Now choose ξ_1 congruent to $\alpha \bmod 3$, to $\beta_1 \bmod 2$, to $\gamma_1 \bmod 1+2i$ and to $\delta_1 \bmod 1-2i$, and similarly for ξ_2, ξ_3, and ξ_4 and then

$$\nu - \xi_1^4 - \xi_2^4 - \xi_3^4 - \xi_4^4 \equiv -11 \pmod{120},$$

which concludes the proof.

We also have the identity

$$120(1+i)x = (x-2+2i)^4 - (x+2-2i)^4 + \{(1+i)x-1\}^4 - \{(1+i)x+1\}^4.$$

Now it is easily seen that for $\nu \in J_4$, the congruences

$$\begin{aligned} \nu - \alpha^4 &\equiv 0 \pmod 3, \\ \nu - \beta_1^4 - \beta_2^4 - \beta_3^4 + \beta_4^4 &\equiv 0 \pmod{1+2i}, \\ \nu - \gamma_1^4 - \gamma_2^4 - \gamma_3^4 + \gamma_4^4 &\equiv 0 \pmod{1-2i}, \\ \nu - \delta_1^4 - \delta_2^4 - \delta_3^4 + \delta_4^4 &\equiv 0 \pmod{8+8i} \end{aligned}$$

can all be satisfied unless $\nu \equiv 10 \pmod{8+8i}$. Thus all such ν can be expressed as the sum or difference of at most eight fourth powers, exactly as before. Finally, if $\nu \equiv 10 \pmod{8+8i}$ then $-\nu \not\equiv 10 \pmod{8+8i}$ and so $-\nu$ can be so expressed. Thus $v(4) \leqslant 8$.

References

[1] Paul T. Bateman and Rosemarie Stemmler, *Waring's Problem for Algebraic Number Fields and primes of the form $(p^r-1)/(p^d-1)$*, Illinois J. Math. 6 (1962), pp. 142–156.

[2] J. H. E. Cohn, *Waring's problem in quadratic number fields*, Acta Arith. 20 (1972), pp. 1–16.

[3] — *Sums of cubes of Gaussian Integers*, Proc. Amer. Math. Soc. 29 (1971), p.426.

[4] Ivan Niven, *Sums of fourth powers of Gaussian Integers*, Bull. Amer. Math. Soc. 47 (1941), pp. 923–926.

[5] Rosemarie Stemmler, *The easier Waring problem in algebraic number fields*, Acta Arith. 6 (1961), pp. 447–468.

ROYAL HOLLOWAY COLLEGE
ENGLEFIELD GREEN, SURREY

ACTA ARITHMETICA
XXIII (1973)

Sur les polynômes à coefficients entiérs et de discriminant donné

par

K. Győry (Debrecen)

Désignons par $\|f\| = \max_{0 \leqslant i \leqslant n} |a_i|$ la hauteur d'un polynôme $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbf{Z}[x]$. Appelons les polynômes $f(x)$ et $f^*(x) \in \mathbf{Z}[x]$ équivalents si l'on a $f^*(x) = f(x+a)$ avec un $a \in \mathbf{Z}$. Dans ce cas pour leur discriminant on obtient $D(f^*) = D(f)$. Donc, s'il y a un polynôme $f(x) \in \mathbf{Z}[x]$ ayant le discriminant D, alors il y en a une infinité. Dans notre travail nous démontrons le théorème suivant:

Théorème. *Soit $D \geqslant 1$ un nombre fixé arbitraire et considérons un polynôme normé $f(x) \in \mathbf{Z}[x]$ tel que $0 < |D(f)| \leqslant D$. Il existe des constantes $c_1(D)$, $c_2(D)$ calculables explicitement et dépendant seulement de D, telles que $\deg f \leqslant c_1(D)$ et $\|f^*\| \leqslant c_2(D)$, où f^* est un polynôme équivalent à f.*

Par conséquent, il n'existe qu'un nombre fini de polynômes normés $f(x) \in \mathbf{Z}[x]$, non équivalents deux à deux, de discriminant $0 < |D(f)| \leqslant D$ et on peut, par un nombre fini d'opérations, déterminer un tel système des polynômes $f(x)$.

