Sur les polynômes à coefficients entiers et de discriminant donné, III

Par K. GYŐRY (Debrecen)

1. Introduction

On appelle les polynômes $f(x)$ et $f^*(x) \in Z[x]$ *équivalents* si $f^*(x)=f(x+a)$ pour un $a \in Z$. $\|f\|$ désigne le maximum des valeurs absolues des coefficients de $f(x)$. Soit $f(x) \in Z[x]$ un polynôme unitaire de degré $k \geqq 3$ et de discriminant $D(f) \neq 0$. En généralisant plusieurs résultats antérieurs (pour la bibliographie du problème voir par exemple [11], [12] ou les paragraphes 2, 3, 4 et 5), nous avons démontré dans [11] (voir encore [10]) qu'il existe un polynôme f^* équivalent à f tel que

$$\|f^*\| < c(k, |D(f)|),$$

où $c=c\,(k, |D(f)|)$ est une constante effectivement calculable qui ne dépend que de k et $|D(f)|$ (dans [12] nous avons même explicité la valeur d'une telle constante en fonction de k et $|D(f)|$). Dans [9], [10], [11] et [12] nous avons donné plusieurs conséquences et applications de ce résultat, par exemple aux polynômes de discriminant donné, aux nombres entiers algébriques de discriminant donné et à la réductibilité des polynômes de la forme $g(f(x))$.

B. N. DELONE et D. K. FADDEEV ([8], p. 412, PROBLEM) ont posé le problème de déterminer tous les polynômes unitaires $f(x) \in Z[x]$ du troisième degré avec un discriminant D donné. Notre résultat mentionné ci-dessus a fourni un algorithme ([11], [12]) pour déterminer tous les polynômes unitaires $f(x) \in Z[x]$ de discriminant D (sans restreindre leurs degrés). De plus, nos théorèmes [11] ont impliqué la solution effective d'un problème de T. NAGELL ([16], p. 276) (une solution non effective se trouve dans le travail [5] de B. J. BIRCH et J. R. MERRIMAN) et la solution effective d'un problème posé dans le livre [18] de W. NARKIEWICZ (voir [18], pp. 130 et 468, Problem 19).

Dans cet article, nous poursuivrons nos recherches relatives aux polynômes de discriminant donné. Nous améliorerons les majorations obtenues dans [11] et [12], nous généraliserons nos résultats antérieurs et les étendrons même aux polynômes $f(x)$ non nécessairement unitaires et de discriminant $D(f)=0$. Aux paragraphes 3, 4 et 5 nous appliquerons nos résultats récents, concernant les polynômes

de discriminant donné, à des nombres algébriques de discriminant donné, à des polynômes irréductibles et à des équations diophantiennes.

Au cours des démonstrations nous utiliserons, entre autres, les récents résultats de H. M. STARK [20] relatifs aux formes linéaires de logarithmes de nombres algébriques.

2. Polynômes de discriminant donné

Désignons par $\|\mathscr{F}\|$ la hauteur d'un polynôme $\mathscr{F}(x_1, \ldots, x_k) \in Z[x_1, \ldots, x_k]$ (c'est-à-dire le maximum des valeurs absolues des ses coefficients). $f^{(j)}$ désigne la dérivée j-ième du polynôme $f(x)$ (où $f^{(0)}=f$) et $D(f^{(j)})$ le discriminant de $f^{(j)}(x)$.

Pour énoncer notre principal résultat nous introduisons quelques constantes et notations. Soient $k \geqq 2$, $0 \leqq j \leqq k-2$ et $A \geqq 1$ des entiers et soient $\varkappa_j > 9\binom{k-j-1}{2}$, $D_i \geqq 0$ $(i=0, \ldots, j)$, $D_j > 0$ des constantes. Soit $M_{k-2} = Ak^2 D_{k-2}$ pour $j=k-2$ et

$$M_j = \exp\{c_1[A^{(k-j-1)(k-j-2)} D_j]^{\varkappa_j}\} \quad \text{pour} \quad 0 \leqq j \leqq k-3.$$

En particulier, soient (avec les notations $\varkappa_0=\varkappa$, $D_0=D$) $M_0=4AD$ pour $k=2$ et

$$M_0 = \exp\{c_3[A^{(k-1)(k-2)} D]^{\varkappa}\} \quad \text{pour} \quad k \geqq 3.$$

Enfin, soient

$$L_j = c_2\left(\ldots\left(M_j^{2(k-j)} + \frac{D_{j-1}^{1/(k-j)}}{A}\right)^{2(k-j+1)} + \ldots\right)^{2(k-1)} + \frac{D_0^{1/(k-1)}}{A}$$

pour $j \geqq 1$ et $L_0=M_0$, où $c_1=c_1(k, j, \varkappa_j)$, $c_2=c_2(k, j)$ et $c_3=c_3(k, \varkappa)$ sont des constantes positives convenables.

Théorème 1. *Soit $\mathscr{F}(x_1, \ldots, x_k) \in Z[x_1, \ldots, x_k]$ et supposons que, pour un entier $A \geqq 1$ donné, le degré de $\mathscr{F}\left(A\binom{k}{1}t, \ldots, A\binom{k}{k}t^k\right)$ en t coïncide avec le degré $m>0$ de $\mathscr{F}(x_1, x_2^2, \ldots, x_k^k)$. Avec les notations précédentes considérons un polynôme $f(x)=a_0x^k+a_1x^{k-1}+\ldots+a_k \in Z[x]$ tel que $D(f^{(j)}) \neq 0$, $|D(f^{(j)})| \leqq D_i$ $(i=0, \ldots, j)$ et $|a_0|=A$. Soient $F \geqq 0$ et $0 \leqq \tau < m/k$ des constantes vérifiant*

$$|\mathscr{F}(a_1, \ldots, a_k)| \leqq F\|f\|^{\tau}. \tag{1}$$

Alors on a

$$\|f\| < A\left\{[\|\mathscr{F}\|(c_4 L_j)^{\deg \mathscr{F}}]^{\min(m-k\tau, 1)} + [(A+1)^{\tau} F\right]^{\min\left(\frac{1}{m-k\tau}, 1\right)}\Bigg\}^{\max\left(\frac{k}{m-k\tau}, k\right)} \tag{2}$$

*avec des constantes $c_1, c_2, c_3, c_4=c_4(k)>0$ effectivement calculables.**)

Si $m \leqq k$, dans (2) on peut omettre le facteur A devant la paranthèse et on peut remplacer $(A+1)^{\tau}$ par 2^{τ} (voir la démonstration).

---

*) *Note ajoutée aux épreuves.* En utilisant un récent résultat de A. BAKER (Acta Arith. 27 (1975), 247—252), dans le Théorème 1 et dans les corollaires les estimations peuvent être améliorées. Par exemple, dans le cas $j=0$, $a_0=1$ on peut prendre $\exp\{c'[D(\log D)^{2k/3}]^{9(k-1)(k-2)/2}\}$ partout au lieu des constantes de la forme $\exp\{cD^{\varkappa}\}$ (où $c'=c'(k)>0$ est effectivement calculable).

Remarque 1.1. Notre Théorème 1 (et ses conséquences) sont valables aussi dans le cas où $D(f)=0$ (par opposition à nos résultats antérieurs). Si $D(f)\neq 0$ et si, pour un $j\geqq 1$, $|D(f^{(j)})|$ est petit par rapport aux $|D(f^{(j-1)})|, \ldots, |D(f)|$, notre Théorème 1 (et ses conséquences) donnent de meilleures majorations que celles qui seraient obtenues dans le cas $j=0$.

Remarque 1.2. Soit $\bar{f}(x)=f\left(\frac{1}{x}\right)x^k=a_kx^k+\cdots+a_0$ et $a_k\neq 0$. Comme $D(\bar{f})=D(f)$, si $|a_0/a_k|$ est relativement grand, en général il vaut mieux appliquer le Théorème 1 à $\bar{f}$ (au lieu de f). Cela concerne toutes les conséquences dans lesquelles $a_0\neq 1$.

Naturellement, la majoration (2) est sans intérêt quand $|a_0|$ (resp. $|a_k|$) est grand par rapport à $\|f\|$ (par exemple $|a_0|=\|f\|$).

Remarque 1.3. Dans le Théorème 1 on peut établir la majoration (2) avec des constantes explicites en k, j aussi (sans utiliser $\varkappa_j$). Pour le faire, il suffit d'appliquer un théorème de A. BAKER [1], établi avec des constantes calculées explicitement, au lieu du théorème de H. M. Stark [20] (voir encore les résultats de [12] dans le cas particulier $a_0=1$, $j=0$). Nous énoncerons quelques conséquences du Théorème 1 avec des constantes explicites aussi.

Remarque 1.4. L'un des théorèmes récents de H. M. STARK ([21], Théorème 1) nous permet, dans le cas $k=3$, de choisir $\varkappa_j>1$ (où $0\leqq j\leqq 1$). Si $k\geqq 3$, $j=0$ et si $f(x)$ est irréductible et normal (c'est-à-dire si l'extension $Q(\alpha)/Q$ est normale pour des racines α de $f(x)$), le Théorème 1 et ses conséquences sont vrais déjà pour $\varkappa>3/2$ (voir la démonstration).

Remarque 1.5. Quand $D(f)\neq 0$, $\deg f$ est majorable par $|D(f)|$ (voir le Théorème 1 dans [12]). En appliquant ce résultat successivement à $f(x), f'(x), \ldots, f^{(k-3)}(x)$, on obtient

$$k=\deg f\leqq \min_{\substack{0\leqq j\leqq k-3\\ D(f^{(j)})\neq 0}}\left\{j+3+\frac{2}{\log 3}\log|D(f^{(j)})|\right\}. \tag{3}$$

Considérons ensuite quelques cas particuliers du Théorème 1, qui concernent les polynômes.

Corollaire 1.1. *Sous les hypothèses du Théorème 1 soient* $j>0$, $D(f^{(j-1)})=\ldots=D(f)=0$ et $0<|D(f^{(j)})|\leqq D_j$. *Alors*

$$\|f\|<A\left\{[(A+1)^\tau F]^{\min\left(\frac{1}{m-k\tau},\,1\right)}+[\|\mathscr{F}\|(M_j')^{\deg\mathscr{F}}]^{\min(m-k\tau,\,1)}\right\}^{\max\left(\frac{k}{m-k\tau},\,k\right)}, \tag{4}$$

où $M_j'=\exp\{c_5[A^{(k-j-1)(k-j-2)}D_j]^{\varkappa_j}\}$ *avec une constante* $c_5=c_5(k,j,\varkappa_j)>0$ *effectivement calculable.*

Corollaire 1.2. *Sous les autres hypothèses du Théorème 1 soit* $f(x)=x^k+a_1x^{k-1}+\ldots+a_k\in Z[x]$ *avec* $0<|D(f)|\leqq D$ *et soit* $\varkappa>9\binom{k-1}{2}$ *une constante. Alors*

$$\|f\|<\left\{[\|\mathscr{F}\|M^{\deg\mathscr{F}}]^{\min(m-k\tau,\,1)}+[2^\tau F]^{\min\left(\frac{1}{m-k\tau},\,1\right)}\right\}^{\max\left(\frac{k}{m-k\tau},\,k\right)}, \tag{5}$$

où $M=\exp\{c_6D^\varkappa\}$ *avec une constante positive* $c_6=c_6(k,\varkappa)$ *effectivement calculable.*

Dans la suite M désignera toujours cette constante.

