Sur l'irréductibilité d'une classe des polynômes II.

Par K. GYŐRY (Debrecen)

1. Introduction

Après que I. SCHUR [22] avait soulevé le problème, de nombreux auteurs, parmi eux G. PÓLYA [17], A. BRAUER [3], L. DORWART et O. ORE [7], L. WEISNER [30], T. TATUZAWA [27] et A. BRAUER et G. EHRLICH [6] ont obtenu des résultats assurant l'irréductibilité sur Q de tels polynômes $F(x)\in Z[x]$ qui prennent des valeurs petites ou des valeurs ayant peu de diviseurs en beaucoup de $x\in Z$. Ces résultats amènent en premier lieu l'irréductibilité des polynômes de forme $g(f(x))$, où $g(x)\in Z[x]$ est linéaire et $f(x)\in Z[x]$ a $l>\frac{\deg f}{2}$ racines différentes en Z. Si pour les valeurs considérées $x\in Z$ nous ne posons aucune restriction dépendant de la distribution des racines des polynômes $F(x)\in Z[x]$ (tels résultats se trouvent par ex. dans [18] et [13]), alors, en général, d'un nombre $\leq\frac{\deg F}{2}$ des valeurs $F(x)$ (c'est-à-dire x) on ne peut déduire l'irréductibilité du polynôme $F(x)$ que dans le cas où $F(x)=g(f(x))$, $g(x)\in Z[x]$ étant un polynôme irréductible de degré >1 et $f(x)\in Z(x]$ ayant plus de $\frac{\deg f}{2}$ racines différentes en Z. Cette question a été soulevée pour les polynômes $f(x)$ ayant des racines différentes en Z (cas $l=\deg f$) et pour les polynômes $g(x)=x^{2^n}+1$ par I. Schur (voir par ex. [4]) et en général, pour des polynômes irréductibles arbitraires $g(x)\in Z[x]$, par A. BRAUER, R. BRAUER et H. HOPF [5].

Appelons les polynômes $f(x)$ et $f^*(x)\in Z[x]$ équivalents si l'on a $f^*(x)=f(x+a)$ pour un $a\in Z$. Du point de vue de l'irréductibilité il suffit évidemment de considérer des polynômes $f(x)$ non équivalents deux à deux.

Après les résultats moins généraux de H. ILLE [12], de U. WEGNER [29] et de DORWART et O. ORE [7], pour des polynômes $g(x)$ de degré $\leqq 4$ A. BRAUER, R. BRAUER et H. HOPF [5] ont même résolu le problème mentionné. Notamment, ils ont démontré l'irréductibilité de $g(f(x))$ pour chaque $g(x)$ fixé de degré $\leqq 4$ et pour tout $f(x)$ du type précédent, sauf pour un nombre fini de $f(x)$ non équivalents deux à deux qui peuvent être effectivement déterminés en subordination de $g(x)$. (Nous remarquons qu'on ne peut pas obtenir des théorèmes d'irréductibilité analogues concernant les polynômes de forme $g(f(x))$ en cas de polynômes $f(x)$, $g(x)$ choisis indépendamment l'un de l'autre.) Les méthodes, utilisées antérieurement, ne peuvent pas être appliquées dans le cas des polynômes $g(x)$ de degré >4, c'est-à-dire dans

le domaine Z le problème ne peut pas être étudié. De ce fait les recherches de cette direction sont arrivées au point mort pour quelques ans.

L'un des théorèmes de CAPELLI (voir [28] ou [19]) permet de réduire le problème de la réductibilité de $g(f(x))$ sur Q à la question de la réductibilité de $f(x)-\alpha$ sur $Q(\alpha)$ (où α désigne une des racines de $g(x)$) et, par conséquent, il permet de diminuer le quotient du degré par le nombre des valeurs entières x convenables (c'est-à-dire le quotient du degré par le nombre des racines entières de $f(x)$). Mais, dans ce cas deux problèmes difficiles se posent. Le premier de ces problèmes est posé par l'existence d'une infinité d'unités de $Q(\alpha)$. En utilisant le théorème de Kronecker concernant les unités des corps cyclotomiques, dans le cas des corps cyclotomiques I. SERES [23], [24], [25] a surmonté cette difficulté. I. Seres a élaboré une méthode et, entre autres, il a démontré la conjecture de I. Schur dans une forme plus générale [23], [24]. Notamment, I. Seres a prouvé que, pour un polynôme cyclotomique $g(x)$ et pour un polynôme $f(x)$ ayant seulement des racines entières rationnelles différentes, $g(f(x))$ est réductible sur Q si et seulement si l'on a $g(x) = x^4-x^2+1$ et $f(x) = x^3-x$. D'autre part, il a résolu [25] le problème de Brauer—Hopf pour tout $g(x)$ dont les racines sont des unités non réelles d'un corps cyclotomique.

L'autre difficulté est le fait que dans $Q(\alpha)$ la valeur absolue de la norme n'est pas une valuation dans $Q(\alpha)$. C'est pourquoi l'irréductibilité des polynômes de forme $g(f(x))$ sur Q ne peut pas être étudiée dans le cas général où $|g(0)| \geqq 1$.

R. REMAK [20] a montré que le théorème mentionné de Kronecker peut être étendu aussi aux unités des corps totalement réels et des extensions quadratiques totalement imaginaires des corps totalement réels (de plus, même pour certaines S-unités de ces corps, voir [9]). Dans [10] nous avons appelé ces corps kroneckeriens ou simplement de *K-corps.**) Dans [9] nous avons démontré (voir aussi [10]) qu'un corps algébrique est un K-corps si et seulement si dans le corps des nombres complexes il a une extension, galoisienne sur Q, dont le sous-corps réel maximal est également galoisien sur Q (voir, par ex. les corps abéliens).

Donc, le premier problème est résolu aussi pour de K-corps non-réels. De plus, en appliquant l'inégalité de norme (voir le lemme 2) que nous avons trouvé en collaboration avec L. LOVÁSZ dans [8] (où nous l'avons employée pour des équations diophantiennes), dans les K-corps non-réels on peut surmonter aussi la seconde difficulté. Ainsi, dans [10], nous avons pu obtenir des résultats du type de Schur aussi sur des K-corps non-réels et, en même temps, nous avons pu généraliser les résultats de I. Seres [23], [24], [25], obtenus sur des corps cyclotomiques. D'autre part, en considérant tous les polynômes irréductibles $g(x)$ ayant des corps de décomposition kroneckeriens non-réels (de tels polynômes sont, par ex., les polynômes cyclotomiques et les polynômes $x^2+ax+b \in Z[x]$ de discriminant négatif), nous avons pu traiter le problème de Brauer—Hopf dans le cas beaucoup plus général où les racines des polynômes $f(x)$ sont non seulement des entiers rationnels mais aussi des nombres réels différents.

Dans le cas classique (où les racines des $f(x)$ sont des nombres différents de Z) nous avons généralisé [10] les théorèmes de I. Seres [23], [24], [25] pour des polynômes $g(x)$ du type précédent et nous avons résolu le problème de Brauer—Hopf pour ces $g(x)$. De plus, également dans [10], nous avons déterminé tous les poly-

*) Le Professeur A. SCHINZEL m'a bien voulu informer du travail cité de R. REMAK le 31 octobre 1971 (voir [10], p. 290).

nômes exceptionnels $f(x)$, $g(x)$ pour lesquels $g(0)=1$, $f(x)=\prod_{i=1}^{m}(x-a_i)$ avec des entiers différents a_i et $g(f(x))$ est réductible sur Q, en généralisant le résultat cité de I. Seres [24] concernant le problème de I. Schur. Les démonstrations se basent sur le rapport, trouvé dans [10], qui existe entre le nombre des facteurs irréductibles de $g(f(x))$ et le nombre de sommets d'un sous-graphe connexe maximal d'un graphe $G(f,g)$ convenablement formé des racines de $f(x)$.

Dans ce travail nous traitons le problème de Brauer—Hopf dans le cas plus général mentionné où les $g(x)$ sont des polynômes du type précédent et où les racines des $f(x)$ sont des nombres réels différents. A l'aide des exemples nous montrerons qu'on ne peut obtenir des théorèmes d'irréductibilité généraux concernant les polynômes $g(f(x))$ que dans le cas où le degré de $f(x)$ est assez grand par rapport au degré de son corps de décomposition ou bien où ce quotient est relativement petit, mais le degré de $f(x)$ est un nombre premier. Dans notre travail nous obtenons des théorèmes d'irréductibilité généraux dans tous les deux cas possibles, et ainsi, pour les polynômes $g(x)$ du type précédent, nous donnons au fait la solution du problème de Brauer—Hopf dans le cas plus général mentionné. En même temps nous montrons que nos théorèmes ne peuvent pas être étendus en général pour des polynômes $f(x)$, $g(x)$ d'autre type.

Dans le cas général la difficulté des problèmes augmente essentiellemenet par rapport à celle des problèmes du cas classique. Au cours des démonstrations nous employons nos résultats mentionnés concernant les K-corps et nous résolvons plusieurs problèmes diophantiens. D'une part nous appliquons les résultats de A. Baker [1] et de A. Baker et J. Coates [2], d'autre part nous utilisons notre théorème concernant les polynômes $f(x)\in Z[x]$ de discriminant donné [11] par lequel nous avons donnè une démonstration constructive d'un problème de T. Nagell [15].

2. Théorèmes

Soient $f(x)$, $g(x)\in Z[x]$ des polynômes normés. Pour que $g(f(x))$ soit irréductible sur Q il faut que $g(x)$ soit irréductible sur Q. De plus, en cas de polynômes de forme $g(f(x))$ on ne peut obtenir des théorèmes d'irréductibilité généraux que dans le cas où il y a quelque rapport entre $f(x)$ et $g(x)$ (voir la Proposition 1). Quant aux polynômes $g(x)$, dans la suite nous verrons que dans ce rapport seulement le paramètre $g^{1/n}(0)$ ($n=\deg g$) joue un rôle. C'est pourquoi, $G\geqq 1$ *étant une constante arbitraire, nous désignons par* $P(G)$ *l'ensemble des polynômes normés* $g(x)\in Z[x]$ *irréductibles sur* Q *pour lesquels* $g^{1/n}(0)\leqq G$ ($n=\deg g$) *et dont le corps de décomposition est un* K*-corps non réel.* Par exemple, tous les polynômes cyclotomiques appartiennent à $P(G)$ pour tout $G\geqq 1$. Considérons de plus tous les polynômes normés $f(x)\in Z[x]$ ayant des racines réelles différentes. Comme nous avons déjà mentionné, pour que $g(f(x))$ soit irréductible sur Q, il faut en général que $\deg f/n_k$ soit assez grand ou bien (lorsque $\deg f/n_k$ est rélativement petit) $\deg f$ soit un nombre premier, où n_k est le degré du corps de décomposition K de $f(x)$ (voir les Propositions 2, 5 et 6).

D'abord, considérons le premier cas. Nous observons préalablement que si $f(x)\in Z[x]$ est un polynôme normé de la forme

$$f(x)=f_1(x)f_2(x),\quad f_2(x)-f_1(x)=1 \tag{2.1}$$

(où $f_1(x), f_2(x) \in Z[x]$) et si pour uner acine α d'un polynôme normé $g(x) \in Z[x]$ on a

$$\alpha = \varphi(\varphi - 1), \tag{2. 2}$$

φ étant entier dans $Q(\alpha)$, alors d'après le lemme 8 $g(f(x))$ est réductible sur Q.

Théorème 1a. *Soit K un corps algébrique réel de degré n_k et de discriminant D_k et galoisien par rapport à Q. Soit de plus $G \geqq 1$ une constante arbitraire. Il existe une constante $c = c(n_k, D_k, G)$ calculable explicitement et dépendant seulement de n_k, D_k et G, telle que si $g(x) \in P(G)$ et si $f(x) \in Z[x]$ est un polynôme normé de degré $> c$ avec des racines différentes de K, alors $g(f(x))$ est irréductible sur Q, sauf dans le cas où une des racines de $g(x)$ satisfait à (2. 2), de plus $f(x)$ est un polynôme de forme (2. 1) et de degré pair, lorsque $g(f(x))$ se décompose en deux facteurs irréductible de degré égal sur Q.*

Donc, pour des polynômes normés $f(x)$ de discriminant $\neq 0$, ayant le même corps de décomposition réel, et pour tout $g(x) \in P(G)$, $g(f(x))$ est irréductible ou le produit de deux facteurs irréductibles de degré égal (cas exceptionnel), en supposant que $\deg f$ est assez grand par rapport aux paramètres du théorème*). Quant au cas exceptionnel, c'est-à-dire à l'existence des polynômes $f(x)$, $g(x)$ à propriété (2. 1) et (2. 2), on peut constater ce qui suit: D'une part, si $n_0 > 1$ est fixé, il n'y a qu'un nombre fini de polynômes $g(x) \in P(G)$ de degré $\leqq n_0$ dont les racines satisfont à (2. 2) et ces polynômes peuvent être effectivement déterminés (voir la Proposition 4). D'autre part, il n'existe probablement aucun polynôme $f(x)$ de la forme (2. 1) et de degré grand par rapport à n_k. Mais la solution de cette question conduit au problème diophantien „idéal" de Tarry—Escott sur les corps algébriques K (voir la Proposition 3) qui n'est pas résolu jusqu'à présent.

Pour des corps quadratiques réels K on peut démontrer une proposition plus précise. D'abord il nous faut remarquer qu'il y a des polynômes $g(x) \in P(G)$ tels que $g(f(x))$ soit réductible sur Q pour une infinité de $f(x) \in Z[x]$ du quatrième degré ayant des racines différentes de K. Si $G \geqq 1$ est fixé, il y a une infinité de tels $g(x)$, mais pour tout $n_0 > 1$ il n'y a qu'un nombre fini de $g(x)$ de degré $\leqq n_0$ et ces $g(x)$ peuvent être déterminés. Enfin, en fixant un tel $g(x)$, on peut déterminer tous les $f(x)$ du type précédent par des formules récurrentes pour lesquels $g(f(x))$ est donc réductible sur Q (voir les Proposition 4 et 5).

Désignons par $\| f \|$ le maximum des valeurs absolues des coefficients d'un polynôme $f(x) \in Z[x]$.