Si $f(x) \in \mathbf{Z}[x]$ est un polynôme normé de degré $n \geqslant 2$, alors $|D(f)| \leqslant (2n\|f\|)^{2n-1}$. Inversement, de notre théorème, il résulte que $n \leqslant c_1(|D(f)|)$ et $\|f^*\| \leqslant c_2(|D(f)|)$ avec les constantes c_1 et c_2 précédentes, où f^* est un polynôme équivalent à f.

Considérons ensuite quelques corollaires de notre théorème.

Corollaire 1. *Soient donnés les nombres $D \geqslant 1$ et $N \geqslant 1$. Il n'existe qu'un nombre fini de polynômes normés $f(x) \in \mathbf{Z}[x]$ tels que $0 < |D(f)| \leqslant D$ et $|f(0)| \leqslant N$ et ces polynômes peuvent être déterminés.*

Ce corollaire reste vrai aussi dans le cas où nous fixons un autre coefficient des polynômes $f(x)$ au lieu de $f(0)$. Cette proposition est une généralisation des théorèmes analogues de Nagell [8], [10] qui concernent les polynômes normés à coefficients entiers de degré $\leqslant 4$ et les nombres algébriques entiers de degré $\leqslant 4$.

Désignons par

$$\Delta(f) = \min_{i \neq j} |\alpha_i - \alpha_j|$$

la distance minimale entre les racines d'un polynôme $f(x) = \prod_{i=1}^{n} (x - a_i)$. Si $f(x) \in \mathbf{Z}[x]$ est un polynôme normé, alors $|D(f)| \geqslant \Delta(f)$. Inversement, on obtient le suivant:

Corollaire 2. *Soit $f(x) \in \mathbf{Z}[x]$ un polynôme normé de degré $\geqslant 2$ et de discriminant $D(f) \neq 0$. Il existe une constante positive $c_3(|D(f)|)$, calculable explicitement et dépendant seulement de $|D(f)|$, telle que*

$$\Delta(f) \geqslant c_3(|D(f)|).$$

De notre théorème on obtient aussi une démonstration constructive d'un problème de T. Nagell [9], concernant les nombres algébriques entiers de discriminant donné. En effet, soit a un nombre algébrique entier, soit $f(x)$ son polynôme minimal et soit $D(a)$ son discriminant (dans le corps $Q(a)$). Alors pour la hauteur de a on a $H(a) = \|f\|$, et $D(a) = D(f)$. Appelons les nombres algébriques entiers a et a' équivalents si le polynôme minimal f^* de a' est équivalent à f, c'est-à-dire si l'on a $a' - a \in \mathbf{Z}$. En considérant maintenant seulement les polynômes irréductibles dans notre théorème, on déduit le

Corollaire 3. *Soit $D \geqslant 1$ un nombre fixé arbitraire et considérons un entier algébrique a tel que $|D(a)| \leqslant D$. Il existe des constantes $c_4(D)$, $c_5(D)$ calculables explicitement et dépendant seulement de D, telles que le degré de a est $\leqslant c_4(D)$ et pour un certain a' équivalent à a on a $H(a') \leqslant c_5(D)$.*

Ici on peut prendre simplement $c_4 = c_1$, $c_5 = c_2$, mais dans la démonstration s'obtiennent aussi des constantes meilleures c_4, c_5.

Ce théorème a été démontré par T. Nagell [8], [9], [10] pour les nombres algébriques entiers de degré $\leqslant 4$. A la fin de mai 1973 M. le Professeur A. Schinzel m'a bien voulu informer d'un travail récent de B. J. Birch et J. R. Merriman [13], dans lequel se trouve un théorème sur les formes binaires de degré et de discriminant donnés duquel on peut déduire notre théorème, sauf la calculabilité effective des constantes. L'idée fondamentale des démonstrations est au fait paraille, mais les démonstrations sont différentes et aucun de nos travaux ne contient l'autre. La méthode de notre travail, que se base sur notre méthode de graphe appliquée antérieurement dans [5] et dans la partie I de [5], a l'avantage d'être effective.