Corollaire 1.3. *Soient $k \geqq 2$, $0 \leqq j \leqq k-2$ des entiers, soit $\varkappa_j > 9\binom{k-j-1}{2}$ une constante et soit $f(x)=a_0x^k+a_1x^{k-1}+\cdots+a_k \in Z[x]$ avec $D(f^{(j)}) \neq 0$, $|D(f^{(i)})| \leqq D_i$ $(i=0, \ldots, j)$ et $0<|a_0|=A$. Si pour un $1 \leqq i \leqq k$ et pour des constantes $A_i \geqq 0$, $0 \leqq \tau < i/k$ on a*

$$|a_i| \leqq A_i \|f\|^{\tau}, \tag{6}$$

alors

$$\|f\| < \left\{[c_4 L_j]^{\min(i-k\tau,\,1)} + [(2^{\tau}A_i]^{\min\left(\frac{1}{i-k\tau},\,1\right)}\right\}^{\max\left(\frac{k}{i-k\tau},\,k\right)} \tag{7}$$

avec les constantes L_j et c_4 figurant dans le Théorème 1.

Cette assertion, dans le cas $k \leqq 4$, $a_0=1$, $j=\tau=0$ et sous une forme non effective, a été démontrée antérieurement par T. NAGELL [14], [15], [17]. Un cas particulier important du Corollaire 1.3 est où $a_0=1$, $j=0$, $i=k$ et $\tau=0$.

Corollaire 1.4. *Soit $f(x) \in Z[x]$ un polynôme unitaire de degré $k \geqq 2$ tel que $0<|D(f)| \leqq D$ et $|f(0)| \leqq N$ et soit $\varkappa > 9\binom{k-1}{2}$ une constante. Alors*

$$\|f\| < [N^{1/k}+M]^k \tag{8}$$

avec la constante ci-dessus $M=\exp\{c_6 D^{\varkappa}\}$ effectivement calculable.

Il en résulte qu'il n'existe qu'un nombre fini de polynômes unitaires $f(x) \in Z[x]$ avec un discriminant $D \neq 0$ donné et avec un terme constant donné et tous ces polynômes sont effectivement déterminables. Cette proposition a été démontrée dans le cas $k=3$ par V. A. TARTAKOVSKIĬ [8] et dans le cas $k \leqq 4$ par T. NAGELL [14], [15], [17] (comme un cas particulier de ses résultats déjà cités).

Nous remarquons que le Corollaire 1.4 est une amélioration du Corollaire 1 dans [11] et du Corollaire 2 dans [12].

D'après le Lemme 4 on peut choisir $c_9=D^{3(k-1)(k-2)}$ dans [12]. En calculant dans [12] avec cette constante, nous obtenons la majoration un peu meilleure

$$\|f^*\| < M^* = \exp\{k^{4k^{12}} D^{6k^8}\} < \exp\exp\{4(\log D)^{13}\}$$

qui correspond à celles (5) et (5′) de [12] et à celle (10) ci-dessous. Dans les Corollaires 1.2 et 1.4 et dans le Théorème 2 (et dans toute la suite de cet article) on peut choisir M^* au lieu de M (M^* est supérieur à M mais calculé explicitement).

Corollaire 1.5. *Soit $f(x)=a_0x^k+a_1x^{k-1}+\cdots+a_k \in Z[x]$ un polynôme de degré $k \geqq 2$ avec $D(f^{(j)}) \neq 0$ pour un $0 \leqq j \leqq k-2$ et soient $\varkappa_j > 9\binom{k-j-1}{2}$, $D_i \geqq |D(f^{(i)})|$ $(i=0, \ldots, j)$, $A=|a_0|>0$ des constantes. Il existe un polynôme f^* équivalent à f tel que*

$$\|f^*\| < L_j \tag{9}$$

avec la constante L_j figurant dans le Théorème 1.

On peut facilement donner un polynôme convenable f^* équivalent à f. En effet, soit $a \in Z$ vérifiant

$$a_1 = a_0 ka + a_1', \quad 0 \leqq a_1' < k|a_0|.$$

Alors pour le polynôme $f^*(x) = f(x-a) = a_0 x^k + a_1' x^{k-1} + \ldots + a_k'$ nous pouvons appliquer le Théorème 1 ou le Corollaire 1.3.[1]) Ce polynôme distingué f^* peut être choisi aussi dans le Corollaire 1.6.

Considérons maintenant le cas particulier où $a_0 = 1$ et $j = 0$.

Corollaire 1.6. *Si $f(x) \in Z[x]$ est un polynôme unitaire de degré $k \geqq 2$ avec $0 < |D(f)| \leqq D$, alors pour toute constante $\varkappa > 9 \binom{k-1}{2}$ il existe un polynôme f^* équivalent à f tel que*

$$\|f^*\| < \exp\{c_7 D^{\varkappa}\}, \tag{10}$$

d'où

$$|D(f)| > c_8 (\log \|f^*\|)^{1/\varkappa}, \tag{11}$$

les constantes $c_7 = c_7(k, \varkappa)$ et $c_8 = c_8(k, \varkappa)$ étant positives et effectivement calculables.

Comme il est connu (voir [8] et le § 5 de cet article), le problème de déterminer les polynômes du troisième degré et de discriminant donné est équivalent à celui de résoudre les équations diophantiennes de la forme $a_0 x^3 + a_1 x^2 y + a_2 x y^2 + a_3 y^3 = m$. En vertu de ce lien, dans le cas $k = 3$ B. N. DELONE [7] (voir encore [8]) a obtenu certains résultats effectifs. Il a déterminé (à l'équivalence près) tous les polynômes unitaires $f^*(x) \in Z[x]$ du troisième degré pour lesquels $-172 \leqq D(f^*) < 0$. Dans [8] B. N. DELONE et D. K. FADDEEV ont posé le problème de déterminer tous les polynômes unitaires $f(x) \in Z[x]$ du troisième degré avec un discriminant donné (p. 412, PROBLEM). Dans [11], nous avons donné en toute généralité (sans restreindre le degré) un algorithme effectif pour déterminer les polynômes unitaires à coefficients entiers avec discriminant donné. (Voir encore [12] et (3), (10)).

Du Corollaire 1.5 il résulte plus généralement que, $k \geqq 2$, $0 \leqq j \leqq k-2$ et $D_j \neq 0$ étant des entiers donnés, il n'existe qu'un nombre fini de polynômes unitaires $f(x) \in Z[x]$ de degré k, deux à deux inéquivalents et vérifiant $D(f^{(j)}) = D_j$ et $D(f) = \ldots = D(f^{(j-1)}) = 0$ (quand $j > 0$), et un tel système de polynômes est effectivement déterminable. Dans le cas $j = 0$ cela implique certains de nos résultats antérieurs obtenus dans [11] et [12].

Corollaire 1.7. *Soit $f(x) = a_0 x^k + a_1 x^{k-1} + \cdots + a_k \in Z[x]$ un polynôme de degré $k \geqq 3$ avec $D(f) \neq 0$ et $0 < |a_0| = A$ et soit $\varkappa > 9 \binom{k-1}{2}$ une constante. Alors*

$$|D(f^{(j)})| < \exp\{c_9 [A^{(k-1)(k-2)} |D(f)|]^{\varkappa}\} \quad (0 \leqq j \leqq k-2) \tag{12}$$

et, en particulier si $a_0 = 1$, on a

$$|D(f^{(j)})| < \exp\{c_9 |D(f)|^{\varkappa}\} \quad (0 \leqq j \leqq k-2) \tag{12'}$$

avec une constante $c_9 = c_9(k, \varkappa) > 0$ effectivement calculable.

---

[1]) Plus précisément, le Théorème 1 et le Corollaire 1.3 n'impliquent que $\|f^*\| < \{c_4 L_j + kA\}^k$ pour ce f^* et cette majoration est plus faible que (9). Mais (9) aussi résulte de la démonstration du théorème. On peut déduire le Théorème 1 et le Corollaire 1.5 l'un de l'autre.

Remarque. Donc, $|D(f')|, \ldots, |D(f^{(k-2)})|$ sont majorables par $|D(f)|$, k et $|a_0|$, et, si $a_0=1$, seulement par $|D(f)|$ et k (de plus, en vertu de notre Théorème 1 obtenu dans [12], seulement par $|D(f)|$).

Corollaire 1.8. *Soit* $f(x)=x^k+a_1x^{k-1}+\ldots+a_k\in Z[x]$ *un polynôme de degré* $k\geqq 3$ *avec* $D(f)\neq 0$ *et soit* $\varkappa>9\binom{k-1}{2}$ *une constante. Il existe un* $a\in Z$ *qui vérifie*

$$|f^{(i)}(a)| < \exp\{c_{10}|D(f)|^{\varkappa}\} \tag{13}$$

simultanément pour tout $0\leqq i\leqq k-1$, *où* $c_{10}=c_{10}(k,\varkappa)>0$ *est une constante effectivement calculable.*

Ce corollaire peut être généralisé, naturellement, pour $j\geqq 0$ et pour des polynômes non nécessairement unitaires.

3. Applications aux nombres algébriques

Dans ce paragraphe nous appliquons nos résultats, relatifs aux polynômes de discriminant donné, aux nombres algébriques de discriminant donné. En même temps, nous améliorons et généralisons certains de nos résultats antérieurs ([11], [12]).

Si α est un nombre algébrique de degré $k\geqq 2$, désignons par $H(\alpha)$ la hauteur de α (le maximum des valeurs absolues des coefficients de son polynôme minimal à coefficients entiers), par $d(\alpha)$ son dénominateur (c'est-à-dire le plus petit entier $a>0$ tel que $a\alpha$ soit entier algébrique) et par $D(\alpha)$ et $N(\alpha)$ respectivement le discriminant et la norme de α relatifs à l'extension $Q(\alpha)/Q$. Soit $f(x)=a_0x^k+a_1x^{k-1}+\ldots+a_k\in Z[x]$ le polynôme minimal de α. On a $H(\alpha)=\|f\|$, $a_0^{2k-2}D(\alpha)=D(f)$, $\deg\alpha=\deg f$, $|a_0N(\alpha)|=|f(0)|$ et $|a_0|\leqq d^k(\alpha)$. Par conséquent, nous pouvons appliquer, dans le cas $j=0$, tous les résultats du § 1 aux nombres algébriques de discriminant donné. Ici nous ne formulons que quelques conséquences. Du Corollaire 1.3 il résulte immédiatement le suivant.

Théorème 2. *Soit* α *un nombre algébrique de degré* $k\geqq 2$ *avec discriminant* $|D(\alpha)|\leqq D$. *Soit* $\varkappa>9\binom{k-1}{2}$ *une constante et soient* $N\geqq 1$, $0\leqq\tau<1$ *des constantes telles que*

$$|N(\alpha)| \leqq N\{H(\alpha)\}^{\tau}. \tag{14}$$

Alors

$$H(\alpha) < \left\{(M'')^{\min((1-\tau)k,1)}+\left[2^{\tau}d^k(\alpha)N\right]^{\min\left(\frac{1}{(1-\tau)k},1\right)}\right\}^{\max\left(\frac{1}{1-\tau},k\right)} \tag{15}$$

avec la constante $M''=\exp\left\{c_6(k,\varkappa)\left[\left(d(\alpha)\right)^{k^2(k-1)}D\right]^{\varkappa}\right\}$ *calculable explicitement. En particulier, si* α *est entier, alors*

$$H(\alpha) < [|N(\alpha)|^{1/k}+M]^k \tag{15'}$$

avec la constante $M=\exp\{c_6(k,\varkappa)D^{\varkappa}\}$ *figurant dans le Corollaire* 1.2.

