}|^{-2-\varepsilon} \to 0$. Donc, en conséquence de l'indépendance linéaire des coefficients différents de zéro, les inconnues correspondantes sont toutes zéro, par ex. $y_4 = 0$. En appliquant ensuite une transformation convenable non singulière $Z = B \cdot Y$ à coefficients entiers pour l'inégalité

$$|y_1 + \gamma_2' y_2 + \gamma_3' y_3| < c_1\,|\mathbf{y}|^{-2-\varepsilon}$$

obtenue de (6), on a pour une infinité de solutions

$$|z_1 + \gamma_2'' z_2 + \gamma_3'' z_3| < c_2\,|\mathbf{z}|^{-2-\varepsilon}; \qquad |\mathbf{z}| = \max(|z_i|), \tag{8}$$

où les coefficients différents de zéro sont linéairement indépendants. Par conséquent $z_1 + \gamma_2'' z_2 + \gamma_3'' z_3 = 0$ sauf pour un nombre fini de $\mathbf{z}$, ainsi en appliquant tour à tour l'inverse des transformation précédentes nous obtenons

$$x_1 + \gamma_2 x_2 + \gamma_3 x_3 + \gamma_4 x_4 = 0$$

$$\delta_2 x_2 + \delta_3 x_3 + \delta_4 x_4 = 0,$$

c'est-à-dire

$$x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 = 0$$

sauf pour un nombre fini de $\mathbf{x}$, contrairement à l'hypothèse.

Démonstration du théorème 1. Selon l'hypothèse les générateurs de K ne sont pas tous réels; soit par exemple α_4 imaginaire. Nous montrerons que tous les conjugués relatifs $\alpha_4^{(1)} = \alpha_4, \ldots, \alpha_4^{(n)}$ de α_4 sont également imaginaires. Le corps K est abélien, par conséquent le sous-corps $R(\alpha_4)$ est également abélien, c'est-à-dire $\alpha_4^{(i)} \in R(\alpha_4)$ pour chaque i. Si maintenant, pour un certain i, $\alpha_4^{(i)}$ était réel, alors tous ses conjugués et particulièrement aussi α_4 appartiendraient à un sous-corps réel de $R(\alpha_4)$, ce qui est impossible.

Supposons maintenant, contrairement à la proposition, que l'équation (1) ait une infinité de solutions $\mathbf{x} = (x_1, x_2, x_3, x_4)$ en entiers rationnels. Alors il existe

un nombre infini de solutions telles que par exemple $|\mathbf{x}| = \max(|x_1|, |x_2|, |x_3|, |x_4|) = |x_1|$. Les points $(1, x_2/x_1, x_3/x_1, x_4/x_1)$ procédant de ces solutions forment un ensemble de points borné et infini dans E_4, par conséquent cet ensemble de points possède un point d'accumulation $0 \neq \mathbf{a} \in E_4$. Prenons une suite partielle de ces points, tendant vers $\mathbf{a}$. Alors il résulte de (1)

$$|N(1+\alpha_2 \cdot x_2/x_1 + \alpha_3 \cdot x_3/x_1 + \alpha_4 \cdot x_4/x_1)| = a|x_1|^{-n} \to 0$$

pour ces solutions, c'est-à-dire vu la continuité de $N(L(\mathbf{x}))$ on a

$$N(L(\mathbf{a})) = L^{(1)}(\mathbf{a}) \ldots L^{(n)}(\mathbf{a}) = 0.$$

Soit par exemple

$$L^{(i_1)}(\mathbf{a}) = \ldots = L^{(i_s)}(\mathbf{a}) = 0,$$

étant évidemment $s \leqq r$. Alors pour les autres formes $L^{(i)}(\mathbf{x})$ et pour chaque $\mathbf{x}$ considéré on a

$$|L^{(i)}(\mathbf{x})| \geqq c_1 |\mathbf{x}|.$$

De plus, d'après le lemme on déduit pour chaque $\mathbf{x}$

$$|L^{(i_k)}(\mathbf{x})| \geqq c_2 |\mathbf{x}|^{-2-\varepsilon}; \qquad k = 1, \ldots, s,$$