Dans [5], à l'aide de notre théorème, nous avons obtenu antérieurement aussi un théorème concernant l'irréductibilité des polynômes de la forme $g(f(x))$ (¹). De notre théorème, il résulte aussi un théorème de M. Fekete [4], notamment que sur le plan complexe un ensemble de

(¹) Les résultats de ce travail ont été présentés aussi dans une conférence que j'ai donné le 29 juin 1972, à Debrecen.

points fermé, borné, à diamètre transfini < 1, ne contient qu'un nombre fini d'ensembles des entiers algébriques conjugués.

Entre temps nous avons calculé explicitement les constantes qui se trouvent dans notre travail. Notamment, on peut prendre

$$c_1 = 2\left(1 + \frac{\log D}{\log 3}\right), \qquad c_4 = \frac{2}{\log 3}\log D,$$

$$c_2 = \exp\exp\exp\{(10\log D)^2\} \quad \text{et} \quad c_3 = |D(f)|\{c_2(|D(f)|)\}^{-c_1(|D(f)|)}.$$

Pour la démonstration, nous aurons besoin d'une remarque et d'un lemme. Si α, β ($\beta \neq 0$) sont des nombres algébriques de hauteur $\leqslant H$ et de degré d_1 et d_2, le degré de $\alpha \pm \beta$, $\alpha \cdot \beta$ et α/β est $\leqslant d_1 d_2$ et la hauteur de ces nombres $\leqslant (4dH^4)^d$, où $d = d_1 d_2$ (voir [1], p. 205).

D'autre part, considérons les solutions $(\beta_1, \beta_2, \beta_3)$ de l'équation

$$(1) \qquad \beta_1 + \beta_2 + \beta_3 = 0, \quad \beta_1\beta_2\beta_3 \neq 0$$

en entiers d'un corps algébrique K de degré n_K et de discriminant D_K. Appelons les solutions $(\beta_1', \beta_2', \beta_3')$ et $(\beta_1'', \beta_2'', \beta_3'')$ de (1) associées si l'on a $(\beta_1'', \beta_2'', \beta_3'') = (\varepsilon\beta_1', \varepsilon\beta_2', \varepsilon\beta_3')$ avec une unité ε de K.

Lemme. *Soit $G \geqslant 1$ une constante. Si $(\beta_1, \beta_2, \beta_3)$ est une solution de (1) en entiers de K telle que*

$$(2) \qquad |N_{K/Q}(\beta_i)| \leqslant G \quad (i = 1, 2, 3),$$

alors il y a une solution $(\beta_1', \beta_2', \beta_3')$ de (1) associée à $(\beta_1, \beta_2, \beta_3)$ telle que $H(\beta_i') \leqslant c_6(G, n_K, D_K)$ $(i = 1, 2, 3)$, où c_6 désigne une constante calculable explicitement, dépendant seulement de G, n_K et D_K.

Démonstration (voir [5]). Au cours de la démonstration de ce lemme nous avons employé les résultats de A. Baker [1] et A. Baker et J. Coates [2] concernant les équations diophantiennes.

Nous remarquons que la fonction obtenue $c_6 = c_6(G, n_K, D_K)$ est monotone croissante en chaque variable.

Dans la suite, $c_7, c_8, \ldots$ désignent des nombres calculables explicitement qui ne dépendent que de D.

Démonstration du théorème. D'abord nous démontrons, le théorème pour des polynômes normés $f(x) \in \mathbf{Z}[x]$ de degré $\geqslant 2$ et irréductibles sur $\mathbf{Z}$. Soit a l'une des racines de $f(x)$ lorsque a est un nombre algébrique entier tel que $|D(a)| \leqslant D$. Désignons par n et D le degré et le discriminant du corps $L = Q(a)$ sur le corps Q des nombres rationnels. D'après $D_L | D(a)$ on a $|D_L| \leqslant D$. De plus, en conséquence de l'inégalité de Minkowski (voir par ex. [11], p. 22) on obtient $n \leqslant c_7(|D_L|) \leqslant c_7(D)$ avec une constante c_7 calculable explicitement.