Théorème 1b. *Soit K un corps quadratique réel de discriminant D_k et soit $G \geqq 1$ une constante. Il existe des constantes $c_1 = c_1(D_k, G)$, $c_2 = c_2(D_k, G)$ calculables explicitement et dépendant seulement de D_k et de G telles que si $g(x) \in P(G)$ et si $f(x) \in Z[x]$ est un polynôme normé avec des racines différentes de K pour lesquels $g(f(x))$ est réductible sur Q, alors, sauf pour les exceptions f, g ci-dessus, $\deg f \leqq c_1$ et $\| f^* \| \leqq c_2$ pour un f^* équivalent à f.*

Donc, sans compter les polynômes exceptionnels $f(x) \in Z[x]$ de degré 4, il n'existe qu'un nombre fini de polynômes normés $f(x) \in Z[x]$ non équivalents deux à deux avec des racines différentes de K pour lesquels $g(f(x))$ peut être réductible sur Q avec un $g(x) \in P(G)$, et on peut, par un nombre fini d'opérations, déterminer

*) Addition. Récemment nous avons calculé explicitement les constantes qui se trouvent dans nos théorèmes.

un tel système des polynômes $f(x)$ qui ne dépend que de G. Ainsi nous donnons la solution du problème de Brauer—Hopf dans une forme plus générale.

Si $K=Q$ est le corps des nombres rationnels, on peut obtenir un résultat encore plus précis.

Théorème 1c. *Soit $G\geqq 1$ une constante. Si $g(x)\in P(G)$ et si $f(x)=\prod_{i=1}^{m}(x-a_i)$ avec des entiers rationnels différents a_i, alors $g(f(x))$ est irréductible sur Q, sauf dans certains cas où $\max_{i,k}|a_i-a_k|\leqq 4G-1$, c'est-à-dire $m\leqq 4G$.*

Notre théorème donne une amélioration du théorème 5 de [10], une généralisation des résultats de I. Seres [23], [25] et, en même temps, la solution du problème original de Brauer—Hopf pour tout $g(x)\in P(G)$, $G\geqq 1$ étant une constante arbitraire. Il en résulte qu'il n'existe qu'un nombre fini de $f(x)$, non équivalents deux à deux, avec des racines différentes de Z pour lesquels $g(f(x))$ peut être réductible avec un $g(x)\in P(G)$, et on peut déterminer effectivement un tel système des $f(x)$ en subordination seulement de G. Enfin, nous remarquons que le théorème 1c ne peut pas être amélioré en général (voir les polynômes exceptionnels $f(x)$ du théorème 6 dans [10]).

Désormais considérons le second cas.

Théorème 2a. *Soit $G\geqq 1$ une constante et soit p un nombre premier. Si $g(x)\in P(G)$ et si $f(x)\in Z[x]$ est un polynôme normé de degré p, irréductible sur Q, et ayant des racines réelles, tel que $g(f(x))$ est réductible sur Q, alors $\|f^*\|\leqq c_1(G,p)$ pour un f^* équivalent à f, $c_1(G,p)$ étant une constante calculable explicitement qui ne dépend que de G et p.*

Dans le cas $p\leqq 3$ l'irréductibilité de $f(x)$ n'est pas nécessaire, c'est-à-dire le théorème suivant est vrai:

Théorème 2 b. *Soit $G\geqq 1$ une constante. Si $g(x)\in P(G)$ et si $f(x)\in Z[x]$ est un polynôme normé de degré $\leqq 3$, avec des racines réelles différentes, tel que $g(f(x))$ est réductible sur Q, alors $\|f^*\|\leqq c_2(G)$ pour un f^* équivalent à f, $c_2(G)$ étant une constante calculable explicitement qui ne dépend que de G.*

Par conséquent, p étant un nombre premier fixé, il n'existe qu'un nombre fini de polynômes normés $f(x)\in Z[x]$ de degré p non équivalents deux à deux et ayant la propriété donnée, pour lesquels $g(f(x))$ peut être réductible sur Q avec un $g(x)\in P(G)$, et on peut, par un nombre fini d'opérations, déterminer un tel système des polynômes $f(x)$ indépendamment du choix des $g(x)$. De plus, en désignant par $D(f)$ le discriminant d'un $f(x)$ considéré, la seule inégalité

$$D(f)>(2G)^{p(p-1)} \tag{2.3}$$

entraîne déjà l'irréductibilité de $g(f(x))$ pour tout $g(x)\in P(G)$ (voir les lemmes 18 et 19).

Nous remarquons que le théorème 2a n'est pas valable pour des degrés composés p (voir la Proposition 6). De plus, les théorèmes 2a et 2b ne peuvent pas être étendus en général pour des polynômes f, g d'autre type (voir la Proposition 7).

Corollaire. Si $f(x)$, $g(x)\in Z[x]$ sont des polynômes normés tels que l'irréductibilité de $g(f(x))$ s'obtient d'un de nos théorèmes précédents, alors le nombre des facteurs irréductibles de $g(f(x))$ sur un K-corps arbitraire est $\leqq \deg g$.

Si L est un K-corps contenant le corps de décomposition de $g(x)$, alors l'estimation, donnée pour le nombre des facteurs irréductibles sur L, ne peut pas être amé-

liorée. En effet, en supposant que $g(x) = (x-\alpha_1)...(x-\alpha_n)$, on a $g(f(x)) = (f(x)-\alpha_1)...(f(x)-\alpha_n)$ sur L.

Comme nous l'avons mentionné déjà dans l'introduction, tous nos théorèmes se basent sur le lemme 9. Notamment, soit $G \geqq 1$ une constante, soit $f(x) = (x-\alpha_1)... ...(x-\alpha_n) \in Z[x]$ avec des racines réelles différentes, prenons le corps $L = Q(\alpha_1, ..., \alpha_n)$ et désignons par $\mathscr{G}(f, G)$ le graphe des couples (α_i, α_k), formées des racines de $f(x)$, et satisfaisant à

$$|N_{L/Q}(\alpha_i - \alpha_k)| > (2G)^{[L:Q]}. \tag{2.4}$$

Si le nombre des sommets d'un sous-graphe connexe maximal de $\mathscr{G}(f, G)$ est s, alors, pour tout $g(x) \in P(G)$, le degré des facteurs irréductibles de $g(f(x))$ sur Q est $\geqq s \deg g$, et par conséquent le nombre de ses diviseurs irréductibles est $\leqq \dfrac{\deg f}{s}$.

Cette proposition ne peut pas être étendue pour des polynômes f, g d'autre type même dans le cas non plus où nous remplaçons le coté droit de (2. 4) par une fonction arbitraire de G et de $[L:Q]$ (voir [10], p. 295). De plus, les estimations obtenues ne peuvent pas être améliorées en général (voir la Proposition 2).

Dans le cas classique on peut aisément étudier le graphe $\mathscr{G}(f, G)$. Mais, dans le cas général où les racines des $f(x)$ sont réelles (et non nécessairement entières rationnelles), la recherche des $f(x)$ tels que $\mathscr{G}(f, G)$ ne contienne aucun sous-graphe connexe ayant beaucoup de sommets (lorsque $g(f(x))$ peut être réductible pour un $g(x) \in P(G)$) conduit à de problèmes diophantiens très compliqués. Au cours de la solution de ces problèmes nous utiliserons, entre autres, que si $D > 1$ est une constante, il n'y a qu'un nombre fini de polynômes normés $f(x) \in Z[x]$ non équivalents deux à deux tels que $0 < |D(f)| \leqq D$, et on peut, par un nombre fini d'opérations, déterminer un tel système des polynômes $f(x)$ (voir [11] et le lemme 20).

3. Polynômes extrêmes et exceptionnels

Dans ce point nous démontrerons à l'aide d'exemples que nos théorèmes ne peuvent pas être améliorés en général et leurs conditions sont nécessaires.

Proposition 1. *Aucun de nos théorèmes ne reste vrai s'il n'y a aucune relation entre les polynômes considérés $f(x)$ et $g(x)$, plus précisément leurs constantes ne peuvent pas être remplaçées par des constantes indépendant de G.*

Démonstration. Quant aux théorèmes 1a, 1b et 1c, nous démontrons la proposition à la fois. Soit K un corps galoisien réel de degré n_k et de discriminant D_k. Alors les constantes, qui se trouvent dans les théorèmes, ne peuvent être remplaçées par aucune constante dépendant seulement de n_k et D_k. En effet, soit $f(x) \in Z[x]$ un polynôme normé ayant un grand degré impair par rapport à n_k et D_k et avec des racines différentes de K. Si $f(i)$ n'est pas réel, alors en choisissant $g(x) = (x-f(i))(x-\overline{f(i)}) \in Z[x]$, d'après $x-i \mid f(x)-f(i)$ et d'après le lemme 8 $g(f(x))$ est réductible sur Q.

Ensuite considérons les théorèmes 2a et 2b. Soit p un nombre premier. Alors les constantes, qui se trouvent dans ces théorèmes, ne peuvent pas être remplaçées par aucune constante dépendant seulement de p. En effet, prenons un polynôme

normé $f(x)\in Z[x]$ de degré p (dans le cas $p\geqq 5$ soit $f(x)$ irréductible), avec des racines réelles différentes, tel que $D(f)$ soit assez grand par rapport à p et $f(i)$ soit non réel. Il y a une infinité de tels polynômes $f(x)$ non équivalents deux à deux. De plus, pour tout f^* équivalent à un tel f, $\|f^*\|$ est également grand par rapport à p. Si maintenant $g(x)=(x-f(i))(x-f(i))\in Z[x]$ pour un des $f(x)$ précédents, le polynôme $g(f(x))$ est réductible sur Q, c'est-à-dire dans ce cas les théorèmes 2a et 2b ne sont pas déjà vrais.

Proposition 2. *Soient $m\geqq 2$, $r\geqq 2$ et s des nombres naturels tels que $m=r\cdot s$. Il existe des polynômes normés $f(x)$, $g(x)\in Z[x]$ satisfaisant aux conditions suivantes:*

(i) $g(x)\in P(G)$ *où* $G=\prod_{j=1}^{[r/2]}(1+j^2)$;

(ii) *le degré de $f(x)$ est m, ses racines sont réelles et différentes, le degré de son corps de décomposition K est $n_k\geqq s$ et, en supposant que $s\geqq 2$, $D(f)$ est arbitrairement grand par rapport à m (et par conséquent aussi par rapport à G);*

(iii) *le graphe $\mathcal{G}(f,G)$, formé à la base de* (2. 4), *se décompose en m/s graphes complets ayant s sommets et disjoints deux à deux;*

(iv) *$g(f(x))$ a un facteur irréductible de degré s* deg g *sur Q.*

Remarque 1. Il en résulte que pour des nombres naturels arbitraires $r>1$ et $r|m$ $(m>r)$ il y a une infinité de polynômes normés $f(x)$ de degré m ayant des racines réelles différentes, et non équivalents deux à deux, pour lesquels $m/n_k\leqq r$ (c'est-à-dire m/n_k est relativement petit par rapport à r et ainsi aussi par rapport à G) et les $g(f(x))$ sont tous réductibles sur Q, où $g(x)\in P(G)$ est un polynôme convenablement choisi (et G est relativement petit par rapport à r).

Remarque 2. De notre proposition on obtient que, dans le lemme 9, l'estimation, obtenue pour le degré des facteurs irréductibles des $g(f(x))$, ne peut pas être en général améliorée (voir encore les théorèmes 1′ et 2′ dans [10]).

Démonstration. Dans le cas $r=2t+1$ soit $h(z)=(z-t)\ldots(z-1)\cdot z\cdot(z+1)\ldots(z+t)$ et dans le cas $r=2t$ soit $h(z)=(z-t)\ldots z\ldots(z+t-1)$, où $h(i)$ est un nombre entier primitif dans $Q(i)$. Soit $g(x)$ le polynôme minimal de $h(i)$. Alors deg $g=2$ et

$$g(0)=h(i)\overline{h(i)}=\begin{cases}[(1+t^2)\ldots(1+1^2)]^2, & \text{si } r=2t+1,\\ (1+t^2)\left[(1+(t-1)^2)\ldots(1+1^2)\right]^2, & \text{si } r=2t,\end{cases}$$

d'où $g^{\frac{1}{2}}(0)\leqq\prod_{j=1}^{[r/2]}(1+j^2)$, c'est-à-dire $g(x)\in P(G)$, où $G=\prod_{j=1}^{[r/2]}(1+j^2)$. Soit ensuite $f_0(x)=\prod_{j=1}^{s}(x-a_j)$, où les a_j sont des nombres entiers rationnels tels que $\min_{i,k\,(i\neq k)}|a_i-a_k|$ soit grand par rapport à m (en supposant que $s\geqq 2$). Dans ce cas $f(x)=h(f_0(x))$ est un polynôme normé de degré m dans $Z[x]$. De plus, d'après un théorème de L. Weisner [30] tous les diviseurs $f_l(x)=f_0(x)+l$ $(|l|\leqq t)$ de $f(x)$ sont irréductibles sur Q, par conséquent le degré du corps de décomposition de $f(x)$ est $\geqq s$. En outre les racines de chaque $f_l(x)$ sont des nombres réels différents (voir aussi, par ex., le travail [30] de L. Weisner). Enfin, les racines de $f(x)$ sont évidemment différentes deux à deux.

Vu que dans le cas $s \geqq 2$ les racines de $f_l(x) = f_0(x) + l$ sont arbitrairement distantes l'un de l'autre (voir également le théorème 1 de L. Weisner [30]), c'est pourquoi d'une part $D(f)$ est arbitrairement grand par rapport à m, d'autre part $\mathcal{G}(f_l, G)$ est complet pour tout l. De plus, $f_k(x) - f_l(x) \neq 0$ étant une petite constante par rapport à r et ainsi aussi par rapport à G, les graphes $\mathcal{G}(f_l, G)$, $\mathcal{G}(f_k, G)$ sont disjoints deux à deux. Enfin, d'après $z - i \mid h(z) - h(i)$ on a $f_0(x) - i \mid h(f_0(x)) - h(i) = f(x) - h(i)$ sur $Q(i)$ d'où, en conséquence du lemme 8, $g(f(x))$ a un diviseur irréductible de degré $s \deg g$ sur Q.

Proposition 3. *Supposons que les racines de* $f_1(x) = \prod_{i=1}^{m} (x - \alpha_i)$, $f_2(x) = \prod_{i=1}^{m} (x - \alpha_i') \in Z[x]$ *sont des nombres différents dans un corps algébrique* K *et supposons que* $f_1(x)$ *et* $f_2(x)$ *satisfont à* (2. 1), *c'est-à-dire on a*

$$f_2(x) - f_1(x) = 1.$$

Alors les racines de $f_1(x)$ *et* $f_2(x)$ *satisfont au système „idéal" d'équations diophantiennes de Tarry—Escott*

$$\alpha_1^k + \cdots + \alpha_m^k = \alpha_1'^k + \cdots + \alpha_m'^k \qquad (k = 1, \ldots, m-1). \tag{3. 1}$$

Démonstration. La proposition s'obtient immédiatement à l'aide des formules de Newton (voir [21], p. 139).