Nous pouvons obtenir de meilleures majorations aussi, si nous tenons compte du discriminant D_K du corps de nombres $K=Q(\alpha)$. Dans la démonstration (quand $k\geqq 3$) on peut choisir $c_9=|D_K|^{3(k-1)(k-2)}$, $c_{10}=D^{n/2}$ et finalement, au lieu de M'', on peut prendre

$$\exp\{c_{11}[|D_K|^{3(k-1)(k-2)}(|D_K|^{3(k-1)(k-2)/2}+\log(d(\alpha)D))]^{1+\varepsilon}\},$$

où $\varepsilon>0$ et $c_{11}=c_{11}(k,\varepsilon)>0$ est une constante effectivement calculable. De plus, nous pouvons remplacer le terme de droite dans (19) et (quand $d(\alpha)=1$) le M dans (15′), (16) et (19′) par cette constante. Si K/Q est normal, dans les exposants de $|D_K|$ on peut omettre le facteur $3(k-1)(k-2)$.

Du Théorème 2 ci-dessus et du Corollaire 4 de [12] s'ensuit une conséquence importante:

Corollaire 2.1. *Il n'existe qu'un nombre fini de nombres algébriques de degré et de discriminant donnés avec norme et dénominateur donnés et tous ces nombres algébriques sont effectivement déterminables. En particulier, il n'existe qu'un nombre fini d'entiers algébriques de discriminant et de norme donnés et tous ces entiers algébriques sont effectivement déterminables.*

Remarque 2.1. Comme nous l'avons déjà mentionné en termes des polynômes au § 1, le Corollaire 2.1 a été démontré pour les entiers algébriques du troisième degré par V. A. TARTAKOVSKIĬ [8], et pour les entiers algébriques de degré $\leqq 4$ par T. NAGELL [14], [15], [17] (sous une forme non effective).

Considérons ensuite le cas particulier où α est unité.

Corollaire 2.2. *Soit ε une unité algébrique de degré $k\geqq 2$ avec discriminant $|D(\varepsilon)|\leqq D$ et soit $\varkappa>9\binom{k-1}{2}$ une constante. Alors*

$$H(\varepsilon) < \exp\{c_{12}D^{\varkappa}\} \tag{16}$$

et

$$|D(\varepsilon)| > c_{13}(\log H(\varepsilon))^{1/\varkappa}, \tag{17}$$

où $c_{12}=c_{12}(k,\varkappa)$ et $c_{13}=c_{13}(k,\varkappa)$ sont des constantes positives effectivement calculables.

Remarque 2.2. Si α est un entier algébrique de degré k, d'après l'inégalité de Minkowski (voir encore [12], Corollaire 4)

$$k \leqq \frac{2}{\log 3}\log|D(\alpha)|. \tag{18}$$

Cela et le Corollaire 2.2 impliquent le Corollaire suivant que nous avons obtenu dans [11] (voir encore [12]).

Corollaire 2.3. *Soit $D\neq 0$ un entier rationnel. Il n'existe qu'un nombre fini d'unités algébriques de discriminant D dans l'anneau des entiers algébriques et toutes ces unités sont effectivement déterminables.*

Remarque 2.3. Le Corollaire 2.3, pour les unités du troisième degré et de degré $\leqq 4$, résulte respectivement des théorèmes cités de V. A. TARTAKOVSKIĬ [8] et de T. NAGELL [14], [15], [17].

Le résultat ci-dessus (Corollaire 2.3) a fourni ([11], [12]) la solution effective d'un problème qui se trouve dans un livre récent de W. NARKIEWICZ ([18], pp. 130 et 468, Problem 19).

Appelons les nombres algébriques α et α' *équivalents,* si $\alpha'-\alpha=a\in Z$, lorsque $f^*(x)=f(x-a)$ pour les polynômes minimaux $f(x)$ et $f^*(x)$ respectivement de α et α'.

Dans le cas $j=0$ le Corollaire 1.5 implique immédiatement ce qui suit:

Théorème 3. *Soit α un nombre algébrique de degré $k\geqq 2$ avec discriminant $|D(\alpha)|\leqq \leqq D$ et soit $\varkappa>9\binom{k-1}{2}$ une constante. Il existe un α' équivalent à α tel que*

$$H(\alpha') < \exp\{c_3[(d(\alpha))^{k^2(k-1)}D]^{\varkappa}\}. \tag{19}$$

Si en particulier α est entier, alors

$$H(\alpha') < \exp\{c_3 D^{\varkappa}\}, \tag{19'}$$

d'où

$$|D(\alpha)| > c_{14}(\log H(\alpha'))^{1/\varkappa}, \tag{20}$$

où $c_3=c_3(k,\varkappa)$ et $c_{14}=c_{14}(k,\varkappa)$ sont des constantes positives effectivement calculables.[2])

De (18) et du Théorème 3 résulte le Corollaire 3 de [11] qui peut être énoncé sous la forme suivante:

Corollaire 3.1. *Soit $D\neq 0$ un entier rationnel. Il n'existe qu'un nombre fini d'entiers algébriques de discriminant D et deux à deux inéquivalents et un tel système des entiers est effectivement déterminable.*

Remarque 3.1. Pour des entiers algébriques de degré $\leqq 4$ cette assertion (sous une forme non effective) a été démontrée par T. NAGELL [15], [16], [17]. NAGELL a conjecturé que c'est vrai en toute généralité [16]. Récemment, B. J. BIRCH et J. R. MERRIMAN [5] ont démontré cette assertion (mais sous une forme non effective). Plus précisément, dans [5] ils ont démontré que, pour des entiers $n\geqq 3$ et $D\neq 0$ donnés, il n'existe qu'un nombre fini de formes binaires $F(x,y)\in Z[x,y]$ de degré n, deux à deux inéquivalentes, avec le même discriminant D (de plus, ils l'ont démontré sous une forme plus générale, sous une forme p-adique et sur des corps de nombres algébriques arbitraires). Cependant, leur démonstration est non effective. Dans [5] Birch et Merriman ont déduit, de leur résultat ci-dessus, l'assertion de notre Corollaire 3.1, mais sous une forme non effective, sans donner un algorithme effectif pour déterminer les entiers algébriques de discriminant donné.

[2]) On peut aisément déterminer le polynôme minimal f^* d'un tel α' (voir la remarque qui suit le Corollaire 1.5).

Comme nous l'avons mentionné au §1, dans [7] (voir encore [8]) B. N. Delone a déterminé, entre autres, tous les entiers α du troisième degré (à l'équivalence près) pour lesquels $0>D(\alpha)\geqq -172$.

Remarque 3.2. Dans (19′) $H(\alpha')$ est majorable par la constante explicite $M^*=\exp\{k^{4k^{12}}D^{6k^8}\}$ aussi.

Remarque 3.3. Si $K=Q(\alpha)$ est une extension normale de Q de degré $k\geqq 3$, alors, d'après la Remarque 1.4, dans les Théorèmes 2 et 3 et dans le Corollaire 3.3 il suffit de supposer que $\varkappa>3/2$. De plus, dans le Corollaire 3.2 on peut prendre $|D_K|$ et $|D_K|^{1/2}$ au lieu de $|D_K|^{3(k-1)(k-2)}$ et $|D_K|^{3(k-1)(k-2)/2}$ respectivement.

Si α est un entier algébrique et si D_K est le discriminant du corps $K=Q(\alpha)$, alors $D(\alpha)=I^2(\alpha)D_K$, où $I(\alpha)$ désigne l'indice de α. Pour des entiers équivalents α, α' on a $I(\alpha)=I(\alpha')$. Désignons par O_K l'anneau des entiers de K. Le Théorème 3 et la remarque qui suit le Théorème 2 impliquent le suivant.

Corollaire 3.2. *Soit K un corps de nombres algébriques de degré $k\geqq 3$ avec discriminant D_K. Soit $\varepsilon>0$ et soit $a\neq 0$ un entier rationnel. Si $\alpha\in O_K$ et si $I(\alpha)=a$, alors il existe un α' équivalent à α pour lequel*

$$H(\alpha') < \exp\{c'_{11}[|D_K|^{3(k-1)(k-2)}(|D_K|^{3(k-1)(k-2)/2}+\log|a|)]^{1+\varepsilon}\}$$

avec une constante positive $c'_{11}=c'_{11}(k,\varepsilon)$ effectivement calculable.

Par conséquent, dans un corps de nombres algébriques donné il n'existe qu'un nombre fini d'entiers deux à deux inéquivalents avec un indice $a\neq 0$ donné et un tel système des entiers est effectivement déterminable.

Enfin, considérons le cas particulier $a=1$. On dit que O_K est *monogène* lorsque $O_K=Z[\alpha]$ avec un $\alpha\in O_K$ (c'est-à-dire lorsque $1, \alpha, \ldots, \alpha^{k-1}$ constituent une base d'entiers dans K).

Corollaire 3.3. *Soit K un corps de nombres algébriques de degré $k\geqq 3$ avec discriminant D_K et soit $\varkappa>9(k-1)(k-2)/2$. Si O_K est monogène et $O_K=Z[\alpha]$, alors il existe un α' équivalent à α tel que*

$$H(\alpha') < \exp\{c''_{11}|D_K|^{\varkappa}\}$$

avec une constante $c''_{11}=c''_{11}(k,\varkappa)>0$ effectivement calculable.

Cela fournit donc un algorithme général pour décider si O_K est monogène ou non et pour déterminer tout $\alpha\in O_K$ pour lequel $O_K=Z[\alpha]$.

4. Applications aux polynômes irréductibles

Nous avons obtenu nos premiers résultats, relatifs aux polynômes de discriminant donné, au cours des démonstrations des théorèmes d'irréductibilité de type de Schur ([9], [10], [11], [12]). En appliquant nos résultats récents obtenus au § 1, nous pouvons généraliser et améliorer certains de nos résultats d'irréductibilité aussi.

Théorème 4. *Soient $f(x), g(x)\in Z[x]$ des polynômes unitaires irréductibles de degré $p\geqq 2$ (p premier) et $n\geqq 2$ respectivement. Supposons que les racines de $f(x)$*

sont réelles et que le corps des racines de $g(x)$ est une extension quadratique totalement imaginaire d'un corps totalement réel.[3]) *Soit $\varkappa > 9p(p-1)^2(p-2)/2$ une constante. Alors $g(f(x))$ est irréductible sur Q, sauf dans certains cas où il existe un $f^*(x)$ équivalent à $f(x)$ tel que*

$$\|f^*\| < \exp\{c_{15}[g(0)]^{\varkappa/n}\}, \tag{21}$$

où $c_{15} = c_{15}(p, \varkappa)$ est une constante positive effectivement calculable.

Remarque 4.1. Le Théorème 4 est une amélioration de notre Théorème 2a dans [9] (voir encore la constante $c_1(G, p)$ dans [12]). Ce Théorème 2a et les autres résultats de [9], [10], [12] et [13] ont donné, dans le cas des $g(x)$ du type précédent et sous une forme plus générale, la solution d'un problème de A. BRAUER, R. BRAUER et H. HOPF [6] qui concerne la réductibilité des polynômes de la forme $g(f(x))$.

Remarque 4.2. Soit $G \geqq 1$ une constante. Le Théorème 4 implique qu'il n'existe qu'un nombre fini de polynômes $f(x)$ deux à deux inéquivalents avec la propriété ci-dessus pour lesquels $g(f(x))$ peut être réductible avec un polynôme unitaire irréductible $g(x)$ tel que $\{g(0)\}^{1/n} \leqq G$ ($n = \deg g$) et dont le corps des racines est une extension quadratique totalement imaginaire d'un corps totalement réel. De plus, un tel système des $f(x)$ est effectivement déterminable.