Si $n = 2$ et $a = x + y\sqrt{D_L}$ $(x, y \in Q)$, alors d'après $D \geqslant |D(a)| = 4y^2|D_L| \geqslant y^2$ on a $|y| \leqslant \sqrt{D}$. En choisissant $a = [x]$, pour $a' = a - a$, on obtient $H(a') \leqslant D^2 + 1$. Dans la suite soit $n \geqslant 3$. Désignons par $a^{(1)}$

$= \alpha, \ldots, \alpha^{(n)}$ les conjugués différents de α. Il existe dans L un élément entier primitif δ tel que pour le maximum $h(\delta)$ des valeurs absolues des conjugués de δ on a $h(\delta) \leq |D_L|^{1/2} \leq D^{1/2}$ (voir par ex. [11], p. 22) et par conséquent $H(\delta) \leq \max_{1\leq k\leq n} \binom{n}{k} h^k(\delta) \leq c_8(D)$. Désignons par $\delta^{(1)} = \delta, \ldots, \delta^{(n)}$ les conjugués de δ, correspondant à $\alpha^{(1)}, \ldots, \alpha^{(n)}$. Alors le degré de $K = Q(\alpha^{(1)}, \ldots, \alpha^{(n)}) = Q(\delta^{(1)}, \ldots, \delta^{(n)})$ est $n_K \leq n! \leq c_9(D)$. Prenons les nombres $l\delta^{(1)} + \delta^{(2)}$ ($l = 0, \ldots, n^4$) et remplaçons $\delta^{(1)}$ et $\delta^{(2)}$ par leurs conjugués $\delta^{(1)}, \ldots, \delta^{(n)}$ indépendamment l'un de l'autre. Il y a au moins un nombre $\sigma_1 = l\delta^{(1)} + \delta^{(2)}$ ($0 \leq l \leq n^4$) tel que les nombres $l\delta^{(i)} + \delta^{(j)}$ ($1 \leq i, j \leq n$) sont différents deux à deux. Alors σ_1 est un élément entier primitif du corps $Q(\delta^{(1)}, \delta^{(2)})$ (voir par ex. [6], p. 709) et $H(\sigma_1) = H(l\delta^{(1)} + \delta^{(2)}) \leq c_{10}(D)$. En répétant ce procédé tout au plus $(n-1)$-fois, nous obtenons un nombre entier primitif σ de K tel que $H(\sigma) \leq c_{11}(D)$ et par conséquent $|D(\sigma)| \leq c_{12}(D)$. Enfin, si nous désignons par D_K le discriminant de K, d'après $D_K | D(\sigma)$ on a $|D_K| \leq c_{12}$, c_{12} étant une constante calculable explicitement, dépendant seulement de D.

De l'égalité

(3) $$D(\alpha) = \prod_{1\leq i<j\leq n} (\alpha^{(j)} - \alpha^{(i)})^2$$

il résulte

$$\prod_{1\leq i<j\leq n} N^2_{K/Q}(\alpha^{(j)}-\alpha^{(i)}) = |D(\alpha)|^{[K:Q]} \leq c_{13}(D),$$

d'où

$$0 < |N_{K/Q}(\alpha^{(j)}-\alpha^{(i)})| \leq c_{13}(D)$$

pour chaque paire i, j ($i \neq j$). D'autre part, pour les indices arbitraires i, j, k différents deux à deux on a

$$(\alpha^{(i)}-\alpha^{(j)}) + (\alpha^{(j)}-\alpha^{(k)}) + (\alpha^{(k)}-\alpha^{(i)}) = 0,$$

c'est-à-dire les nombres entiers $(\alpha^{(i)}-\alpha^{(j)}, \alpha^{(j)}-\alpha^{(k)}, \alpha^{(k)}-\alpha^{(i)})$ différents de zéro satisfont à la fois à l'équation (1) et à l'inégalité (2) avec $G = c_{13}(D)$. D'après notre lemme il existe donc une solution $(\beta_1^{(ijk)}, \beta_2^{(ijk)}, \beta_3^{(ijk)})$ de (1) en entiers de K, associée à la solution $(\alpha^{(i)}-\alpha^{(j)}, \alpha^{(j)}-\alpha^{(k)}, \alpha^{(k)}-\alpha^{(i)})$, telle que $\max_{1\leq s\leq 3} H(\beta_s^{(ijk)}) \leq c_{14}(D)$ indépendamment de i, j, k. Donc, avec une unité $\varepsilon \in K$ on a

$$\alpha^{(1)}-\alpha^{(2)} = \varepsilon\beta_1^{(123)}, \quad \alpha^{(2)}-\alpha^{(3)} = \varepsilon\beta_2^{(123)}, \quad \alpha^{(3)}-\alpha^{(1)} = \varepsilon\beta_3^{(123)}.$$

