Sur une classe des corps de nombres algébriques et ses applications

Par K. GYŐRY (Debrecen)

A la mémoire de Monsieur le Professeur Andor Kertész)*

1. Introduction

Dans cet article, nous étudions les extensions quadratiques totalement imaginaires des corps de nombres algébriques totalement réels (de tels corps de nombres sont, par exemple, les extensions abéliennes non réelles du corps Q des nombres rationnels) et certaines de leurs applications récentes. Ces corps de nombres possèdent plusieurs propriétés particulières qui sont bien utilisables au cours des applications. Dans notre travail nous ajoutons quelques nouvelles caractérisations (Théorème 1) aux caractérisations connues de ces corps, qui se montrent très utiles. Nous établissons certaines nouvelles propriétés de ces corps de nombres (Théorèmes 2, 3, 4 et leurs conséquences) et, nous résumons les applications que nous avons obtenu dans [15], [16], [17], [18] et [19] à l'aide de ces propriétés. (Nous remarquons que certains de ces résultats ne peuvent pas être étendus aux autres corps de nombres algébriques).

Dans toute la suite de ce paragraphe, soit K une extension quadratique totalement imaginaire d'un corps de nombres algébriques K_0 totalement réel (c'est l'assertion (a) concernant K dans le Théorème 1). Ces corps de nombres, sous les formes (a)$\Leftrightarrow$(b)[1]), avaient été utilisés plusieurs fois dans la théorie des nombres (voir par exemple [41], [45] et [12]). Dans le cas particulier où $S=S_\infty$, (a)$\Leftrightarrow$(g) a été démontré par R. REMAK [32], [33] (et ainsi il a étendu le théorème de Kronecker concernant les unités des corps cyclotomiques aux corps de nombres de type (a)[2]). Grâce à (a)$\Leftrightarrow$(g), au cours de certaines applications des corps de nombres

---

*) Dédié le 29 juin 1974.

[1]) Les énoncés précis des assertions (a), (b), (c), (d), (e), (f) et (g) se trouvent dans notre Théorème 1.

[2]) Dans [15], nous avons appelé "allowed" originairement les corps de nombres de type (c). Dans [16] et [17] les corps de nombres de type (a)$\Leftrightarrow$(b)$\Leftrightarrow$(c)$\Leftrightarrow$(g) sont appelés kroneckeriens non réels ou simplement de K-corps non réels (vu que le théorème de Kronecker peut être étendu à leurs unités). Le 31 octobre 1971 M. le Professeur A. Schinzel a bien voulu attirer mon attention sur les travaux [32], [33] et [9]. Antérieurement, dans [32] et [33], R. Remak a appelé ces corps de nombres "Einheitsdefekt". L'assertion (a)$\Leftrightarrow$(g) (dans le cas particulier $S=S_\infty$) se trouve déjà aussi dans le travail [20] de E. Hecke.

Note ajoutée aux épreuves. G. Shimura (Introduction to the arithmetic theory of automorphic functions, Iwanami—Princeton) appelle „CM—fields" ces corps, et dans les travaux récents de *R. Gold* (J. Number Theory, 6 (1974), 369—373) et *A. Candiotti* (Compositio Math. 29 (1974), 89—111) ils sont appelés „J—fields".

de type (a), on peut surmonter la difficulté que cause l'existence d'une infinité d'unités. La démonstration de (g)⇒(f) (sous la hypothèse $S=S_\infty$) se trouve dans [33] (p. 48) et dans le travail [9] de P. DÉNES. La propriété (g) implique une relation simple entre les régulateurs de K et K_0. En employant cette relation R. REMAK [32], [33] a démontré que la valeur absolue du discriminant d'un corps de nombres K est majorable explicitement par $[K:Q]$ et par la valeur absolue du régulateur de K, sauf les cas où K est de type (a) et toutes les unités de K sont réelles. (e)⇒(a)⇒(b) (dans le cas particulier $r=1$) a été démontré par G. SHIMURA et Y. TANIYAMA [41]. Inversement, la démonstration de (a)⇒(e) est triviale. Enfin, nous avons obtenu (c)⇒(d) (dans le cas particulier $S=S_\infty$) en collaboration avec L. LOVÁSZ dans [15].

Dans les corps de nombres algébriques de type (a)⇔...⇔(g), grâce à leurs propriétés particulières, on a réussi (partiellement ou complètement) résoudre plusieurs problèmes dont la résolution semble actuellement très difficile en général ou bien elle n'est même pas possible (car l'assertion en question n'est pas vraie pour des corps de nombres quelconques). Ici nous ne mentionnons que deux importants problèmes.

Sur les corps de nombres de type (a)⇔(b) G. SHIMURA et Y. TANIYAMA [41] ont obtenu des résultats très importants dans la théorie du corps de classes. Ils ont obtenu certains corps de classes de ces corps de nombres par multiplication complexe des variétés abéliennes, et ils ont donné explicitement les groups d'idéaux correspondants, en généralisant les résultats antérieurs obtenus sur Q et sur les corps quadratiques imaginaires (pour les résultats récents de ce type voir l'ouvrage [42] de G. SHIMURA).

En utilisant la rélation mentionnée entre les régulateurs de K et K_0, du théorème de Brauer—Siegel il résulte qu'un corps de nombres K_0 totalement réel fixé n'a qu'un nombre fini d'extensions quadratiques totalement imaginaires K avec le même nombre de classes h (cf. L. J. GOLDSTEIN [13]), de plus, c'est vrai aussi pour tous les corps de nombres de type (a)⇔(g) et de degré borné (voir K. UCHIDA [49]), mais ces résultats ne sont pas effectifs. Récemment,*) sous certaines restrictions relatives à K_0 et h, L. J. GOLDSTEIN [13], [14] et J. E. SUNLEY [47] ont obtenu des résultats effectifs qui se rattachent aux théorèmes célèbres (rélatifs au cas $K_0=Q$) de A. BAKER et de H. M. STARK.

K étant un corps de nombres, l'application $\alpha\to|\mathrm{Norm}_{K/Q}(\alpha)|(\alpha\in K)$ n'est pas une valeur absolue sur K. Ce fait entraîne beaucoup de difficultés dans la théorie des corps de nombres algébriques et dans ses applications. Dans les corps de nombres K de type (a)⇔...⇔(g) on peut surmonter cette difficulté dans certaines investigations, en employant une inégalité de norme (voir le Théorème 3 et ses corollaires) que (sous une forme moins générale) nous avons obtenue originairement en collaboration avec L. LOVÁSZ dans [15]. Cette inégalité est également une propriété caractéristique de ces corps de nombres (voir le Théorème 1). Notamment (nous la présentons ici sous une forme particulière), si $\alpha\in K$, alors

$$(1)\qquad \{N_{K/Q}(\alpha)\}^{2/n}\geqq\{N_{K/Q}(\mathrm{Re}\,\alpha)\}^{2/n}+\{N_{K/Q}(i\,\mathrm{Im}\,\alpha)\}^{2/n}\quad(n=[K:Q]).$$

*) *Note ajoutée aux épreuves.* Voir encore: *K. Uchida*, Relative class numbers of normal CM—fields, Tôhoku Math. J. 25 (1973), 347—353 et *H. M. Stark*, Some Effective Cases of the Brauer—Siegel Theorem, Inv. Math. 23 (1974), 135—152.

Cette inégalité s'est montrée fondamentale au cours de nos recherches concernant les nouvelles propriétés et les applications de ces corps de nombres (voir [15], [16], [17], [18], [19] et les § 3—6 de cet article). Au § 3, de notre Théorème 3 nous déduisons quelques autres inégalités de norme, et au § 4, à partir de celles-ci, nous obtenons aussi quelques inégalités de discriminant.

Aux § 5 et 6 nous résumons les résultats que nous avons obtenu (à l'aide des propriétés mentionnées de ces corps de nombres) dans la théorie des équations diophantiennes [15], [19] et dans la théorie des polynômes irréductibles [16], [17], [18]. Ainsi dans [15], entre autres, nous avons donné la démonstration effective d'une conjecture*) concernant les équations diophantiennes du type „norme-forme" (voir Z. I. BOREVICH—I. R. SHAFAREVITCH [4]) dans le cas des formes à 3 inconnues qui se décompose en facteurs linéaires dans un corps de nombres de type (c), ce résultat se rattachant aux théorèmes effectifs célèbres obtenus dans le cas à 2 inconnues par A. BAKER [1]. Dans [16], [17], nous avons donné, entre autres, la solution, sous une forme plus générale, d'un problème (posé en 1926 par A. BRAUER, R. BRAUER et H. HOPF [5], et relatif à l'irréductibilité des polynômes de la forme $g(f(x))$) pour tous les polynômes $g(x)$ ayant des corps des racines de type (a)$\Leftrightarrow \ldots \Leftrightarrow$(g) (de tels polynômes sont par exemple les polynômes cyclotomiques et les polynômes $x^2+ax+b \in Z[x]$ de discriminant négatif). Dans [18], nous avons étendu nos investigations même aux polynômes de la forme $g(f(x_1, \ldots, x_N))$, en nous rattachant à un théorème général de A. SCHINZEL [34].

Les démonstrations des Théorèmes 1, 2, 3, 4 et de leurs corollaires se trouvent au paragraphe 7.

2. Caractérisations des extensions quadratiques totalement imaginaires des corps de nombres totalement réels

Dans ce paragraphe, nous résumons, d'une part, quelques caractérisations connues des extensions quadratiques totalement imaginaires des corps de nombres totalement réels, d'autre part, nous généralisons certaines de leurs caractérisations connues. En outre, nous ajoutons de nouvelles caractérisations aux caractérisations connues, qui ont été très utiles au cours des applications (voir l'introduction et les travaux [15], [16], [17], [18], [19]).

Soit K un corps de nombres algébriques, et désignons par K_0 son sous-corps réel maximal et par $K\psi$ ou $\overline{K}$ son corps conjugué complexe dans le corps C des nombres complexes (de même, soit désigné par $\alpha\psi$ ou $\bar{\alpha}$ le conjugué complexe d'un nombre $\alpha \in K$). Soit S_∞ l'ensemble des valeurs absolues archimédiennes normalisées[3]) sur K. Si pour un corps de nombres non réel K on a $\overline{K}=K$, l'extension K/K_0 est quadratique, et, si φ est une valeur absolue non-archimédienne normalisée, alors $\bar{\varphi}(\alpha) \overset{\text{def}}{=} \varphi(\bar{\alpha})$ est également une valeur absolue non-archimédienne normalisée sur K.

*) En 1970 W. M. SCHMIDT [36] a démontré cette conjecture (sous une forme non effective).

[3]) Les valeurs absolues archimédiennes (resp. non-archimédiennes) s'appellent non ultramétriques (resp. ultramétriques ou p-adiques) aussi (cf. N. BOURBAKI, Algèbre commutative, Chap. 6, Paris).

Dans la suite nous ne considérons que les valeurs absolues non triviales.

Appelons φ *réel*, si l'on a $\bar{\varphi}(\alpha)=\varphi(\alpha)$ pour tout $\alpha\in K$. D'après un théorème connu il existe une infinité de valeurs absolues réelles sur K.

Nous aurons besoin de la notation suivante: Soit $E^{(r)}_{K/Q}(\alpha)$ la fonction symétrique élémentaire de degré r des conjugués de $\alpha\in K$ sur Q. En particulier, $E^{(1)}_{K/Q}(\alpha)=\mathrm{Tr}_{K/Q}(\alpha)$ et $E^{(n)}_{K/Q}(\alpha)=N_{K/Q}(\alpha)$ (où $n=[K:Q]$). En outre, $E^{(r)}_{K/Q}(\alpha)\in Q$ pour tout $1\leqq r\leqq n$ et, si α est entier, $E^{(r)}_{K/Q}(\alpha)\in Z$.

Théorème 1. *Pour un corps de nombres algébriques non réel K de degré n, les assertions suivantes sont équivalentes:*

(a) *K est une extension quadratique totalement imaginaire d'un corps de nombres totalement réel*

(b) *$K\psi=K$ et $\sigma\psi=\psi\sigma$ pour chaque Q-isomorphisme σ de K dans C*

(c) *Il existe un corps de nombres algébriques $F\supseteqq K$ tel que les extensions F/Q et F_0/Q sont normales*

(d) *$\overline{K}=K$. Soit $S\supseteqq S_\infty$ un ensemble fini de valeurs absolues normalisées tel que chaque $\varphi\in S^*=S\setminus S_\infty$ soit réel. Il existe une constante $0<c\leqq 1$ telle que*

$$\left|N_{K/Q}(\alpha)\prod_{\varphi\in S^*}\varphi(\alpha)\right|\geqq c\left|N_{K/Q}(\mathrm{Re}\,\alpha)\prod_{\varphi\in S^*}\varphi(\mathrm{Re}\,\alpha)\right| \tag{2}$$

pour tout $\alpha\in K$, ou bien

$$\geqq c\left|N_{K/Q}(i\,\mathrm{Im}\,\alpha)\prod_{\varphi\in S^*}\varphi(i\,\mathrm{Im}\,\alpha)\right|$$

pour tout $\alpha\in K$

(e) *$\overline{K}=K$ et, pour un $1\leqq r<n$ fixé et pour tout $\alpha\in K$ $(\alpha\neq 0)$, on a*

$$E^{(r)}_{K/Q}(\alpha\bar{\alpha})>0 \tag{3}$$

(f) *$\overline{K}=K$ et si $S\supseteqq S_\infty$ est un ensemble fini de valeurs absolues tel que chaque $\varphi\in S\setminus S_\infty$ est réel, alors pour toute S-unité ε on a $\bar{\varepsilon}=\zeta\varepsilon$ avec une racine de l'unité $\zeta\in K$*

(g) *$\overline{K}=K$. Soit $S\supseteqq S_\infty$ un ensemble fini de valeurs absolues tel que chaque $\varphi\in S\setminus S_\infty$ soit réel. Désignons par V, U_s et U_s^0 respectivement le groupe des racines de l'unité, le groupe des S-unités et le groupe des S-unités réelles dans K. Alors $[U_s:\{V, U_s^0\}]\leqq 2$.*

Considérons deux conséquences du Théorème 1:

Corollaire 1.1. *Soient $K_1, \ldots, K_m$ $(m\geqq 2)$ des corps de nombres totalement réels ou des extensions quadratiques totalement imaginaires des corps de nombres totalement réels. Les sous-corps, les intersections et les composés de ces corps sont des corps de nombres de même type*.*

Corollaire 1.2. *Si K est un corps de nombres algébriques de degré n et de type* (a)$\Leftrightarrow\ldots\Leftrightarrow$(g), *alors pour tout $\alpha\in K$:*

$$\binom{n}{r+1}^{\frac{1}{r+1}}\{E^{(r)}_{K/Q}(\alpha\bar{\alpha})\}^{\frac{1}{r}}\geqq\binom{n}{r}^{\frac{1}{r}}\{E^{(r+1)}_{K/Q}(\alpha\bar{\alpha})\}^{\frac{1}{r+1}}\quad(r=1,\ldots,n-1). \tag{4}$$

**Note ajoutée aux épreuves.* Dans le livre récent de *G. Shimura* (Introduction to the arithmetic theory of automorphic functions, Iwanami-Princeton, § 5.5.) on trouve les assertions suivantes: Le composé des corps de nombres de type (a)$\Leftrightarrow$(b) (CM-fields) est de type (a)$\Leftrightarrow$(b). L'extension normale de Q engendrée par un corps be nombres de type (a)$\Leftrightarrow$(b) est également de type (a)$\Leftrightarrow$(b).