Si $p \leqq 3$, les conditions du Théorème 4 peuvent être affaiblies.

Théorème 4'. *Soient $f(x)$, $g(x) \in Z[x]$ des polynômes unitaires de degré $p \geqq 3$ (p preimer) et $n \geqq 2$ respectivement. Supposons que les racines $f(x)$ sont réelles et que $g(x)$ est irréductible et son corps des racines est une extension quadratique totalement imaginaire d'un corps totalement réel. Soit $\varkappa > 9p(p-1)^2(p-2)/2$ une constante. Alors $g(f(x))$ est irréductible sur Q, sauf dans certains cas où il existe un f^*, équivalent à f, vérifiant* (21).

A l'aide des Lemmes 1, 2 et 3, on peut considérablement améliorer aussi l'estimation de notre Théorème 1a dans [9] (et la constante $c(n_k, D_K, G)$ dans [12]). Nous remarquons qu'il n'existe pas de polynômes exceptionnels dans le Théoreme 1a dans [9] (voir [13]).

5. Applications aux équations diophantiennes

Le lien entre la détermination des polynômes à coefficients entiers (et des entiers algébriques) avec discriminant donné et la résolution effective de certaines équations diophantiennes à coefficients entiers a été découvert par B. N. DELONE [7], B. N. DELONE et D. K. FADDEEV [8] et T. NAGELL [14], [15], [16], [17]. Cependant les auteurs ont conclu en premier lieu dans l'une des directions (et seulement dans le cas du degré $\leqq 4$), des résultats concernant les équations diophantiennes aux polynômes de discriminant donné, et la plupart de leurs résultats sont non effectifs. Nous avons réussi à obtenir nos résultats dans [11], [12] et dans le présent travail d'une manière différente, sans utiliser le lien mentionné. Par conséquent, à partir les théorèmes concernant les polynômes de discriminant donné, nous pouvons obtenir des résultats

[3]) Soit par exemple $g(x)$ un polynôme cyclotomique ou un polynôme quadratique de discriminant négatif.

dans la direction opposée aussi, à certaines équations diophantiennes et dans le cas du degré arbitraire et ces résultats seront (par opposition à ceux antérieurs) tous effectifs.

a) *Résolution des équations diophantiennes du type discriminant*

Soit $k \geqq 2$ un nombre entier. Appelons le polynôme $D(x_1, \ldots, x_k) \in Z[x_1, \ldots, x_k]$ du type discriminant d'ordre k, si

$$D(x_1, \ldots, x_k) = D(f(x)),$$

où $D(f(x))$ est le discriminant de $f(x)=x^k+x_1x^{k-1}+\cdots+x_k$ comme polynôme en x. On a par exemple

$$D(x_1, x_2) = x_1^2 - 4x_2$$

et

$$D(x_1, x_2, x_3) = 18x_1x_2x_3 + x_1^2x_2^2 - 4x_2^3 - 4x_3x_1^3 - 27x_3^2.$$

Soit $D \neq 0$ un nombre entier rationnel et considérons l'équation diophantienne du type discriminant

$$D(x_1, \ldots, x_k) = D. \tag{22}$$

Pour que (22) soit soluble en entiers rationnels, il faut que $k \leqq 2 + 2(\log 3)^{-1} \cdot \log |D|$ (voir le Théorème 1 dans [12]).

Si (22) admet une solution $(x_1^*, \ldots, x_k^*) \in Z^k$, alors il admet une infinité de solutions. Notamment, si $f^*(x)=x^k+x_1^*x^{k-1}+\cdots+x_k^*$ avec la solution $(x_1^*, \ldots, x_k^*)$ considérée, alors tous les $(x_1, \ldots, x_k) \in Z^k$, vérifiant

$$f(x) = x^k + x_1x^{k-1} + \ldots + x_k = f^*(x+a) \tag{23}$$

pour un $a \in Z$, seront également des solutions de (22) et

$$(x_1, \ldots, x_k) = \left(\frac{f^{*(k-1)}(a)}{(k-1)!}, \ldots, f^*(a) \right) \quad (a \in Z). \tag{24}$$

Appelons *famille de solutions* un ensemble des solutions de la forme (24) qui s'obtiennent d'une solution $(x_1^*, \ldots, x_k^*)$ fixée de l'équation (22) (quand a parcourt l'ensemble des nombres entiers rationnels).

Le Corollaire 1.6 nous permet de donner la solution complète des équations diphantiennes du type discriminant.

Théorème 5. *Soient $k \geqq 2$ et $D \neq 0$ des entiers rationnels et soit $\varkappa > 9 \binom{k-1}{2}$ une constante. Chaque famille de solutions de l'équation diophantienne* (22) *possède un représentant $(x_1^*, \ldots, x_k^*)$ ayant la propriété*

$$\max_{1 \leqq i \leqq k} (|x_i^*|) < \exp\{c_7 |D|^{\varkappa}\}, \tag{25}$$

où $c_7 = c_7(k, \varkappa)$ est la constante positive effectivement calculable figurant dans le Corollaire 1.6.

Donc, on peut décider la solubilité de (22) et on peut déterminer un représentant dans chaque famille de solutions. De plus, d'après la remarque qui suit le Corollaire 1.5, toute famille de solutions a un représentant unique $(x_1^*, \ldots, x_k^*)$ vérifiant (25)

et $0 \leqq x_1^* < k$, qui peut être aisément déterminé en connaissance d'un représentant arbitraire de la famille de solutions.

Nous remarquons qu'on pourrait définir le polynôme du type discriminant d'ordre k plus généralement, sous la forme $D(x_0, \ldots, x_k) = D(f(x))$, où $f(x) = x_0 x^k + \ldots + x_k$. Si nous tenons compte encore les discriminants des dérivées de $f(x)$, on peut permettre aussi le cas $D = 0$. De plus, tous les résultats du § 2 (sauf les Corollaires 1.7 et 1.8) peuvent être formulés aux équations diophantiennes. Ici nous ne présentons que le Corollaire 1.3 dans le cas $j = 0$, $a_0 = 1$.

Théorème 6. *Soient* $k \geqq 2$, $D \neq 0$, $1 \leqq i \leqq k$ *des nombres entiers et soient* $\varkappa > 9\binom{k-1}{2}$, $A_i \geqq 0$ *des constantes. Si* $(x_1, \ldots, x_k) \in Z^k$ *est une solution de l'équation* (22) *telle que*

$$|x_i| \leqq A_i, \tag{26}$$

alors

$$\max_{1 \leqq l \leqq k} (|x_l|) < [A_i^{1/i} + M]^k, \tag{27}$$

où $M = \exp\{c_6 |D|^{\varkappa}\}$ *avec la constante* $c_6 = c_6(k, \varkappa) > 0$ *effectivement calculable figurant dans le Corollaire 1.2.*

Le Théorème 6 nous permet de donner la solution complète de certaines équations diophantiennes à deux inconnues. En effet, $F(x, y) \in Z[x, y]$ étant un polynôme tel que $F(x, y) = D(a_1, \ldots, a_{i-1}, x_i, \ldots, x_j, a_{j+1}, \ldots, a_k)$ $(k \geqq 3)$, où $x_i = x$, $x_j = y$ pour certains $1 \leqq i < j \leqq k$ et $a_s \in Z (s = 1, \ldots, k;\ s \neq i, j)$, alors, d'après le Théorème 6, l'équation $F(x, y) = D$ ($D \neq 0$ entier) n'admet qu'un nombre fini de solutions en entiers rationnels et toutes les solutions (x, y) entières sont effectivement déterminables. Nous remarquons que, en général (dans la majorité des cas), les théorèmes effectifs connus de C. RUNGE [19], A. BAKER [2], [3] et A. BAKER et J. COATES [4] ne sont pas applicables pour ces équations à deux inconnues. De plus, en choisissant convenablement les a_s, le Théorème 6 implique certains résultats effectifs connus. Par exemple, pour les solutions (x, y) en entiers rationnels de l'équation hyperelliptique particulière

$$y^{k-1} - x^k = a$$

on a (en vertu du Théorème 6, avec les choix $a_1 = \ldots = a_{k-2} = 0$, $x_{k-1} = -kx$, $x_k = (k-1)y$ et $D = k^k (k-1)^{k-1} \cdot a$)

$$\max(|x|, |y|) < \exp\{c_{16} |a|^{\varkappa}\},$$

où $\varkappa > 9\binom{k-1}{2}$ et la constante $c_{16} = c_{16}(k, \varkappa)$ est positive et effectivement calculable. En particulier, cela implique[4]) le célèbre théorème de A. BAKER [2] concernant l'équation de Mordell.

Nous étudierons les applications aux équations à deux inconnues dans un travail ultérieur.

---

[4]) Récemment, dans le cas $k = 3$ H. M. STARK [21] a obtenu une meilleure majoration pour $\max(|x|, |y|)$.

b) *Sur les "discriminant form" équations* [5])

Soit $K=Q(\alpha)$ un corps de nombres algébriques de degré $k\geqq 2$ et les conjugués de α soient $\alpha^{(1)}=\alpha, \ldots, \alpha^{(k)}$. Soit $M=\{\alpha_1, \ldots, \alpha_m\}$ un module dans K et soit $\alpha_s^{(i)}$ le conjugué de α_s correspondant à $\alpha^{(i)}$ $(s=1, \ldots, m;\ i=1, \ldots, k)$. Posons

$$L^{(i)}(x) = \alpha_1^{(i)}x_1 + \cdots + \alpha_m^{(i)}x_m \quad (i = 1, \ldots, k)$$

et considérons la forme à coefficients rationnels de degré $k(k-1)$

$$D_{K/Q}(\alpha_1 x_1 + \cdots + \alpha_m x_m) = \prod_{1\leqq i<j\leqq k} \left(L^{(j)}(x) - L^{(i)}(x)\right)^2. \tag{28}$$

Supposons qu'il existe un $\beta=\alpha_1 x_1^0+\cdots+\alpha_m x_m^0 \in M$, primitif dans K (c'est-à-dire soit M un module de degré k), lorsque $D_{K/Q}(\alpha_1 x_1^0+\cdots+\alpha_m x_m^0)=D_{K/Q}(\beta)$. C'est pourquoi nous appelons «*discriminant forms*»[5] les formes de la forme (28). Par exemple, si $K=Q(\sqrt[3]{a})$ où $a\neq d^3$ (d entier), alors

$$D_{K/Q}(x_1\sqrt[3]{a}+x_2\sqrt[3]{a^2}) = -27a^2(x_1^3-ax_2^3)^2.$$

Du Théorème 3, en tenant compte de la remarque qui suit le Théorème 2, on peut déduire le suivant.

Théorème 7. *Soit K un corps de nombres algébriques de degré $k\geqq 3$ avec discriminant D_K. Soient $1, \alpha_1, \ldots, \alpha_m (m\geqq 2)$ des nombres Q-linéairement indépendants dans K avec $H(\alpha_i)\leqq H$ $(i=1, \ldots, m)$ et le plus petit commun multiple de leurs dénominateurs soit $\leqq A$. Soient $D\neq 0$ un nombre rationnel et $\varepsilon>0, \varkappa>9\binom{k-1}{2}$ des constantes. Si $(x_1, \ldots, x_m)\in Z^m$ est une solution de l'équation diophantienne*

$$D_{K/Q}(\alpha_1 x_1 + \cdots + \alpha_m x_m) = D, \tag{29}$$

alors on a

$$\max_{1\leqq i\leqq m}(|x_i|) < (AH)^{m-1}\exp\{c_{17}[|D_K|^{3(k-1)(k-2)}(|D_K|^{3(k-1)(k-2)/2}+\log|AD|)]^{1+\varepsilon}\} \tag{30}$$

et

$$\max_{1\leqq i\leqq m}(|x_i|) < (AH)^{m-1}\exp\{c_{18}|A^{k(k-1)}D|^{\varkappa}\} \tag{31}$$

avec des constantes positives $c_{17}=c_{17}(k, \varepsilon)$ et $c_{18}=c_{18}(k, \varkappa)$ effectivement calculables.