Si $n > 3$, on obtient avec une unité $\varepsilon' \in K$

$$\alpha^{(1)}-\alpha^{(2)} = \varepsilon'\beta_1^{(12i)}, \quad \alpha^{(2)}-\alpha^{(i)} = \varepsilon'\beta_2^{(12i)}, \quad \alpha^{(i)}-\alpha^{(1)} = \varepsilon'\beta_3^{(12i)}$$

pour chaque $n \geq i > 3$. Il en résulte $\varepsilon' = \varepsilon\beta_1^{(123)}/\beta_1^{(12i)}$, c'est-à-dire avec $\varrho_i = \beta_2^{(12i)}\beta_1^{(123)}/\beta_1^{(12i)}$ on a $\alpha^{(2)}-\alpha^{(i)} = \varepsilon\varrho_i$ et $H(\varrho_i) \leq c_{15}(D)$. De plus, pour $k \neq 2, i$ on a

$$\alpha^{(2)}-\alpha^{(i)} = \varepsilon''\beta_1^{(2ik)}, \quad \alpha^{(i)}-\alpha^{(k)} = \varepsilon''\beta_2^{(2ik)}, \quad \alpha^{(k)}-\alpha^{(2)} = \varepsilon''\beta_3^{(2ik)}$$

avec une unité $\varepsilon'' \in K$, d'où $\varepsilon'' = \varepsilon\varrho_i/\beta_1^{(2ik)}$, $\alpha^{(i)}-\alpha^{(k)} = \varepsilon\varrho_i\beta_2^{(2ik)}/\beta_1^{(2ik)} = \varepsilon\varrho_{ik}$ et $H(\varrho_{ik}) \leq c_{16}(D)$, indépendamment de i, k. Par conséquent pour chaque paire d'indices i, k ($i \neq k$) on a

$$\alpha^{(i)}-\alpha^{(k)} = \varepsilon\varrho_{ik}, \quad H(\varrho_{ik}) \leq c_{16}(D)$$

avec la même unité $\varepsilon \in K$, c_{16} étant une constante calculable explicitement, dépendant seulement de D. Ainsi de (3) on déduit

$$\varepsilon^{n(n-1)} = D(\alpha)\Big(\prod_{1\leq i<k\leq n} \varrho_{ik}^2\Big)^{-1},$$

d'où l'on obtient $H(\varepsilon^{n(n-1)}) \leq c_{17}(D)$ avec une constante c_{17} également calculable explicitement. Si $h(x)$ désigne le polynôme minimal de $\varepsilon^{n(n-1)}$, alors le polynôme minimal de ε divise $h(x^{n(n-1)})$, d'où on obtient $H(\varepsilon) \leq c_{18}(D)$ avec une constante c_{18} calculable explicitement (voir [12], p. 176, Hilfssatz 3). Enfin, pour chaque paire d'indices i, k ($i \neq k$) on a

$$\alpha^{(i)}-\alpha^{(k)} = \sigma_{ik}, \quad H(\sigma_{ik}) \leq c_{19}(D),$$

c_{19} étant une constante calculable explicitement et dépendant seulement de D.