$\varepsilon > 0$ étant une constante arbitraire et $c_2 > 0$ une constante convenablement choisie. Donc, pour les $\mathbf{x}$ considérés on a

$$a = |N(L(\mathbf{x}))| \geqq c_3 |\mathbf{x}|^{-2s-\varepsilon'+n-s} \geqq c_3 |\mathbf{x}|^{n-3r-\varepsilon'},$$

ce qui est impossible d'après $n - 3r \geqq 1$.

Enfin nous prouvons la conjecture pour $m = 4$ dans le cas où K est un corps abélien imaginaire et son degré n'est divisible ni par 3 ni par 4.

Théorème 3. *Soit K un corps abélien imaginaire de degré n tel que $3 \nmid n$ et $4 \nmid n$ et soient $1, \alpha_2, \alpha_3, \alpha_4 \in K$ linéairement indépendats tels que $K = R(\alpha_2, \alpha_3, \alpha_4)$. Alors l'équation* (1) *n'admet qu'un nombre fini de soutions $\mathbf{x} = (x_1, x_2, x_3, x_4)$ en entiers rationnels.*

DÉMONSTRATION DU THÉORÈME 3. Supposons, contrairement à la proposition, que l'équation (1) a une infinité de solutions $\mathbf{x} = (x_1, x_2, x_3, x_4)$ pour un $a \in R$. D'après l'hypothèse on en conclut $a \neq 0$. En multipliant l'équation (1) par un nombre entier d^n nous obtenons l'équation

$$N(\Theta_1 x_1 + \Theta_2 x_2 + \Theta_3 x_3 + \Theta_4 x_4) = a',$$

où les nombres $\Theta_i = d\alpha_i$ sont déjà entiers dans K. Vu que le nombre des idéaux principaux de norme donnée est fini, il existe un système fini des nombres non associés $\beta_1, \ldots, \beta_k$ tel que pour un j fixé et pour une infinité de solutions $\mathbf{x}$, on a

$$\Theta_1 x_1 + \Theta_2 x_2 + \Theta_3 x_3 + \Theta_4 x_4 = \beta_j \varepsilon; \qquad 1 \leqq j \leqq k$$

avec des unités ε convenablement choisies. Vu que le corps K est abélien, d'après le théorème de Kronecker—Weber il existe un corps cyclotomique $L \supseteq K$. Par conséquent $\varepsilon \in L$ et ainsi d'après le théorème de Kronecker on a $\varepsilon = \zeta\varepsilon_1$, étant $\zeta \in L$ une

racine de l'unité et ε_1 une unité réelle (non nécessairement dans K). On en conclut pour un ζ fixé

$$x_1+\alpha_2 x_2+\alpha_3 x_3+\alpha_4 x_4 = d^{-1}\beta_j\zeta\varepsilon_1. \tag{9}$$

Maintenant il existe une transformation non singulière $X' = A\cdot X$ à coefficients entiers telle que de (9) on déduit avec une constante entière rationnelle c

$$x_1'+\alpha_2' x_2'+\alpha_3' x_3'+\alpha_4' x_4' = cd^{-1}\beta_j\zeta\varepsilon_1, \tag{10}$$

où les éléments différents de zéro parmi Im α_2', Im α_3', Im α_4', par exemple Im α_l', ..., Im $\alpha_4'(2\leqq l\leqq 4)$, sont déjà linéairement indépendants dans R. En prenant le conjugué complexe de (10) on a

$$x_1'+\bar\alpha_2' x_2'+\bar\alpha_3' x_3'+\bar\alpha_4' x_4' = cd^{-1}\bar\beta_j\bar\zeta\varepsilon_1,$$