En particulier, on a

$$\left(\frac{\mathrm{Tr}_{K/Q}(\alpha\bar{\alpha})}{n}\right)^n \geqq N_{K/Q}(\alpha\bar{\alpha}), \tag{5}$$

et l'égalité ne peut avoir lieu que si $\alpha\bar{\alpha}\in Q$.

En employant un des théorèmes de C. L. Siegel ([44], Théorème 1), l'inégalité (5) peut être encore améliorée d'une manière évidente. A l'aide de certaines inégalités connues (voir par exemple [3]), on peut obtenir d'autres inégalités aussi concernant $\alpha\bar{\alpha}$ (sous les hypothèses du corollaire 1.2).

Dans la suite nous complétons notre Théorème 1 avec quelques remarques.

Remarque 1.1. Le Théorème 1 peut être énoncé aussi de manière qu'il caractérise à la fois les corps de nombres totalement réels et leurs extensions quadratiques totalement imaginaires (cf. [16], [18]), en modifiant convenablement (a), (d), (f), (g) (lorsque K est réel, il faut supposer qu'il soit totalement réel). [16] et [18] ne contiennent que l'équivalence de (a), (b), (c) et (g) vu que elle a été suffisante pour les applications obtenues dans [16] et [18].

Remarque 1.2. Quelques-unes des assertions (b), ..., (g) sont équivalentes à (a) aussi sous des formes plus faibles. Notamment, il suffit de supposer que: $[U_s: \{V, U_s^0\}]<\infty$ dans (g); $E_{K/Q}^{(r)}(\alpha\bar{\alpha})$ soit borné inférieurement dans (e); l'inégalité (2) ait lieu pour les associés d'un seul S-entier non réel $\alpha\in K$ (voir la démonstration).

Remarque 1.3. On peut aisément vérifier que dans le cas des valeurs absolues non réelles (a)$\Rightarrow$(d), (a)$\Rightarrow$(f) et (a)$\Rightarrow$(g) ne restent pas vrais, c'est-à-dire notre théorème ne peut pas être étendu aux valeurs absolues non réelles.

Nous remarquons que (e), dans le cas où $r=n$, n'est pas une propriété caractéristique des corps de nombres considérés.

Remarque 1.4. Comme nous les avons citées dans l'introduction, les assertions (a)$\Leftrightarrow$(g), (g)$\Rightarrow$(f), (c)$\Rightarrow$(d) (dans le cas particulier $S=S_\infty$), (e)$\Rightarrow$(a) (dans le cas particulier $r=1$) et (a)$\Leftrightarrow$(b) avaient été déjà connues antérieurement.

Remarque 1.5. Dans l'assertion (c) l'extension F/F_0 est évidemment quadratique, c'est-à-dire le corps de nombres F est également un corps de nombres de type (a).

Remarque 1.6. Si le corps de nombres K est donné par le polynôme minimal $g(x)$ d'un élément primitif α de K, à l'aide des coefficients de $g(x)$ on peut aisément décider si K est de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g) ou non. Soit $g(x)=(x-\alpha_1)\ldots(x-\alpha_n)$ avec des racines non réelles $\alpha_1, \ldots, \alpha_n$ dans C. En connaissance des coefficients de $g(x)$ on peut construire les polynômes $P(x)=\prod_{i=1}^{n} g(x+\alpha_i)\in Q[x]$ et $R(x)=\prod_{i=1}^{n} g(x-\alpha_i)\in$ $\in Q[x]$. K est de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g) si et seulement si tous les facteurs irréductibles de $P(x)$ et de $R(x)$ possèdent les propriétés suivantes: Si une racine d'un facteur est réelle (resp. imaginaire pure), alors toutes ses racines sont réelles (resp. imaginaires pures). En effet, si K est de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g), alors en vertu de (b) et (c), les racines des facteurs de $P(x)$ et $R(x)$ satisfont à la condition ci-dessus. Réciproquement, si les racines de $P(x)$ et $R(x)$ satisfont à la condition, alors $\alpha+\bar{\alpha}$ est totalement réel et tous les conjugués de $\alpha-\bar{\alpha}$ sont imaginaires purs pour chaque racine α de $g(x)$. Soit σ un Q-isomorphisme de l'extension normale de Q engendrée par K dans C.

Il résulte que $(\alpha+\bar{\alpha})\sigma\psi = (\alpha+\bar{\alpha})\sigma$ et $(\alpha-\bar{\alpha})\sigma\psi = -(\alpha-\bar{\alpha})\sigma$, d'où $\alpha\sigma\psi = \alpha\psi\sigma$. Ainsi K possède la propriété (c) (pour la déduction voir la démonstration de (b)⇒(c)) et, en même temps, les propriétés (a)⇔...⇔(g).

Enfin, nous voudrions présenter quelques propriétés des nombres premiers "réels" utilisés dans [16] et [18] au cours de nos investigations relatives aux polynômes irréductibles. Soit K un corps de nombres de type (a)⇔...⇔(g). Appelons "*réel*" le nombre premier rationnel p dans K lorsque toutes les valeurs absolues non archimédiennes telles que $\varphi(p)\neq 1$ sont réelles. Si F est l'extension normale de Q engendrée par K et si p est un nombre premier "réel" et non ramifié dans F (donc p ne divise pas la valeur absolue du discriminant $D_{F/Q}$ de F), alors p est évidemment "réel" aussi dans K. De plus, si $\varphi^*(p)\neq 1$ pour une valeur absolue φ^* non archimédienne réelle sur F, alors, en vertu de (b) et (c), on peut aisément démontrer que toutes les valeurs absolues φ^* non archimédiennes telles que $\varphi^*(p)\neq 1$ sont également réelles. Comme le nombre des valeurs absolues réelles sur F est infini, il en résulte qu'il existe une infinité de nombres premiers qui sont "réels" dans F (et ainsi dans K aussi). D'un théorème connu de D. Hilbert ([21], p. 377.) on obtient l'assertion suivante ([18]):

Proposition. *Soit F un corps de nombres algébriques de type* (a)⇔...⇔(g) *et normal sur Q, soient F_0 son sous-corps réel maximal et $\mu\in F_0$ un entier totalement positif lorsque $F=F_0(\sqrt{-\mu})$. Un nombre premier rationnel $p\nmid 2D_{F/Q}N_{F_0/Q}(-\mu)$ est "réel" dans F si, et seulement si, $-\mu$ est un non résidu quadratique* (mod p) *dans F_0. Par conséquent, si $N_{F_0/Q}(-\mu)$ est un non-résidu quadratique* (mod p), *alors p est "réel" dans F.*

Pour reconnaître si un nombre premier rationnel p est "réel" ou non dans K, on peut donner aussi l'algorithme suivante: Soient $g(x)$ et $g_0(x)$ les polynômes minimaux d'un entier primitif de K et de K_0 respectivement. D'après un théorème connu le nombre premier rationnel $p\nmid D(g)$, $D(g_0)$*) est "réel" dans K si, et seulement si, le nombre des facteurs est égal dans la décomposition en facteurs irréductibles de $g(x)$ et de $g_0(x)$ (mod p).

3. Inégalités de norme

Dans ce paragraphe, nous énonçons les inégalités de norme, mentionnées dans l'introduction, et quelques-unes de leurs conséquences. A l'aide de ces inégalités, dans [15], [16], [17], [18], [19] nous avons réussi à surmonter la difficulté due au fait que l'application $\alpha\to|N_{K/Q}(\alpha)|$ ($\alpha\in K$, K étant un corps de nombres) n'est pas valeur absolue sur K.

Tout d'abord nous donnons une généralisation non p-adique des inégalités de norme (pour la définition de $E^{(r)}_{K/Q}(\alpha)$ voir le paragraphe 2).

Théorème 2. *Soit K une extension quadratique totalement imaginaire d'un corps de nombres totalement réel avec $n=[K:Q]$ et soit $1\leqq r\leqq n$ un entier. Si $\alpha_1, \ldots, \alpha_k\in K$ ($\alpha_i\neq 0$; $i=1, \ldots, k$), alors $E^{(r)}_{K/Q}(\alpha_i\bar{\alpha}_i)>0$ ($i=1, \ldots, k$) et $\{E^{(r)}_{K/Q}(\alpha_1\bar{\alpha}_1+\ldots+\alpha_k\bar{\alpha}_k)\}^{1/r} \geqq \{E^{(r)}_{K/Q}(\alpha_1\bar{\alpha}_1)\}^{1/r}+\ldots+\{E^{(r)}_{K/Q}(\alpha_k\bar{\alpha}_k)\}^{1/r}$, et l'égalité a lieu si et seulement si $r=1$ ou $\alpha_i\bar{\alpha}_i=\lambda_i\alpha_1\bar{\alpha}_1$, où $\lambda_i\in Q$ ($i=1, \ldots, k$).*

*) $D(g)$ et $D(g_0)$ signifient les discriminants de $g(x)$ et de $g_0(x)$.

Remarque 2.1. Notre théorème fournit une généralisation de l'assertion (a)⇒(e) (voir le Théorème 1).

Remarque 2.2. Sous les hypothèses du Théorème 2 on obtient ($\alpha\in K$)

$$\{E^{(r)}_{K/Q}(\alpha\bar{\alpha})\}^{1/r} \geqq \{E^{(r)}_{K/Q}((\operatorname{Re}\alpha)^2)\}^{1/r}+\{E^{(r)}_{K/Q}(-(i\operatorname{Im}\alpha)^2)\}^{1/r} \quad (r=1,\ldots,n)$$

(pour la déduction voir la démonstration du Théorème 3).

Comme $E^{(n)}_{K/Q}=N_{K/Q}$ et $N_{K/Q}(\alpha_i\bar{\alpha}_i)=N^2_{K/Q}(\alpha_i)$ $(i=1,\ldots,k)$, du Théorème 2 on obtient immédiatement l'inégalité suivante:

Corollaire 2.1. *Sous les hypothèses du Théorème* 2 *on a*

$$\{N_{K/Q}(\alpha_1\bar{\alpha}_1+\ldots+\alpha_k\bar{\alpha}_k)\}^{1/n} \geqq \{N_{K/Q}(\alpha_1)\}^{2/n}+\ldots+\{N_{K/Q}(\alpha_k)\}^{2/n},$$

l'égalité n'étant vraie que si $\alpha_i\bar{\alpha}_i=\lambda_i\alpha_1\bar{\alpha}_1$, *où* $\lambda_i\in Q$ $(i=k,\ldots,k)$.

Si le polynôme minimal d'un nombre algébrique α est $a_0x^k+\ldots+a_k\in Z[x]$, désignons par $H(\alpha)=\max\limits_{0\leqq i\leqq k}|a_i|$ *la hauteur* de α. Du Théorème 2, à l'aide d'un résultat de C. L. SIEGEL ([43], Hilfssatz 3, p. 176), on obtient le corollaire suivant:

Corollaire 2.2. *Soient* α_1, α_2 *des entiers algébriques dans un corps de nombres de type* (a)⇔...⇔(g) *et soient les degrés de* $\alpha_1\bar{\alpha}_1$, $\alpha_2\bar{\alpha}_2$ *et* $\alpha_1\bar{\alpha}_1+\alpha_2\bar{\alpha}_2$ *respectivement* d_1, d_2 *et* d. *Alors*

$$2(d_1d_2)!\,\{dH(\alpha_1\bar{\alpha}_1+\alpha_2\bar{\alpha}_2)\}^{\frac{d_1d_2}{d}} \geqq H(\alpha_1\bar{\alpha}_1)+H(\alpha_2\bar{\alpha}_2).$$

Le corollaire 2.2 implique aussi une inégalité analogue à celle qui se trouve dans la remarque 2.2.

Du corollaire 2.1 on peut déduire le Théorème 3 qui (sous une forme plus faible) est au fait contenu dans le Théorème 1. Nous voudrions souligner son rôle, c'est pourquoi nous l'énonçons en tant qu'un théorème à part.