Considérons de nouveau le nombre entier primitif δ dans L, utilisé déjà précédemment. Il existe une constante $c_{20}(D)$ calculable explicitement telle que $\Delta(\delta) = |D(\delta)| \leq c_{20}$. Dans L il y a une base des entiers de la forme

$$(1, w_1, \ldots, w_{n-1}) = \Big(1, \frac{\psi_1(\delta)}{\Delta_1}, \ldots, \frac{\psi_{n-1}(\delta)}{\Delta_{n-1}}\Big),$$

où $\psi_s(\delta) = \delta^s + a_{s1}\delta^{s-1} + \ldots + a_{ss}$, $\Delta_s, a_{sr} \in \mathbf{Z}$ et $\Delta_s | \Delta(\delta)$, $|a_{sr}| \leq \Delta(\delta)$ pour tout $1 \leq s, r \leq n-1$ ([3], p. 11). On en déduit qu'il existe une constante $c_{21}(D)$ calculable explicitement pour laquelle $H(w_s) \leq c_{21}$ ($1 \leq s \leq n-1$).

Considérons la représentation $\alpha = \alpha^{(1)} = x_0 + x_1 w_1 + \ldots + x_{n-1}w_{n-1}$ de α ($x_i \in \mathbf{Z}$; $1 \leq i \leq n-1$) et prenons le nombre $\alpha' = x_1 w_1 + \ldots + x_{n-1}w_{n-1}$ équivalent à α. Alors pour les conjugués de α' on a $\alpha'^{(i)} - \alpha'^{(k)} = \alpha^{(i)} - \alpha^{(k)} = \sigma_{ik}$. Désignons par $w_s^{(1)} = w_s, \ldots, w_s^{(n)}$ ($1 \leq s \leq n-1$) les conjugués de w_s correspondant à $\alpha^{(1)}, \ldots, \alpha^{(n)}$ et considérons le système d'équations

$$\sigma_{1,n} = \alpha'^{(1)} - \alpha'^{(n)} = x_1(w_1^{(1)} - w_1^{(n)}) + \ldots + x_{n-1}(w_{n-1}^{(1)} - w_{n-1}^{(n)}),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_{n-1,n} = \alpha'^{(n-1)} - \alpha'^{(n)} = x_1(w_1^{(n-1)} - w_1^{(n)}) + \ldots + x_{n-1}(w_{n-1}^{(n-1)} - w_{n-1}^{(n)})$$

en $x_1, \ldots, x_{n-1}$. Le déterminant de ce système d'équations est $\pm\sqrt{D_L}$, par conséquent en éliminant les inconnues x_i, nous obtenons $|x_i| \leq c_{22}(D)$

et finalement $H(a') \leqslant c_{23}(D)$ avec des constantes c_{22}, c_{23} calculables explicitement et dépendant seulement de D.

Ensuite, considérons un polynôme normé $f(x) \in \mathbf{Z}[x]$ réductible sur Q tel que $0 < |D(f)| \leqslant D$ et prenons la décomposition $f(x) = f_1(x) \ldots f_r(x)$ en facteurs $f_i(x) \in \mathbf{Z}[x]$ irréductibles sur Q. Vu que $D(f) \neq 0$, les facteurs f_i sont différents deux à deux.

Si $f_i(x)$ est linéaire pour un i, soit dans la suite $D(f_i) = 1$. Désignons par $R(f_i, f_j)$ le résultant de f_i et f_j. Alors d'après

$$D(f) = \prod_{i=1}^{r} D(f_i) \prod_{1 \leqslant i < j \leqslant r} R^2(f_i, f_j) \tag{4}$$

nous obtenons

$$0 < |D(f_i)| \leqslant D \qquad (i = 1, \ldots, r).$$

Comme nous l'avons démontré, il y a un polynôme f_i^* équivalent à f_i pour chaque i tel que $\deg f_i^* \leqslant c_7(D)$, $\|f_i^*\| \leqslant c_{23}(D)$, où c_7, c_{23} désignent les constantes obtenues antérieurement. Si f_i est linéaire, soit par exemple $f_i^*(x) = x$. De plus, si f_i et f_j sont équivalents, choisissons les polynômes f_i^* et f_j^* identiques et fixons un système des f_i^* qui possèdent une telle propriété. Alors on peut écrire $f_i(x) = f_i^*(x + a_i)$ avec des nombres entiers rationnels convenables a_i. De (4) on obtient

$$0 < |R(f_i, f_j)| = \left|R\big(f_i^*(x+a_i), f_j^*(x+a_j)\big)\right| \leqslant \sqrt{D} \tag{5}$$