c'est-à-dire

$$(\alpha_l'-\bar\alpha_l')x_l'+\ldots+(\alpha_4'-\bar\alpha_4')x_4' = cd^{-1}(\beta_j\zeta-\bar\beta_j\bar\zeta)\varepsilon_1$$

pour une infinité de solutions $\mathbf{x}'=(x_1', x_2', x_3', x_4')$. Soit

$cd^{-1}(\beta_j\zeta-\bar\beta_j\bar\zeta)(\alpha_l'-\bar\alpha_l')^{-1}=\gamma\in L$ et considérons l'équation

$$N_{L/R}\left(x_l'+\ldots+\frac{\operatorname{Im}\alpha_4'}{\operatorname{Im}\alpha_l'}x_4'\right) = N_{L/R}(\gamma\varepsilon_1) = \text{const} \tag{11}$$

Vu que $3\nmid n$ et $4\nmid n$, le module $\left\{1, \ldots\frac{\operatorname{Im}\alpha_4'}{\operatorname{Im}\alpha_l'}\right\}$ est non dégénéré et par conséquent l'équation (11) n'a qu'un nombre fini de solutions $x_l', \ldots, x_4'$ en entiers rationnels. Ainsi pour la même unité ε_1 (10) admet nécessairement une infinité de solutions $\mathbf{x}'=(x_1', x_2', x_3', x_4')$ où $x_l', \ldots, x_4'$ sont fixés. Enfin, en écrivant $\alpha_l' x_l'+\ldots+\alpha_4' x_4'=\eta$ nous obtenons l'équation

$$N_{L/R}(x_1'+\ldots+\alpha_{l-1}'x_{l-1}') = N_{K/R}(x_1'+\ldots+\alpha_{l-1}'x_{l-1}')^{[L:K]} =$$

$$= N_{L/R}(cd^{-1}\beta_j\zeta\varepsilon_1-\eta) = \text{const},$$

avec un nombre infini de solutions $x_1', \ldots, x_{l-1}'$ en entiers rationnels, ce qui est une contradiction d'après les conditions du théorème.

§ 3. Formes décomposables dans un corps cyclotomique

Dans la suite soit ζ une racine primitive p-ième de l'unité p étant un nombre premier et soit $K=R(\zeta)$. Nous étudierons seulement le cas où $a=1$, $\alpha_i=\zeta^{i-1}$ et $m=8$, en généralisant un théorème tout récent de T. NAGELL [5].

Théorème 4. *Soit $p>37$ un nombre premier et ζ une racine primitive p-ième de l'unité. Alors l'équation*

$$N(x_1+\zeta x_2+\ldots+\zeta^7 x_8) = 1 \tag{12}$$

n'a qu'un nombre fini de solutions $\mathbf{x}=(x_1, \ldots, x_8)$ en entiers rationnels.

On peut démontrer de manière analogue que pour $m=5,6$ la même proposition est valable aussi dans le cas $p>13$, de plus dans le cas $m=3,4$ il suffit de supposer qu'on a $p>5$. Par conséquent le théorème cité de Siegel ne contient pas notre théorème.

Pour la démonstration nous aurons besoin des lemmes suivants:

Lemme 1. *Si l'on a* $m<\frac{p-1}{2}$, *alors tous les déterminants d'ordre* $(m+1)$ *de la matrice*

$$\begin{pmatrix} 1 & \zeta+\zeta^{-1} & \dots & \zeta^m+\zeta^{-m} \\ 1 & \zeta^2+\zeta^{-2} & \dots & \zeta^{2m}+\zeta^{-2m} \\ \vdots & & & \\ 1 & \zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}} & \dots & \zeta^{\frac{p-1}{2}m}+\zeta^{\frac{p+1}{2}m} \end{pmatrix} \tag{13}$$

sont différents de zéro.

DÉMONSTRATION. En combinant les colonnes de la matrice nous obtenons un déterminant du type de Vandermonde

$$\begin{pmatrix} 1 & \zeta+\zeta^{-1} & \dots & (\zeta+\zeta^{-1})^m \\ 1 & \zeta^2+\zeta^{-2} & \dots & (\zeta^2+\zeta^{-2})^m \\ \vdots & & & \\ 1 & \zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}} & \dots & \left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)^m \end{pmatrix},$$

ce qui prouve notre proposition.