Théorème 3. *Soit* K *une extension quadratique totalement imaginaire d'un corps de nombres totalement réel et soient* S_1 *et* S_2 *des ensembles finis des ses valeurs absolues non-archimédiennes normalisées respectivement réelles et non réelles. On a pour tout* $\alpha\in K$

$$\{N_{K/Q}(\alpha)\prod_{\varphi\in S_1}\varphi(\alpha)\prod_{\varphi\in S_2}\max(\varphi(\alpha),\varphi(\bar{\alpha}))\}^{2/n} \geqq \tag{6}$$

$$\geqq \Big\{\prod_{\varphi\in S_1\cup S_2}\varphi(2)\Big\}^{2/n}\Big[\Big\{N_{K/Q}(\operatorname{Re}\alpha)\prod_{\varphi\in S_1\cup S_2}\varphi(\operatorname{Re}\alpha)\Big\}^{2/n}+$$

$$+\Big\{N_{K/Q}(i\operatorname{Im}\alpha)\prod_{\varphi\in S_1\cup S_2}\varphi(i\operatorname{Im}\alpha)\Big\}^{2/n}\Big] \quad (n=[K:Q]).$$

En particulier, dans le cas où S_1, $S_2=\emptyset$,

$$\{N_{K/Q}(\alpha)\}^{2/n} \geqq \{N_{K/Q}(\operatorname{Re}\alpha)\}^{2/n}+\{N_{K/Q}(i\operatorname{Im}\alpha)\}^{2/n}, \tag{7}$$

l'égalité n'étant vraie que si $\operatorname{Re}\alpha=0$, $i\operatorname{Im}\alpha=0$ *ou* $\left(\dfrac{\operatorname{Re}\alpha}{i\operatorname{Im}\alpha}\right)^2\in Q$.

Remarque 3.1. Comme nous l'avons mentionné dans l'introduction, nous avons trouvé l'inégalité (7) (sous une forme un peu plus particulière) dans [15], en collaboration avec L. Lovász.

Remarque 3.2. Dans (6), on ne peut pas remplacer $\max(\varphi(\alpha), \varphi(\bar{\alpha}))$ par $\varphi(\alpha)$ ($\varphi \in S_2$). Dans le cas contraire, si α est un entier et si $\operatorname{Re}\alpha$, $i \operatorname{Im}\alpha$ sont également des entiers et $(\alpha, 2)=1$, d'après la formule du produit (6) entraîne une contradiction. Par conséquent, nos théorèmes relatifs aux équations diophantiennes et aux polynômes irréductibles, obtenus à l'aide de (6), ne peuvent pas être étendus à tous les nombres premiers seulement pour une infinité de nombres premiers (à savoir aux nombres premiers „réels": voir [16], [18], [19] et les § 5, 6).

Remarque 3.3. On peut donner la condition de l'égalité aussi dans [6] avec certaines conditions supplémentaires dépendant des φ.

Remarque 3.4. Le Théorème 3 implique (a)⇒(d) (cf. le Théorème 1).

Considérons quelques conséquences de notre Théorème 3. Comme pour un nombre premier p on a $|N_{K/Q}(\alpha)|_p = \prod_{\varphi;\,\varphi(p)\neq 1} \varphi(\alpha)$ (les φ sont des valeurs absolues non-archimédiennes normalisées sur K), en choisissant convenablement l'ensemble de valeurs absolues S_1, du Théorème 3 on obtient immédiatement le

Corollaire 3.1. *Soit K un corps de nombres de degré n et de type* (a)⇔...⇔(g), *et soit P un ensemble fini des nombres premiers impairs „réels" dans K. On a*

$$\Big\{N_{K/Q}(\alpha) \prod_{p\in P} |N_{K/Q}(\alpha)|_p\Big\}^{2/n} \geqq \tag{8}$$

$$\geqq \Big\{N_{K/Q}(\operatorname{Re}\alpha) \prod_{p\in P} |N_{K/Q}(\operatorname{Re}\alpha)|_p\Big\}^{2/n} + \Big\{N_{K/Q}(i\operatorname{Im}\alpha) \prod_{p\in P} |N_{K/Q}(i\operatorname{Im}\alpha)|_p\Big\}^{2/n}.$$

Remarque 3.4. De (8) on obtient

$$\Big\{N_{K/Q}(\alpha) \prod_{p\in P} |N_{K/Q}(\alpha)|_p\Big\}^{2} \geqq \tag{9}$$

$$\geqq 2^n \Big\{N_{K/Q}(\operatorname{Re}\alpha) \prod_{p\in P} |N_{K/Q}(\operatorname{Re}\alpha)|_p\Big\}\Big\{N_{K/Q}(i\operatorname{Im}\alpha) \prod_{p\in P} |N_{K/Q}(i\operatorname{Im}\alpha)|_p\Big\}.$$

Corollaire 3.2. *Soit K un corps de nombres de type* (a)⇔...⇔(g). *Soient $\alpha, \beta \in K$ des entiers différents de zéro tels que α/β soit non réel et $\alpha+\beta$ soit réel ou imaginaire pur. Alors on a*

$$N_{K/Q}\left(\frac{\alpha+\beta}{2}\right) \leqq N_{K/Q}(\alpha\beta), \tag{10}$$

et l'égalité a lieu si, et seulement si, α/β est imaginaire pur et a) *$\alpha-\bar{\alpha}$ est une unité lorsque $\alpha+\beta$ est réel, ou bien* b) *$\alpha+\bar{\alpha}$ est une unité lorsque $\alpha+\beta$ est imaginaire pur.*

Remarque 3.5. Pour les α, β précédents (10) implique immédiatement l'inégalité suivante:

$$N_{K/Q}\left(\frac{\alpha+\beta}{2}\right) \leqq \frac{N^2_{K/Q}(\alpha) + N^2_{K/Q}(\beta)}{2}. \tag{11}$$

Remarque 3.6. On peut énoncer (10) aussi sous une forme p-adique (avec des nombres premiers "réels"). Pour démontrer cette proposition il suffit d'utiliser la forme p-adique du Théorème 3, c'est-à-dire le corollaire 3.1.

Corollaire 3.3. *Soit α un nombre algébrique appartenant à un corps de nombres de type* (a)$\Leftrightarrow\ldots\Leftrightarrow$(g). *Désignons par $g(x)$, $g_R(x)$ et $g_I(x)$ les polynômes minimaux respectifs des nombres α, $\operatorname{Re}\alpha$ et $i\operatorname{Im}\alpha$ et par n, k et l leurs degrés respectifs Alors on a*

$$\{g^2(x)\}^{1/n} \geqq \{g_R^2(x)\}^{1/k} + \{g_I^2(0)\}^{1/l} \tag{12}$$

pour tout nombre réel x.

4. Inégalités de discriminant

Dans la suite nous établissons quelques inégalités de discriminant dans les corps de nombres de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g).

Désignons par $D(\alpha)$ le discriminant d'un nombre algébrique α dans le corps de nombres $Q(\alpha)$. En outre, si $K'\subset K$ sont des corps de nombres tels que $K'\neq K$ et si $K=K'(\alpha)$, désignons par $D_{K/K'}(\alpha)$ le discriminant de α sur K'.

Théorème 4. *Soit α un nombre algébrique de degré n tel que $K=Q(\alpha)$ soit une extension quadratique totalement imaginaire d'un corps de nombres totalement réel et les degrés $k=[K'\colon Q]$ et $l=[K''\colon Q]$ de $K'=Q(\operatorname{Re}\alpha)$ et $K''=Q(i\operatorname{Im}\alpha)$ soient supérieurs à* 1. *Alors*

$$|D(\alpha)|^{2/n} \geqq \left|\left(D(\operatorname{Re}\alpha)\right)^{\left(\frac{n}{k}\right)^2} N_{K'/Q}\left(D_{K/K'}(\alpha)\right)\right|^{2/n} + \tag{13}$$

$$+\left|\left(D(i\operatorname{Im}\alpha)\right)^{\left(\frac{n}{l}\right)^2} N_{K''/Q}\left(D_{K/K''}(\alpha)\right)\right|^{2/n},$$

et l'égalité a lieu si et seulement si $k=l=2$.

Si $l=n$ (c'est-à-dire si $K''=K$) soit par définition $D_{K/K}(\alpha)=1$ dans (13). Nous ne considérons pas les cas triviaux $k=1$ et $l=1$, car dans le cas $k=1$ on a $\operatorname{Re}\alpha\in Q$ et $D(i\operatorname{Im}\alpha)=D(\alpha)$, et dans le cas $l=1$ on a $i\operatorname{Im}\alpha=0$ et $D(\operatorname{Re}\alpha)=D(\alpha)$.

Considérons quelques conséquences immédiates du Théorème 4.

Corollaire 4.1. *Sous les hypothèses du Théorème 4 on a*

$$|D(\alpha)|^{2/n} \geqq |D(\operatorname{Re}\alpha)|^{2n/k^2} + |D(i\operatorname{Im}\alpha)|^{2n/l^2}, \tag{14}$$

à condition que α soit entier.

Corollaire 4.2. *Soient α, $\operatorname{Re}\alpha$ et $i\operatorname{Im}\alpha$ des entiers satisfaisant aux conditions du Théorème 4 et soient $g(x)$, $g_R(x)$ et $g_I(x)$ les polynômes minimaux respectifs de α, $\operatorname{Re}\alpha$ et $i\operatorname{Im}\alpha$. Alors on a*

$$|D(g)|^{2/n} \geqq |D(g_R)|^{2n/k^2} + |D(g_I)|^{2n/l^2}. \tag{15}$$

Corollaire 4.3. *Sous les hypothèses du Théorème 4, on a*

$$|D(\alpha)|^2 \geqq 2^n |D(\operatorname{Re}\alpha)|^{\left(\frac{n}{k}\right)^2} \cdot |D(i \operatorname{Im}\alpha)|^{\left(\frac{n}{l}\right)^2} \tag{16}$$

pour tout entier α.

Soit α un entier satisfaisant aux conditions du Théorème 4, et, avec les notations ci-dessus, désignons respectivement par D_K, $D_{K'}$ et $D_{K''}$ le discriminant de K, K' et K''. Soit $I(\alpha) \in Z$ l'indice de α pour lequel donc $|D(\alpha)| = I^2(\alpha)|D_K|$.

Corollaire 4.4. *Mêmes données et hypothèses que dans le Théorème 4. Si de plus* α, $\operatorname{Re}\alpha$ *et* $i \operatorname{Im}\alpha$ *sont entiers, alors on a*

$$|D(\alpha)|^{2/n} \geqq |D_K|^{2/n} \left\{ |D_{K'}|^{\frac{2(n-k)}{k^2}} + |D_{K''}|^{\frac{2(n-l)}{l^2}} \right\} \tag{17}$$

et

$$\{I(\alpha)\}^{4/n} \geqq |D_{K'}|^{\frac{2(n-k)}{k^2}} + |D_{K''}|^{\frac{2(n-l)}{l^2}}. \tag{18}$$

Pour énoncer la dernière conséquence, il nous faut introduiser une notation. Avec les notations précédentes, $1, \operatorname{Re}\alpha, \ldots, (\operatorname{Re}\alpha)^{k-1}$ forment une base de K'/Q, $1, (i \operatorname{Im}\alpha), \ldots, (i \operatorname{Im}\alpha)^{n/k-1}$ forment une base de K/K' et $(i \operatorname{Im}\alpha)^s (\operatorname{Re}\alpha)^r$ $\left(s=0, \ldots, \ldots, \frac{n}{k}-1;\ r=0, \ldots, k-1\right.$ est une base de K/Q qui sera désignée plus brièvement par $i \operatorname{Im}\alpha \times \operatorname{Re}\alpha$. De la même façon, désignons par $\operatorname{Re}\alpha \times i \operatorname{Im}\alpha$ la base $(\operatorname{Re}\alpha)^u \cdot (i \operatorname{Im}\alpha)^v \left(u=0, \ldots, \frac{n}{l}-1;\ v=0, \ldots, l-1\right)$ de K/Q. En désignant par $D(i \operatorname{Im}\alpha \times \operatorname{Re}\alpha)$ le discriminant de la base $i \operatorname{Im}\alpha \times \operatorname{Re}\alpha$, d'après un théorème connu (cf. M. EICHLER [10], p. 44) on a

$$D(i \operatorname{Im}\alpha \times \operatorname{Re}\alpha) = N_{K'/Q}(D_{K/K'}(i \operatorname{Im}\alpha)) \{D_{K'/Q}(\operatorname{Re}\alpha)\}^{[K:K']}$$

et de la même manière pour $D(\operatorname{Re}\alpha \times i \operatorname{Im}\alpha)$. On en déduit

Corollaire 4.5. *Les hypothèses et notations étant celles du corollaire précédent, on a*

$$|D(\alpha)|^{2/n} \geqq |D(i \operatorname{Im}\alpha \times \operatorname{Re}\alpha)|^{2/n} \cdot |D(\operatorname{Re}\alpha)|^{\frac{2(n-k)}{k^2}} + \tag{19}$$

$$+ |D(\operatorname{Re}\alpha \times i \operatorname{Im}\alpha)|^{2/n} \cdot |D(i \operatorname{Im}\alpha)|^{\frac{2(n-l)}{l^2}} \geqq |D(i \operatorname{Im}\alpha \times \operatorname{Re}\alpha)|^{2/n} + |D(\operatorname{Re}\alpha \times i \operatorname{Im}\alpha)|^{2/n}.$$

5. Applications aux équations diophantiennes

Dans la suite nous donnons un résumé de nos résultats, relatifs aux équations diophantiennes, et obtenus à l'aide de nos Théorèmes 1 et 3.

a) *Sur les solutions* β_1, β_2 *en entiers algébriques de norme bornée de l'équation diophantienne* $\beta_1 + \beta_2 = \beta$

Dans la théorie des équations diophantiennes et dans ses applications, de nombreux problèmes nous conduisent à la question de résoudre l'équation

$$\beta_1 + \beta_2 = \beta \tag{20}$$

en entiers β_1, β_2 de norme bornée d'un corps de nombres algébriques K (voir par exemple C. L. SIEGEL [43], T. NAGELL [25], [26], A. BAKER [1], K. GYŐRY [16], [17]*)). D'après un théorème de C. L. SIEGEL [43], (20) n'a qu'un nombre fini de solutions dans K (voir [27]) et les solutions eventuelles peuvent être effectivement déterminées à l'aide des résultats de A. BAKER (cf. [17]*)).