En particulier, si $\alpha_1, \ldots, \alpha_m$ sont des entiers dans K, on peut choisir $A=1$ dans (30) et (31).

Il est intéressant d'observer que H ne figure dans l'exposant ni dans (30) ni dans (31).

Comme le «discriminant form» $D_{K/Q}(\alpha_1 x_1+\cdots+\alpha_m x_m)$ est produit des «norm forms» (de plus, dans certains cas la puissance d'un seul «norm form»), de notre Théorème 7 nous pouvons déduire des résultats concernant la résolubilité effective des «norm form» équations. Ce sera l'objet d'une prochaine publication.

[5]) Utilisant la terminologie anglaise, cette appellation correspond à celles "norm form" et "index form".

Soit $M \neq 0$ un module du corps de nombres K tel que l'espace vectoriel engendré par M sur Q ne contienne pas Q. Du Théorème 7 il résulte que dans M il n'existe qu'un nombre fini d'éléments de discriminant D donné pour tout nombre rationnel $D \neq 0$ (et tous ces éléments sont effectivement déterminables). On peut aisément vérifier que la condition concernant M est nécessaire. A cette fin considérons un module $M = \{\alpha_1, \ldots, \alpha_m\}$ tel que $1, \alpha_1, \ldots, \alpha_m$ soient Q-linéairement dépendants. Si (29) admet une solution $(x_1, \ldots, x_m)$ en entiers rationnels et si $u_1\alpha_1 + \cdots + u_m\alpha_m \in Z$ avec des entiers rationnels $u_1, \ldots, u_m$ non tous nuls, alors $(x_1+u_1, \ldots, x_m+u_m)$ est également une solution de (29). Ainsi, de la solubilité de (29) il résulte qu'il a une infinité de solutions (mais on peut effectivement déterminer un ensemble fini de solutions $(x_{1i}, \ldots, x_{mi})$ $(i=1, \ldots, l)$ tel qu'on ait, pour toute solution $(x_1, \ldots, x_m)$, $(x_1-x_{1i})\alpha_1 + \ldots + (x_m-x_{mi})\alpha_m \in Q$ pour un $1 \leqq i \leqq l$).

Soit ensuite en particulier O un ordre du corps de nombres algébriques K de degré $k \geqq 3$ et soit $1, \alpha_1, \ldots, \alpha_{k-1}$ une base de O. Alors il est bien connu que

$$D_{K/Q}(\alpha_1 x_1 + \cdots + \alpha_{k-1}x_{k-1}) = [F(x_1, \ldots, x_{k-1})]^2 D_O, \tag{32}$$

où D_O signifie le discriminant de O et $F(x_1, \ldots, x_{k-1}) \in Z[x_1, \ldots, x_{k-1}]$ est une forme décomposable de degré $\frac{k(k-1)}{2}$. Si $\alpha = \alpha_1 x_1^0 + \cdots + a_{k-1}x_{k-1}^0 \in O$ $(x_1^0, \ldots, x_{k-1}^0 \in Z)$, alors $F(x_1^0, \ldots, x_{k-1}^0) = I(\alpha)$ est l'indice de α dans O. C'est pourquoi la forme $F(x_1, \ldots, x_{k-1})$ est appelée «*index form*» de la base $1, \alpha_1, \ldots, \alpha_{k-1}$ de O. (Pour un exposé détaillé des «index forms» du troisième degré voir [8].) (32) assure le lien entre les nombres algébriques de discriminant donné et les équations diophantiennes du type $F(x_1, \ldots, x_{k-1}) = a$, où $F(x_1, \ldots, x_{k-1})$ est un «index form» (dans le cas $k=3$ voir B. N. Delone et D. K. Faddeev [8] et T. Nagell [14]).

Corollaire. *Soit K un corps de nombres algébriques de degré $k \geqq 3$ et soit O un ordre dans K avec une base $1, \alpha_1, \ldots, \alpha_{k-1}$, où $H(\alpha_i) \leqq H$ $(i=1, \ldots, k-1)$. Désignons par $F(x_1, \ldots, x_{k-1})$ le «index form» de cette base de O et soit $\varkappa > 9(k-1)(k-2)$ une constante. Si $(x_1, \ldots, x_{k-1}) \in Z^{k-1}$ est une solution de l'équation*

$$F(x_1, \ldots, x_{k-1}) = a \quad (a \neq 0 \text{ entier rationnel}), \tag{33}$$

alors on a

$$\max_{1 \leqq i \leqq k-1} (|x_i|) < \exp\{c_{19}|aH^{k-1}|^{\varkappa}\},$$

où $c_{19} = c_{19}(k, \varkappa)$ est une constante positive calculable effectivement.

Si en particulier O_K est l'anneau des entiers de K avec un index form $F(x_1, \ldots, x_{k-1})$ et $a = \pm 1$, alors on peut déterminer toutes les solutions éventuelles de $F(x_1, \ldots, x_{k-1}) = \pm 1$ et ainsi tout $\alpha \in O_K$ pour lequel $O_K = Z[\alpha]$ (voir encore le Corollaire 3.3).

Il est connu (voir B. N. Delone et D. K. Faddeev [8]) que toute forme irréductible $F(x, y) \in Z[x, y]$ du troisième degré est le «index form» d'une base $1, \alpha_1, \alpha_2$ convenable d'un ordre convenable et, en connaissance des coefficients de $F(x, y)$, $H(\alpha_1)$ et $H(\alpha_2)$ peuvent être aisément déterminés. Ainsi de ce dernier Corollaire résulte un cas particulier (le cas des équations cubiques) du célèbre théorème de A. Baker [2] concernant l'équation de Thue.

6. Démonstrations

La démonstration du Théorème 1 est basée sur la démonstration de notre Théorème 2 publié dans [12]. Nous conserverons les notations de [12] et nous n'entrerons dans les détails de la démonstration que là où elle est différente de celle donnée dans [12].

Nous remplacerons le Lemme 2 de [12] (Théorème de A. Baker [1]) par un théorème récent de H. M. Stark [20].

Soient $\alpha_1, \ldots, a_m$ des nombres algébriques non nuls de degré $\leqq n$ et de hauteur $H(\alpha_i) \leqq A_i$ $(i=1, \ldots, m)$, où $A_i \geqq e$ pour tout i. Désignons par $\log \alpha_1, \ldots, \log \alpha_m$ les valuers principales des logarithmes. Alors il est vrai le suivant.

Lemme 1. (H. M. Stark [20]). *Soient $\beta_1, \ldots, \beta_m$ des nombres algébriques de degré $\leqq n$ et de hauteur $\leqq B$. Si $B < H^{\log H}$, $\varepsilon > 0$, $\delta > 0$ des constantes et si*

$$0 < |\beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m| < e^{-\delta H},$$

alors

$$H < c_{20} \left(\prod_{j=1}^{m} \log A_j \right)^{1+\varepsilon}, \tag{34}$$

où $c_{20} = c_{20}(m, n, \varepsilon, \delta)$ est une constante positive effectivement calculable.

Nous appliquerons ce profond résultat dans le cas particulier où $\beta_i = b_i \in Z$ $(i = 1, \ldots, m)$. Plus précisément, nous utiliserons sa conséquence que voici (pour la déduction voir [2], p. 176): Si les α_i ci-dessus et les nombres entiers rationnels $b_1, \ldots, b_{m-1}$ de valeur absolue $\leqq B$ satisfont à

$$0 < |\alpha_1^{b_1} \ldots \alpha_{m-1}^{b_{m-1}} - \alpha_m| < e^{-\delta H} \tag{35}$$

et $mB < H^{\log H}$, alors on a (34).

Dans la suite soit K un corps de nombres algébriques de degré n_K, son régulateur soit R et la valeur absolue de son discriminant soit D. Si $K = Q(\alpha)$, désignons par $\alpha^{(1)}, \ldots, \alpha^{(n_K)}$ les conjugués de α ordonnés de telle manière que $\alpha^{(1)}, \ldots, \alpha^{(s)}$ soient réels et $\alpha^{(s+1)}, \ldots, \alpha^{(s+t)}$ soient des conjugués complexes de $\alpha^{(s+t+1)}, \ldots, \alpha^{(s+2t)}$ respectivement $(s+2t=n_K)$. Posons $r = s+t-1$, soit $e_i = 1$ pour $i=1, \ldots, s$ et $e_i = 2$ pour $i = s+1, \ldots, s+t$. Enfin, désignons par $h(\alpha)$ le maximum des valeurs absolues des conjugués de α.

Lemme 2. (H. M. Stark [21]). *Soit $r \geqq 1$. Il existe des unités indépendantes $\eta_1, \ldots, \eta_r$ dans K vérifiant*

$$\prod_{j=1}^{r} \log A_j \leqq c_{21} R \leqq c_{22} (\log D)^{n_K - 1} D^{1/2}, \tag{36}$$

où $A_j = \max(e, h(\eta_j))$, de plus les valeurs absolues des coefficients de l'inverse de la matrice $\|e_i \log |\eta_j^{(i)}|\|$ $(i, j = 1, \ldots, r)$ sont $\leqq c_{23}$, où c_{21}, c_{22} et c_{23} sont des constantes positives effectivement calculables qui ne dépendent que de n_K.

Démonstration: voir [21], p. 253—254.

Considérons les solutions $(\beta_1, \beta_2, \beta_3)$ de l'équation

$$\beta_1+\beta_2+\beta_3 = 0, \quad \beta_1\beta_2\beta_3 \neq 0 \tag{37}$$

en entiers de K. Appelons les solutions $(\beta_1', \beta_2', \beta_3')$ et $(\beta_1'', \beta_2'', \beta_3'')$ associées, quand $(\beta_1'', \beta_2'', \beta_3'')=(\varepsilon\beta_1', \varepsilon\beta_2', \varepsilon\beta_3')$ avec une unité ε de K. Soit $n \geqq \max(n_K, 4)$ une constante.

Le lemme suivant est une amélioration du Lemme 4 dans [12].

Lemme 3. *Avec les notations ci-dessus soient $G \geqq 1$ et $\varepsilon>0$ des constantes et soit $(\beta_1, \beta_2, \beta_3)$ une solution de* (37) *en entiers de K vérifiant*

$$|N_{K/Q}(\beta_i)| \leqq G \quad (i = 1, 2, 3). \tag{38}$$

Alors il existe une solution $(\beta_1', \beta_2', \beta_3')$ de (37), *associée à $(\beta_1, \beta_2, \beta_3)$, telle que*

$$h(\beta_i') < \exp\{c_{24}[R^2(\log G + R)]^{1+\varepsilon}\} < \exp\{c_{26}[c_{25}^2(\log G + c_{25})]^{1+\varepsilon}\} \quad (i = 1, 2, 3), \tag{39}$$

où $c_{25}=(\log D)^{n-1}\sqrt{D}$ et $c_{24}=c_{24}(n, \varepsilon)$, $c_{26}=c_{26}(n, \varepsilon)$ sont des constantes positives effectivement calculables.

Démonstration. Nous suivrons la démonstration du Lemme 4 de [12].