Lemme 2. *Tous les déterminante d'ordre* 4 *de la matrice*

$$\begin{pmatrix} \zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}} & \zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}} & \zeta^{\frac{p-5}{2}}+\zeta^{\frac{p+5}{2}} & \zeta^{\frac{p-7}{2}}+\zeta^{\frac{p+7}{2}} \\ (\zeta^2)^{\frac{p-1}{2}}+(\zeta^2)^{\frac{p+1}{2}} & & \dots & (\zeta^2)^{\frac{p-7}{2}}+(\zeta^2)^{\frac{p+7}{2}} \\ \vdots & & & \vdots \\ \left(\zeta^{\frac{p-1}{2}}\right)^{\frac{p-1}{2}}+\left(\zeta^{\frac{p-1}{2}}\right)^{\frac{p+1}{2}} & & \dots & \left(\zeta^{\frac{p-1}{2}}\right)^{\frac{p-7}{2}}+\left(\zeta^{\frac{p-1}{2}}\right)^{\frac{p+7}{2}} \end{pmatrix} \tag{14}$$

sont différents de zéro.

DÉMONSTRATION. En écrivant la matrice (14) dans la forme

$$\left\| \zeta^{k\frac{p-1}{2}}+\zeta^{k\frac{p+1}{2}},\ \left(\zeta^{k\frac{p-1}{2}}\right)^3+\left(\zeta^{k\frac{p+1}{2}}\right)^3,\ \left(\zeta^{k\frac{p-1}{2}}\right)^5+\left(\zeta^{k\frac{p+1}{2}}\right)^5,\ \left(\zeta^{k\frac{p-1}{2}}\right)^7+\left(\zeta^{k\frac{p+1}{2}}\right) \right\|$$

et en combinant convenablement les colonnes de cette matrice, nous obtenons également un déterminant du type de Vandermonde

$$\left\| \zeta^{k\frac{p-1}{2}}+\zeta^{k\frac{p+1}{2}},\ \left(\zeta^{k\frac{p-1}{2}}+\zeta^{k\frac{p+1}{2}}\right)^3,\ \left(\zeta^{k\frac{p-1}{2}}+\zeta^{k\frac{p+1}{2}}\right)^5,\ \left(\zeta^{k\frac{p-1}{2}}+\zeta^{k\frac{p+1}{2}}\right)^7 \right\|,$$

où les générateurs sont différents.

Dans la suite, désignons par N_1 la norme dans le corps $R(\zeta+\zeta^{-1})$.

Lemme 3. L'équation

$$N_1(y_1+(\zeta+\zeta^{-1})y_2+(\zeta^2+\zeta^{-2})y_3+(\zeta^3+\zeta^{-3})y_4)=\pm 1 \tag{15}$$

n'admet qu'un nombre fini de solutions $\mathbf{y}=(y_1, y_2, y_3, y_4)$ *en supposant que* $p>37$.

DÉMONSTRATION. Le degré de la forme (15) est $\frac{p-1}{2}$. Si r désigne le nombre défini au début du § 2, alors d'après le lemme 1 on a $r=3$, c'est-à-dire $\frac{p-1}{2}>6r$ et en conséquence du résultat cité l'équation (15) n'admet en effet qu'un nombre fini de solutions en entiers rationnels.

Lemme 4. *L'équation*

$$N_1\left[\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)y_1+\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)y_2+\left(\zeta^{\frac{p-5}{2}}+\zeta^{\frac{p+5}{2}}\right)y_3+\right.$$
$$\left.+\left(\zeta^{\frac{p-7}{2}}+\zeta^{\frac{p-7}{2}}\right)y_4\right]=\pm 1 \tag{16}$$

n'admet qu'un nombre fini de solutions $\mathbf{y}=(y_1, y_2, y_3, y_4)$ *en entiers rationnels, en supposant que* $p>37$.