Remarque. Dans le cas $m > 10$ nous ne connaissons aucune solution non triviale de (3. 1) dans Z (voir aussi [21]). De plus, nous ne connaissons pas de solutions non triviales de (3. 1) dans le cas non plus où m est grand par rapport au degré de K. En même temps nous remarquons que, d'après les conditions supplémentaires, s'il y a une solution non triviale de (3. 1) en entiers de K, alors on en ne déduit pas nécessairement l'existence des polynômes $f_1(x)$, $f_2(x)$ de la forme (2. 1).

Les exemples du théorème 6 dans [10] (cas $m = 2$) montrent que, pour tout $G \geqq 1$, il y a une infinité de polynômes $g(x) \in P(G)$ dont les racines satisfont à (2. 2). Mais, $n_0 > 1$ étant un nombre fixé, le nombre des polynômes $g(x) \in P(G)$ de degré $\leqq n_0$ est déjà fini. Pour que nous puissons utiliser cette proposition aussi dans le cas du théorème 1b, nous la démontrons dans une forme plus générale.

Proposition 4. *Soit* $G \geqq 1$ *une constante et soient* $n_0 > 1$, $t \neq 0$ *des nombres entiers rationnels. Il n'existe qu'un nombre fini de polynômes* $g(x) \in P(G)$ *de degré* $\leqq n_0$ *tels que pour une racine* α *de* $g(x)$

$$\alpha = \varphi(\varphi - t) \tag{3. 2}$$

ait une solution φ *en entiers de* $Q(\alpha)$ *et ces* $g(x)$ *peuvent être déterminés par un nombre fini d'opérations.*

Remarque. Donc, si $n_0 > 1$ est fixé, dans le théorème 1a il n'y a qu'un nombre fini de polynômes $g(x) \in P(G)$ de degré $\leqq n_0$ pour lesquels $g(f(x))$ peut être réductible avec un polynôme $f(x)$ exceptionnel de forme (2. 1) (s'il en existe).

Démonstration. D'après $\deg g = n \leqq n_0$ et $g^{1/n}(0) \leqq G$ on a $g(0) \leqq G^{n_0} = g_0$. Ainsi, en introduisant la notation $\chi = \varphi - t$, il suffit de déterminer toutes les solutions de l'équation $\varphi - \chi = t$ en entiers non réels kroneckeriens de degré $\leqq n_0$ et de norme

$\leqq g_0$. Soit φ, χ une telle solution. Avec les notations $\bar{\varphi}/\varphi=\varrho$, $\bar{\chi}/\chi=\sigma$ $(\varrho, \sigma \in Q(\varphi))$ de l'équation $\varphi-\chi=t$ et de son conjugué complexe on obtient $\varphi=\frac{t(1-\sigma)}{\varrho-\sigma}$, $\chi=\frac{t(1-\varrho)}{\varrho-\sigma}$. Ensuite désignons par $\varrho=\varrho^{(1)}, \ldots, \varrho^{(n')}$, $(n' \leqq n_0)$ les conjugués différents de ϱ et soit $h(x)=\prod_{i=1}^{n'}(x-\varrho^{(i)}) \in Q[x]$. D'après le théorème du point 2 de [10] le corps normal K de $Q(\varphi)$ sur Q dans le corps complexe est un K-corps et, par conséquent, $\varrho^{(i)}=(\bar{\varphi}/\varphi)^{(i)}=\overline{\varphi^{(i)}}/\varphi^{(i)}$ pour tout i, d'où $|\varrho^{(i)}|=1$. Il en résulte que le maximum des valeurs absolues des coefficients de $h(x)$ est $\leqq c_1(n') \leqq c_1(n_0)$, où c_1 est une constante calculable explicitement. Le produit de $h(x)$ par $N_{K/Q}(\varphi) \leqq g_0^{n_0!}$ est un polynôme à coefficients entiers algébriques et ainsi il appartient à $Z[x]$. Pour la hauteur de ϱ il en résulte $H(\varrho) \leqq c_2(n_0, g_0)$ et de manière analogue pour $H(\sigma)$. On en déduit $H(\varphi)$, $H(\chi) \leqq c_3(n_0, g_0, t)$ avec une constante c_3 calculable explicitement (voir la remarque devant le lemme 15). Ainsi on peut déterminer le polynôme minimal de tous ces φ et en même temps aussi celui des $\varphi(\varphi-t)$. Si le degré de $\varphi(\varphi-t)$ et de φ (c'est-à-dire le degré de leurs polynômes minimaux) est égal, alors le polynôme minimal $g(x)$ du nombre $\alpha=\varphi(\varphi-t)$ satisfait aux conditions de la proposition.

Ensuite prenons les polynômes exceptionnels du théorème 1b. Soit K un corps quadratique réel de discriminant D_k et soit $t \in Z$ $(t \neq 0)$. Soient $f_1(x)$ et $f_2(x) \in Z[x]$ des polynômes normés quadratiques avec des racines différentes de K tels que $f_1(x)$ soit irréductible, $f_2(x)$ soit réductible sur Q et on ait

$$f_1(x)-f_2(x)=t. \tag{3.3}$$

Alors on peut écrire $f_1(x)=(x-\alpha^{(1)})(x-\alpha^{(2)})$, $f_2(x)=(x-a_1)(x-a_2)$ avec des $a_1, a_2 \in Z$. De plus, 1, $\frac{\sqrt{D_k}}{2}$ $(D_k \equiv 0 \pmod 4)$ ou 1, $\frac{1+\sqrt{D_k}}{2}$ $(D_k \equiv 1 \pmod 4)$ forme une base des entiers dans K, ainsi $\alpha^{(1)}=x_1+y_1\sqrt{D_k}$, $\alpha^{(2)}=x_1-y_1\sqrt{D_k}$, où dans le premier cas $x_1, 2y_1 \in Z$ et dans le second cas $x_1-y_1, 2y_1 \in Z$. Par conséquent, de (3.3) on obtient $a_1+a_2=2x_1$ et l'équation de Pell

$$(a_1-x_1)^2-D_k y_1^2=(x_1-a_2)^2-D_k y_1^2=t. \tag{3.4}$$

Inversement, si pour un D_k et pour un t (3.4) a une solution en a_1, a_2, x_1, y_1 du type précédent, alors les polynômes $f_1(x)$, $f_2(x)$ convenablement formés satisfont à (3.3) et ils possèdent les propriétés mentionnées ci-dessus. Dans ce cas (3.4) et (3.3) ont une infinité de solutions et ces solutions peuvent être représentées de manière connue par des formules récurrentes de nombre fini.

Proposition 5. *Soit $G \geqq 1$ une constante. Supposons que pour une α des racines d'un $g(x) \in P(G)$ et pour un $t \in Z$ $(0<|t| \leqq (2G^2)^2)$ $\alpha=\varphi(\varphi-t)$ possède une solution φ en entiers de $Q(\alpha)$. Soit de plus K un corps quadratique réel de discriminant D_k. S'il existe des polynômes $f_1(x)$, $f_2(x)$ du type précédent satisfaisant à (3.3), alors il y en a une infinité qui peuvent être représentés par des formules récurrentes et, pour tout $f(x)=f_1(x)f_2(x)$, formé d'une telle couple $f_1(x), f_2(x), g(f(x))$ est réductible sur Q.*

Remarque 1. Soient $G \geqq 1$ et $n_0 > 1$ des constantes fixées. En conséquence de la proposition 4 on peut déterminer tous les $g(x) \in P(G)$ de degré $\leqq n_0$ pour lesquels (3. 2) est résoluble pour un $t \in Z$ fixé, où $0 < |t| \leqq (2G^2)^2$. De plus, si $g(x)$ est un de ces polynômes et si K est un corps quadratique réel, on peut représenter tous les $f(x)$ satisfaisant aux conditions de la proposition 5.

Remarque 2. Comme nous l'avons mentionné dans le point 2, il y a une infinité de polynômes normés $f(x) \in Z[x]$ du quatrième degré, non équivalents deux à deux et ayant des racines différentes du même corps quadratique réel, pour lesquels $g(f(x))$ est réductible avec des $g(x)$ convenablement choisis.

Démonstration. Il suffit de démontrer que, pour les polynômes $f(x)$, $g(x)$ satisfaisant aux conditions de la proposition, $g(f(x))$ est réductible sur Q. D'après le lemme 8 il suffit donc de prouver que $f(x)-\alpha$ est réductible sur $Q(\alpha)$. Mais en conséquence de $f(x)=f_1(x)f_2(x)$, $f_1(x)-f_2(x) = t$ et de $\alpha = \varphi(\varphi - t)$ on a

$$f(x)-\alpha = f_1(x)f_2(x)-\varphi(\varphi-t) = f_2(x)[f_2(x)+t]-\varphi(\varphi-t) =$$

$$= [f_2(x)+\varphi][f_2(x)+t-\varphi]$$

et puisque $\varphi \in Q(\alpha)$, notre proposition est démontrée.

Proposition 6. *Soit $r=2$ ou 3 et soit $m>3$ un nombre naturel divisible par r. Soit de plus $G \geqq \sqrt{53}$. Il y a un $g(x) \in P(G)$ et il y a une infinité de polynômes normés $f(x) \in Z[x]$ de degré m avec des racines réelles différentes, non équivalents deux à deux et irréductibles sur Q, pour lesquels $g(f(x))$ est réductible sur Q.*

Remarque. Il en résulte que ni le théoreme 2a ni le lemme 18 ne peut pas être étendu en général pour des exposants composés.

DÉMONSTRATION. Soit $h(x) \in Z[x]$ un polynôme normé de degré r avec des racines réelles différentes et irréductible sur Q, tel que $h(i)$ soit non réel. Dans le cas $r=2$ prenons par ex. $h(x) = x^2+x-1$ et, dans le cas $r=3$, soit $h(x) = x^3-6x+2$. Soit $g(x) = (x-h(i))(x-\overline{h(i)}) \in Z[x]$. Alors $g^{1/2}(0) < \sqrt{53}$, par conséquent pour le G considéré on a $g(x) \in P(G)$. Ensuite soit $s = \dfrac{m}{r} \geqq 2$ et soit $s(x) = \prod_{j=1}^{s} (x-a_j)$ avec des entiers a_j distants l'un de l'autre. Alors, d'après le théorème cité de A. Brauer, R. Brauer et H. Hopf [5] $f(x)=h(s(x))$ est un polynôme de degré m irréductible sur Q et ses racines sont réelles. De plus, en conséquence de

$$s(x)-i \mid h(s(x))-h(i) = f(x)-h(i)$$

et du lemme 8, $g(f(x))$ a un facteur irréductible de degré s deg g sur Q. Enfin, vu que les a_j sont choisis arbitrairement, notre proposition est démontrée.

Proposition 7. *Les théorèmes 2a et 2b ne restent pas valables, si les racines des polynômes $f(x)$ ne sont pas tous réelles ou bien si le corps de décomposition des $g(x)$ n'est pas un K-corps non réel.*

DÉMONSTRATION. La démonstration se base sur le fait que pour les polynômes normés $h(x) \in Z[x]$ et $f(x) = x+g(x)h(x)$ on a $g(x) \mid g(f(x))$, c'est-à-dire $g(f(x))$ est réductible sur Q.

Soit d'abord $g(x) = x^2+1$ qui appartient à $P(G)$ pour tout $G \geqq 1$ et prenons les polynômes $f(x) = x+(x^2+1)^2(x-a)$ avec des $a \in Z$ tels que $2 \| a$. Il y a une infinité de tels polynômes $f(x)$ non équivalents deux à deux, qui sont irréductibles sur Q d'après le critère de Schönemann—Eisenstein et pour lesquels $g(f(x))$ est réductible sur Q.

D'autre part, soit p un nombre premier. Il y a une infinité de polynômes normés irréductibles $f^*(x) \in Z[x]$ de degré p, ayant des racines réelles et non équivalents deux à deux, tels que $f^*(0) = \mp 1$ (prenons, par exemple, les polynômes minimaux des unités différentes de ± 1 des corps abéliens de degré p). Pour chaque $f^*(x)$ prenons le polynôme $f(x) = f^*(x \pm 1)$ étant également irréductible sur Q et ayant des racines réelles. Ainsi, dans le premier cas $(f^*(0) = 1)$ on a $x-1 | f(x)-f(1) = f(x)-1$ et dans le second cas $(f^*(0) = -1)$ on a $x+1 = x-(-1) | f(x)-f(-1) = f(x)+1$. Donc, en choisissant $g(x) = x-1$ ou $x+1$ respectivement, nous obtenons que $g(x) | g(f(x))$ pour tout $f(x)$. Par conséquent, dans ces cas les théorèmes 2a et 2b (et les lemmes 18 et 19) ne sont pas valables.

4. Démonstrations des théorèmes

Dans les lemmes 1—10 L désigne toujours un K-corps non réel. Nous aurons besoin de quelques propriétés de ces corps que nous avons obtenues dans [8], [9] et [10].

Lemme 1. *Les sous-corps, les intersections et les compositions de K-corps sont également de K-corps dans le corps des nombres complexes.*

DÉMONSTRATION: voir [9].

Nous avons trouvé l'inégalité (4. 1) originairement en collaboration avec L. Lovász [8] dans la forme $|N_{L/Q}(\alpha)| \geqq |N_{L/Q}(\operatorname{Re}\alpha)|, |N_{L/Q}(i \operatorname{Im}\alpha)|$, où L désigne un K-corps galoisien.

Lemme 2. *Soit L un K-corps non réel de degré n et soit $\alpha \in L$. Alors*

$$\{N_{L/Q}(\alpha)\}^{2/n} \geqq \{N_{L/Q}(\operatorname{Re}\alpha)\}^{2/n} + \{N_{L/Q}(i \operatorname{Im}\alpha)\}^{2/n}. \tag{4. 1}$$

Ici l'égalité s'obtient si et seulement si $\operatorname{Re}\alpha = 0$, $i \operatorname{Im}\alpha = 0$ *ou* $\left(\frac{\operatorname{Re}\alpha}{i \operatorname{Im}\alpha}\right)^2 \in Q$.