Il suffit de considérer le cas où $r>0$. Soit $(\beta_1, \beta_2, \beta_3)$ une solution de (37) avec la propriété (38). Considérons un système d'unités indépendantes $\eta_1, \ldots, \eta_r$ satisfaisant à l'assertion du Lemme 2. Nous obtenons (20), (21) et (22) dans [12], avec $c_{27}R$ au lieu de n^2c_3 (où c_{27} est une constante positive effectivement calculable qui ne dépend que de n). On obtient, de la même façon que dans [12], que

$$H\left(\frac{\gamma_i}{\gamma_j}\right) < G^2 \exp\{c_{28} R\}.$$

Soit maintenant dans l'équation (22) de [12] $X=\max\limits_{1\leqq i\leqq r}|x_i|$, $Y=\max\limits_{1\leqq i\leqq r}|y_i|$ et

$$X \geqq Y > c_{29}(\log G + R) \tag{40}$$

avec une constante $c_{29}=c_{29}(n)>0$ effectivement calculable qui sera déterminée ultérieurement. Comme dans [12], la constante c' soit déterminée de telle manière que

$$c'X = \left|\log|\gamma_1^{(J)}/\beta_1'^{(J)}|\right| = \max_{1\leqq j\leqq r}\left|\log|\gamma_1^{(j)}/\beta_1'^{(j)}|\right|,$$

où c' est supérieur à une constante positive $c_{30}=c_{30}(n)$ calculable explicitement (voir [12]). Pour un indice l convenable on obtient (voir [2] et [12])

$$\frac{|\beta_1'^{(l)}|}{|\gamma_2^{(l)}|} < e^{\log G + c_{31}R - \frac{c'X}{n}} \leqq e^{\log G + c_{31}R - \frac{c'Y}{n}}.$$

Si $c_{29}=2nc_{31}c'^{-1}$, alors d'après (40) on a

$$\log G + c_{31}R - \frac{c'Y}{n} \leqq -c_{32}Y,$$

où $c_{32}=c'/2n>c_{30}/2n$. Il en résulte que

$$\frac{|\beta_1'^{(l)}|}{|\gamma_2^{(l)}|}=\left|\frac{\gamma_1^{(l)}}{\gamma_2^{(l)}}\eta_1^{(l)x_1}\dots\eta_r^{(l)x_r}\right|=\left|\eta_1^{(l)y_1}\dots\eta_r^{(l)y_r}+\frac{\gamma_3^{(l)}}{\gamma_2^{(l)}}\right|<e^{-\delta Y},$$

où $\delta=c_{30}/2n>0$. $\varepsilon>0$ étant une constante arbitraire, d'après la remarque qui suit le Lemme 1 il existe une constante positive c_{33}, effectivement calculable et ne dépendant que de n et ε, telle que

$$Y<c_{33}\left(\log A_{r+1}\prod_{j=1}^{r}\log H(\eta_j)\right)^{1+\varepsilon},$$

où $A_{r+1}=H(\gamma_3/\gamma_2)$. Avec la notation $A_j=\max\left(e,h(\eta_j)\right)$ $(j=1,\dots,r)$, en vertu de la majoration

$$H(\eta_j)\leqq(2h(\eta_j))^n\leqq 2^nA_j^n,$$

nous avons

$$Y<c_{34}\left(\log A_{r+1}\prod_{j=1}^{r}\log A_j\right)^{1+\varepsilon}.$$

Mais d'après le Lemme 2

$$\prod_{j=1}^{r}\log A_j\leqq c_{21}R\leqq c_{22}(\log D)^{n-1}D^{1/2}$$

avec les constantes c_{21}, $c_{22}>0$ figurant dans le Lemme 2. Comme

$$\log A_{r+1}\leqq c_{35}(\log G+R),$$

on obtient

$$Y<c_{36}[R(\log G+R)]^{1+\varepsilon}=c_{37} \tag{41}$$

avec des constantes positives $c_{35}=c_{35}(n)$ et $c_{36}=c_{36}(n,\varepsilon)$ qui sont effectivement calculables.

Il en résulte que pour l'un au moins de X et Y, par exemple pour Y on a (41). Alors (suivant la démonstration de [12]) d'après le Lemme 2 $h(\eta_j)<\exp\{c_{38}R\}$ et

$$h(\beta_1')\leqq h(\beta_3')+h(\beta_2')\leqq h(\gamma_3)+h(\gamma_2)\left(\prod_{j=1}^{r}h(\eta_j)^{n_K-1}\right)^{Y}\leqq$$

$$\leqq G^{1/n_K}e^{c_{27}R}+G^{1/n_K}e^{c_{27}R+c_{38}rR(n_K-1)c_{37}}\leqq$$

$$\leqq\exp\{c_{39}Rc_{37}\}=\exp\{c_{40}[R^2(\log G+R)]^{1+\varepsilon}\}\leqq$$

$$\leqq\exp\{c_{41}[c_{25}^2(\log G+c_{25})]^{1+\varepsilon}\},$$

où $c_{25}=(\log D)^{n-1}D^{1/2}$ et c_{39}, c_{40}, c_{41} sont des constantes positives, effectivement calculables, dépendant seulement de ε et n. La majoration obtenue est évidemment valable aussi pour $h(\beta_2')$, $h(\beta_3')$.

Lemme 4. (H. M. STARK, [22]) *Soient $K_1,\dots,K_a$ des corps de nombres algébriques et soit $M=K_1\dots K_a$. Si $[K_i:Q]=n_i$ et $m=[M:Q]$, alors pour leurs dicriminants on a*

$$D_M\Big|\prod_{i=1}^{a}D_{K_i}^{m/n_i}.$$

Nous aurons encore besoin du lemme suivant.

Lemme 5. *Soit* $f(x)=a_0x^k+a_1x^{k-1}+\cdots+a_k$ *un polynôme à coefficients réels tel que* $|a_0|\geqq 1$. *Soient* A, B, C, ϱ *des constantes et* α *un nombre réel vérifiant*

$$1 \leqq A \leqq |a_0|, \quad |a_1|+\ldots+|a_k| \leqq B$$

et

$$|f(\alpha)| \leqq C|\alpha|^{\varrho}, \quad |\alpha| \geqq 1, \quad 0 \leqq \varrho < k.$$

Alors

$$|\alpha| \leqq \left[(B/A)^{\min(k-\varrho,1)}+(C/A)^{\min\left(\frac{1}{k-\varrho},1\right)}\right]^{\max\left(\frac{1}{k-\varrho},1\right)}.$$

Démonstration. D'après l'hypothèse

$$C|\alpha|^{\varrho} \geqq |f(\alpha)| \geqq |a_0\alpha^k|-|a_1\alpha^{k-1}+\cdots+a_k| \geqq A|\alpha|^k-B|\alpha|^{k-1},$$

d'où

$$C/A \geqq |\alpha|^{k-\varrho}\left(1-\frac{B/A}{|\alpha|}\right). \tag{42}$$

Si $B=0$ ou $C=0$, on obtient immédiatement la majoration désirée. Soit donc $B, C>0$. Ici on peut supposer $1-\dfrac{B/A}{|\alpha|}>0$.

Considérons d'abord le cas où $k-\varrho\geqq 1$. D'après (42) il résulte que

$$|\alpha| \leqq \max\left\{\sigma(C/A)^{1/(k-\varrho)}, \frac{\sigma}{\sigma-1}B/A\right\}$$

pour tout $\sigma>1$. Vu que $\sigma(C/A)^{1/(k-\varrho)}$, comme fonction de σ, est strictement croissante sur l'intervalle $(1, \infty)$ et $\dfrac{\sigma}{\sigma-1}B/A$ est strictement décroissante, la fonction de droite atteint son minimum lorsque les deux membres sont égaux. En exprimant σ de l'équation obtenue de cette manière, on déduit

$$|\alpha| \leqq B/A+(C/A)^{1/(k-\varrho)}.$$

Considérons ensuite le cas où $0<k-\varrho<1$. Du (42) il résulte que

$$|\alpha| \leqq \max\left\{\frac{1}{(1-\sigma)^{1/(k-\varrho)}}(C/A)^{1/(k-\varrho)}, \frac{B/A}{\sigma^{1/(k-\varrho)}}\right\}$$

pour tout $0<\sigma<1$. Au coté droit considérons les deux membres comme fonctions de σ. Le premier est strictement croissant sur l'intervalle $(0, 1)$ et le second est strictement décroissant. La fonction de droite atteint donc son minimum lorsque les membres sont égaux. Par conséquent, on a

$$|\alpha| \leqq [(B/A)^{k-\varrho}+C/A]^{1/(k-\varrho)}$$

et notre proposition se trouve démontrée.

Démonstration du Théorème 1. Nous démontrerons le théorème en plusieurs étapes. Nous prouverons d'abord l'assertion du Corollaire 1.5.

Considérons tout d'abord le cas particulier $j=0$, $a_0=1$. Au cours de la démonstration nous suivrons la démonstration de notre Théorème 2 obtenu dans [12] et nous ne détaillerons que les modifications nécessaires. Dans la suite c_9, c_{10}, c_{11}, c_{12} et c_{20} signifieront les constantes figurant dans [12] (qui diffèrent des constantes utilisées aux paragraphes précédents).

Nous supposons d'abord que $f(x)$ est irréductible sur Q. Dans le cas $k=2$, on obtient trivialement, d'après [12], $\|f^*\| \leqq |D(f)|$ pour un f^* convenable. Si $k \geqq 3$, dans [12] le degré n_{ijl} de K_{ijl} est $\leqq k(k-1)(k-2)=n$. $Q(\alpha^{(i)})$, $Q(\alpha^{(j)})$ et $Q(\alpha^{(l)})$ sont de degré k et leurs discriminants sont en valeur absolue $\leqq D_0=D$. Ainsi, en employant le Lemme 4, dans (28) (voir [12]) on peut prendre

$$|D_{K_{ijl}}| \leqq D^{3(k-1)(k-2)} = c_9,$$

de plus, si $L=Q(\alpha)$ est une extension normale de Q, nous obtenons

$$|D_{K_{ijl}}| \leqq D = c_9.$$

Soit $\varepsilon>0$ une constante qui sera déterminée ultérieurement. Posons $c_{11}=(\log c_9)^{n-1}\sqrt{c_9}$ et $c_{10}=D^{n/2}$. En appliquant notre Lemme 3 au lieu du Lemme 2 de [12], on obtient

$$\max_{1 \leqq s \leqq 3} h(\beta_s^{(ijl)}) < \exp\{c_{42}[c_{11}^2(c_{11}+\log c_{10})]^{1+\varepsilon}\} = c_{12}$$

avec une constante positive $c_{42}=c_{42}(k, \varepsilon)$ effectivement calculable.

Soit $\varkappa=\varkappa_0>9\binom{k-1}{2}$ une constante. Suivons la démonstration donnée dans [12]. En calculant avec $c_9=D^{3(k-1)(k-2)}$ et $\varepsilon=\dfrac{\varkappa}{9(k-1)(k-2)}-\dfrac{1}{2}$, il résulte que

$$H(\alpha') = \|f^*\| < c_{12}^{6kn} \leqq \exp\{c_{43}D^{\varkappa}\}, \tag{43}$$

où $c_{43}=c_{43}(k, \varkappa)$ est une constante positive effectivement calculable.

Si $Q(\alpha)$ est une extension normale de Q, en calculant avec $c_9=D$, dans (43) il suffit de supposer que $\varkappa>3/2$.