pour tout i, j $(i \neq j)$. Soit L_{ij} le corps de décomposition de $f_i^*(x) f_j^*(x)$. Alors $[L_{ij}: Q] \leqslant [c_7^2]!$ Désignons par α_i et α_j une racine de f_i^* et f_j^* respectivement et soient

$$f_i^* = \prod_{u=1}^{k} (x - \alpha_i^{(u)}), \quad f_j^* = \prod_{v=1}^{l} (x - \alpha_j^{(v)}) \quad (\alpha_i^{(1)} = \alpha_i,\ \alpha_j^{(1)} = \alpha_j).$$

En conséquence des égalités $H(\alpha_i) = \|f_i^*\|$ et $H(\alpha_j) = \|f_j^*\|$ on a $H(\alpha_i - \alpha_j) \leqslant c_{24}(D)$ et $\deg(\alpha_i - \alpha_j) \leqslant c_7^2$ avec une constante c_{24} calculable explicitement. Soit $F_{ij}(x) = x^N + b_1 x^{N-1} + \ldots + b_N \in \mathbf{Z}[x]$ le polynôme minimal de $\alpha_j - \alpha_i$, où $N = \deg F_{ij} \leqslant c_7^2$ et $\max\limits_{1 \leqslant k \leqslant N} |b_k| = \|F_{ij}\| \leqslant c_{24}$. Alors

$$R\big(f_i^*(x+a_i), f_j^*(x+a_j)\big) = \prod_{\substack{1 \leqslant u \leqslant k \\ 1 \leqslant v \leqslant l}} \big((\alpha_i^{(u)} - a_i) - (\alpha_j^{(v)} - a_j)\big).$$

Si $L_{ij} \neq Q$, prenons ici la norme des deux cotés dans L_{ij}. De (5) il résulte

$$\begin{aligned} c_{25}(D) &\geqslant \left|N_{L_{ij}/Q}\big((\alpha_i - a_i) - (\alpha_j - a_j)\big)\right| \\ &= \left|N_{L_{ij}/Q}\big((a_j - a_i) - (\alpha_j - \alpha_i)\big)\right| \geqslant |F_{ij}(a_j - a_i)|. \end{aligned}$$

Ici $|a_j - a_i| \leqslant c_{25} + c_7^2 \cdot c_{24} = c_{26}$, parce que dans le cas contraire, on obtiendrait

$$\begin{aligned} |F_{ij}(a_j - a_i)| &= |(a_j - a_i)^N + b_1(a_j - a_i)^{N-1} + \ldots + b_N| \\ &\geqslant |a_j - a_i|^{N-1}\big(|a_j - a_i| - \{|b_1| + \ldots + |b_N|\}\big) \\ &\geqslant |a_j - a_i| - c_7^2 \cdot c_{24} > c_{25}. \end{aligned}$$

Par conséquent, si $f_i^* = f_j^*$ (lorsque f_i est équivalent à f_j et $a_i \neq a_j$), alors le nombre des f_i équivalents au même f_i^* est $\leqslant c_{26} + 1 = c_{27}$. D'autre part, le nombre des f_i^* différents est $\leqslant c_7(2c_{23} + 1) = c_{28}$. On en déduit que le nombre des facteurs irréductibles de $f(x)$ est $\leqslant c_{27} \cdot c_{28} = c_{29}$ et ainsi $\deg f \leqslant c_7 \cdot c_{29} = c_{30}$ avec une constante c_{30} calculable explicitement, dépendant seulement de D.

Enfin, prenons par exemple le polynôme $f^*(x) = f(x - a_1)$ équivalent à $f(x)$ et considérons la décomposition $f^*(x) = f_1'(x) \ldots f_r'(x) = f_1(x - a_1) \ldots f_r(x - a_1)$. D'après $f_i'(x) = f_i(x - a_1) = f_i^*\big(x + (a_i - a_1)\big)$ on a $\|f_i'\| \leqslant c_{31}$ et finalement $\|f^*\| \leqslant c_{32}$, où les constantes c_{31}, c_{32} ne dépendent que de D et elles sont également calculables explicitement.