DÉMONSTRATION: voir [9], dans le cas spécial $S_1, S_2 = \varnothing$.

Lemme 3. *Soit L un K-corps non réel et soient $0 \neq \alpha, \beta \in L$ des entiers. Si α/β est non réel, mais $\alpha \pm \beta$ est réel ou purement imaginaire, alors on a*

$$N_{L/Q}\left(\frac{\alpha \pm \beta}{2}\right) \leqq N_{L/Q}(\alpha\beta) \leqq \frac{N^2_{L/Q}(\alpha) + N^2_{L/Q}(\beta)}{2}. \tag{4. 2}$$

DÉMONSTRATION: voir également [9] ou [10].

Lemme 4. *Soit L un K-corps non réel, soit $\pi(x) \in L[x]$ à coefficients entiers et soient α_i, α_k des entiers réels dans L. Si l'on a*

$$N_{L/Q}(\alpha_i - \alpha_k) > 2^{[L:Q]} N_{L/Q}(\pi(\alpha_i)\pi(\alpha_k)) > 0, \tag{4. 3}$$

alors

$$\overline{\pi(\alpha_i)}\pi^{-1}(\alpha_i) = \overline{\pi(\alpha_k)}\pi^{-1}(\alpha_k).$$

DÉMONSTRATION: voir le lemme 7 du travail [10] dans le cas spécial S_1, $S_2 = \varnothing$.

Si L est un K-corps et $\pi(x) = \beta_0 x^k + \cdots + \beta_k \in L[x]$, désignons par $\overline{\pi(x)}$ le polynôme $\bar{\beta}_0 x^k + \cdots + \bar{\beta}_k \in L[x]$.

Lemme 5. *Soit L un K-corps non réel et soit $\pi(x)$ un polynôm à coefficients entiers sur L. S'il existe des entiers réels $\alpha_1, \ldots, \alpha_s$ ($s > \deg \pi$) dans L tels que leurs couples (α_i, α_k) satisfaisant à* (4. 3) *forment un graphe connexe ayant s sommets, alors on a $\overline{\pi(x)} = \varrho\pi(x)$ avec un certain $\varrho \in L$.*

DÉMONSTRATION: voir le lemme 8 dans [10].

Si $f(x) = \gamma_0 x^l + \cdots + \gamma_l \in L[x]$, $\operatorname{Re} f(x) = \operatorname{Re}\gamma_0 x^l + \cdots + \operatorname{Re}\gamma_l$, $i \operatorname{Im} f(x) = i \operatorname{Im}\gamma_0 x^l + \cdots + i \operatorname{Im}\gamma_l$ et si L est un K-corps, alors on a $\operatorname{Re} f(x), i \operatorname{Im} f(x) \in L[x]$. De plus, si $f(x)$ est normé et irréductible sur L et si $\operatorname{Re} f(x)$, $i \operatorname{Im} f(x) \neq 0$, alors on a nécessairement $(\operatorname{Re} f(x), i \operatorname{Im} f(x)) = \text{const}$.

Lemme 6. *Soit L un K-corps non réel et soit $f(x)$ un polynôm sur L tel que* $(\operatorname{Re} f(x), i \operatorname{Im} f(x)) = \text{const}$. *Alors $f(x)$ n'a aucun diviseur $\pi(x) \neq \text{const}$. du type $\overline{\pi(x)} = \varrho\pi(x)$ ($\varrho \in L$) dans $L[x]$.*

DÉMONSTRATION: voir le lemme 9 dans [10].

Lemme 7. *Soit L un K-corps non réel, soit $f_1(x) \in L[x]$ normé avec des coefficients entiers réels et soit $f(x) = f_1(x) \prod_{i=1}^{s} (x - \alpha_i) + \alpha$, où $\alpha_1, \ldots, \alpha_s$ ($s \geqq 2$) sont des entiers réels différents et α est un entier non réel dans L. Soit de plus L' un K-corps arbitraire. Si les couples (α_i, α_k) satisfaisant à*

$$N_{L/Q}(\alpha_i - \alpha_k) > 2^{[L:Q]} N_{L/Q}(\alpha) > 0 \tag{4.4}$$

forment un graphe connexe ayant s sommets, alors $f(x)$ n'a aucun diviseur irréductible de degré $< s$ sur L'. Par conséquent, si $s > \dfrac{\deg f}{2}$, alors $f(x)$ est irréductible sur L'.

Remarque. Le lemme 7 est une amélioration du théorème 2 de [10]. Dans [10] nous avons prouvé que ce lemme ne peut pas être étendu pour des corps d'autre type même dans le cas où au côté droit de (4. 4) se trouve une fonction arbitraire des paramètres $[L:Q]$ et $N_{L/Q}(\alpha)$.

DÉMONSTRATION. D'abord nous prouvons que $f(x)$ n'a aucun diviseur irréductible de degré $< s$ sur L.

Supposons qu'il existe une décomposition

$$f(x) = \pi_1(x)\pi_2(x); \quad \pi_1(x), \pi_2(x) \in L[x],$$

$\pi_1(x)$ étant un polynôme de degré $< s$. Alors on peut supposer que les polynômes $\pi_1(x)$ et $\pi_2(x)$ ont des coefficients entiers. De $f(\alpha_k) = \alpha \neq 0$ on déduit

$$\pi_1(\alpha_k)\pi_2(\alpha_k) \neq 0 \qquad (k = 1, \ldots, s)$$

et

$$\alpha\bar{\alpha} = f(\alpha_i)\overline{f(\alpha_k)} = \pi_1(\alpha_i)\pi_2(\alpha_i)\overline{\pi_1(\alpha_k)\pi_2(\alpha_k)} = \pi_1(\alpha_i)\overline{\pi_1(\alpha_k)}\pi_2(\alpha_i)\overline{\pi_2(\alpha_k)}.$$

Mais
$$N_{L/Q}(\overline{\pi_j(\alpha_k)}) = N_{L/Q}(\pi_j(\alpha_k)) \qquad (j=1, 2;\ k=1, \ldots, s),$$
par conséquent de (4. 4) il résulte
$$N^2_{L/Q}(\alpha_i-\alpha_k) > 2^{2[L:Q]}N_{L/Q}(\alpha\bar{\alpha}) = 2^{2[L:Q]}N_{L/Q}(\pi_1(\alpha_i)\pi_1(\alpha_k))N_{L/Q}(\pi_2(\alpha_i)\pi_2(\alpha_k)) > 0$$
pour chaque couple (α_i, α_k) satisfaisant à (4. 4). On en déduit
$$N_{L/Q}(\alpha_i-\alpha_k) > 2^{[L:Q]}N_{L/Q}(\pi_1(\alpha_i)\pi_1(\alpha_k)) > 0$$
ou
$$N_{L/Q}(\alpha_i-\alpha_k) > 2^{[L:Q]}N_{L/Q}(\pi_2(\alpha_i)\pi_2(\alpha_k)) > 0.$$

Donc, d'après le lemme 4 on obtient
$$\frac{\overline{\pi_1(\alpha_i)}}{\pi_1(\alpha_i)} = \frac{\overline{\pi_1(\alpha_k)}}{\pi_1(\alpha_k)} \quad \text{ou} \quad \frac{\overline{\pi_2(\alpha_i)}}{\pi_2(\alpha_i)} = \frac{\overline{\pi_2(\alpha_k)}}{\pi_2(\alpha_k)},$$
c'est-à-dire
$$\pi_1(\alpha_i)\overline{\pi_1(\alpha_k)} \quad \text{ou} \quad \pi_2(\alpha_i)\overline{\pi_2(\alpha_k)}$$
est réel. Mais
$$\pi_1(\alpha_i)\overline{\pi_1(\alpha_k)}\pi_2(\alpha_i)\overline{\pi_2(\alpha_k)} = f(\alpha_i)\overline{f(\alpha_k)} = \alpha\bar{\alpha} \neq 0$$
est également réel, ainsi $\pi_1(\alpha_i)\overline{\pi_1(\alpha_k)}$ et $\pi_2(\alpha_i)\overline{\pi_2(\alpha_k)}$ sont simultanément réels. Donc, on a
$$\overline{\pi_1(\alpha_i)}\pi_1^{-1}(\alpha_i) = \overline{\pi_1(\alpha_k)}\pi_1^{-1}(\alpha_k) = \varrho \in L$$
pour chaque (α_i, α_k) satisfaisant à (4. 4). Vu que le graphe de ces couples (α_i, α_k) est connexe, il en résulte $\overline{\pi_1(\alpha_i)} = \varrho\pi_1(\alpha_i)$ $(i=1, \ldots, s)$.

Soit
$$\pi_1(x) = \beta_0 x^k + \cdots + \beta_k \qquad (k<s)$$
et substituons les $\alpha_1, \ldots, \alpha_{k+1}$ dans $\pi_1(x)$. Alors du système d'équations obtenu on déduit
$$\beta_j = \sum_{l=1}^{k+1} \sigma_{jl}\pi_1(\alpha_l) \qquad (j=0, \ldots, k)$$
avec des nombres réels $\sigma_{jl} \in L$. D'après $\overline{\pi_1(\alpha_l)} = \varrho\pi_1(\alpha_l)$ on en déduit nécessairement $\bar{\beta}_j/\beta_j = \varrho$ $(j=0, \ldots, k)$, c'est-à-dire $\overline{\pi_1(x)} = \varrho\pi_1(x)$, ce qui entraîne une contradiction d'après le lemme 6.

Soit maintenant L' un K-corps arbitraire et désignons par L'' la composition de L et L'. Alors d'après le lemme 1 L'' est également un K-corps. Il suffit de démontrer que $f(x)$ n'a aucun diviseur irréductible de degré $<s$ sur L''. Mais $L'' \supseteq L$ et, si nous prenons la $[L'':L]$-ième puissance de tous les deux côtés de (4. 4), nous obtenons
$$N_{L''/Q}(\alpha_i-\alpha_k) > 2^{[L'':Q]}N_{L''/Q}(\alpha) > 0.$$

Par conséquent, en appliquant le résultat, obtenu précédemment, pour $f(x)$ et pour L'' au lieu de L, notre proposition est démontrée.

Lemme 8. (CAPELLI*)) *Soient $f(x)$ et $g(x)$ des polynômes normés à coefficients rationnels, soit $g(x)$ irréductible sur Q et soit α une de ses racines dans le corps des nombres complexes. Si*

$$f(x)-\alpha = \pi_1^{k_1}(x) \dots \pi_r^{k_r}(x)$$

est une décomposition en facteurs normés irréductibles sur $Q(\alpha)=K$, alors

$$g(f(x)) = \prod_{i=1}^{r} N^{k_i}(\pi_i(x)) \qquad (N \text{ désigne } N_{K(x)/Q(x)}) \tag{4.5}$$

est une décomposition en facteurs irréductibles sur Q.

DÉMONSTRATION: voir [28] ou [19].

Dans le lemme suivant soit $f(x)\in Z[x]$ normé et supposons qu'il existe un $f_1(x)|f(x), f_1(x)\in Z[x]$ ayant des racines réelles différentes. Désignons par L le corps de décomposition de $f_1(x)$. Alors le lemme suivant est vrai:

Lemme 9. *Soit $G\geqq 1$ une constante et soit $g(x)$ un polynôme arbitraire tel que $g(x)\in P(G)$. Si le graphe des couples (α_i, α_k), formées des racines de $f_1(x)$ et satisfaisant à*

$$|N_{L/Q}(\alpha_i-\alpha_k)| > (2G)^{[L:Q]}, \tag{4.6}$$

contient un sous-graphe connexe ayant s sommets, alors $g(f(x))$ n'a aucun diviseur irréductible de degré $<s \deg g$ sur Q, par conséquent le nombre de ses diviseurs irréductibles est $\leqq \frac{\deg f}{s}$ et en particulier de $s > \frac{\deg f}{2}$ il résulte l'irréductibilité de $g(f(x))$ sur Q.

Remarque. Ce lemme est une amélioration des théorèmes 1′ et 2′ de [10], et avec son aide on peut aisément améliorer aussi le théorème 3 de [10].

DÉMONSTRATION. Vu que les corps de décomposition de $f_1(x)$ et $g(x)$ sont des K-corps, d'après le lemme 1 le corps de décomposition L' de $f_1(x)g(x)$ est également un K-corps. De plus, on obtient

$$N_{L'/Q}(\alpha_i-\alpha_k) > (2G)^{[L':Q]}$$

pour chaque couple (α_i, α_k) satisfaisant à (4. 6).

Soit $g(x) = \prod_{i=1}^{n} (x-\beta_i)$ dans le corps des nombres complexes et soit, par exemple, $\beta_1=\beta$. Désignons par $\alpha_1, \dots, \alpha_s$ les racines de $f_1(x)$ qui forment un graphe connexe ayant s sommets ($s\leqq \deg f_1$). Alors on peut écrire

$$f(x)-\beta = h(x) \prod_{j=1}^{s} (x-\alpha_j)-\beta,$$

$h(x)\in L[x]$ étant un polynôme normé avec des coefficients entiers réels. D'après le lemme 8 il suffit de considérer le cas $s\geqq 2$.

*) CAPELLI a démontré ce lemme originairement dans une forme moins générale (voir [28]).

On a évidemment

$$G^{[L':Q]} \geqq \{g(0)\}^{[L':Q]/n} = \{N_{Q(\beta)/Q}(\beta)\}^{[L':Q]/[Q(\beta):Q]} = N_{L'/Q}(\beta).$$

Par conséquent pour les couples (α_i, α_k) satisfaisant à (4. 6) on a

$$N_{L'/Q}(\alpha_i - \alpha_k) > (2G)^{[L':Q]} \geqq 2^{[L':Q]} N_{L'/Q}(\beta) > 0.$$

D'après le lemme 7 il en résulte que $f(x)-\beta$ n'a aucun diviseur irréductible de degré $<s$ sur L', et par conséquent sur $Q(\beta)$ non plus. Enfin, du lemme 8 on déduit que le degré de chaque diviseur irréductible de $g(f(x))$ est $\geqq s \deg g$, c'est-à-dire le nombre de ses diviseurs irréductibles est $\leqq \dfrac{\deg f}{s}$. Donc, en particulier, de $s > \dfrac{\deg f}{2}$ on déduit que $g(f(x))$ est irréductible sur Q.

Lemme 10. *Soient $f(x), g(x) \in Z[x]$ des polynômes satisfaisant aux conditions du lemme 9. Alors le nombre des diviseurs irréductibles de $g(f(x))$ sur un K-corps arbitraire est* $\leqq \deg g \left[\dfrac{\deg f}{s}\right]$.