DÉMONSTRATION. D'après le lemme 2 on a $r=3$ aussi dans ce cas, c'est-à-dire $\frac{p-1}{2}>6r$, ce qui prouve notre proposition.

DÉMONSTRATION DU THÉORÈME 4. De l'équation (12) on conclut

$$x_1+\zeta x_2+\ldots+\zeta^7 x_8=\zeta^{-h}\varepsilon_1, \tag{17}$$

ε étant une unité réelle dans $R(\zeta)$ et $0\leqq h<p$ un entier. On en déduit

$$\zeta^h x_1+\zeta^{h+1}x_2+\ldots+\zeta^{h+7}x_8=\varepsilon$$

et son conjugué complexe

$$\zeta^{-h}x_1+\zeta^{-h-1}x_2+\ldots+\zeta^{-h-7}x_8=\varepsilon.$$

En multipliant par ζ^{h+7} leur différence on a

$$(\zeta^{2h+7}-\zeta^7)x_1+\ldots+(\zeta^{2h+14}-1)x_8=0. \tag{18}$$

Il faut maintenant distinguer plusieurs cas:

1. Si $h=0$, alors on a $x_1=\pm 1$ et $x_2=\ldots=x_8=0$.
2. Dans le cas $14<2h+14<p-1$ on déduit $x_1=\ldots=x_8=0$.
3. Si $2h+14=p-1$, alors en appliquant l'égalité $\zeta^{p-1}=-1-\zeta-\ldots-\zeta^{p-2}$ nous obtenons de nouveau $x_1=\ldots=x_8=0$.
4. Pour $2h+14=p+1$ on conclut analoguement $x_1=\ldots=x_6=0$, $x_7=x_8=\pm 1$.

5. Pour $2h+14 = p+3$ on a $x_1=x_2=x_3=x_4=0$ et $x_5=x_8$, $x_6=x_7$. Donc, d'après (17)

$$\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)x_5+\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)x_6 = \varepsilon$$

d'où

$$N_1\left[\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)x_5+\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)x_6\right] = \pm 1$$

n'ayant qu'un nombre fini de solutions x_5, x_6 en entiers rationnels.

6. Pour $2h+14 = p+5$ on a $x_1=x_2=0$, $x_3=x_8$, $x_4=x_7$, $x_5=x_6$ et par conséquent

$$N_1\left[\left(\zeta^{\frac{p-5}{2}}+\zeta^{\frac{p+5}{2}}\right)x_3+\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)x_4+\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)x_5\right] = \pm 1$$

qui n'admet qu'un nombre fini de solutions x_3, x_4, x_5 en entiers rationnels d'après le lemme 4.

7. Si $2h+14 = p+7$, alors on a nécessairement

$$x_1=x_8,\ x_2=x_7,\ x_3=x_6,\ x_4=x_5,$$

c'est-à-dire

$$N_1\left[\left(\zeta^{\frac{p-7}{2}}+\zeta^{\frac{p+7}{2}}\right)x_1+\left(\zeta^{\frac{p-5}{2}}+\zeta^{\frac{p+5}{2}}\right)x_2+\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)x_3+\right.$$
$$\left.+\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)x_4\right] = \pm 1$$

également avec un nombre fini de solutions x_1, x_2, x_3, x_4.

8. Si $2h+14 = p+9$, alors on a

$$x_1=x_6,\ x_2=x_5,\ x_3=x_4,\ x_7=x_8=0$$

et d'après (17)

$$N_1\left[\left(\zeta^{\frac{p-5}{2}}+\zeta^{\frac{p+5}{2}}\right)x_1+\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)x_2+\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)x_3\right] = \pm 1$$

avec un nombre fini de solutions x_1, x_2, x_3 en entiers rationnels.