T. NAGELL, au cours de ses recherches mentionnées ci-dessus, est parvenu à l'équation plus particulière

$$\varepsilon_1 + \varepsilon_2 = m \quad (0 \neq m \in Z) \tag{21}$$

en unités ε_1, ε_2 d'un corps de nombres K, et dans le cas $m=1$, il a posé le problème de déterminer toutes les solutions de (21) dans un corps de nombres K fixé. T. NAGELL [31] a appelé *exceptionnelles* ces unités. Dans [27] et [29] (voir encore [30]) il a déterminé toutes les unités exceptionnelles des corps de nombres de rang $\leqq 1$ (c'est-à-dire lorsque le rang du groupe des unités est $\leqq 1$), et dans [31] il a déterminé toutes les unités exceptionnelles de certains corps de nombres algébriques de rang 2. Nous remarquons que, pour $m=1$ (et pour tout m fixé), (21) a d'ailleurs une infinité de solutions ε_1, ε_2 en unités de tous les corps de nombres de degré $\leqq n$; de telles solutions sont, par ex., les racines des équations $x(x-1)(x-a_2)\ldots$ $\ldots(x-a_n)\pm 1 = 0$, $1<a_2<\ldots<a_n$ étant des entiers rationnels.

Dans [17] nous avons démontré (voir la Proposition 4 et sa démonstration) que, pour un $\beta \in Z$ fixé, (20) n'a qu'un nombre fini de solutions β_1, β_2 en entiers non réels de norme inférieure à une borne donnée de tous les corps de nombres de degré $\leqq n$ et de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g) et les solutions eventuelles peuvent être effectivement déterminées. On peut facilement vérifier que (21) n'est résoluble en unités non réelles des corps de nombres de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g) que dans le cas où $m = \pm 1, \pm 2$. De plus, dans [16] (voir les lemmes 12 et 14) nous avons déterminé explicitement toutes les solutions pour $m=1$, 2, (il suffit évidemment de considérer les cas $m=1$, 2). Notamment, l'assertion suivante est vraie:

Théorème 5. *Soient ε_1, ε_2 des solutions de* (21) *en unités non réelles des corps de type* (a)$\Leftrightarrow\ldots\Leftrightarrow$(g). *Si $m=1$, alors avec des racines de l'unité ζ_1, ζ_2 convenablement choisies*

$$\varepsilon_1 = \frac{1-\zeta_2}{\zeta_1-\zeta_2}, \quad \varepsilon_2 = \frac{\zeta_1-1}{\zeta_1-\zeta_2},$$

où chacun des $\zeta_1, \zeta_2\ (\neq\zeta_1)$ ζ_1/ζ_2 est une racine primitive p^z-ième de l'unité avec le même p^z (p nombre premier) ou bien aucun d'eux n'est une racine primitive p^z-ième de l'unité (p nombre premier). Si $m=2$, on a

$$\varepsilon_1 = 1-\zeta, \quad \varepsilon_2 = 1+\zeta,$$

où ζ est une racine primitive n-ième de l'unité telle que $n \neq p^z, 2p^z$ (p nombre premier).

*) *Note ajoutée aux épreuves.* Des majorations explicites se trouvent par exemple dans notre travail „Sur les polynômes à coefficients entiers et de discriminant donné, II". Publ. Math. (Debrecen), 21 (1974), 125—144.

Notre Théorème 5 donne explicitement toutes les unités non réelles exceptionnelles des corps de nombres de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g).

Dans [16], [18] et [19] (voir encore les § 5 b et 6) nous avons obtenu pluisieurs applications du Théorème 5 aux équations diophantiennes et aux polynômes irréductibles.

b) *Sur les équations diophantiennes à deux inconnues*

Soit $F(x, y) = a_0x^n+a_1x^{n-1}y+\ldots+a_ny^n\in Z[x, y]$ une forme de degré $n\geqq 2$ et soit $G(x, y)\in Z[x, y]$ un polynôme de degré $k<n$. A. SCHINZEL [35] a démontré que l'équation

$$F(x, y) = G(x, y) \tag{22}$$

n'admet qu'on nombre fini de solutions x, y en entiers rationnels, à condition que $F(x, y)$ ne soit pas une puissance, à un facteur constant près, d'une forme linéaire ou quadratique indéfinie. La démonstration n'est pas effective. Toutefois, si $G(x, y)\equiv m$ est une constante $\neq 0$, c'est-à-dire si (22) est de la forme

$$F(x, y) = m \tag{23}$$

et x, y est une solution en entiers rationnels de (23), alors d'après un théorème célèbre de A. BAKER [1] on a $\max(|x|, |y|)\leqq c(n, |m|, \|F\|)$ avec une constante c donnée explicitement, où $\|F\|$ désigne le maximum des valeurs absolues des coefficients de F. Nous remarquons que si $F(x, y)$ est défini (positif ou négatif), alors on peut aisément majorer les solutions aussi dans le cas de l'équation (22).

Soit, en particulier, $F(x, y)$ une forme telle que tous ses facteurs irréductibles soient construits sur un corps de nombres de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g) (c'est-à-dire les corps des racines des facteurs irréductibles soient tous de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g); de telles formes sont par exemple les formes $F(x, y)$ où $F(z, 1)$ est le produit des polynômes cyclotomiques et des polynômes quadratiques de discriminant négatif). Dans [19], à l'aide de nos Théorèmes 1 et 3, nous démontrons que, avec les notations précédentes, on a

$$\max(|x|, |y|) \leqq \left\{2^n\binom{k+2}{2}\|G\|\right\}^{\frac{1}{n-k}}\cdot\{\max(|a_0|, |a_n|)\}^{\frac{n-1}{n-k}} \tag{24}$$

pour toute solution x, y de (22). Dans le cas particulier où $G(x, y)\equiv m$ (c'est-à-dire dans le cas de l'équation (23)) cette majoration peut être améliorée davantage, à savoir on a

$$|x| \leqq 2|a_n|^{1-\frac{1}{n}}\cdot|m|^{1/n}, \quad |y| \leqq 2|a_0|^{1-\frac{1}{n}}\cdot|m|^{1/n}. \tag{25}$$

Les constantes dans (24) et (25) ne dépendent pas de $\|F\|$ (seulement de $|a_0|$ et $|a_n|$) et la majoration (25) est beaucoup meilleure que la majoration obtenue par A. BAKER [1] dans le cas général. De plus, les majorations (25) ne peuvent pas être améliorées en m (parce que dans le cas où $a_0=a_n=1$ et $m=m_1^n$ ($m_1\in Z$), $x=0$, $y=m_1=m^{1/n}$ est une solution de (23)). Enfin, notre résultat n' est pas vrai en général, dans le cas des formes d'autre type (voir, par exemple, $F(x, y)=x(x-b_2y)\ldots(x-b_ny)+y^n$ et $m=1$, $0<b_2<\ldots<b_n$ étant des entiers).

Désignons par M le nombre de solutions de (22) en entiers rationnels. Pour des $F(x, y)$ irréductibles et pour des $G(x, y)$ de degré $k < n-2$ H. DAVENPORT et K. F. ROTH [8] ont majoré M par une constante calculée explicitement qui ne dépend que de n, $\|F\|$ et $\|G\|$. Dans le cas où $G(x, y) \equiv m \in Z$, D. J. LEWIS et K. MAHLER [23] ont amélioré notablement cette majoration. Dans [19], nous avons obtenu une meilleure majoration dans le cas particulier où $F(x, y)$ est construit sur un corps de nombres de type (a)$\Leftrightarrow \ldots \Leftrightarrow$(g). Nous avons majoré explicitement M par une borne relativement petite qui ne dépend que de n et du nombre des facteurs premiers distincts de m.

Si $m=1$, d'après un théorème de V. A. TARTAKOVSKIĬ [48], $M \leqq 235n^6$. On peut facilement voir qu'en général M dépend de n. T. NAGELL [28] a démontré que $M \leqq 8$ pour les polynômes cyclotomiques $F(x, 1)$, et $M \leqq 6$ pour les polynômes $F(x, 1)$ qui engendrent un corps cyclotomique p^z-ième ($p \geqq 3$ nombre premier), de plus, étant donné un M, il a déterminé toutes les formes $F(x, y)$ de ce type pour lesquelles $F(x, y)=1$ a exactement M solutions. Dans [19], en utilisant nos Théorèmes 1, 3 et 5, nous avons généralisé ces résultats de T. Nagell. Nous avons démontré que M est pair et $\leqq 8$, à condition que $F(x, 1)$ engendre un corps de nombres de type (a)$\Leftrightarrow \ldots \Leftrightarrow$(g). Nous avons caractérisé toutes les formes pour lesquelles M prend une valeur donnée $\leqq 8$ et, en même temps, nous avons déterminé les solutions de l'équation $F(x, y)=1$.

c) *Sur les équations diophantiennes du type „norme-forme"*

En généralisation de l'équation (23), considérons l'équation diophantienne

$$\text{Norm}_{K/Q}(x_1 + \alpha_2 x_2 + \ldots + \alpha_k x_k) = m \quad (m \in Q), \tag{26}$$

où $M=\{1, \alpha_2, \ldots, \alpha_k\}$ est un module dans le corps de nombres $K=Q(\alpha_2, \ldots, \alpha_k)$, les générateurs étant Q-linéairement indépendants. On appelle M *dégénéré* (cf. Z. I. BOREVICH—I. R. SHAFAREVITCH [4]) lorsque l'espace vectoriel L sur Q, engendré par M, contient un sous-espace L' tel que $\mu L' = K'$ pour un $\mu \in K$ et pour un sous-corps $K' \subsetneqq K$ différent de Q et des corps quadratiques imaginaires. Comme il est connu, si M est dégénéré, alors, pour un $m \in Q$ convenablement choisi, (26) a une infinité de solutions $(x_1, \ldots, x_k) \in Z^k$. Réciproquement, W. M. SCHMIDT [36] (voir encore [37]) a démontré que, si M est non-dégénéré et m est fixé, (26) n'admet qu'un nombre fini de solutions en entiers rationnels. Ainsi dans [36] W. M. SCHMIDT a prouvé, entre autres, la conjecture qui se trouve dans le livre de Z. I. BOREVICH et I. R. SHAFAREVITCH [4]. Les théorèmes de Schmidt ne sont pas toutefois éffectifs, ils ne donnent aucun algorithme pour déterminer les solutions éventuelles. Dans le cas $k=2$, en 1968 A. BAKER [1] a donné une majoration explicite pour $\max(|x_1|, |x_2|)$, x_1, x_2 étant une solution arbitraire de (26) (voir encore la partie b) dans ce §).

Dans le cas où $k=3$ et K est de type (a)$\Leftrightarrow \ldots \Leftrightarrow$(g), nous avons donné, en collaboration avec L. LOVÁSZ [15], une démonstration effective de la conjecture mentionnée ci-dessus, en utilisant le théorème de A. Baker et l'inégalité de norme. (Donc, dans ce cas particulier, le théorème de W. M. Schmidt est vrai sous une forme effective aussi). Plus précisément, nous avons démontré le théorème suivant:

Théorème 6. *Soit K une extension quadratique totalement imaginaire d'un corps de nombres totalement réel. Soit $\{1, \alpha_2, \alpha_3\}$ un module non réel et non-dégénéré de K avec des généreateurs Q-linéairement indépendants et soit $H(\alpha_i) \leqq H$ $(i=1, 2)$*[4]*. Alors, pour toute solution de l'équation*

$$N_{K/Q}(x_1+\alpha_2 x_2+\alpha_3 x_3) = m \quad (m \in Q) \tag{27}$$

on a

$$\max(|x_1|, |x_2|, |x_3|) \leqq c(n, m, H) \quad (n = [K:Q])$$

avec une constante $c(n, m, H)$ calculable explicitement et ne dépendant que de n, m et H.

Remarque 6.1. Dans [15] nous avons démontré ce théorème originairement pour des corps de nombres de type (c) (cf. le Théorème 1). Mais, à cause de notre Théorème 1, ce résultat peut être énoncé aussi sous cette forme.

Remarque 6.2. La constante $c(n, m, H)$ ci-dessus est calculée explicitement dans [15]. En employant les améliorations récentes du théorème de A. Baker, relatif à la forme linéaire de logarithmes de nombres algébriques (voir*) A. BAKER et H. M. STARK [2] et N. I. FEL'DMAN [11]) on peut notablement améliorer notre majoration.

Remarque 6.3. A l'aide du théorème de J. COATES [7] ou de V. G. SPRINDZUCK [46] et de la forme p-adique de notre théorème 3, on peut énoncer et démontrer le Théorème 6 même sous une forme p-adique (avec des nombres premiers "réels").

Remarque 6.4. De notre théorème, on peut déduire des résultats effectifs concernant l'approximation des formes linéaires $x_1+\alpha_2 x_2+\alpha_3 x_3$ (pour la démonstration voir le cas $k=2$ dans [1]).