DÉMONSTRATION. Désignons par L' le corps de décomposition de $f_1(x)g(x)$. Il suffit de démontrer que le nombre des diviseurs irréductibles de $g(f(x))$ est $\leqq \deg g \left[\dfrac{\deg f}{s}\right]$ sur L'', L'' étant un K-corps arbitraire tel que $L'' \supseteq L'$.

Soit $g(x) = \prod_{i=1}^{n} (x-\beta_i)$ dans le corps des nombres complexes et prenons la décomposition

$$g(f(x)) = (f(x)-\beta_1)\ldots(f(x)-\beta_n)$$

sur L', où les facteurs ne sont pas nécessairement irréductibles sur L'. Au cours de la démonstration du lemme 9 nous avons prouvé que de (4. 6) il résulte

$$N_{L'/Q}(\alpha_i - \alpha_k) > 2^{[L':Q]} N_{L'/Q}(\beta_i) > 0 \qquad (i = 1, \ldots, n).$$

Par conséquent, d'après le lemme 7 le degré des diviseurs irréductibles de $f(x)-\beta_i$ $(i=1, \ldots, n)$ est $\geqq s$ sur L'', c'est-à-dire le nombre des diviseurs irréductibles de $f(x)-\beta_i$ est $\leqq \left[\dfrac{\deg f}{s}\right]$. Il en résulte que sur L'' le nombre des diviseurs irréductibles de $g(f(x))$ est $\leqq n\left[\dfrac{\deg f}{s}\right] = \deg g \left[\dfrac{\deg f}{s}\right]$.

Dans la suite désignons par $h(\gamma)$ le maximum des valeurs absolues des conjugués du nombre algébrique γ. Si γ est entier, alors on a évidemment $h(\gamma) \geqq 1$. De plus, si d et $H(\gamma)$ désignent le degré et la hauteur de γ respectivement, alors $h(\gamma) \leqq dH(\gamma)$ (voir A. Baker [1], p. 177.). Enfin, en supposant que γ est un entier algébrique, on a $H(\gamma) \leqq \max_{1 \leqq k \leqq d} \binom{d}{k} h^k(\gamma). \leqq (2h(\gamma))^d$.

Dans les lemmes 11—17 soit $K = Q(\alpha)$ un corps algébrique de degré $n_k > 1$ et de discriminant D_k, α étant un entier algébrique. Désignons par $\alpha^{(1)}, \ldots, \alpha^{(n_k)}$ les conjugués de α arrangés de telle manière que $\alpha^{(1)}, \ldots, \alpha^{(s)}$ soient tous réels et $\alpha^{(s+1)}, \ldots$ $\ldots, \alpha^{(s+t)}$ soient les conjugués complexes de $\alpha^{(s+t+1)}, \ldots, \alpha^{(s+2t)}$ respectivement.

Ainsi on a $n_k = s+2t$. $\theta \in K$ étant un nombre arbitraire, désignons par $\theta^{(1)}, \ldots, \theta^{(n_k)}$ les conjugués de θ correspondants aux conjugués $\alpha^{(1)}, \ldots, \alpha^{(n_k)}$ de α. Soit $r = s+t-1$, et soit $D \geqq |D_k|$ une constante arbitraire.

Lemme 11. (A. BAKER [1]). *Dans K il y a des unités $\eta_1, \ldots, \eta_r$ telles que*

$$|\log |\eta_k^{(j)}|| \leqq \frac{1}{2} \log D \qquad (1 \leqq j, k \leqq r;\ j \neq k) \tag{4.7}$$

et

$$r! \log D \leqq \log |\eta_k^{(k)}| \leqq 2(r!+1) D^{(n_k+1)/2} \log D \qquad (1 \leqq k \leqq r). \tag{4.8}$$

Remarque. Dans [1] Baker a démontré ce lemme originairement avec $D(\alpha)$ au lieu de D_k. Notre proposition s'obtient immédiatement de la démonstration de Baker, en prenant une base des entiers de K au lieu de la base $1, \alpha, \ldots, \alpha^{n_k-1}$.

On en déduit aisément le lemme suivant:

Lemme 12. *Pour les unités $\eta_1, \ldots, \eta_r$ précédentes on a*

$$\log h(\eta_i) \leqq 2n_k! |D_k|^{(n_k+1)/2} \log |D_k| = c_1(n_k, D_k) \qquad (i = 1, \ldots, r). \tag{4.9}$$

DÉMONSTRATION. Employons le lemme 11 avec $D = |D_k|$. Si pour un $1 \leqq i \leqq r$ fixé $h(\eta_i) = \max\limits_{1 \leqq j \leqq r} |\eta_i^{(j)}|$, alors notre assertion s'obtient du lemme 11. Si $h(\eta_i) = |\eta_i^{(s+t)}|$, alors de

$$1 = |N(\eta_i)| = |\eta_i^{(1)}| \ldots |\eta_i^{(s)}| \, |\eta_i^{(s+1)}|^2 \ldots |\eta_i^{(s+t)}|^2$$

on déduit

$$0 < \log h(\eta_i) = \log |\eta_i^{(s+t)}| = \frac{1}{e_{s+t}} \left| \log |\eta_i^{(1)}| + \cdots + 2 \log |\eta_i^{(s+t-1)}| \right|,$$

où $e_{s+t} = 1$ si $t = 0$, et $e_{s+t} = 2$ dans le cas $t > 0$. Donc, d'après (4. 7) et (4. 8) on déduit (4. 9).

Lemme 13 (A. BAKER [1]). *Soit K un corps algébrique de degré n_k et de discriminant D_k avec des unités $\eta_1, \ldots, \eta_r$ ayant la propriété précédente. Si $\beta \in K$ est un entier, il existe un $\gamma = \beta \eta_1^{b_1} \ldots \eta_r^{b_r}$ $(b_i \in Z)$ tel que*

$$\log h(\gamma) \leqq n_k^2 c_1(n_k, D_k) + \frac{1}{n_k} \log |N_{K/Q}(\beta)|. \tag{4.10}$$

Remarque. La démonstration résulte des lemmes 11 et 12 (voir [1], p. 188 et 205), en remplaçant D par $|D_k|$.

Lemme 14 (A. BAKER—J. COATES [2]). *Soit K un corps algébrique de degré n_k et de discriminant D_k. Soient $\alpha_1, \ldots, \alpha_n \in K$ $(n \geqq 3)$ des entiers différents deux à deux et soit $\sigma \in K$ $(\sigma \neq 0)$ un entier. Si $\max(h(\sigma), h(\alpha_1), \ldots, h(\alpha_n)) \leqq H$, alors on a $H(x), H(y) \leqq c_2(n_k, D_k, n, H)$ pour chaque solution x, y de l'équation*

$$(x - \alpha_1 y) \ldots (x - \alpha_n y) = \sigma \tag{4.11}$$

en entiers de K, où c_2 est une constante calculable explicitement et dépendant seulement de n_k, D_k, n et de H.

Remarque. La démonstration du lemme se trouve dans [2], à la page 601. Dans la démonstration les constantes sont calculables et elles ne dépendent que de n_k, n, H et de la constante D du lemme 11. En choisissant $D=|D_k|$, on peut obtenir une constante c_2, calculable explicitement et dépendant seulement de n, n_k, D_k et H, telle que $H(x), H(y)\leqq c_2$ pour chaque solution x, y de (4. 11) en entiers de K.

Nous remarquons que si α et β sont des nombres algébriques de degré d_1 et d_2 respectivement et si $H(\alpha), H(\beta)\leqq H$, alors le degré de $\alpha\pm\beta$, $\alpha\cdot\beta$ et α/β $(\beta\neq 0)$ est $\leqq d=d_1d_2$ et la hauteur de ces nombres est $\leqq(4dH^4)^d$ (voir [1], p. 205.).

Lemme 15. *Soit K un corps algébrique de degré n_k et de discriminant D_k et soient $\alpha, \beta, \gamma\neq 0$ des entiers dans K tels que* $\max(h(\alpha), h(\beta), h(\gamma))\leqq H$. *Il existe une constante $c_3(n_k, D_k, H)$, calculable explicitement, telle que $H(x), H(y)\leqq c_3$ pour chaque solution x, y de l'équation*

$$\alpha x^3+\beta y^3 = \gamma \tag{4. 12}$$

en entiers de K.

DÉMONSTRATION. Avec les notations $x'=\alpha x$, $\beta'=\alpha^2\beta$, $\gamma'=\alpha^2\gamma$ il suffit de considérer l'équation $x'^3+\beta' y^3 = \gamma'$, où pour $h(\beta')$, $h(\gamma')$ on peut donner une borne supérieure dépendant de H. Désignons par $\sqrt[3]{\beta'}$ l'une des troisièmes racines de β' $(\beta'\neq 0)$. Si $\varrho^3=1$ $(\varrho\neq 1)$, dans $L=K(\sqrt[3]{\beta'}, \varrho)$ on peut écrire

$$(x'+\sqrt[3]{\beta'}\, y)(x'+\varrho\sqrt[3]{\beta'}\, y)(x'+\varrho^2\sqrt[3]{\beta'}\, y) = \gamma', \tag{4. 13}$$

les $\varrho^k\sqrt[3]{\beta'}$ $(k=0, 1, 2)$ étant différents. Le degré de ces nombres algébriques est $\leqq 3n_k$. Si $h(x)\in Z[x]$ est le polynôme minimal de β', alors le polynôme minimal de $\varrho^k\sqrt[3]{\beta'}$ divise $h(x^3)$ dans $Z[x]$. Donc, on a $H(\varrho^k\sqrt[3]{\beta'})\leqq(3n_k)^{3n_k}H(\beta')$ d'après un lemme de C. SIEGEL (voir [26], p. 176., Hilfssatz 3.). Ainsi, on peut obtenir une borne supérieure, calculable explicitement et dépendant de n_k et H, aussi pour $h(\varrho^k\sqrt[3]{\beta'})$. De plus, dans K il y a un élément δ entier primitif tel que $h(\delta)\leqq|D_k|^{1/2}$ (voir, par ex. [16], p. 22.).

Le degré de $Q(\delta, \sqrt[3]{\beta'})$ est $\leqq 3n_k^2=N$. Par conséquent parmi les $l\delta+\sqrt[3]{\beta'}$ $(l=0, \ldots, N^4)$ il existe au moins un nombre ayant la propriété qu'en remplaçant le nombre δ et $\sqrt[3]{\beta'}$ par leurs conjugués respectifs, les nombres obtenus seront différents deux à deux. En désignant par σ_1 un nombre à cette propriété, σ_1 sera un élément entier primitif du corps $Q(\delta, \sqrt[3]{\beta'})$ (voir par ex. [14], p. 73., Satz 709). et pour $H(\sigma_1) = H(l\delta+\sqrt[3]{\beta'})$ on peut donner une borne supérieure dépendant seulement de $H(\delta), H(\sqrt[3]{\beta'})$ et n_k, c'est-à-dire de n_k, D_k et H. En adjoignant ϱ au corps $Q(\sigma_1)$, on obtient déjà le corps $L=Q(\sigma_2)$ avec un nombre entier σ_2 et on peut donner de la même façon une borne supérieure, calculable explicitement et dépendant

seulement des paramètres précédents, pour le degré, pour la hauteur et ainsi aussi pour le discriminant de σ_2, qui est valable aussi pour le discriminant $|D_L|$ de L d'après $D_L|D(\sigma_2)$. Par suite, en conséquence du lemme 14 on peut obtenir une borne supérieure, calculable explicitement et dépendant de n_k, D_k et H pour $H(x')$, $H(y)$, x', y étant une solution arbitraire de (4. 13) en entiers de L. Enfin, il en résulte qu'on peut évidemment donner une borne supérieure aussi pour la hauteur des solutions x, y de (4. 12) en entiers de K.

Dans ce qui suit nous désignons par K un corps algébrique de degré n_k et de discriminant D_k. Considérons les solutions $(\beta_1, \beta_2, \beta_3)$ de l'équation

$$\beta_1+\beta_2+\beta_3 = 0, \quad \beta_1\beta_2\beta_3 \neq 0 \tag{4. 14}$$

en entiers de K. Appelons les solutions $(\beta_1', \beta_2', \beta_3')$ et $(\beta_1'', \beta_2'', \beta_3'')$ associées entre eux, si $(\beta_1'', \beta_2'', \beta_3'')=(\varepsilon\beta_1', \varepsilon\beta_2', \varepsilon\beta_3')$ avec une unité ε de K.

Lemme 16. *Soit $G' \geqq 1$ une constante et soit $(\beta_1, \beta_2, \beta_3)$ une solution de* (4. 14) *telle que*

$$|N_{K/Q}(\beta_1)|, |N_{K/Q}(\beta_2)|, |N_{K/Q}(\beta_3)| \leqq G'. \tag{4. 15}$$

Alors il existe une solution $(\beta_1', \beta_2', \beta_3')$ de (4. 14) *associée à $(\beta_1, \beta_2, \beta_3)$ telle que* $\max(h(\beta_1'), h(\beta_2'), h(\beta_3') \leqq c_4(n_k, D_k, G')$. *Par conséquent, le nombre des solutions de* (4. 14) *satisfaisant à* (4. 15) *et non associées deux à deux est $\leqq c_5(n_k, D_k, G')$, c_4 et c_5 étant des constantes calculables explicitement et dépendant seulement de n_k, D_k et G'*).*

Démonstration. Soit $(\beta_1, \beta_2, \beta_3)$ une solution de (4. 14) en entiers de K, satisfaisant à l'inégalité (4. 15). Désignons par $\eta_1, \ldots, \eta_r$ les unités obtenues dans les lemmes 11 et 12. Alors, d'après le lemme 13 il existe des entiers γ_i dans K de la forme $\gamma_i=\beta_i\eta_1^{b_{i1}}\ldots\eta_r^{b_{ir}}$ $(b_{ij}\in Z,\ i=1, 2, 3)$ tels que

$$h(\gamma_i) \leqq c_6(n_k, D_k, G') \tag{4. 16}$$

avec une constante c_6 calculable explicitement. De (4. 14) il résulte

$$\gamma_1\eta_1^{c_{11}} \ldots \eta_r^{c_{1r}} + \gamma_2\eta_1^{c_{21}} \ldots \eta_r^{c_{2r}} = -\gamma_3,$$

avec des $c_{ij}\in Z$ convenablement choisis, où $(\gamma_1\eta_1^{c_{11}}\ldots\eta_r^{c_{1r}}, \gamma_2\eta_1^{c_{21}}\ldots\eta_r^{c_{2r}}, \gamma_3)=$ $=(\beta_1', \beta_2', \beta_3')$ est une solution de (4. 14) associée à $(\beta_1, \beta_2, \beta_3)$. Mais l'égalité précédente peut être écrite sous la forme

$$\gamma_1^* x^3 + \gamma_2^* y^3 = \gamma_3, \tag{4. 17}$$

où $\gamma_i^* = -\gamma_i\eta_1^{c_{i1}^*}\ldots\eta_r^{c_{ir}^*}$ et $c_{ij}^*=0$, 1 ou 2 $(i=1, 2;\ j=1, \ldots, r)$. D'après le lemme 12 pour $h(\gamma_i^*)$ on peut donner une borne supérieure calculable explicitement et dépendant seulement de n_k, D_k et G'. Ainsi, d'aprés le lemme 15 on peut également donner une borne superieure pour $H(x)$, $H(y)$, c'est-à-dire pour $H(\gamma_1^* x^3)$, $H(\gamma_2^* y^3)$, $H(\beta_i')$, $h(\beta_i')$ et, enfin, aussi pour le nombre des solutions.