Démonstration du corollaire 1. Soit $f(x) \in \mathbf{Z}[x]$ normé et tel que $0 < |D(f)| \leqslant D$ et $|f(0)| \leqslant N$. Alors d'après notre théorème pour un f^* équivalent à f on a $\deg f = \deg f^* \leqslant c_1(D)$, $\|f^*\| \leqslant c_2(D)$ avec les constantes c_1, c_2 obtenues dans le théorème. Soit $f^*(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, où $|a_i| \leqslant c_2$ et soit $f(x) = f^*(x + a)$ avec un $a \in \mathbf{Z}$. Nous montrerons que $|a| \leqslant \max(c_1 \cdot c_2 + 1, N) = c(D, N)$. En effet, dans le cas contraire

$$\begin{aligned} |f(0)| = |f^*(a)| &= |a^n + a_1 a^{n-1} + \ldots + a_n| \\ &\geqslant |a|^n - (|a_1| + \ldots + |a_n|)|a|^{n-1} \geqslant |a|(|a| - c_1 \cdot c_2) > N, \end{aligned}$$

ce qui est impossible. Donc, on a $\|f(x)\| = \|f^*(x+a)\| \leqslant c'(D, N)$, où c' ne dépend que de D et N et il est calculable explicitement.

Démonstration du corollaire 2. Soit $f(x) \in \mathbf{Z}[x]$ un polynôme normé quelconque de discriminant $\neq 0$. D'après notre théorème $\deg f \leqslant c_1(|D(f)|)$ et pour un polynôme f^* équivalent à f on a $\|f^*\| \leqslant c_2(|D(f)|)$. Soit $f^*(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ lorsque $n = \deg f^* \leqslant c_1$ et $\Delta(f^*) = \Delta(f)$, $D(f^*) = D(f)$. Si $L(f^*) = 1 + |a_1| + \ldots + |a_n|$, alors $L(f^*) \leqslant 2n\|f^*\| \leqslant c'(|D(f)|)$. Par conséquent, d'après un théorème de K. Mahler [7]

$$\Delta(f^*) > 3n^{-(n+2)/2} |D(f^*)| L(f^*)^{-(n-1)} \geqslant c''(|D(f^*)|)$$

et ainsi en effet on a

$$\Delta(f) > c''(|D(f)|),$$

où c'' est une constante calculable explicitement et dépendant seulement de $|D(f)|$.

Travaux cités

[1] A. Baker, *Contributions to the theory of diophantine equations*, Philos. Trans. Roy. Soc. London, Ser. A, 263 (1968), p. 173–208.

[2] — and J. Coates, *Integer points on curves of genus* 1, Proc. Cambridge Philos. Soc. 67 (1970), p. 595–602.

[3] W. E. H. Berwick, *Integral bases*, Cambridge Tracts, No. 22, New York and London 1964.

[4] M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Zeitschr. 17 (1923), p. 228–249.

[5] K. Győry, *Sur l'irréductibilité d'une classe des polynômes, II*, Publ. Math. Debrecen 19 (1972), sous presse.

[6] E. Landau, *Vorlesungen über Zahlentheorie, III*, Leipzig 1927.

[7] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11 (1964), p. 257–262.

[8] T. Nagell, *Contributions à la théorie des modules et des anneaux algébriques*, Arkiv för Mat. 6 (1965), p. 161–178.

[9] — *Sur les discriminant des nombres algébriques*, Arkiv för Mat. 7 (1967), p. 265–282.

[10] — *Quelques propriétés des nombres algébriques du quatrième degré*, Arkiv för Mat. 7 (1969), p. 517–525.

[11] O. Ore, *Les corps algébriques et la théorie des idéaux*, Mémorial Sci. Math., Paris, 64 (1934).

[12] C. Siegel, *Approximation algebraischer Zahlen*, Math. Zeitschr. 10 (1921), p. 173–213.

[13] B. J. Birch and J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. 24 (1972), pp. 385–394.

INSTITUT DE MATHÉMATIQUES DE L'UNIVERSITÉ DE DEBRECEN,
Hongrie

Received on 9. 10. 1972 (334)

and in revised form on 27. 7. 1973