6. Applications aux polynômes irréductibles

Soit $f(x) = (x-a_1) \ldots (x-a_m)$ avec des entiers rationnels a_i distincts et soit $g(x) \in Z[x]$ un polynôme unitaire (donc son coefficient dominant soit égal à 1; cf. [16] et [17] où on appelle normés ces polynômes). Pour que $g(f(x))$ soit irréductible sur Q, il faut que $g(x)$ soit également irréductible sur Q. La question de la réductibilité des polynômes $g(f(x))$ a été posée pour les polynômes $g(x) = x^{2^n}+1$ par I. SCHUR (voir par ex. [6]) et en général, pour des polynômes irréductibles arbitraires $g(x) \in Z[x]$, par A. BRAUER, R. BRAUER et H. HOPF [5]. Après certains résultats moins généraux (pour l'aperçu de la bibliographie du problème voir [16] et [17]) dans [5] les auteurs ont même résolu le problème pour des polynômes $g(x)$ de degré <4. Plus précisément, ils ont démontré que, pour un $g(x)$ fixé de degré <4, il n'existe qu'un nombre fini de polynômes $f(x)$ du type précédent et deux à deux inéquivalents[5]) pour lesquels $g(f(x))$ peuvent être réductibles. Dans [38], [39], [40] I. SERES a développé une méthode et, en utilisant le théorème de Kronecker concernant les unités des corps cycloto-

[4]) $H(\alpha_i)$ signifie la hauteur de α_i.

[5]) On appelle les polynômes $f(x)$ et $f^*(x)$ *équivalents* si l'on a $f^*(x) = f(x+a)$ avec un $a \in Z$.

*) *Note ajoutée aux épreuves.* Voir encore les travaux récents de *N. I. Feldman* (Dokl. Akad. Nauk SSSR, 207 (1972), 41—43), *H. M. Stark* (Diophantine Approximation and Its Applications, Acad. Press, 1973) et *A. Baker* (Acta Arith. 24 (1973), 33—36).

miques, il a démontré l'irréductibilité des $g(f(x))$ pour tout polynôme cyclotomique $g(x)$ et pour tout $f(x)$ du type précédent, sauf la seule exception $g(x) = x^4-x^2+1$, $f(x) = x^3-x$ ([39]). Par là I. Seres a démontré la conjecture de I. Schur sous une forme plus générale. En outre, il a résolu [40] le problème de Brauer—Hopf pour tout $g(x)$ dont les racines sont unités non réelles d'un corps cyclotomique arbitraire.

A l'aide de l'inégalité de norme (Théorème 3), dans [17] (voir encore [16]) nous avons obtenu le résultat suivant:

Théorème 7. *Soit* $f(x)=(x-a_1)\dots(x-a_m)$ *avec des entiers rationnels* a_i *distincts et soit* $g(x)\in Z[x]$ *un polynôme unitaire irréductible avec un corps des racines de type* (a)$\Leftrightarrow\dots\Leftrightarrow$(g). *Alors* $g(f(x))$ *est irréductible sur* Q, *sauf dans certains cas où* $\max_{i,k}|a_i-a_k| \leqq$ $\leqq 4\{g(0)\}^{1/n}-1$, *c'est-à-dire où* $m\leqq 4\{g(0)\}^{1/n}$ $(n=\deg g)$.

Notre théorème donne la solution du problème de Brauer—Hopf pour tout $g(x)$ dont le corps des racines est une extension quadratique totalement imaginaire d'un corps de nombres totalement réel (de tels polynômes sont par exemple les polynômes cyclotomique) et, en même temps, il donne la généralisation des résultats de I. Seres [38], [40]. En outre, en utilisant notre Théorème 5, dans [16] (cf. le Théorème 6 dans [16]) nous avons déterminé tous les polynômes exceptionnels $f(x)$, $g(x)$ du théorème ci-dessus pour lesquels $g(0)=1$ et $g(f(x))$ est réductible sur Q, et ainsi nous avons généralisé le résultat cité de I. Seres [39], relatif au problème de I. Schur.

Dans [16] et [17] nous avons étendu nos résultats, obtenus sur Q, aussi aux polynômes considérés sur des corps de nombres de type (a)$\Leftrightarrow\dots\Leftrightarrow$(g). Également dans [17], pour les $g(x)$ précédents, nous avons donné au fait la solution du problème de Brauer—Hopf dans le cas plus général où les racines des $f(x)$ sont des nombres réels distincts.

Enfin, nous avons étendu certains de nos résultats aussi aux polynômes de la forme $g(f(x_1, \dots, x_r))=g(f(X))$ ([18]), en nous rattachant à un théorème général de A. Schinzel [34] qui concerne la réductibilité des polynômes de la forme $g(f_1(X_1), \dots, f_r(X_r))$ sur des corps arbitraires. Dans le cas $r=1$ ce théorème général de A. Schinzel n'est pas vrai en général, mais il reste valable pour les polynômes f, g considérés dans [18]. Nous n'énonçons notre théorème que pour $r=2$, toutefois ce théorème est vrai aussi pour $r>2$ (avec une restriction relative à f; [18]).

Théorème 8. *Soit* $g(x)\in Z[x]$ *un polynôme linéaire (tel que* $g(0)\neq 0$*) ou bien un polynôme irréductible ayant un corps des racines de type* (a)$\Leftrightarrow\dots\Leftrightarrow$(g). *Soit* $f(x_1, x_2)\in Z[x_1, x_2]$ *et soit* $f_1(x_1, x_2)$ *un diviseur irréductible de* f *tel que*

$$f_1(x_1, x_2) = 0$$

ait une infinité de solutions x_1, x_2 *en entiers rationnels. Alors les degrés des diviseurs irréductibles de* $g(f(x_1, x_2))$ *sont* $\leqq \deg f_1 \cdot \deg g$ *et ainsi le nombre de ses diviseurs irréductibles* $\leqq \dfrac{\deg f}{\deg f_1}$. *En particulier, si* $\deg f_1 > \dfrac{\deg f}{2}$, *alors* $g(f(x_1, x_2))$ *est irréductible sur* Q.

Nous remarquons que la minoration concernant les degrés des diviseurs irréductibles de $g(f(x_1, x_2))$ ne peut pas être améliorée en général. En outre, on peut étendre notre théorème aussi aux polynômes $g(x)$, $f(x)$ considérés sur les corps de nombres de type (a)$\Leftrightarrow\dots\Leftrightarrow$(g), à condition que $g(x)=c_0x+c_1$ (c_0 soit réel et c_1 non réel) et les coefficients de $f(x)$ soient réels.

7. Démonstrations des théorèmes

Nous démontrerons d'abord le Théorème 1. Les démonstrations des assertions (a)⇔(b), (e)⇒(a) (pour $r=1$) (a)⇔(g), (g)⇒(f) et (c)⇒(d) (dans le cas particulier $S=S_\infty$) se trouvent dans la littérature (voir l'introduction). Dans la suite nous allons démontrer l'équivalence de toutes les assertions (a), (b), (c), (d), (e), (f), (g). Ainsi, d'une part, l'équivalence de certaines assertions connues sera démontrée sous une forme un peu plus générale (pour $S \supseteq S_\infty$); d'autre part, nous pouvons un peu simplifier aussi les démonstrations des équivalences des assertions connues. On pourrait démontrer l'équivalence de façon cyclique. Toutefois (a)⇒(e) et (a)⇒(d) seront démontrés par les Théorèmes 2 et 3 plus généraux. Il suffit donc de démontrer (e)⇒(b)⇒(c)⇒(a) et puis (d)⇒(f)⇒(g)⇒(a).

Démonstration du Théorème 1. Pour la démonstration de (e)⇒(b) nous aurons besoin du lemme suivant:

Lemme. *Soit $n>2$ un nombre pair et soient r, s, t des nombres naturels tels que $0<r<n$ et $2s+2t=n$. Désignons par $E_r(z)$ la fonction symétrique élémentaire de degré r des $z_1, \ldots, z_n$. On peut choisir les valeurs des z_i de manière que $z_1=z_2, \ldots, \ldots, z_{2s-1}=z_{2s}>0$, $z_{2s+1}=\ldots=z_n<0$ et que $E_r(z)$ prenne des valeurs positives et négatives aussi.*

Démonstration du lemme. Considérons d'abord le cas où $r \geqq 2s$. Soient $z_1=\ldots=z_{2s-2}=c>0$ (pour $s>1$) $z_{2s-1}=z_{2s}$, et $z_{2s+1}=\ldots=z_n=d<0$ avec des valeurs c, z_{2s}, d qui seront déterminées ultérieurement. Considérons $E_r(z)$ avec ce $z=(z_1, \ldots, z_n)$ comme polynôme en c. Le coefficient dominant (qui est $E_r(z)$ pour $s=1$) est égal à

$$\binom{n-2s}{r-2s} d^{r-2s} z_{2s}^2 + \binom{n-2s}{r-2s+1} \cdot 2d^{r-2s+1} \cdot z_{2s} + \binom{n-2s}{r-2s+2} d^{r-2s+2} =$$

$$= \binom{n-2s}{r-2s} d^{r-2s} \cdot f(z_{2s}, d),$$

où

$$f(z_{2s}, d) = z_{2s}^2 + \frac{2(n-r)}{r-2s+1} d \cdot z_{2s} + \frac{(n-r)(n-r-1)}{(r-2s+1)(r-2s+2)} d^2.$$

Comme $f(z_{2s}, d)$ est quadratique en z_{2s} avec une racine positive (d'après $d<0$), on peut choisir les valeurs de $z_{2s}>0$ et $d<0$ de manière que $f(z_{2s}, d)$ prenne des valeurs positives et négatives. Si c est suffisamment grand (lorsque $s>1$), il en résulte que $E_r(z)$ prend des valeurs positives et négatives aussi.

Prenons maintenant le cas où $r<2s$. Soit $r=2u+v$, où $u \geqq 0$ et $v=1$ ou 2. Soient $z_1=\ldots=z_{2u}=c>0$ (si $u \geqq 1$), $z_{2u+1}=\ldots=z_{2s}>0$ et $z_{2s+1}=\ldots=z_n=d<0$ avec des valeurs c, d, z_{2s} qui seront déterminées ultérieurement. En considerant $E_r(z)$ comme polynôme en c, le coefficient dominant (qui est $E_r(z)$ pour $u=0$) est

$$\binom{2s-2u}{v} z_{2s}^v + \binom{2s-2u}{v-1} \binom{n-2s}{1} d z_{2s}^{v-1} + \binom{n-2s}{2} (v-1) d^2.$$

Si $v=1$, on peut choisir convenablement $z_{2s}>0$ et $d<0$ de manière que ce coefficient prenne des valeurs positives et négatives. Si $v=2$, nous obtenons un polynôme quad-

ratique en z_{2s} avec une racine positive (étant $d<0$). Par conséquent, ce coefficient peut être également positif et négatif aussi. Ainsi, si c est suffisamment grand (cas $u>0$), $E_r(z)$ prend en effet des valeurs positives et négatives aussi.

Démonstration de (e)⇒(b). L'idée fondamentale de la démonstration est due à G. Shimura et Y. Taniyama (voir la démonstration du cas $r=1$ dans [41], à la page 41).

Soit désigné par K_0 le sous-corps réel maximal de K. Puisque $\overline{K}=K$, l'extension K/K_0 est quadratique et n est pair.

D'abord nous allons démontrer que K_0 est totalement réel. Dans le cas contraire, soient $\sigma_1, \ldots, \sigma_s$ et $\tau_1, \bar{\tau}_1, \ldots, \tau_t, \bar{\tau}_t$ $(s, t>0)$ les Q-isomorphismes, respectivement réels et non réels, de K_0 dans C. En vertu du lemme, on peut choisir les valeurs des $z_1, \ldots, z_n$ de manière que $z_1=z_2, \ldots, z_{2s-1}=z_{2s}>0$, $z_{2s+1}=\ldots=z_n=d<0$ et $E_r(z)<0$. Employons le théorème d'approximation pour K_0. Il existe un $\alpha\in K_0$ tel que

$$|\alpha\sigma_j-\sqrt{z_{2j}}|<\varepsilon \quad (j=1, \ldots, s), \quad |\alpha\tau_j-(a+bi)|<\varepsilon \quad (j=1, \ldots, t) \quad (\varepsilon \text{ constant}),$$

où a, b sont des nombres réels, $a^2-b^2=d$ et $|ab|$ sont suffisamment petits. Il en résulte que

$$|\alpha^2\sigma_j-z_{2j}|<\varepsilon' \quad (1\leqq j\leqq s), \quad |\alpha^2\tau_j-d|=|\alpha^2\bar{\tau}_j-d|<\varepsilon' \quad (1\leqq j\leqq t)$$

avec une constante $\varepsilon'>0$ convenablement choisie. Si $\varepsilon, \varepsilon'>0$ sont suffisamment petits, les signes de $E^{(r)}_{K/Q}(\alpha^2)$ et de $E_r(z)$ sont identiques, ce qui entraîne une contradiction.

Supposons que K n'est pas totalement imaginaire. Soient $\sigma_1, \ldots, \sigma_{s'}$ et $\tau_1, \bar{\tau}_1, \ldots, \tau_{t'}, \bar{\tau}_{t'}$ $(s', t'>0)$ ses Q-isomorphismes respectivement réels et non réels dans C (où $s'=2s$ est pair). Soient $z_1=z_2, \ldots, z_{2s-1}=z_{2s}>0$, $z_{2s+1}=\ldots=z_n=d<0$ choisis de manière que pour r pair soit $E_r(z)<0$ et pour r impair soit $E_r(z)>0$.