Lemme 17. *Soit K un corps algébrique de degré n_k et de discriminant D_k, soit $G' \geqq 1$ une constante et soit $f(x) = \prod_{i=1}^{m}(x-\alpha_i)$ avec des entiers différents α_i dans*

*) Addition. Les constantes c_4, c_5 peuvent être encore un peu améliorées.

K. Désignons par $\mathcal{G}(f, G')=\mathcal{G}(f)$ *le graphe des couples* (α_i, α_k) *satisfaisant à l'inégalité*

$$|N_{K/Q}(\alpha_i-\alpha_k)| > G'. \tag{4.18}$$

Il y a une constante $c_7(n_k, D_k, G')$, *calculable explicitement et dépendant seulement de* n_k, D_k *et* G', *telle que dans le cas* $m=\deg f>c_7$ *ou* $\mathcal{G}(f)$ *a un sous-graphe connexe ayant plus de* $m/2$ *sommets ou bien* $\mathcal{G}(f)$ *se constitute de deux graphes complets ayant* $m/2$ *sommets et disjoints l'un de l'autre.*

Remarque. Soit particulierement K un K-corps non réel, soit $\alpha\in K$ $(\alpha\neq 0)$ un entier non réel et soient $\alpha_1, \ldots, \alpha_m\in K$ des entiers réels différents. Si m est assez grand par rapport à n_k, $|D_k|$ et $N_{K/Q}(\alpha)$, alors d'après les lemmes 7 et 17 $f(x) = \prod_{i=1}^{m}(x-\alpha_i)+\alpha$ est irréductible sur tout K-corps ou bien il se décompose en deux facteurs irréductibles de degré $m/2$ sur K (en supposant que m est pair).

C'est probablement le premier cas qui se réalise toujours concernant $\mathcal{G}(f)$ dans le lemme, mais pour démontrer cette conjecture il faudrait résoudre un problème diophantien très difficile (voir la Proposition 3).

Démonstration. Supposons que $\mathcal{G}(f)$ n'a aucun sous-graphe connexe ayant plus de $m/2$ sommets. Alors $\mathcal{G}(f)$ se constitue au moins de deux sous-graphes connexes de sommets $\leqq m/2$, disjoints deux à deux (en considérant les sous-graphes ayant un sommet aussi comme connexes). Soient ces sous-graphes $\mathcal{G}_1, \ldots, \mathcal{G}_s$, lorsque $\mathcal{G}(f) = \bigcup_{i=1}^{s}\mathcal{G}_i$.

Considérons d'abord le cas $s\geqq 3$. Désignons par $\overline{\mathcal{G}}$ le complémentaire du graphe $\mathcal{G}(f)$. Choisissons deux graphes, par ex. $\mathcal{G}_i$ et $\mathcal{G}_k$, des graphes précédents de telle manière que le nombre de sommets de $\mathcal{G}_i$ et de $\mathcal{G}_k$ soit minimal. Prenons un sommet α_i et α_k de $\mathcal{G}_i$ et de $\mathcal{G}_k$ respectivement. Soient $\alpha_{i_1}, \ldots, \alpha_{i_r}$ les sommets des autres sous-graphes. D'après l'hypothèse $r\geqq m/3$. Considérons dans $\overline{\mathcal{G}}$ tous les triangles ayant les sommets α_i, α_k et α_{i_t} $(t=1, \ldots, r)$. Alors, d'après la définition de $\overline{\mathcal{G}}$ on a

$$|N_{K/Q}(\alpha_k-\alpha_{i_t})|, |N_{K/Q}(\alpha_{i_t}-\alpha_i)|, |N_{K/Q}(\alpha_i-\alpha_k)| \leqq G' \tag{4.19}$$

et

$$(\alpha_k-\alpha_{i_t})+(\alpha_{i_t}-\alpha_i)+(\alpha_i-\alpha_k) = 0. \tag{4.20}$$

Vu que $D(f)\neq 0$, les différences considérées satisfont à (4. 14) et (4. 15). Les $(\alpha_k-\alpha_{i_t}, \alpha_{i_t}-\alpha_i, \alpha_i-\alpha_k)$ $(t=1, \ldots, r)$ sont des solutions de (4. 14) non associées deux à deux. En effet, si $(\alpha_k-\alpha_{i_{t'}}, \alpha_{i_{t'}}-\alpha_i, \alpha_i-\alpha_k)$ et $(\alpha_k-\alpha_{i_{t''}}, \alpha_{i_{t''}}-\alpha_i, \alpha_i-\alpha_k)$ sont associées, alors $\alpha_k-\alpha_{i_{t'}} = \alpha_k-\alpha_{i_{t''}}$ et $\alpha_{i_{t'}}-\alpha_i = \alpha_{i_{t''}}-\alpha_i$, par conséquent $\alpha_{i_{t'}}=\alpha_{i_{t''}}$, ce qui est impossible. Ainsi, d'après le lemme 16 on a $r\leqq c_5(n_k, D_k, G')$ avec la constante c_5 qui se trouve dans le lemme 16. Donc, on obtient $m\leqq 3c_5$, c'est-à-dire dans le cas $m>3c_5$ on a nécessairement $s<3$.

Ensuite considérons le cas $s=2$. Vu que $\mathcal{G}(f) = \mathcal{G}_1\cup\mathcal{G}_2$ et le nombre des sommets de $\mathcal{G}_1$ et de $\mathcal{G}_2$ est $\leqq m/2$, nous obtenons ici nécessairement une égalité, c'est-à-dire $m=2m'$, m' étant le nombre des sommets de $\mathcal{G}_1$ et aussi de $\mathcal{G}_2$. Si par exemple $\mathcal{G}_1$ n'est pas complet, alors il existe des sommets α_i, α_k dans $\mathcal{G}_1$ tels que

$(\alpha_i, \alpha_k) \notin \mathcal{G}_1$. Dans ce cas désignons par $\alpha_{i_1}, \ldots, \alpha_{i_{m'}}$, les sommets de $\mathcal{G}_2$. Vu que $\mathcal{G}_1$ et $\mathcal{G}_2$ sont disjoints, on a $(\alpha_k, \alpha_{i_t}), (\alpha_{i_t}, \alpha_i) \in \bar{\mathcal{G}}$ pour tout $1 \leqq t \leqq m'$, c'est-à-dire

$$|N_{K/Q}(\alpha_k - \alpha_{i_t})|, |N_{K/Q}(\alpha_{i_t} - \alpha_i)|, |N_{K/Q}(\alpha_i - \alpha_k)| \leqq G'$$

et

$$(\alpha_k - \alpha_{i_t}) + (\alpha_{i_t} - \alpha_i) + (\alpha_i - \alpha_k) = 0$$

pour tout $1 \leqq t \leqq m'$. Il en résulte de la manière précédente que $m' \leqq c_5$ avec la constante c_5 précédente. Par conséquent, si $s=2$ et $m > 2c_5$, alors $\mathcal{G}_1$ et $\mathcal{G}_2$ sont complets. Ainsi, on peut choisir $c_7(n_k, D_k, G') = 3c_5$ et notre proposition se trouve démontrée.

DÉMONSTRATION *du théorème1 a*. Soit $f(x) = \prod_{i=1}^{m} (x - \alpha_i) \in Z[x]$ avec des entiers différents α_i dans K et soit $g(x) \in P(G)$. Soit $G' = (2G^2)^{n_k}$ et prenons le graphe $\mathcal{G}(f)$ des couples (α_i, α_k) satisfaisant à l'inégalité (4. 18). D'après le lemme 17 il y a une constante $c_8(n_k, D_k, G) = c_7(n_k, D_k, G')$ calculable explicitement telle que dans le cas $m > c_8$ $\mathcal{G}(f)$ a un sous-graphe connexe ayant plus de $m/2$ sommets ou bien $\mathcal{G}(f)$ se constitue de deux graphes complets $\mathcal{G}_1, \mathcal{G}_2$ ayant $m/2$ sommets et disjoints l'un de l'autre. D'après $(2G^2)^{n_k} \geqq (2G)^{n_k}$ et d'après le lemme 9 on en déduit que $g(f(x))$ est irréductible sur Q ou bien il se décompose en deux diviseurs irréductibles de degré $\deg g$. $m/2$ (m étant pair). Dans le premier cas notre proposition est démontrée, ainsi dans la suite nous ne considérons que le second cas.

Donc, soit $f(x) \in Z[x]$ un polynôme normé de degré $m = 2m' > c_8$ avec des racines différentes de K, tel que $g(f(x))$ soit réductible sur Q pour un $g(x) \in P(G)$ lorsque $\mathcal{G}(f)$ se constitue de deux graphes complets $\mathcal{G}_1$ et $\mathcal{G}_2$ ayant m' sommets respectifs et disjoints l'un de l'autre. Soit $f(x) = f_1(x) f_2(x)$, $f_1(x) = \prod_{i=1}^{m} (x - \alpha_i)$, $f_2(x) = \prod_{i=1}^{m} (x - \alpha_i')$ où $\mathcal{G}_1$ et $\mathcal{G}_2$ contient les racines de $f_1(x)$ et de $f_2(x)$ comme sommets respectivement. D'après l'hypothèse $g(f(x))$ est réductible, ainsi par suite du lemme 9, il se décompose nécessairement en deux diviseurs irréductibles de degré m' $\deg g$. Si l'on désigne par α une des racines de $g(x)$ dans le corps complexe, d'après le lemme 8 on peut écrire

$$f(x) - \alpha = f_1(x) f_2(x) - \alpha = \pi_1(x) \pi_2(x) \tag{4. 21}$$

avec des polynômes normés $\pi_1(x), \pi_2(x) \in Q(\alpha)[x]$ à coefficients entiers et de degré $m' = m/2$. Désignons par L la composition de K et du corps de décomposition de $g(x)$. D'après le lemme 1 L est un K-corps non réel. Soit

$$\pi_1(x) = f_1(x) + \varphi_1(x) = f_2(x) + \varphi_1'(x), \tag{4. 22}$$

où $\varphi_1(x), \varphi_1'(x) \in L[x]$ sont des polynômes à coefficients entiers et de degré $\leqq m' - 1$. De plus, d'après la définition de $f_1(x)$ on a $\varphi_1(\alpha_i) = \pi_1(\alpha_i) \neq 0$ $(1 \leqq i \leqq m')$. Vu que $(\alpha_i, \alpha_k) \in \mathcal{G}(f)$ pour tout couple i, k $(1 \leqq i, k \leqq m'; i \neq k)$, on a pour ces couples

$$\begin{aligned} N_{L/Q}(\alpha_i - \alpha_k) > (2G^2)^{n_k [L:K]} &\geqq 2^{[L:Q]} \{g^2(0)\}^{[L:Q]/n} = \\ &= 2^{[L:Q]} \{N_{Q(\alpha)/Q}(\alpha^2)\}^{[L:Q]/n} = 2^{[L:Q]} N_{L/Q}(\alpha^2) = \\ &= 2^{[L:Q]} N_{L/Q}(\pi_1(\alpha_i) \pi_2(\alpha_i) \pi_1(\alpha_k) \pi_2(\alpha_k)) \geqq \\ \geqq 2^{[L:Q]} N_{L/Q}(\pi_1(\alpha_i) \pi_1(\alpha_k)) &= 2^{[L:Q]} N_{L/Q}(\varphi_1(\alpha_i) \varphi_1(\alpha_k)) > 0. \qquad (n = \deg g) \end{aligned}$$

Mais le graphe des couples (α_i, α_k) est connexe et a $m' > \deg \varphi_1$ sommets, d'où il résulte d'après le lemme 5, que $\overline{\varphi_1(x)} = \varrho_1 \varphi_1(x)$ avec un $\varrho_1 \in L$. On peut démontrer de manière analogue que $\overline{\varphi_1'(x)} = \varrho_1' \varphi_1'(x)$ avec un certain $\varrho_1' \in L$. Si maintenant les polynômes $\varphi_2(x), \varphi_2'(x) \in L[x]$ à coefficients entiers et de degré $\leqq m'-1$ sont définis par

$$\pi_2(x) = f_1(x) + \varphi_2(x) = f_2(x) + \varphi_2'(x), \tag{4.23}$$

alors on peut démontrer de la même façon que $\overline{\varphi_2(x)} = \varrho_2 \varphi_2(x)$ et $\overline{\varphi_2'(x)} = \varrho_2' \varphi_2'(x)$, où $\varrho_2, \varrho_2' \in L$.