Enfin, supposons que $f(x)$ est réductible et soit

$$f(x) = f_1(x) \dots f_r(x)$$

sa décomposition en polynômes irréductibles dans $Z[x]$, lorsque $0<|D(f_i)| \leqq D$ pour tout $1 \leqq i \leqq r$. Par suite de (43) il existe un polynôme f_i^* équivalent à f_i tel que

$$\|f_i^*\| < \exp\{c_i(k_i, \varkappa_i')D^{\varkappa_i'}\} \quad (i = 1, \dots, r),$$

où $k_i=\deg f_i$, $\varkappa_i'>9\binom{k_i-1}{2}$ et la constante positive $c_i(k_i, \varkappa_i')$ est effectivement calculable pour tout i. Cela implique

$$\|f_i^*\| < \exp\{c_{44}(k, \varkappa)D^{\varkappa}\} = c_{20} \quad (i = 1, \dots, r),$$

d'où il s'ensuit (voir [12]) la majoration désirée.

Considérons ensuite le cas $j=0$, $a_0 \neq 1$ (dans le Corollaire 1.5). Soit $f(x)= =a_0x^k+a_1x^{k-1}+\cdots+a_k \in Z[x]$ $(k \geqq 2)$ et considérons le polynôme $F(a_0x)=(a_0x)^k+ +a_1(a_0x)^{k-1}+\cdots+a_0^{k-1}a_k=a_0^{k-1}f(x)$, où $F(y)=y^k+a_1y^{k-1}+\cdots+a_0^{k-1}a_k \in Z[y]$ est unitaire. On peut aisément vérifier que

$$|D(F)| = |a_0|^{(k-1)(k-2)} \cdot |D(f)|.$$

Soit $\varkappa > 9\binom{k-1}{2}$. Comme nous l'avons démontré précédemment, il existe un $a \in Z$ tel que

$$\|F^*\| < \exp\{c_{45}(k, \varkappa)|D(F)|^{\varkappa}\},$$

où $F^*(y)=F(y+a)$. Soient t, t' des nombres entiers vérifiant $a=a_0t+t'$, $0 \leqq t' < |a_0|$ et soit $\eta=\dfrac{t'}{a_0}$. On voit facilement que

$$F^*(a_0x) = F(a_0x+a) = a_0^{k-1}\left[a_0\left(x+\frac{a}{a_0}\right)^k+a_1\left(x+\frac{a}{a_0}\right)^{k-1}+\cdots+a_k\right] = a_0^{k-1}h(x).$$

Cela entraîne $h(x-\eta)=f(x+t)=f^*(x) \in Z[x]$ et

$$\|h\| \leqq \max(|a_0|, \|F^*\|),$$

d'où, par suite de $|a_0|=A$ et $|D(f)| \leqq D$, pour $k \geqq 3$ on obtient

$$\|f^*\| \leqq \max_{0 \leqq i \leqq k} \frac{|h^{(i)}(-\eta)|}{i!} \leqq c_{46}\|h\| < \exp\{c_{47}[A^{(k-1)(k-2)}D]^{\varkappa}\} \tag{44}$$

avec une constante positive $c_{47}=c_{47}(k, \varkappa)$ effectivement calculable. Enfin, en utilisant la majoration obtenue dans le cas $k=2$ et $a_0=1$, si $k=2$ il résulte que

$$\|f^*\| \leqq 3AD. \tag{44'}$$

Dans la suite nous étendrons l'assertion démontrée ci-dessus au cas $j \geqq 0$. Soit $0<j \leqq k-2$ un entier et soit $0<|D(f^{(j)})| \leqq D_j$. Comme nous l'avons démontré ci-dessus, il existe un polynôme $f^{(j)}(x-a)$, équivalent à $f^{(j)}(x)$, satisfaisant à (44) ou (44'). Autrement dit, si

$$f^*(x) = f(x-a) = a_0x^k+a_1^*x^{k-1}+\cdots+a_k^*, \quad k-j \geqq 3 \quad \text{et} \quad \varkappa_j > 9\binom{k-j-1}{2},$$

alors

$$\max_{1 \leqq i \leqq k-j}(|a_i^*|) \leqq \|f^{*(j)}\| < \exp\{c_{48}[A^{(k-j-1)(k-j-2)}D_j]^{\varkappa_j}\} = c_{49}$$

avec une constante positive $c_{48}=c_{48}(k, j, \varkappa_j)$ effectivement calculable, et si $k-j=2$, alors (avec le choix $a_0^*=a_0$) on a

$$\max_{0 \leqq i \leqq 2}(|a_i^*|) \leqq 2k^2AD_{k-2} = c'_{49}.$$

Considérons la forme de déterminant de $D(f^{*(j-1)})$. Développons-la et considérons-la comme polynôme en a_{k-j+1}^*

$$D(f^{(j-1)}) = D(f^{*(j-1)}) = A_0a_{k-j+1}^{*k-j}+A_1a_{k-j+1}^{*k-j-1}+\cdots+A_{k-j}.$$

Soit d'abord $k-j \geqq 3$ et appliquons le Lemme 5 pour majorer $|a^*_{k-j+1}|$. Ici

$$|A_0| > |a_0|^{k-j+1} \quad \text{et} \quad \sum_{i=1}^{k-j} |A_i| \leqq c_{50}(k,j)|a_0| c_{49}^{2(k-j)}.$$

Par conséquent, d'après le Lemme 5 on a

$$|a^*_{k-j+1}| \leqq A^{-(k-j)} c_{50}(k,j) c_{49}^{2(k-j)} + \frac{|D(f^{(j-1)})|^{1/(k-j)}}{A} \leqq$$

$$\leqq \exp\{c_{51}[A^{(k-j-1)(k-j-2)} D_j]^{\varkappa_j}\} + \frac{D_{j-1}^{1/(k-j)}}{A}.$$

En répétant ce procédé successivement pour $|a^*_{k-j+2}|, \ldots, |a^*_k|$, il résulte que

$$\|f^*\| < c_{53}\left(\ldots\left(\left(\exp\{c_{52}[A^{(k-j-1)(k-j-2)} D_j]^{\varkappa_j}\} + \frac{D_{j-1}^{1/(k-j)}}{A}\right)^{2(k-j+1)} + \right.\right.$$

$$\left.\left. + \frac{D_{j-2}^{1/(k-j+1)}}{A}\right)^{2(k-j+2)} + \cdots\right)^{2(k-1)} + \frac{D_0^{1/(k-1)}}{A} = L_j \tag{45}$$

avec des constantes positives $c_{52} = c_{52}(k, j, \varkappa_j)$ et $c_{53}(k, j)$ effectivement calculables.

Si $j = k-2$, en calculant avec c'_{49}, il résulte que dans (45) on peut prendre $(2k^2 A D_{k-2})^4$ au lieu de $\exp\{c_{52}[A^{(k-j-1)(k-j-2)} D_j]^{\varkappa_j}\}$.

Comme

$$f(x) = f^*(x+a) = f^*(a) + \frac{f^{*\prime}(a)}{1!} x + \cdots + \frac{f^{*(k)}(a)}{k!} x^k,$$

$$a_i = \frac{f^{*(k-i)}(a)}{(k-i)!} \quad (i = 0, \ldots, k)$$

est un polynôme de degré i en a et son coefficient dominant est $\binom{k}{i} a_0$. Substituons ces formes de $a_1, \ldots, a_k$ à $\mathscr{F}(x_1, \ldots, x_k)$. En vertu de la restriction concernant $\mathscr{F}$, $\mathscr{F}(a_1, \ldots, a_k)$ sera un polynôme de degré m en a, c'est-à-dire on peut écrire

$$\mathscr{F}(a_1, \ldots, a_k) = B_0 a^m + B_1 a^{m-1} + \cdots + B_m = g(a),$$

où $g(x) \in Z[x]$.

Dans (1) le membre de droite

$$F\|f\|^\tau = F\left\{\max_{0 \leqq i \leqq k} \frac{|f^{*(i)}(a)|}{i!}\right\}^\tau.$$

Considérons le cas où $|a| > kL_j$. Alors

$$F\|f\|^\tau \leqq (A+1)^\tau F \cdot |a|^{k\tau}$$

et ainsi

$$|g(a)| \leqq (A+1)^\tau F \cdot |a|^{k\tau}. \tag{46}$$

Appliquons le Lemme 5. Si dans $\mathscr{F}(x_1, \ldots, x_k)$ un terme de la forme $bx_1^{l_1} \ldots x_k^{l_k}$, après la substitution $x_i = a_0 \binom{k}{i} a^i$ $(i=1, \ldots, k)$, sera de degré m en a, alors son coefficient sera divisible par $a_0^{l_1+\cdots+l_k}$, d'où

$$|B_0| \geqq A. \tag{47}$$

Nous allons majorer ensuite la somme $\sum_{i=1}^{m} |B_i|$. Substituons $x_i = \dfrac{f^{*(k-i)}(a)}{(k-i)!}$ à un terme arbitraire $bx_1^{l_1} \ldots x_k^{l_k}$ de $\mathscr{F}$ et puis ordonnons-le suivant les puissances décroissantes de a. La somme des valeurs absolues des coefficients est majorable par

$$\|\mathscr{F}\| \left[\binom{k}{k-1}^{l_1} \ldots \binom{k}{1}^{l_{k-1}} \binom{k}{0}^{l_k} \right] L_j^{l_1+\ldots+l_k} 2^{l_1} \ldots (k+1)^{l_k} \leqq \|\mathscr{F}\| (c_{54} L_j)^{\deg \mathscr{F}},$$

où $c_{54} = c_{54}(k)$ est une constante positive effectivement calculable. Comme dans $\mathscr{F}$ le nombre de termes est $\leqq \binom{\deg \mathscr{F} + k}{k} \leqq c_{55}^{\deg \mathscr{F}}$, il en résulte que

$$\sum_{i-1}^{m} |B_i| \leqq \|\mathscr{F}\| (c_{56} L_j)^{\deg \mathscr{F}}$$

avec une constante $c_{56} = c_{56}(k) > 0$ effectivement calculable. Appliquons maintenant le Lemme 5 pour $g(x)$. Nous aurons

$$|a| \leqq \left[\left(\frac{\|\mathscr{F}\| (c_{56} L_j)^{\deg \mathscr{F}}}{A} \right)^{\min (m-k\tau, 1)} + \left(\frac{(A+1)^\tau F}{A} \right)^{\min \left(\frac{1}{m-k\tau}, 1 \right)} \right]^{\max \left(\frac{1}{m-k\tau}, 1 \right)}$$

qui est évidemment vrai aussi dans les cas où $|a| \leqq kL_j$. Enfin, si $|a| > 2^k$, alors

$$\|f\| = \max_{0 \leqq i \leqq k} \left\{ \frac{|f^{*(i)}(a)|}{i!} \right\} \leqq A|a|^k + kL_j |a|^{k-1} = |a|^{k-1} (A|a| + kL_j) \leqq$$

$$\leqq A \left\{ [\|\mathscr{F}\| (c_{57} L_j)^{\deg \mathscr{F}}]^{\min (m-k\tau, 1)} + [(A+1)^\tau F]^{\min \left(\frac{1}{m-k\tau}, 1 \right)} \right\}^{\max \left(\frac{k}{m-k\tau}, k \right)}$$

avec une constante $c_{57} = c_{57}(k, j, \varkappa_j) > 0$ convenable qui est effectivement calculable, où, dans le cas $m \leqq k$, le facteur A figurant devant la paranthèse $\{\ldots\}$ peut être omis et $(A+1)^\tau$ peut être remplacé par 2^τ. Cela est évidemment vrai aussi pour $|a| \leqq 2^k$ et ainsi notre théorème se trouve démontré.