On peut écrire $K=K_0(\varrho)$, où $\varrho^2\in K_0$ et $\bar{\varrho}=-\varrho$. Il en résulte que $\alpha\varrho\cdot\overline{\alpha\varrho}=-\alpha^2\varrho^2$ pour tout $\alpha\in K_0$, et, d'après $E^{(r)}_{K/Q}(\alpha\varrho\cdot\overline{\alpha\varrho})>0$ on a

$$E^{(r)}_{K/Q}(\alpha\varrho\cdot\overline{\alpha\varrho})=E^{(r)}_{K/Q}(-\alpha^2\varrho^2)=\begin{cases} E^{(r)}_{K/Q}(\alpha^2\varrho^2)>0 & \text{pour } r \text{ pair},\\ -E^{(r)}_{K/Q}(\alpha^2\varrho^2)>0 & \text{pour } r \text{ impair}.\end{cases}$$

Si les isomorphismes de K_0 dans C sont $\sigma_1, \ldots, \sigma_s, \tau_1, \ldots, \tau_{t'}$, à cause du théorème d'approximation il existe un $\alpha\in K_0$ tel que

$$\left|\alpha\sigma_j-\frac{\sqrt{z_{2j}}}{|\varrho\sigma_j|}\right|<\varepsilon \quad (1\leqq j\leqq s), \quad \left|\alpha\tau_j-\frac{\sqrt{|d|}}{|\varrho\tau_j|}\right|<\varepsilon \quad (1\leqq j\leqq t'),$$

d'où

$$|(\alpha^2\varrho^2)\sigma_j-z_{2j}|<\varepsilon' \quad (1\leqq j\leqq s), \quad |(\alpha^2\varrho^2)\tau_j-d|<\varepsilon' \quad (1\leqq j\leqq t')$$

avec des constantes $\varepsilon, \varepsilon'>0$ suffisamment petites. Alors les signes de $E^{(r)}_{K/Q}(\alpha^2\varrho^2)$ et de $E_r(z)$ sont identiques, ce qui est impossible.

Soit ensuite $\beta=\alpha_1+\varrho\alpha_2$ $(\alpha_1, \alpha_2\in K_0)$ un nombre arbitraire dans K et soit φ un

Q-isomorphisme de K dans C. On obtient

$$\beta\psi\varphi = (\alpha_1 - \varrho\alpha_2)\varphi = \alpha_1\varphi - (\varrho\varphi)\alpha_2\varphi = (\alpha_1\varphi + (\varrho\varphi)\alpha_2\varphi)\psi =$$
$$= (\alpha_1 + \varrho\alpha_2)\varphi\psi = \beta\varphi\psi,$$

ce qui prouve notre assertion.

Démonstration de (b)⇒(c). Soit F l'extension normale de Q engendrée par K dans C, F_0 son sous-corps réel maximal et $G=\mathrm{Gal}\,(F/Q)$. Si $\sigma^*\in G$ et σ est la restriction de σ^* à K, alors $K\sigma=K_\sigma$ est un conjugué de K, et, reciproquement, tous les conjugués de K sont de cette forme. Soit H_σ le sous-groupe de G correspondant à K_σ. Soit $\tau^*\in G$ et soit τ sa restriction à K_σ Comme $\sigma\tau$ est également un Q-isomorphisme de K, d'après (b) on a $\overline{K}_\sigma=K\sigma\psi=K\psi\sigma=K\sigma$ (non point par point) et

$$K_\sigma\tau^*\psi = K(\sigma\tau)\psi = (K\psi)\sigma\tau = (K\sigma)\psi\tau = K_\sigma\psi\tau^*$$

point par point, c'est-à-dire $\tau^*\psi\tau^{*-1}\psi^{-1}\in \bigcap_{\sigma\ \text{isom. de}\ K} H_\sigma = \{1\}$. Donc $\tau^*\psi=\psi\tau^*$ pour tout $\tau^*\in G$, ainsi $\{\psi\}$ est un sous-groupe normal dans G et, par conséquent, l'extension F_0/Q est normale.

Démonstration de (c)⇒(a). Désignons par K_0 le sous-corps réel maximal de K. Il résulte de l'hypothèse que K est totalement imaginaire et K_0 est totalement réel. De plus, le sous-groupe $\{\psi\}\subseteqq G=\mathrm{Gal}\,(F/Q)$, qui correspond au sous-corps F_0, est normal dans G. Soit H le sous-groupe de G correspondant à K. Puisque $\psi^2=1$, on a $(\alpha\psi)H=(\alpha H)\psi=\alpha\psi$ pour tout $\alpha\in K$, c'est-à-dire H laisse invariant $\overline{K}$ aussi point par point, d'où $\overline{K}\subseteqq K$ et ainsi $\overline{K}=K$. Si $K=Q(\alpha)$, alors $\alpha+\bar{\alpha}$ et $\alpha\bar{\alpha}\in K_0$, donc K/K_0 est quadratique.

Démonstration de (d)⇒(f). Supposons que

$$\Big|N_{K/Q}(\alpha)\prod_{\varphi\in S^*}\varphi(\alpha)\Big| \geqq c\Big|N_{K/Q}(\mathrm{Re}\,\alpha)\prod_{\varphi\in S^*}\varphi(\mathrm{Re}\,\alpha)\Big|$$

pour tout $\alpha\in K$ avec une constante $0<c\leqq 1$. Soit $\alpha\in K$ un S-entier non réel et soit ε une S-unité. On peut supposer ε non réel at ainsi $\bar{\varepsilon}$ est également une S-unité dans K. D'après l'hypothèse on a pour tout entier k

$$\Big|N_{K/Q}(\alpha\varepsilon^k)\prod_{\varphi\in S^*}\varphi(\alpha\varepsilon^k)\Big| \geqq c\Big\{2^n\prod_{\varphi\in S^*}\varphi(2)\Big\}^{-1}\Big|N_{K/Q}(\alpha\varepsilon^k+\overline{\alpha\varepsilon^k})\prod_{\varphi\in S^*}\varphi(\alpha\varepsilon^k+\overline{\alpha\varepsilon^k})\Big|.$$

Si $\zeta=\bar{\varepsilon}/\varepsilon$, on en déduit

$$\Big\{2^n\prod_{\varphi\in S^*}\varphi(2)\Big\}\Big|N_{K/Q}(\alpha)\prod_{\varphi\in S^*}\varphi(\alpha)\Big| \geqq c\Big|N_{K/Q}(\alpha+\zeta^k\bar{\alpha})\prod_{\varphi\in S^*}\varphi(\alpha+\zeta^k\bar{\alpha})\Big|$$

pour tout entier k. Supposons que ζ n'est pas racine de l'unité. Alors les nombres $\beta_k=\alpha+\zeta^k\bar{\alpha}$ sont des S-entiers distincts. Par conséquent, pour une suite infinie de ces β_k, on a

$$N_{K/Q}(\beta_k)\prod_{\varphi\in S^*}\varphi(\beta_k) = a$$

avec un $a\in Z$ fixé ($a\neq 0$). Il en résulte que, pour un S-entier $\beta\neq 0$ et pour une sous-suite infinie β_{i_k} des β_k, on a $\beta_{i_k}=\alpha+\zeta^{i_k}\bar{\alpha}=\varrho_{i_k}\beta$, ϱ_{i_k} étant des S-unités. Ainsi

l'équation diophantienne

$$\alpha + x\bar{\alpha} + y\beta = 0$$

a une infinité de solutions x, y en S-unités de K, contrairement à un théorème connu (voir [22], p. 134).

Dans le cas où

$$\left|N_{K/Q}(\alpha) \prod_{\varphi \in S^*} \varphi(\alpha)\right| \geqq c\left|N_{K/Q}(i \operatorname{Im} \alpha) \prod_{\varphi \in S^*} \varphi(i \operatorname{Im} \alpha)\right|$$

pour tout $\alpha \in K$, on peut démontrer (d)⇒(f) de la même façon. Donc, ζ est nécessairement une racine de l'unité.

Démonstration de (f)⇒(g). Soit $\varepsilon \in U_S$. Si ε est réel, alors $\varepsilon \in U_S^0$. Dans le cas contraire $\bar{\varepsilon} = \zeta\varepsilon$ avec une racine de l'unité ζ, où $\bar{\varepsilon}$ est également une S-unité. Si $\zeta = \zeta_1^{2k}$ avec une racine de l'unité $\zeta_1 \in K$, alors $\bar{\varepsilon}/\zeta_1^k = \varepsilon/\zeta_1^{-k} = \eta$ est une S-unité réelle, autrement dit $\varepsilon \in \{V, U_S^0\}$. Si $\zeta = \zeta_1^{2k+1}$ avec une racine de l'unité $\zeta_1 \in K$, et si pour une autre S-unité ϱ on a $\bar{\varrho} = \zeta_1^{2l+1}\varrho$, alors $\bar{\varepsilon}/\bar{\varrho} = \zeta_1^{2(k-l)} \cdot \varepsilon/\varrho$, c'est-à-dire $\varepsilon/\varrho \in \{V, U_S^0\}$. Par conséquent $[U_S : \{V, U_S^0\}] \leqq 2$.

Démonstration de (g)⇒(a). Il résulte de $\overline{K} = K$ que K/K_0 est quadratique (K_0 désigne le sous-corps réel maximal de K). Les valeurs absolues $\varphi \in S \setminus S_\infty$ sont toutes réelles, ainsi chaque $\varphi \in S$ est l'unique prolongement de la valeur absolue correspondante φ_0 de K_0. Désignons par S^0 l'ensemble de ces φ_0 et soit S_∞^0 l'ensemble des valeurs absolues archimédiennes sur K_0. Si U_{S^0} désigne le groupe des S^0-unités de K_0, alors $U_{S^0} = U_S^0$. En effet, étant donné un $\alpha \in K_0$, $\alpha \in U_S^0$ si et seulement si $\varphi(\alpha) = 1$ pour tout $\varphi \notin S$, c'est-à-dire si $\varphi_0(\alpha) = 1$ pour tout $\varphi_0 \notin S^0$ et ainsi $\alpha \in U_{S^0}$. Soit Card $(S \setminus S_\infty) = \text{Card}\,(S^0 \setminus S_\infty^0) = k$, les nombres des corps conjugués réels de K et K_0 soient respectivement s et s_0, et ceux des corps conjugués complexes de K et K_0 soient $2t$ et $2t_0$. D'après un théorème connu, U_S est donc produit direct de V par un groupe abélien libre de rang $s+t+k-1$, et U_{S^0} est le produit direct de $\{-1\}$ par un groupe abélien libre de rang s_0+t_0+k-1. Puisque $U_{S^0} = U_S^0$ et $[U_S : \{V, U_S^0\}] < \infty$, il en résulte que $s+t+k-1 = s_0+t_0+k-1$, d'où $s+t = s_0+t_0$ et $[K_0 : Q] = s_0+2t_0 \geqq$ $\geqq s_0+t_0 = s+t \geqq \dfrac{s+2t}{2} = \dfrac{[K:Q]}{2}$. Donc, on obtient $s=0$ et $t_0=0$, et (g)⇒(a) est démontré.

Démonstration du corollaire 1.1. En vertu de notre Théorème 1 (voir (a)⇔(c)), les deux premières parties de notre assertion sont triviales. Pour démontrer la troisième assertion il suffit de considérer le cas où $m=2$, et où K_1/Q et K_2/Q sont normaux et au moins l'un d'eux, par ex. K_1/Q, n'est pas réel. $K = \{K_1, K_2\}$ est normal sur Q. Soit $G = \text{Gal}\,(K/Q)$ son groupe de Galois, et soient H_1 et H_2 les sous-groupes normaux correspondant respectivement à K_1 et K_2, où $H_1 \cap H_2 = \{1\}$. On a Gal $(K_1/Q) \cong G/H_1$ et Gal $(K_2/Q) \cong G/H_2$. Considérons ψ (c'est-à-dire l'automorphisme $\alpha \to \bar{\alpha}$ de C) comme élément de G. D'après le Théorème 1 on a $(H_i\varphi)(H_i\psi) =$ $= (H_i\psi)(H_i\varphi)$ $(i=1, 2)$ pour tout $\varphi \in G$, d'où $H_i\varphi\psi = H_i\psi\varphi$ $(i=1, 2)$ et $\varphi\psi\varphi^{-1}\psi^{-1} \in$ $\in H_1$, H_2 qui implique $\varphi\psi\varphi^{-1}\psi^{-1} \in H_1 \cap H_2 = \{1\}$, c'est-à-dire $\varphi\psi = \psi\varphi$. Il en résulte, également d'après le Théorème 1, que K est un corps de nombres de type (a)⇔...⇔(g), et notre assertion est démontrée.

Démonstration du corollaire 1.2. Soient $\sigma_1, \ldots, \sigma_n$ les Q-isomorphismes de K dans le corps C des nombres complexes. $\alpha\bar{\alpha} \in K_0$ et d'après le Théorème 1 on obtient $(\alpha\bar{\alpha})\sigma_i = (\alpha\sigma_i)(\bar{\alpha}\sigma_i) = (\alpha\sigma_i)(\overline{\alpha\sigma_i}) \geqq 0$ pour tout i. En employant une inégalité connue (voir [3], Chapitre 1, § 12), on en déduit (4), qui implique immédiatement (5).

Pour démontrer le Théorème 2 nous aurons besoin du lemme suivant dû à M. MARCUS et L. LOPEZ [24]. Si $a=(a_1, \ldots, a_n)$ est un vecteur à coordonnées réelles, désignons par $E_r(a)$ la fonction symétrique élémentaire de degré r de ses coordonnées.