De (4. 22) et (4. 23) on déduit

$$\frac{\overline{\pi_1(\alpha_i)}}{\pi_1(\alpha_i)} = \frac{\overline{\varphi_1(\alpha_i)}}{\varphi_1(\alpha_i)} = \varrho_1 \quad \text{et} \quad \frac{\overline{\pi_2(\alpha_i)}}{\pi_2(\alpha_i)} = \frac{\overline{\varphi_2(\alpha_i)}}{\varphi_2(\alpha_i)} = \varrho_2,$$

et en conséquence de (4. 21) il en résulte

$$\varrho = \frac{\bar{\alpha}}{\alpha} = \frac{\overline{\pi_1(\alpha_i)\pi_2(\alpha_i)}}{\pi_1(\alpha_i)\pi_2(\alpha_i)} = \varrho_1 \varrho_2. \tag{4.24}$$

On peut prouver de manière analogue que $\varrho_1' \varrho_2' = \varrho$. En conséquence de (4. 22) et (4. 23) on peut écrire (4. 21) sous la forme

$$f_1(x) f_2(x) - \alpha = \pi_1(x)\pi_2(x) = \{f_1(x) + \varphi_1(x)\}\{f_2(x) + \varphi_2'(x)\},$$

c'est-à-dire

$$-\alpha = f_1(x)\varphi_2'(x) + f_2(x)\varphi_1(x) + \varphi_1(x)\varphi_2'(x). \tag{4.25}$$

Mais les racines, et par conséquent aussi les coefficients de $f_1(x)$ et de $f_2(x)$ sont réelles. Donc, en prenant le conjugué complexe de (4. 25), on obtient

$$-\varrho\alpha = \varrho_2' f_1(x)\varphi_2'(x) + \varrho_1 f_2(x)\varphi_1(x) + \varrho_1 \varrho_2' \varphi_1(x)\varphi_2'(x). \tag{4.26}$$

En multipliant (4. 25) par ϱ_2' et en prenant la différence de ce produit et de (4. 26) on a

$$\varphi_1(x) | \alpha\varrho - \alpha\varrho_2' = \alpha\varrho_2'(\varrho_1' - 1). \tag{4.27}$$

Supposons que $\alpha\varrho_2'(\varrho_1' - 1) = 0$, c'est-à-dire $\varrho_1' = 1$ ou $\varrho_2' = 0$. Ici $\varrho_2' = 0$ est évidemment impossible. Si $\varrho_1' = 1$, alors on a $\varrho_2' = \varrho$. Dans ce cas, en multipliant (4. 25) par ϱ et en divisant la différence de ce produit et de (4. 26) par $\varphi_1(x) \neq 0$, on déduit

$$0 = (\varrho - \varrho_1) f_2(x) + \varrho(1 - \varrho_1)\varphi_2'(x).$$

Mais $\deg f_2 = m'$ et $\deg \varphi_2' \leqq m' - 1$, d'où il résulte $\varrho_1 = \varrho = \varrho_1 \varrho_2$, de plus, de l'égalité obtenue on déduit $1 - \varrho_1 = 0$, ce qui entraîne $\varrho = 1$ et $\bar{\alpha} = \alpha$ d'après (4. 24). C'est une contradiction d'après l'hypothèse concernant $g(x)$.

Donc, $\alpha\varrho_2'(\varrho_1' - 1) \neq 0$ et par conséquent $\varphi_1(x) = \varphi_1 \neq 0$ est un entier dans L. Ainsi, dans (4. 25) $\varphi_2'(x)$ est également une constante, car dans le cas contraire le degré du côte droit de (4. 25) serait au moins $m' + 1$. On en déduit que $\varphi_2'(x) = \varphi_2' \neq 0$ est également un entier dans L. On peut démontrer de la même façon que $\varphi_1'(x) = \varphi_1' \neq 0$, $\varphi_2(x) = \varphi_2 \neq 0$ sont des entiers dans L.

De (4. 22) et (4. 23) on conclut

$$f_1(x)-f_2(x)=\varphi_1'-\varphi_1=\varphi_2'-\varphi_2, \tag{4.28}$$

d'où, en éliminant $f_1(x)$ et en le substituant dans (4. 25), nous obtenons

$$-(\alpha+\varphi_1'\varphi_2')=(\varphi_1+\varphi_2')f_2(x).$$

Il en résulte $\alpha+\varphi_1'\varphi_2'=0$ et $\varphi_1+\varphi_2'=0$, c'est-à-dire $\varphi_2'=-\varphi_1$. Par suite de (4. 28) on en déduit $\varphi_1'=-\varphi_2$ et

$$f_2(x)-f_1(x)=\varphi_1+\varphi_2, \quad \alpha=-\varphi_1\varphi_2. \tag{4.29}$$

Vu que $f_1(x)$ et $f_2(x)$ sont des polynômes à coefficients réels, $\varphi_1+\varphi_2$ est réel et ainsi φ_1, φ_2 sont des entiers non réels dans L. De plus, $\varphi_2/\varphi_1=\eta$ est non réel, parce que dans le cas contraire on aurait $\varphi_1+\varphi_2=\varphi_1(1+\eta)=\bar{\varphi}_1(1+\eta)$ et $\eta=-1$, c'est-à-dire $\varphi_1+\varphi_2=0$ et $f_1(x)=f_2(x)$, ce qui est impossible.

Nous allons démontrer que $\varphi_1+\varphi_2$ est une unité dans K, en supposant que l'on a encore $m>2(2G)^{n_k}=c_9(G, n_k)$, c'est-à-dire $c_9\geqq 2\{2g^{1/n}(0)\}^{n_k}$. En effet, si $\varphi_1+\varphi_2$ n'est pas une unité dans K, alors pour un idéal premier P de K on a $P^l\|\varphi_1+\varphi_2$, c'est-à-dire $N(P^l)\leqq|N_{K/Q}(\varphi_1+\varphi_2)|$ avec un entier rationnel $l\geqq 1$. Dans ce cas d'après le lemme 3 on obtient

$$\begin{aligned}\{N(P^l)\}^{[L:K]} &\leqq N_{L/Q}(\varphi_1+\varphi_2)\leqq 2^{[L:Q]}N_{L/Q}(\varphi_1\varphi_2)= \\ &=2^{[L:Q]}N_{L/Q}(\alpha)=2^{[L:Q]}\{g(0)\}^{[L:Q]/n}<(\tfrac{1}{2}c_9)^{[L:K]}; \qquad (n=\deg g).\end{aligned} \tag{4.30}$$

Il y a une classe résiduaire (mod P) dans laquelle se trouvent au moins $m'/N(P)$ éléments parmi les nombres $\alpha_1, \ldots, \alpha_{m'}$; soient ces éléments par exemple $\alpha_1, \ldots, \alpha_{m''}$ $(m''\geqq m'/N(P))$. Considérons maintenant l'égalité (4. 29) (mod P). Alors nous obtenons

$$(x-\alpha_1)^{m''}(x-\alpha_{m''+1})\ldots(x-\alpha_{m'})\equiv(x-\alpha_1')\ldots(x-\alpha_{m'}') \pmod{P}$$

Mais la décomposition des polynômes en facteurs irréductibles (mod P) est unique, par conséquent on peut écrire, par exemple, $\alpha_1'\equiv\cdots\equiv\alpha_{m''}'\equiv\alpha_1 \pmod{P}$. De (4. 29) on déduit

$$\prod_{i=1}^{m'}(\alpha_1-\alpha_i')=\varphi_1+\varphi_2,$$

d'où $P^{m''}|\varphi_1+\varphi_2$ et $m''\leqq l$. D'autre part, en conséquence de notre hypothèse et de (4. 30) on a

$$m>c_9\geqq 2N^l(P)\geqq 2lN(P),$$

c'est-à-dire

$$m''\geqq\frac{m'}{N(P)}=\frac{m}{2N(P)}>l$$

et c'est une contradiction. Donc, si $m>c_8, c_9$, alors de (4. 29) on obtient

$$f_2(x)-f_1(x)=(x-\alpha_1')\ldots(x-\alpha_{m'}')-(x-\alpha_1)\ldots(x-\alpha_{m'})=\varepsilon \tag{4.31}$$

avec une unité $\varepsilon\in K$ réelle.

Enfin, nous montrerons que $\varepsilon=\pm 1$, $f_1(x)$ et $f_2(x)\in Z[x]$ et α est de la forme (2. 2). Désignons par $S_i(f_1)$, $S_i(f_2)$ et $S_i(f_1f_2)$ la i-ième function symétrique élé-

mentaire des racines de f_1, f_2 et $f_1 f_2$ respectivement ($i=1, 2, \ldots$) et soit $S_0(f_1)=$ $=S_0(f_2)=1$. Alors on a

$$S_i(f_1 f_2) = \sum_{k=0}^{i} S_{i-k}(f_1) S_k(f_2) \qquad (i=1, \ldots, m'). \tag{4.32}$$

D'après $f(x)=f_1(x)f_2(x)\in Z[x]$ on déduit $S_i(f_1 f_2)\in Z$ ($i=1, \ldots, 2m'$). De plus, en conséquence de la rélation qui existe entre les racines et les coefficients, de (4. 31) on déduit

$$S_i(f_1) = S_i(f_2) \qquad (i=1, \ldots, m'-1) \tag{4.33}$$

et

$$S_{m'}(f_2) = S_{m'}(f_1) \pm \varepsilon.$$

Ainsi dans le cas $i=1$ de (4. 32) et de (4. 33) on conclut $S_1(f_1 f_2)=2S_1(f_1)$, c'est-à-dire $S_1(f_1)\in Q$. Mais $S_1(f_1)$ est un entier dans K, ainsi on a nécessairement $S_1(f_1)=$ $=S_1(f_2)\in Z$. Supposons que pour $k=1, \ldots, i-1$ ($i \leqq m'-1$) on a $S_k(f_1)=$ $=S_k(f_2)\in Z$. Alors, d'après (4. 32)

$$S_i(f_1 f_2) - \sum_{k=1}^{i-1} S_{i-k}(f_1) S_k(f_2) = S_i(f_1) + S_i(f_2) = 2S_i(f_1),$$

d'où $2S_i(f_1)\in Z$, par conséquent $S_i(f_1)=S_i(f_2)\in Q$. D'autre part, ces nombres sont entiers dans K, ainsi $S_i(f_1)=S_i(f_2)\in Z$. De (4. 32) on déduit de la même façon

$$S_{m'}(f_1) + S_{m'}(f_2) = S_{m'}(f_1 f_2) - \sum_{k=1}^{m'-1} S_{m'-k}(f_1) S_k(f_2) = u, \tag{4.34}$$

u étant un nombre entier rationnel. De plus, d'après

$$S_{m'}(f_1) S_{m'}(f_2) = S_{2m'}(f_1 f_2) = v \tag{4.35}$$

on a $v=S_{m'}(f_1)S_{m'}(f_2)\in Z$. Il en résulte que $S_{m'}(f_1)$ et $S_{m'}(f_2)$ sont des racines de l'équation

$$t^2 - ut + v = 0,$$

d'où

$$S_{m'}(f_2) = \frac{u \pm \sqrt{u^2-4v}}{2} \tag{4.36}$$

et

$$S_{m'}(f_1) = \frac{u \mp \sqrt{u^2-4v}}{2},$$

c'est-à-dire

$$\pm\varepsilon = S_{m'}(f_2) - S_{m'}(f_1) = \pm\sqrt{u^2-4v}.$$

Vu que ε est une unité réelle dans K, on déduit $u^2-4v > 0$. D'autre part, dans le cas $u^2-4v > 1$ on obtiendrait

$$|N_{K/Q}(\varepsilon)| = \left|N_{K/Q}\left(\pm\sqrt{u^2-4v}\right)\right| > 1,$$

ce qui est impossible (ε étant une unité). Ainsi, en conséquence de $u, v\in Z$ on a nécessairement $u^2-4v = 1$, $\varepsilon=\pm 1$ et $u\equiv 1 \pmod 2$. Donc, de (4. 36) il résulte que $S_{m'}(f_1)$, $S_{m'}(f_2)\in Z$ et on en déduit $f_1(x), f_2(x)\in Z[x]$, car $f_1(x)$ et $f_2(x)$ sont des

polynômes normés. De plus, d'après $\varphi_1+\varphi_2=\varepsilon=\pm 1$ et (4. 22) on a $\varphi_1=\pi_1(x)-f_1(x)\in Q(\alpha)$ et $\varphi_2\in Q(\alpha)$, tandis que de (4. 29) on déduit $\alpha=-\varphi_1(\pm 1-\varphi_1)=\varphi_1(\varphi_1\mp 1)$ et enfin $\alpha=\varphi(\varphi-1)$, en choisissant $\varphi=\varphi_1$ ou $\varphi=-\varphi_1$.

Donc, si $m>c_8$, c_9 et $g(f(x))$ est réductible, alors α est, en effet, de la forme (2. 2) et $f(x)$ peut s'écrire sous la forme $f(x)=f_1(x)f_2(x)$ avec des polynômes $f_1(x)$, $f_2(x)$ à coefficients entiers rationnels tels que $f_2(x)-f_1(x)=\pm 1$, ce qui prouve notre assertion.

DÉMONSTRATION *du théorème 1b*. Désignons par $c(D_k, G)$ la constante $c(2, D_k, G)$ obtenue dans le théorème 1a. Si $f(x)$ et $g(x)$ satisfont aux conditions du théorème 1b, alors, d'après le théorème 1a, en cas de $m=\deg f>c(D_k, G)$ $g(f(x))$ est irréductible sur Q ou bien $f(x)$ est de la forme (2. 1) et les racines de $g(x)$ satisfont à (2. 2). Nous allons montrer que dans ce cas il n'y a pas de polynômes exceptionnels $f(x)$ de la forme (2. 1) de degré «grand». Dans le cas contraire on pourrait écrire $f(x)=f_1(x)f_2(x)$ et

$$f_2(x)-f_1(x)=p_{21}(x)\dots p_{2s}(x)-p_{11}(x)\dots p_{1r}(x)=1, \tag{4. 37}$$

$p_{ij}(x)\in Z[x]$ étant des polynômes normés de degré $\leqq 2$. Alors, dans cette décomposition de $f_1(x)$ et $f_2(x)$ il y a tout au plus quatre polynômes $p(x)$ linéaires. En effet, si l'on a, par exemple $p_{2i}(x)=x-a_i'$ $(i=1, \dots, 5)$, alors $|p_{11}(a_i')|=1$ pour cinq entiers rationnels a_i', ce qui est impossible. Donc, en cas de $m>44$, $f_1(x)$ a un diviseur irréductible du deuxième degré, par ex. $p_{11}(x)=(x-\alpha^{(1)})(x-\alpha^{(2)})$ et $f_2(x)$ a au moins neuf diviseurs irréductibles du deuxième degré, par ex. $p_{2i}(x)=(x-\alpha_i^{(1)})(x-\alpha_i^{(2)})$ $(1\leqq i\leqq 9)$. De (4. 37) il résulte

$$N_{K/Q}(\alpha_i^{(1)}-\alpha^{(1)}),\ N_{K/Q}(\alpha_i^{(1)}-\alpha^{(2)})=\pm 1.$$

Par conséquent, il y a au moins trois i différents, par exemple $i=1, 2, 3$, pour lesquels du coté droit des égalités suivantes se trouve le même signe, par ex. $+$ et $-$, c'est-à-dire

$$N_{K/Q}(\alpha_i^{(1)}-\alpha^{(1)})=(\alpha_i^{(1)}-\alpha^{(1)})(\alpha_i^{(2)}-\alpha^{(2)})=1,$$

$$N_{K/Q}(\alpha_i^{(1)}-\alpha^{(2)})=(\alpha_i^{(1)}-\alpha^{(2)})(\alpha_i^{(2)}-\alpha^{(1)})=-1.$$

Mais ce système d'équations n'admet au plus que deux solutions $(\alpha_i^{(1)}, \alpha_i^{(2)})$ en nombres complexes, ce qui entraîne une contradiction. Donc, en cas de $m>44$ il n'y a pas de polynômes $f(x)$ exceptionnels de la forme (2. 1) et, d'après le théorème 1a, de $m=\deg f>\max(c(D_k, G), 44)=c_1(D_k, G)$ il résulte l'irréductibilité de $g(f(x))$ sur Q.