9. Dans le cas $2h+14 = p+11$ nous obtenons

$$x_1=x_4,\ x_2=x_3,\ x_5=x_6=x_7=x_8=0,$$

d'où

$$N_1\left[\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)x_1+\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)x_2\right] = \pm 1$$

ayant un nombre fini de solutions x_1, x_2 en entiers rationnels.

10. Dans le cas $2h+14 = p+13$ on peut aisément voir

$$x_1=x_2 = \pm 1,\ x_3=\ldots=x_8=0.$$

11. Dans le cas $p+15 \leqq 2h+14<2p$ on a

$$x_1=\ldots=x_8=0.$$

12. Si $2h+14 = 2p$, alors nous aurons d'une façon analogue

$$x_1=\ldots=x_7=0,\ x_8 = \pm 1.$$

13. Si $2h+14 = 2p+2$, alors

$$x_1 = \ldots = x_5 = 0, \quad x_6 = x_8,$$

d'où

$$N_1(x_7 + (\zeta + \zeta^{-1})x_6) = \pm 1$$

n'ayant qu'un nombre fini de solutions x_6, x_7 en entiers rationnels d'après le lemme 3.

14. Si $2h+14 = 2p+4$, alors

$$x_1 = x_2 = x_3 = 0, \quad x_4 = x_8, \quad x_5 = x_7$$

et en conséquence de (17)

$$N_1(x_6 + (\zeta + \zeta^{-1})x_5 + (\zeta^2 + \zeta^{-3})x_4) = \pm 1.$$

Mais cette équation n'a qu'un nombre fini de solutions x_6, x_5, x_4 d'après le lemme 3.

15. Dans le cas $2h+14 = 2p+6$ on conclut

$$x_1 = 0, \quad x_2 = x_8, \quad x_3 = x_7, \quad x_4 = x_6$$

et

$$N_1(x_5 + (\zeta + \zeta^{-1})x_4 + (\zeta^2 + \zeta^{-2})x_3 + (\zeta^3 + \zeta^{-3})x_2) = \pm 1$$

avec un nombre fini de solutions en x_5, x_4, x_3, x_2.

16. Dans le cas $2h+14 = 2p+8$ on a

$$x_1 = x_7, \quad x_2 = x_6, \quad x_3 = x_5, \quad x_8 = 0,$$

d'où

$$N_1(x_4 + (\zeta + \zeta^{-1})x_3 + (\zeta^2 + \zeta^{-2})x_2 + (\zeta^3 + \zeta^{-3})x_1) = \pm 1$$

avec un nombre fini de solutions.

17. Si $2h+14 = 2p+10$, alors il résulte

$$x_1 = x_5, \quad x_2 = x_4, \quad x_6 = x_7 = x_8 = 0,$$

et

$$N_1(x_3 + (\zeta + \zeta^{-1})x_2 + (\zeta^2 + \zeta^{-2})x_1) = \pm 1$$

également avec un nombre fini de solutions en x_3, x_2, x_1.

18. Enfin dans le cas $2h+14 = 2p+12$ on déduit

$$x_1 = x_3, \quad x_4 = x_5 = \ldots = x_8 = 0,$$

c'est-à-dire

$$N_1(x_2 + (\zeta + \zeta^{-1})x_1) = \pm 1$$

ayant également un nombre fini de solutions en entiers rationnels.

Donc, l'équation (12) n'admet en effet qu'un nombre fini de solutions en entiers rationnels.

Enfin nous montrerons que pour $p > 37$ et $m = 4$ on peut aisément obtenir une borne supérieure concernant le nombre de solutions, en utilisant le résultat connu de H. DAVENPORT et K. F. ROTH concernant le nombre de solutions de certaines équations à deux inconnues. Il est probable toutefois que dans ce cas particulier la borne obtenue peut être encore substantiellement diminuée.