Lemme. *Soient* $a_1=(a_{11}, \ldots, a_{1n})$, $a_2=(a_{21}, \ldots, a_{2n})$ *des vecteurs à coordonnées positives. On a*

$$\{E_r(a_1+a_2)\}^{1/r} \geqq \{E_r(a_1)\}^{1/r} + \{E_r(a_2)\}^{1/r} \quad (r = 1, \ldots, n), \tag{28}$$

l'égalité n'étant vraie que si $r=1$ *ou* $a_2=\lambda a_1$ *avec un nombre réel* λ.

Démonstration: voir [24].

Démonstration du Théorème 2. Si $a_1, \ldots, a_k$ sont des vecteurs de dimension n avec des coordonnées positives, le lemme entraîne

$$\{E_r(a_1 + \ldots + a_k)\}^{1/r} \geqq \{E_r(a_1)\}^{1/r} + \ldots + \{E_r(a_k)\}^{1/r} \quad (r = 1, \ldots, n). \tag{29}$$

En outre, dans (29) l'égalité a lieu si et seulement si $r=1$ ou $a_i=\lambda_i a_1$ $(i=1, \ldots, k)$ avec des nombres $\lambda_i>0$ réels.

Soit K_0 le sous-corps réel maximal de K (K_0 est totalement réel). Comme $\alpha_i \in K$, $\alpha_i\bar{\alpha}_i \in K_0$, c'est-à-dire $\alpha_i\bar{\alpha}_i$ est totalement réel pour tout $i=1, \ldots, k$. On obtient

$$(\alpha_i\bar{\alpha}_i)\sigma = \left(\frac{\alpha_i+\bar{\alpha}_i}{2}\right)^2\sigma - \left(\frac{\alpha_i-\bar{\alpha}_i}{2}\right)^2\sigma \quad (i = 1, \ldots, k)$$

pour tout Q-isomorphisme σ de K dans C. Puisque $\frac{\alpha_i+\bar{\alpha}_i}{2}$ est totalement réel, on a

$$\left(\frac{\alpha_i+\bar{\alpha}_i}{2}\right)^2\sigma = \left[\left(\frac{\alpha_i+\bar{\alpha}_i}{2}\right)\sigma\right]^2 \geqq 0 \quad (i = 1, \ldots, k).$$

En outre $\frac{a_i-\bar{\alpha}_i}{2}$ et tous ses conjugués sont imaginaires purs, d'où

$$-\left(\frac{\alpha_i-\bar{\alpha}_i}{2}\right)^2\sigma = -\left[\left(\frac{\alpha_i-\bar{\alpha}_i}{2}\right)\sigma\right]^2 \geqq 0 \quad (i = 1, \ldots, k).$$

Par conséquent, si $\alpha_i \neq 0$, alors $\alpha_i\bar{\alpha}_i$ sont totalement positifs $(i=1, \ldots, k)$. Si nous désignons par a_i le vecteur dont les coordonnées se constituent des conjugués de $\alpha_i\bar{\alpha}_i$, on obtient $E^{(r)}_{K/Q}(\alpha_i\bar{\alpha}_i)>0$ $(1 \leqq r \leqq n;\ 1 \leqq i \leqq k)$, de plus, (29) implique l'inégalité annoncée, dans laquelle l'égalité a lieu si, et seulement si, $r=1$ ou

$$\frac{(\alpha_i\bar{\alpha}_i)\sigma}{(\alpha_1\bar{\alpha}_1)\sigma} = \left(\frac{\alpha_i\bar{\alpha}_i}{\alpha_1\bar{\alpha}_1}\right)\sigma = \lambda_i \quad (i = 1, \ldots, k)$$

pour tout σ, c'est-à-dire si $\alpha_i\bar{\alpha}_i = \lambda_i\alpha_1\bar{\alpha}_1$, où $\lambda_i \in Q$ $(i = 1, \ldots, k)$.

Démonstration du Théorème 3. Si K_0 est le sous-corps réel maximal de K, d'après $\alpha\in K$ il résulte que $\operatorname{Re}\alpha\in K_0$ est totalement réel et tous les conjugués de $i\operatorname{Im}\alpha\in$ $\in K$ sont imaginaires purs. Employons le corollaire 2.1 dans le cas où $k=2$ avec le choix $\alpha_1=\operatorname{Re}\alpha$, $\alpha_2=i\operatorname{Im}\alpha$. On obtient $\alpha_1\bar{\alpha}_1+\alpha_2\bar{\alpha}_2=\alpha\bar{\alpha}$, et, en vertu de $N_{K/Q}(\alpha\bar{\alpha})=N^2_{K/Q}(\alpha)$, on en déduit immédiatement (7). Si $\operatorname{Re}\alpha=0$ ou $i\operatorname{Im}\alpha=0$, alors dans (7) une égalité se trouve évidemment. Si $\operatorname{Re}\alpha$, $i\operatorname{Im}\alpha\neq 0$, d'après le corollaire 2.1, dans (7) l'égalité a lieu si, et seulement si, $\alpha_2\bar{\alpha}_2=\lambda\alpha_1\bar{\alpha}_1$, c'est-à-dire si $\left(\dfrac{\operatorname{Re}\alpha}{i\operatorname{Im}\alpha}\right)^2=-\lambda^{-1}\in Q$.

Enfin, nous allons démontrer l'inégalité (6). Soit φ une valeur absolue non archimédienne normalisée sur K. Si φ est réel, alors

$$\varphi(\alpha\pm\bar{\alpha})\leqq\max\left(\varphi(\alpha),\varphi(\bar{\alpha})\right)=\varphi(\alpha),$$

c'est-à-dire

$$\varphi(2)\varphi(\operatorname{Re}\alpha),\quad \varphi(2)\varphi(i\operatorname{Im}\alpha)\leqq\varphi(\alpha) \tag{30}$$

pour tout $\alpha\in K$. Si φ est non réel, on obtient

$$\varphi(2)\varphi(\operatorname{Re}\alpha),\quad \varphi(2)\varphi(i\operatorname{Im}\alpha)\leqq\max\left(\varphi(\alpha),\varphi(\bar{\alpha})\right)\quad(\alpha\in K). \tag{31}$$

Considérons les inégalités (30) et (31) pour chaque $\varphi\in S_1$ et $\varphi\in S_2$. Il résulte que

$$\Big\{\prod_{\varphi\in S_1}\varphi(\alpha)\prod_{\varphi\in S_2}\max\left(\varphi(\alpha),\varphi(\bar{\alpha})\right)\Big\}^{2/n}\geqq$$

$$\geqq\Big\{\prod_{\varphi\in S_1\cup S_2}\varphi(2)\varphi(\operatorname{Re}\alpha)\Big\}^{2/n},\quad\Big\{\prod_{\varphi\in S_1\cup S_2}\varphi(2)\varphi(i\operatorname{Im}\alpha)\Big\}^{2/n}.$$

En comparant ces inégalités avec (7), on obtient (6).

Démonstration du corollaire 3.2. Si $\alpha+\beta=\gamma$ est réel, alors $\bar{\alpha}+\bar{\beta}=\gamma$, d'où

$$2i\operatorname{Im}\alpha\bar{\beta}=\alpha\bar{\beta}-\bar{\alpha}\beta=(\alpha+\beta)\bar{\beta}-(\bar{\alpha}+\bar{\beta})\beta=$$

$$=\gamma\bar{\beta}-\gamma\beta=\gamma(\bar{\beta}-\beta)=-2\gamma i\operatorname{Im}\beta\in K.$$

Comme α/β n'est pas réel, $0\neq\beta-\bar{\beta}=2i\operatorname{Im}\beta\in K$ et il est un entier. En appliquant l'inégalité (7), il en résulte que

$$N_{K/Q}(\alpha+\beta)=N_{K/Q}(\gamma)\leqq N_{K/Q}(\gamma\cdot 2i\operatorname{Im}\beta)=$$

$$=N_{K/Q}(2i\operatorname{Im}\alpha\bar{\beta})\leqq N_{K/Q}(2\alpha\bar{\beta})=N_{K/Q}(2)N_{K/Q}(\alpha\beta),$$

d'où (10). De plus, dans ce cas, l'égalité a lieu dans (10) si et seulement si $2i\operatorname{Im}\beta=$ $=\beta-\bar{\beta}$ et $\alpha-\bar{\alpha}$ sont des unités et $\operatorname{Re}\alpha\bar{\beta}=0$, c'est-à-dire si α/β est imaginaire pur.

Considérons ensuite le cas où $\alpha+\beta=\gamma$ est imaginaire pur et ainsi $\bar{\alpha}+\bar{\beta}=-\gamma$, $\operatorname{Re}\alpha$, $\operatorname{Re}\beta\neq 0$. Alors

$$2i\operatorname{Im}\alpha\bar{\beta}=\alpha\bar{\beta}-\bar{\alpha}\beta=(\alpha+\beta)\bar{\beta}-(\bar{\alpha}+\bar{\beta})\beta=$$

$$=\gamma\bar{\beta}+\gamma\beta=\gamma(\beta+\bar{\beta})=\gamma\cdot 2\operatorname{Re}\beta,$$

où $2\operatorname{Re}\beta = \beta+\bar{\beta}\in K$ est un entier. En utilisant de nouveau (7), il résulte que

$$N_{K/Q}(\alpha+\beta) = N_{K/Q}(\gamma) \leqq N_{K/Q}(\gamma\cdot 2\operatorname{Re}\beta) =$$
$$= N_{K/Q}(2i\operatorname{Im}\alpha\bar{\beta}) \leqq N_{K/Q}(2\alpha\bar{\beta}) = N_{K/Q}(2)N_{K/Q}(\alpha\beta),$$

qui implique (10), et l'égalité a lieu si et seulement si $2\operatorname{Re}\beta = \beta+\bar{\beta}$ et $\alpha+\bar{\alpha}$ sont des unités et $\operatorname{Re}\alpha\bar{\beta}=0$, c'est-à-dire α/β est imaginaire pur.

Démonstration du corollaire 3.3. Il suffit de considérer le cas où α n'est pas réel. D'après le Théorème 1 $K=Q(\alpha)$ est un corps de nombres de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g) et de degré n. Soient $K'=Q(\operatorname{Re}\alpha)$ et $K''=Q(i\operatorname{Im}\alpha)$. Prenons le nombre $\beta = x-\alpha\in K$ avec un nombre rationnel x arbitraire. Du Théorème 3 il résulte que

$$\{g^2(x)\}^{1/n} = \{N_{K/Q}(x-\alpha)\}^{2/n} \geqq \{N_{K/Q}(x-\operatorname{Re}\alpha)\}^{2/n} + \{N_{K/Q}(i\operatorname{Im}\alpha)\}^{2/n} =$$
$$= \{N_{K'/Q}(x-\operatorname{Re}\alpha)\}^{2/k} + \{N_{K''/Q}(i\operatorname{Im}\alpha)\}^{2/l} = \{g_R^2(x)\}^{1/k} + \{g_I^2(0)\}^{1/l}.$$

Mais Q est partout dense dans le corps R des nombres réels, ce qui achève la démonstration.

Démonstration du Théorème 4. Soient $\varphi_1, \ldots, \varphi_n$ les Q-isomorphismes distincts de $K=Q(\alpha)$ dans C. Si $\alpha\varphi_1=\alpha$, alors la différente de α est

$$\delta(\alpha) = (\alpha-\alpha\varphi_2)\ldots(\alpha-\alpha\varphi_n)$$

et son discriminant

$$D(\alpha) = D_{K/Q}(\alpha) = (-1)^{\binom{n}{2}}N_{K/Q}(\delta(\alpha)).$$

D'après le Théorème 1 on a

$$2\operatorname{Re}(\alpha\varphi_j) = \alpha\varphi_j+\overline{\alpha\varphi}_j = (\alpha+\bar{\alpha})\varphi_j = 2(\operatorname{Re}\alpha)\varphi_j \quad (1\leqq j\leqq n)$$

et de façon analogue pour $i\operatorname{Im}\alpha$. Soit $L=Q(\alpha_1,\ldots,\alpha_n)$ et $[L:Q]=N$. En vertu du Théorème 1 L est également un corps de nombres de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g), et du Théorème 3 il résulte que

$$(32)\qquad |D(\alpha)|^{2/n} = |D(\alpha)|^{\frac{2[L:K]}{N}} = \left|N_{L/Q}\left((\alpha-\alpha\varphi_2)\ldots(\alpha-\alpha\varphi_n)\right)\right|^{2/N} =$$
$$= \prod_{j=2}^{n}|N_{L/Q}(\alpha-\alpha\varphi_j)|^{2/N} \geqq \prod_{j=2}^{n}\left\{\left|N_{L/Q}(\operatorname{Re}\alpha-(\operatorname{Re}\alpha)\varphi_j)\right|^{2/N} + \right.$$
$$\left. + \left|N_{L/Q}(i\operatorname{Im}\alpha-(i\operatorname{Im}\alpha)\varphi_j)\right|^{2/N}\right\}.$$

Il n'y a que k nombres distincts dans l'ensemble $\operatorname{Re}\alpha$, $(\operatorname{Re}\alpha)\varphi_2, \ldots, (\operatorname{Re}\alpha)\varphi_n$ et chacun d'eux figurant n/k fois (et de manière analogue aussi pour $i\operatorname{Im}\alpha, \ldots, (i\operatorname{Im}\alpha)\varphi_n$). Désignons par $\delta(\operatorname{Re}\alpha)$ la différente de $\operatorname{Re}\alpha$ et considérons le produit des termes $N_{L/Q}(\operatorname{Re}\alpha-(\operatorname{Re}\alpha)\varphi_j)$ $(j=2,\ldots,n)$ qui sont différents de zéro dans (32). On a

$$\prod_{\varphi_j;\ \operatorname{Re}\alpha\neq(\operatorname{Re}\alpha)\varphi_j}\left|N_{L/Q}(\operatorname{Re}\alpha-(\operatorname{Re}\alpha)\varphi_j)\right| = \left|N_{L/Q}\left((\delta(\operatorname{Re}\alpha))^{n/k}\right)\right| =$$
$$= \left|N_{K'/Q}(\delta(\operatorname{Re}\alpha))\right|^{[L:K']\frac{n}{k}} = |D(\operatorname{Re}\alpha)|^{\frac{nN}{k^2}}.$$