Démonstration du Corollaire 1.7. Appliquons le Corollaire 1.5 dans le cas $j=0$. Soit $\varkappa > 9 \binom{k-1}{2}$ une constante. Il existe un f^* équivalent à f tel que

$$\|f^*\| < \exp \{c_3 [A^{(k-1)(k-2)} |D(f)|]^\varkappa\} = L_0.$$

On en déduit

$$\|f^{*(j)}\| < c_{58} L_0 \quad (j = 0, \ldots, k-2),$$

d'où

$$|D(f^{(j)})| = |D(f^{*(j)})| \leqq c_{59} A \cdot L_0^{2(k-j)-2} =$$

$$= \exp\{c_{60}[A^{(k-1)(k-2)}|D(f)|]^{\varkappa}\}$$

avec des constantes positives $c_{58}=c_{58}(k,j)$, $c_{59}=c_{59}(k,j)$, $c_{60}=c_{60}(k,j,\varkappa)$ qui sont effectivement calculables.

Pour démontrer les Théorèmes 4 et 4′ nous aurons besoin des lemmes suivants.

Lemme 6. *Soient $f(x), g(x)\in Z[x]$ des polynômes unitaires irréductibles de degré $p\geqq 2$ et $n\geqq 2$ respectivement. Supposons que les racines de $f(x)$ sont réelles et $f(\alpha)=0$ implique que $Q(\alpha)$ est primitif (c'est-à-dire, soit par exemple p premier) et que le corps des racines de $g(x)$ est une extension quadratique totalement imaginaire d'un corps totalement réel. Si*

$$D(f) > \{2g^{1/n}(0)\}^{p(p-1)},$$

alors $g(f(x))$ est irréductible sur Q.

Démonstration: voir dans [9].

Lemme 7. *Soit $f(x)\in Z[x]$ un polynôme unitaire de degré p, $2\leqq p\leqq 3$, et soit $g(x)$ un polynôme unitaire avec la même propriété que dans le Lemme 6. Si*

$$D(f) > \{2g^{1/n}(0)\}^{p(p-1)} \quad (n = \deg g),$$

alors $g(f(x))$ est irréductible sur Q.

Démonstration: voir dans [9].

Enfin, nous utiliserons le lemme suivant qui (sous une forme un peu différente) se trouve également dans [9].

Lemme 8. *Soit $f(x)\in Z[x]$ un polynôme unitaire ayant des racines réelles avec corps des racines L et soit $g(x)$ un polynôme ayant la propriété donnée dans le Lemme 6. Soient $\alpha_1, \ldots, \alpha_p$ des racines distinctes de $f(x)$. Si le graphe des couples (α_i, α_k) vérifiant*

$$|N_{L/Q}(\alpha_i - \alpha_k)| > \{2g^{1/n}(0)\}^{[L:Q]} \quad (n = \deg g)$$

contient un sous-graphe connexe ayant s sommets, alors $g(f(x))$ n'a aucun diviseur irréductible de degré $<s \deg g$ sur Q.

Démonstration du Théorème 4. En vertu du Lemme 6 il suffit de considérer le cas où

$$0 < D(f) \leqq \{2g^{1/n}(0)\}^{p(p-1)}. \tag{48}$$

En appliquant maintenant le Corollaire 1.6, nous obtenons immédiatement (21).

Démonstration du Théorème 4′. En conséquence du Lemme 7, il suffit de considérer les cas où $D(f)$ vérifie (48) ou $D(f)=0$. Mais, d'après le Corollaire 1.6, (48) implique (21). Supposons $D(f)=0$ lorsque $f(x)$ possède des racines multiples. Si $f(x)$ n'a pas deux racines différentes, c'est-à-dire si $f(x)=(x-a)^p$ pour un $a\in Z$,

alors $f^*(x)=f(x+a)=x^p$ satisfait à (21). Il reste à prouver (21) dans le cas où $f(x)$ est de la forme

$$f(x) = (x-a)(x-b)^2,$$

où $a, b \in Z$. Appliquons le Lemme 8 pour $g(x)$ et $f(x)$. Soit en particulier $L=Q$. Si $|b-a|>2g^{1/n}(0)$, d'après le Lemme 8 $g\big(f(x)\big)$ est irréductible. D'autre part, si $|b-a| \leqq 2g^{1/n}(0)$, alors pour $f^*(x)=x^2\big(x-(a-b)\big)$ équivalent à f on a

$$\|f^*\| \leqq 2g^{1/n}(0),$$

et cela implique (21).

Démonstration du Théorème 7. Soit $(x_1, \ldots, x_m) \in Z^m$ une solution arbitraire de l'équation (29). Avec la notation $\beta=\alpha_1 x_1+\cdots+\alpha_m x_m$ on a $D_{K/Q}(\beta)=D\neq 0$, ainsi β est un élément primitif dans K. Si a désigne le plus petit commun multiple des dénominateurs de $\alpha_1, \ldots, \alpha_m$, alors $a \leqq A$ et $\alpha_i'=a\alpha_i$ $(i=1, \ldots, m)$ et $\beta'=a\beta=\alpha_1' x_1+\cdots$ $\cdots+\alpha_m' x_m$ sont déjà entiers et

$$|D_{K/Q}(\beta')| \leqq A^{k(k-1)}|D|.$$

Employons le Théorème 3 et la remarque qui suit le Théorème 2. Il existe donc un

$$\beta^* = x_0+\alpha_1' x_1+\ldots+\alpha_m' x_m \quad (x_0 \in Z),$$

équivalent à β', pour lequel

$$h(\beta^*) \leqq kH(\beta^*) < \exp\{c_{62}|A^{k(k-1)}D|^{\varkappa}\}$$

et

$$h(\beta^*) \leqq kH(\beta^*) < \exp\{c_{63}[|D_K|^{3(k-1)(k-2)}(|D_K|^{3(k-1)(k-2)/2}+\log|AD|)]^{1+\varepsilon}\},$$

où $c_{62}=c_{62}(k, \varkappa)$ et $c_{63}=c_{63}(k, \varepsilon)$ sont des constantes positives effectivement calculables.

Considérons les conjugués $\beta^{*(1)}=\beta^*, \ldots, \beta^{*(k)}$ de β^* sous la forme

$$\beta^{*(i)} = x_0+\alpha_1'^{(i)} x_1+\cdots+\alpha_m'^{(i)} x_m \quad (i=1, \ldots, k). \tag{49}$$

Comme $1, \alpha_1, \ldots, \alpha_m$ sont Q-linéairement indépendants, $1, \alpha_1', \ldots, \alpha_m'$ sont également Q-linéairement indépendants. Par conséquent, $1, \alpha_1', \ldots, \alpha_m'$ peuvent être étendus en une base de K, et ainsi il existe des indices $i_0, \ldots, i_m$ tels que

$$\Delta = \begin{vmatrix} 1 & \alpha_1'^{(i_0)} & \ldots & \alpha_m'^{(i_0)} \\ \vdots & & & \\ 1 & \alpha_1'^{(i_m)} & \ldots & \alpha_m'^{(i_m)} \end{vmatrix} \neq 0.$$

Δ est entier algébrique et tous ses conjugués sont des déterminants de cette forme (avec des indices $i_0, \ldots, i_m$ convenables). Parmi les conjugués de Δ il y a au moins un de valeur absolue $\geqq 1$. Nous pouvons supposer que $|\Delta| \geqq 1$. Considérons dans (49) les $i_0, \ldots, i_m$-ièmes équations. En exprimant $x_1, \ldots, x_m$ du système d'équations obtenu, d'après l'inégalité de Hadamard on obtient pour tout $1 \leqq i \leqq m$

$$|x_i| \leqq \frac{(m+1)^{(m+1)/2}h(\beta^*)\prod\limits_{j,\, j\neq i} h(\alpha_j')}{|\Delta|} \leqq (AH)^{m-1}\exp\{c_{64}|A^{k(k-1)}D|^{\varkappa}\}$$

avec une constante $c_{64}=c_{64}(k, \varkappa)>0$ effectivement calculable. Nous pouvons obtenir (30) d'une manière analogue.

Démonstration du Corollaire du Théorème 7. Soit $(x_1, \ldots, x_{k-1}) \in Z^{k-1}$ une solution arbitraire de l'équation (33). Désignons par D_O le discriminant de l'ordre O. On a, d'une part,

$$D_{K/Q}(\alpha_1 x_1 + \cdots + \alpha_{k-1} x_{k-1}) = [F(x_1, \ldots, x_{k-1})]^2 D_O = a^2 \cdot D_O,$$

et d'autre part, en conséquence de $h(\alpha_i) \leqq kH(\alpha_i) \leqq kH$,

$$|D_O| \leqq k^{3k-1} \cdot H^{2(k-1)}.$$

Enfin, d'après le Théorème 7, il en résulte que

$$\max_{1 \leqq i \leqq k-1} (|x_i|) < \exp\{c_{65} |aH^{k-1}|^{\varkappa}\},$$

où $c_{65} = c_{65}(k, \varkappa)$ est une constante positive effectivement calculable.

Bibliographie

[1] A. Baker, Linear forms in the logarithms of algebraic numbers, IV., *Mathematika* **15** (1968), 204—216.

[2] A. Baker, Contributions to the theory of Diophantine equations, *Philos. Trans. Roy. Soc. London, Ser. A.*, **263** (1968), 173—208.

[3] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439—444.

[4] A. Baker—J. Coates, Integer points on curves of genus 1, *Proc. Camb. Phil. Soc.* **67** (1970), 595—602.

[5] B. J. Birch—J. R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc.* **25** (1972), 385—394.

[6] A. Brauer, R. Brauer und H. Hopf, Über die Irreduzibilität einiger spezieller Klassen von Polynomen, *Jber. Deutsch. Math. Verein.* **35** (1926), 99—112.

[7] B. N. Delone (Delaunay), Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante, *Math. Z.*, **31** (1930), 1—26.

[8] B. N. Delone—D. K. Faddeev, The Theory of Irrationalities of the Third Degree, Amer. Math. Soc., *Providence*, 1964 (Translated from the Russian (1940) ed.)

[9] K. Győry, Sur l'irréductibilité d'une classe des polynômes, II., *Publ. Math. (Debrecen)*, **19** (1972), 293—326.

[10] K. Győry, Investigations diophantiennes dans la théorie des polynômes irréductibles (en hongrois) *Debrecen*, 1972, pp. 1—172.

[11] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, *Acta Arith.* **23** (1973), 419—426.

[12] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, II., *Publ. Math. (Debrecen)* **21** (1974), 125—144.

[13] K. Győry, Sur l'irréductibilité d'une classe des polynômes, III., en préparation.

[14] T. Nagell, Zur Theorie der Kubischen Irrationalitäten, *Acta Math.*, **55** (1929), 33—65.

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

[16] T. Nagell, Sur les discriminants des nombres algébriques, *Arkiv för Mat.*, **7** (1967), 265—282.

[17] T. Nagell, Quelques propriétés des nombres algébriques du quatrième degré, *Arkiv för Mat.*, **7** (1969), 517—525.

[18] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, *Warszawa*, 1974.

[19] C. Runge, Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, *J. Reine Angew. Math.* **100** (1887), 425—435.

[20] H. M. Stark, Further Advences in the Theory of Linear Forms in Logarithms, Diophantine Approximation and Its Applications, pp. 255—294, Academic Press, *New York and London*, 1973.

[21] H. M. Stark, Effective estimates of solutions of some diophantine equations, *Acta Arith.*, **24** (1973), 251—259.

[22] H. M. Stark, Some Effective Cases of the Brauer-Siegel Theorem, *Inv. Math.*, **23** (1974), 135—152.

(Reçu le 28 mars 1974)