Théorème 5. *Soit $p>37$ un nombre premier. Alors le nombre de solutions en entiers rationnels de l'équation*

$$N(x_1+\zeta x_2+\zeta^2 x_3+\zeta^3 x_4)=1 \tag{19}$$

est au plus

$$3\cdot 2^{(p+3)\left(\frac{p-1}{2}\right)^2}+3\exp\left[643\left(\frac{p-1}{2}\right)^2\right]+6.$$

DÉMONSTRATION. Il suffit de considérer les solutions de l'équation (12) où $x_5=\ldots=x_8=0$. Dans les cas 1,8 et 10 nous n'obtenons que deux solutions pour chacun. Dans le cas 9 on a $x_1=x_4$, $x_2=x_3$, d'où

$$N_1\left[\left(\zeta^{\frac{p-3}{2}}+\zeta^{\frac{p+3}{2}}\right)x_1+\left(\zeta^{\frac{p-1}{2}}+\zeta^{\frac{p+1}{2}}\right)x_2\right]=\pm 1.$$

ou plus simplement

$$N_1(x_2-x_1+(\zeta+\zeta^{-1})x_1)=\pm 1. \tag{20}$$

Dans le cas 17 on a $x_1=0$, $x_2=x_4$ et

$$N_1(x_3+(\zeta+\zeta^{-1})x_2)=\pm 1. \tag{21}$$

Enfin dans le cas 18 nous obtenons $x_1=x_3$, $x_4=0$ et

$$N_1(x_2+(\zeta+\zeta^{-1})x_1)=\pm 1, \tag{22}$$

alors que dans le reste des cas l'équation (12) c'est-à-dire (19) n'admet aucune solution en nombres eintiers rationnels.

Mais les formes (20), (21) et (22) sont irréductibles à coefficients entiers et de degré $\frac{p-1}{2}>3$. En plus d'après $|\zeta^k+\zeta^{-k}|\leqq 2$ les valeurs absolues de leurs $(s+1)$-ièmes coefficients sont $<2^s\binom{\frac{p-1}{2}}{s}$ et on en conclut que le maximum de leurs coefficients est $<2^{\frac{p-1}{2}}$. Par conséquent, d'après le théorème de Davenport et Roth, le nombre de solutions de (20), (21) et (22) est au plus

$$2^{(p+3)\left(\frac{p-1}{2}\right)^2}+\exp\left[643\left(\frac{p-1}{2}\right)^2\right]$$

pour chacun, et cela démontre notre théorème.

Remarque. Comme nous l'avons mentionné, ce théorème est vrai déjà pour $p>5$. La condition $p>37$ n'a été nécessaire que pour pouvoir appliquer le théorème 4. De plus, dans le cas $p=5$ l'équation (19) a déjà une infinité de solutions en entiers rationnels, (20), (21) et (22) étant des équations de Pell.

Enfin nous notons que dans le cas $p>5$ et $m=4$ on peut obtenir une borne supérieure effective aussi pour $\max(|x_1|, |x_2|, |x_3|, |x_4|)$, en utilisant les résultats les plus récents de A. BAKER.

Bibliographie

[1] S. I. Borewicz—I. R. Šafarevič, Zahlentheorie, *Basel* und *Stuttgart*, 1966.
[2] H. Davenport—K. F. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 160—167.
[3] K. Győry, Sur une classe des équations diophantiennes, *Publ. Math. Debrecen* **16** (1968), sous presse.
[4] Б. Г. Мойшезон, Представление чисел разложимыми формами, Мат. Сборник **56** (1962), 173—206.
[5] T. Nagell, Sur les discriminants des nombres algébriques, *Ark. Mat.* **7** (1967), 265—282.
[6] W. M. Schmidt, Some diophantine equations in three variables with only finitely many solutions, *Mathematika* **14** (1967), 113—120.
[7] C. L. Siegel, Approximation algebraischer Zahlen, *Math. Z.* **10** (1921), 173—213.
[8] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. Reine Angew. Math.* **135** (1909), 284—305.
[9] W. M. Schmidt, On simultaneous approximations of two algebraic numbers by rationals, *Acta Math.* **119** (1967), 27—50.

(Reçu le 27 février 1968.)