Prenons ensuite dans (32) le produit des termes $N_{L/Q}(i\,\mathrm{Im}\,\alpha-(i\,\mathrm{Im}\,\alpha)\varphi_j)$ pour lesquels $\mathrm{Re}\,\alpha=(\mathrm{Re}\,\alpha)\varphi_j$ $(2\leqq j\leqq n)$. Le nombre de ces φ est $n/k-1$, ces φ soient par ex. $\varphi_2, \ldots, \varphi_{\frac{n}{k}}$ $\left(\text{où } \frac{n}{k}>1\right)$. Comme $i\,\mathrm{Im}\,\alpha\in K$ et $Q(i\,\mathrm{Im}\,\alpha, \mathrm{Re}\,\alpha)=K$, $i\,\mathrm{Im}\,\alpha$ est de degré n/k sur K'. Puisque les éléments de K' restent invariants pour les isomorphismes $\varphi_1, \ldots, \varphi_{n/k}$ et puisque $(i\,\mathrm{Im}\,\alpha)\varphi_1 = i\,\mathrm{Im}\,\alpha, \ldots, (i\,\mathrm{Im}\,\alpha)\varphi_{n/k}$ sont deux à deux distincts, ces nombres sont les conjugués de $i\,\mathrm{Im}\,\alpha$ sur K'. On obtient donc

$$\prod_{\varphi_j\,(j\geqq 2);\ \mathrm{Re}\,\alpha=(\mathrm{Re}\,\alpha)\varphi_j} \left|N_{L/Q}(i\,\mathrm{Im}\,\alpha-(i\,\mathrm{Im}\,\alpha)\varphi_j)\right| = \prod_{j=2}^{n/k}\left|N_{L/Q}(i\,\mathrm{Im}\,\alpha-(i\,\mathrm{Im}\,\alpha)\varphi_j)\right| =$$
$$= \left|N_{L/Q}(\delta_{K/K'}(i\,\mathrm{Im}\,\alpha))\right| = \left|N_{K'/Q}(N_{L/K'}(\delta_{K/K'}(i\,\mathrm{Im}\,\alpha)))\right| =$$
$$= \left|N_{K'/Q}(N_{K/K'}(\delta_{K/K'}(i\,\mathrm{Im}\,\alpha))^{[L:K]})\right| = \left|N_{K'/Q}(D_{K/K'}(i\,\mathrm{Im}\,\alpha))\right|^{N/n}.$$

Répétons ce procédé aussi pour $i\,\mathrm{Im}\,\alpha$ et $\mathrm{Re}\,\alpha$. S'il y a au moins un φ_j tel que $(\mathrm{Re}\,\alpha)\varphi_j\neq\mathrm{Re}\,\alpha$ et $(i\,\mathrm{Im}\,\alpha)\varphi_j\neq i\,\mathrm{Im}\,\alpha$, on en déduit

$$|D(\alpha)|^{2/n} \geqq |D(\mathrm{Re}\,\alpha)|^{\frac{2n}{k^2}}\cdot\left|N_{K'/Q}(D_{K/K'}(i\,\mathrm{Im}\,\alpha))\right|^{2/n} +$$
$$+|D(i\,\mathrm{Im}\,\alpha)|^{\frac{2n}{l^2}}\cdot\left|N_{K''/Q}(D_{K/K''}(\mathrm{Re}\,\alpha))\right|^{2/n}.$$

Puisque $D_{K/K'}(i\,\mathrm{Im}\,\alpha) = D_{K/K'}(\alpha)$ et $D_{K/K''}(\mathrm{Re}\,\alpha) = D_{K/K''}(\alpha)$, dans ce cas (13) est démontré.

Il nous faut encore considérer le cas où $(\mathrm{Re}\,\alpha)\varphi_j = \mathrm{Re}\,\alpha$ ou $(i\,\mathrm{Im}\,\alpha)\varphi_j = i\,\mathrm{Im}\,\alpha$ pour tout j. Mais le nombre des Q-isomorphismes (y compris l'identité), qui laissent invariants $\mathrm{Re}\,\alpha$ (resp. $i\,\mathrm{Im}\,\alpha$) est n/k (resp. n/l). Par conséquent, le nombre des isomorphismes qui laissent invariants au moins l'un des $\mathrm{Re}\,\alpha$ et $i\,\mathrm{Im}\,\alpha$ est $\leqq\frac{n}{k}+\frac{n}{l}-1$, d'où, d'après l'hypothèse, $n\leqq\frac{n}{k}+\frac{n}{l}-1$ et $1+\frac{1}{n}\leqq\frac{1}{k}+\frac{1}{l}$, qui est impossible.

Le raisonnement ci-dessus et le théorème 3 utilisé impliquent que dans (13) l'égalité a lieu si et seulement si $(\mathrm{Re}\,\alpha)\varphi_j\neq\mathrm{Re}\,\alpha$ et $(i\,\mathrm{Im}\,\alpha)\varphi_j\neq i\,\mathrm{Im}\,\alpha$ ne se réalisent à la fois que pour un seul j et que si, pour ce j, $\left(\frac{\mathrm{Re}\,(\alpha-\alpha\varphi_j)}{i\,\mathrm{Im}\,(\alpha-\alpha\varphi_j)}\right)^2\in Q$. Dans ce cas le nombre des isomorphismes φ_j, qui laissent invariants au moins l'un des $\mathrm{Re}\,\alpha$ et $i\,\mathrm{Im}\,\alpha$, est $n-1\leqq\frac{n}{k}+\frac{n}{l}-1$, d'où $1\leqq\frac{1}{k}+\frac{1}{l}$ et finalement $k=l=2$, $n=4$. Réciproquement, soit $\alpha=\mathrm{Re}\,\alpha+i\,\mathrm{Im}\,\alpha$ tel que les nombres $\mathrm{Re}\,\alpha$ et $i\,\mathrm{Im}\,\alpha$ soient quadratiques. Alors le corps de nombres $K=Q(\alpha)$ est de type (a)$\Leftrightarrow\ldots\Leftrightarrow$(g) et satisfait aux conditions du théorème avec $k=l=2$. En outre, on voit facilement que dans (13) on trouve, en effet, une égalité.

Démonstration du corollaire 4.4. Soient $D_{K/K'}$ et $D_{K/K''}$ les discriminants de K respectivement sur K' et K'' (dans le cas où $K''=K$, soit $D_{K/K}=1$). On a $D_{K/K'}|D_{K/K'}(\alpha)$, $D_{K/K''}|D_{K/K''}(\alpha)$ et $D_{K'}|D(\mathrm{Re}\,\alpha)$, $D_{K''}|D(i\,\mathrm{Im}\,\alpha)$. En vertu de la formule de transitivité

$$D_K = N_{K'/Q}(D_{K/K'})D_{K'}^{[K:K']} = N_{K''/Q}(D_{K/K''})D_{K''}^{[K:K'']},$$

(13) implique (17), d'où l'on obtient immédiatement (18).

Bibliographie

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

[2] A. Baker—H. M. Stark, On a fundamental inequality in number theory, *Ann. of Math.*, **94** (1971), 355—369.

[3] E. F. Beckenbach—R. Bellman, Inequalities, *Berlin*, 1961.

[4] S. I. Borewicz—I. R. Šafarevič, Zahlentheorie, *Basel* und *Stuttgart*, 1966.

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

[6] A. Brauer—R. Brauer, Über Irreduzibilitätskriterien von I. Schur und G. Pólya, *Math. Z.* **40** (1936), 242—265.

[7] J. Coates, An effective p-adique analogue of a theoreme of Thue, *Acta Arith.* **15** (1969), 279—305.

[8] H. Davenport—K. F. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 160—167.

[9] P. Dénes, Über Einheiten von algebraischen Zahlkörpern, *Monatsh. Math.* **55** (1951), 161—163.

[10] M. Eichler, Einführung in die Theorie der algebraischen Zahlen und Funktionen, *Basel* und *Stuttgart*, 1963.

[11] Н. И. Фельдман, Эффективное степенное усиление теоремы Лиувилля, *Изв. АН. СССР, Сер. мат.*, **35** (1971), 973—990.

[12] H. Furuya, On the divisibility by 2 of the relative class numbers of imaginary number fields, *Tôhoku Math. J.* **23** (1971), 207—218.

[13] L. J. Goldstein, A Generalization of Stark's Theorem, *J. Number Theory*, **3** (1971), 323—346.

[14] L. J. Goldstein, Relativ imaginary quadratic fields of low class number, *Bull. Amer. Math. Soc.* **78** (1972), 80—81.

[15] K. Győry—L. Lovász, Representation of integers by norm-forms, II., *Publ. Math. (Debrecen)*, **17** (1970), 173—181.

[16] K. Győry, Sur l'irréductibilité d'une classe des polynômes, I., *Publ. Math. (Debrecen)*, 18 (1971), 289—307.

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

[18] K. Győry, Investigations diophantiennes dans la théorie des polynômes irréductibles, Kandidátusi disszertáció (Thèse), *Debrecen*, 1972, p. 1—172, *(en hongrois)*.

[19] K. Győry, Représentation des nombres par des formes binaires, *en préparation*.

[20] E. Hecke, Bestimmung der Klassenzahl einer neuen Reihe von algebraischen Zahlkörpern, *Nachr. Akad. Wiss. Göttingen, Math.-Phys. Klasse* (1921), 1—23. (Voir encore Mathematische Werke de E. Hecke, *Göttingen*, 1951.)

[21] D. Hilbert, Gesammelte Abhandlungen, I, *Berlin*, 1970.

[22] S. Lang, Diophantine geometry, *Int. Tracts*, No 11, *New York—London*, 1962.

[23] D. J. Lewis—K. Mahler, On the representation of integers by binary forms, *Acta Arith.* **6** (1961), 333—363.

[24] M. Marcus—L. Lopez, Inequalities for symmetric functions and Hermitian matrices, *Canad. J. Math.* **9** (1957), 305—312.

[25] T. Nagell, Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante, *Math. Z.*, **28** (1928), 10—29.

[26] T. Nagell, Les points exceptionnels rationnels sur certaines cubiques du premier genre, *Acta Arith.*, **5** (1959), 333—357.

[27] T. Nagell, Sur une propriété des unités d'un corps algébrique, *Ark. Mat.* **5** (1964), 343—356.

[28] T. Nagell, Sur les représentations de l'unité par les formes binaires biquadratiques du premier rang, *Ark. Mat.* **5** (1965), 477—521.

[29] T. Nagell, Sur les unités dans les corps biquadratiques primitifs du premier rang, *Ark. Mat.* **7** (1968), 359—394.

[30] T. Nagell, Quelques problèmes relatifs aux unités algébriques, *Ark. Mat.* **8** (1970), 115—127.

[31] T. Nagell, Sur un type particulier d'unités algébriques, *Ark. Mat.* **8** (1970), 163—184.

[32] R. Remak, Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers, *Compositio Math.* **10** (1952), 245—285.

[33] R. Remak, Über algebraische Zahlkörper mit schwachem Einheitsdefekt, *Compositio Math.* **12** (1954), 35—80.

[34] A. SCHINZEL, Reducibility of polynomials in several variables, *Bull. Acad. Polon. Sci., Ser. Sci. Math. Astr. Phys.*, **11** (1963), 633—638.
[35] A. SCHINZEL, An improvement of Runge's theorem on diophantine equations, *Commentarii Pontif. Acad. Sci.*, **2**, No 20 (1968), 1—9.
[36] W. M. SCHMIDT, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* **191** (1971), 1—20.
[37] W. M. SCHMIDT, Approximation to algebraic numbers, *Enseignement Math.* **17** (1971), 188—253.
[38] I. SERES, Lösung und Verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome *Acta Math. Acad. Sci. Hung.* **7** (1956), 151—157.
[39] I. SERES, Über die Irreduzibilität gewisser Polynome, *Acta Arith.* **8** (1963), 321—341.
[40] I. SERES, Irreducibility of polynomials, *J. Algebra*, **2** (1965), 283—286.
[41] G. SHIMURA—Y. TANIYAMA, Complex multiplication of abelian varieties and its applications to number theory, *Math. Soc. Japan*, 1961.
[42] G. SHIMURA, Automorphic Functions and Number Theory, *Lecture Notes*, No 54, *Berlin*, 1968.
[43] C. L. SIEGEL, Approximation algebraischen Zahlen, *Math. Z.* **10** (1921), 173—213.
[44] C. L. SIEGEL, The trace of totally positive and real algebraic integers, *Ann. of Math.* **46** (1945), 302—312.
[45] C. J. SMYTH, Closed sets of algebraic numbers in complete fields, *Mathematika* **17** (1970), 199—205.
[46] В. Г. Спринджук, Новое применение p-адического анализа к представлениям чисел бинарными формами, *Изв. АН СССР, Сер. мат.*, **34** (1970), 1038—1063.
[47] J. E. SUNLEY, On the class numbers of totally imaginary quadratic extensions of totally real fields, *Bull. Amer. Math. Soc.* **78** (1972), 74—76.
[48] В. А. Тартаковский, Равномерная оценка количества представлений единицы бинарной формой степени $n \geqq 3$, *Докл. Акад. Наук СССР* **193** (1970), 764.
[49] K. UCHIDA, Class numbers of imaginary abelian number fields, I, *Tôhoku Math. J.* **23** (1971), 97—104.

(Reçu le 18 juin 1972.)