Dans la suite il suffit donc de considérer le cas où $m=\deg f\leqq c_1$. Alors $f(x)$ peut s'écrire sous la forme

$$f(x)=\prod_{j=1}^{k}(x-a_j)\prod_{i=1}^{l}p_i(x)=\prod_{j=1}^{k}(x-a_j)\prod_{i=1}^{l}(x-\alpha_i^{(1)})(x-\alpha_i^{(2)}) \tag{4. 38}$$

avec des entiers rationnels différents a_j et avec des polynômes normés $p(x)\in Z[x]$ du deuxième degré et irréductibles sur Q dont les racines $\alpha_i^{(1)}$, $\alpha_i^{(2)}$ appartiennent à K (et naturellement on a $k+2l=m\leqq c_1(D_k, G)$). Nous montrerons qu'il y a une constante $c_2(D_k, G)$ calculable explicitement telle que $\|f^*\|\leqq c_2(D_k, G)$ pour un polynôme $f^*(x)$ équivalent à $f(x)$, en supposant que $g(f(x))$ est réductible sur Q

pour un $g(x)\in P(G)$ (sauf pour certains $g(x)$ et certains $f(x)$ du quatrième degré que nous allons déterminer dans la suite).

Dans le cas $l=0$ cette proposition s'obtient immédiatement du théorème 1c avec une constante c_2 calculable explicitement et dépendant seulement de G.

Dans la suite nous nous occuperons du cas $l>0$. D'abord nous représentons les racines des diviseurs irréductibles $p_i(x)$ de $f(x)$ sous la forme la plus favorable. Désignons simplément par d le discriminant D_k de K. Alors $K=Q(\sqrt{d})$, d étant positif. 1 et w forment une base des entiers de K, où

$$w=\begin{cases}\dfrac{\sqrt{d}}{2}, & \text{si } d\equiv 0 \pmod 4,\\[2ex] \dfrac{1+\sqrt{d}}{2}, & \text{si } d\equiv 1 \pmod 4.\end{cases}$$

Si maintenant $\alpha=u+vw$ $(u, v\in Z)$ est un entier arbitraire dans K, alors en appliquant la substitution $x=u$, $y=\dfrac{v}{2}$ (premier cas) ou $x=u+\dfrac{v}{2}$, $y=\dfrac{v}{2}$ (second cas), on peut écrire $\alpha=x+y\sqrt{d}$, où $x, 2y\in Z$ (premier cas), $x-y, 2y\in Z$ (second cas). On en déduit que dans (4. 38) $\alpha_i^{(1)}$ et $\alpha_i^{(2)}$ peuvent être représentés sous la forme

$$\alpha_i^{(1)}=x_i+y_i\sqrt{d},\quad \alpha_i^{(2)}=x_i-y_i\sqrt{d},\qquad y_i\neq 0, \tag{4.39}$$

où donc $x_i, 2y_i\in Z$ et $x_i-y_i, 2y_i\in Z$ respectivement $(i=1, \ldots, l)$.

D'abord considérons le cas $k=0$, c'est-à-dire prenons tous les polynômes $f(x)$ de la forme (4. 38) à propriété précédente et n'ayant pas de racines entières rationnelles. Représentons les racines des $f(x)$ sous la forme (4. 39) et désignons par $\mathcal{G}(f, G)=\mathcal{G}(f)$ le graphe des couples $(\alpha_i^{(j)}, \alpha_k^{(j')})$ $(j, j'=1, 2;\ 1\leqq i, k\leqq l)$ satisfaisant à

$$|N_{K/Q}(\alpha_i^{(j)}-\alpha_k^{(j')})|>(2G^2)^2. \tag{4.40}$$

Nous allons démontrer que $\mathcal{G}(f)$ est connexe pour chaque $f(x)$ excepté peut être lorsque $\max\limits_i |y_i|\leqq c''$ et (pour $l>1$) $\max\limits_{i,k} |x_i-x_k|\leqq c'$, c'est-à-dire lorsque $\|f^*\|\leqq c'''$ pour un $f^*(x)$ équivalent à $f(x)$, $c'=c'(d, G)$, $c''=c''(d, G)$ et $c'''=c'''(d, G)$ étant des constantes calculables explicitement et dépendant seulement de d et G. Ces polynômes, nous les appelons exceptionnels. Si maintenant $f(x)$ n'est pas exceptionnel, c'est-à-dire si $\mathcal{G}(f)$ est connexe, alors d'après le lemme 9 $g(f(x))$ est irréductible sur Q pour tout $g(x)\in P(G)$ et notre proposition (dans le cas $k=0$) est démontrée.

Prenons d'abord le cas $l=1$. En cas de $|N_{K/Q}(\alpha_1^{(1)}-\alpha_1^{(2)})|=|N_{K/Q}(2y_1\sqrt{d})|=4dy_1^2>(2G^2)^2$ $\mathcal{G}(f)$ est connexe. D'autre part, si $|y_1|\leqq G^2/\sqrt{d}$, alors il y a un polynôme f^* équivalent à f pour lequel $\|f^*\|\leqq c^*(G, d)$ avec une constante c^* calculable explicitement.

Considérons ensuite le cas $l>1$. Soit $f(x)$ représenté de nouveau sous la forme

$$f(x)=\prod_{i=1}^{l}(x-\alpha_i^{(1)})(x-\alpha_i^{(2)}) \tag{4.41}$$

et considérons les représentations de forme (4. 39) des $\alpha_i^{(1)}$, $\alpha_i^{(2)}$. Supposons que pour un $1 \leqq j \leqq l$

$$|y_j| > c'' = \max\left\{\frac{(2G^2)^2}{d}, \frac{G^2}{\sqrt{d}}\right\}. \tag{4.42}$$

Pour tout $i \neq j$ prenons

$$N_{K/Q}(\alpha_j^{(1)} - \alpha_j^{(2)}) = N_{K/Q}(2y_j\sqrt{d}) = 4dy_j^2, \tag{4.43}$$

$$N_{K/Q}(\alpha_i^{(1)} - \alpha_j^{(1)}) = N_{K/Q}(\alpha_i^{(2)} - \alpha_j^{(2)}) = (x_i - x_j)^2 - d(y_i - y_j)^2 \tag{4.44}$$

et

$$N_{K/Q}(\alpha_i^{(1)} - \alpha_j^{(2)}) = N_{K/Q}(\alpha_i^{(2)} - \alpha_j^{(1)}) = (x_i - x_j)^2 - d(y_i + y_j)^2. \tag{4.45}$$

De (4. 42) et (4. 43) il résulte $(\alpha_j^{(1)}, \alpha_j^{(2)}) \in \mathcal{G}(f)$. De plus, pour tout $i \neq j$ la valeur absolue de (4. 44) ou de (4. 45) est $> (2G^2)^2$, c'est-à-dire $(\alpha_i^{(1)}, \alpha_j^{(1)})$ et $(\alpha_i^{(2)}, \alpha_j^{(2)})$ ou $(\alpha_i^{(1)}, \alpha_j^{(2)})$ et $(\alpha_i^{(2)}, \alpha_j^{(1)}) \in \mathcal{G}(f)$, parce que dans le cas contraire pour la valeur absolue de la différence de (4. 44) et (4. 45) on obtiendrait $|2dy_j| \leqq |4dy_iy_j| \leqq 2(2G^2)^2$, ce qui est impossible d'après (4. 42). Par conséquent, de (4. 42) on déduit que $\mathcal{G}(f)$ est connexe.

Ensuite supposons que $\max\limits_{1 \leqq i \leqq l} |y_i| \leqq c''$, mais $\max\limits_{i,k} |x_i - x_k| > c' = 2\sqrt{4dc''^2 + (2G^2)^2}$.

On peut supposer que $x_1 \leqq \cdots \leqq x_l$ et, pour tout $1 \leqq i \leqq l$, $x_l - x_i$ ou $x_i - x_1 \geqq \frac{x_l - x_1}{2} > c'/2 > \sqrt{4dc''^2 + (2G^2)^2}$. Si par exemple $x_i - x_1 > c'/2$, alors en prenant $j = 1$, le côté droit de (4. 44) et de (4. 45) est $> (2G^2)^2$, par conséquent $(\alpha_i^{(1)}, \alpha_1^{(1)})$, $(\alpha_i^{(2)}, \alpha_1^{(2)})$, $(\alpha_i^{(1)}, \alpha_1^{(2)})$ et $(\alpha_i^{(2)}, \alpha_1^{(1)}) \in \mathcal{G}(f)$, c'est-à-dire le sous-graphe formé de $\alpha_1^{(1)}$, $\alpha_1^{(2)}$, $\alpha_i^{(1)}$, $\alpha_i^{(2)}$ est connexe. On peut montrer de la même façon que le sous graphe formé de $\alpha_1^{(1)}$, $\alpha_1^{(2)}$, $\alpha_l^{(1)}$, $\alpha_l^{(2)}$ est également connexe. Vu que pour tout i le graphe formé des sommets $\alpha_i^{(1)}$, $\alpha_i^{(2)}$, $\alpha_1^{(1)}$, $\alpha_1^{(2)}$ ou $\alpha_i^{(1)}$, $\alpha_i^{(2)}$, $\alpha_l^{(1)}$, $\alpha_l^{(2)}$ est connexe, $\mathcal{G}(f)$ est également connexe. Enfin, si $\max\limits_{1 \leqq i \leqq l} |y_i| \leqq c''$ et $\max\limits_{i,k} |x_i - x_k| \leqq c'$, alors f est équivalent à un polynôme f^* tel que $\|f^*\| \leqq c'''(d, G)$, c''' étant une constante calculable explicitement.

Soit ensuite $m \leqq c_1$ un nombre naturel et prenons une couple l, k, où l et k sont des nombres naturels tels que $2l + k = m$. Le nombre de ces couples l, k est $\leqq c_1$. Donc, il suffit de démontrer que si pour une couple l, k fixé et pour un polynôme normé $f(x) \in Z[x]$ de la forme (4. 38) le graphe $\mathcal{G}(f)$ ne contient aucun sous-graphe ayant plus de $\frac{\deg f}{2}$ sommets, alors il y a un polynôme $f^*(x)$ équivalent à $f(x)$ tel que $\|f^*\| \leqq c_2(D_k, G)$ (sauf les exceptions obtenues dans le cas $l = 1$, $k = 2$), où c_2 est une constante calculable explicitement. En conséquence du lemme 9 il en résultera l'irréductibilité de $g(f(x))$ pour tout $g(x) \in P(G)$, sauf peut être dans le cas où $\|f^*\| \leqq c_2(D_k, G)$ pour un polynôme $f^*(x)$ équivalent à $f(x)$.

Dans la représentation $f(x)$ de la forme (4. 38) soit

$$f_1(x) = \prod_{i=1}^{t} (x - \alpha_i^{(1)})(x - \alpha_i^{(2)}) \quad \text{et} \quad f_2(x) = \prod_{j=1}^{k} (x - a_j).$$

Désignons par $\mathcal{G}(f_1)$, $\mathcal{G}(f_2)$ et $\mathcal{G}(f)$ les graphes formés à la base de l'inégalité (4. 40) des racines de $f_1(x)$, $f_2(x)$ et de $f(x)$ respectivement. Soient $\alpha_i^{(1)}$, $\alpha_i^{(2)}$ de la forme (4. 39) aussi dans ce qui suit.

Dans la suite nous allons distinguer de nouveau plusieurs cas. Les racines de $f_2(x)$ soient arrangées de telle manière que $a_1 < \cdots < a_k$ $(k \geqq 1)$.

D'abord considérons le cas $k=1$. Si $\max\limits_{1 \leqq i \leqq l} |y_i| > c''$ ou bien (pour $l>1$) $\max\limits_{i,k} |x_i - x_k| > c'$ avec les constantes introduites dans le cas $k=0$, alors $\mathscr{G}(f_1)$ est connexe. Mais dans ce cas le graphe $\mathscr{G}(f)$, ayant $2l+1$ sommets, contient un sous-graphe ayant plus de $\frac{2l+1}{2} = \frac{m}{2}$ sommets, notamment le graphe $\mathscr{G}(f_1)$. D'autre part, si $\max\limits_{1 \leqq i \leqq l} |y_i| \leqq c''$ et (pour $l>1$) $\max\limits_{i,j} |x_i - x_j| \leqq c'$, mais $\max\limits_{i} |x_i - a_1| > \sqrt{dc''^2 + (2G^2)^2} + c'$, alors on a

$$|x_j - a_1| = |(x_i - a_1) - (x_i - x_j)| \geqq |x_i - a_1| - |x_i - x_j| > \tag{4.46}$$

$$> \left(\sqrt{dc''^2 + (2G^2)^2} + c'\right) - c' = \sqrt{dc''^2 + (2G^2)^2} = \bar{c}$$

pour tout $1 \leqq j \leqq l$. Ainsi d'après $(x_j - a_1)^2 > dc''^2 + (2G^2)^2 \geqq dy_j^2 + (2G^2)^2$ on déduit

$$|N_{K/Q}(\alpha_j^{(1)} - a_1)| = |N_{K/Q}(\alpha_j^{(2)} - a_1)| = |(x_j - a_1)^2 - dy_j^2| > (2G^2)^2 \tag{4.47}$$

pour tout $1 \leqq j \leqq l$. Donc, $(\alpha_j^{(1)}, a_1)$ et $(\alpha_j^{(2)}, a_1) \in \mathscr{G}(f)$ et il en résulte que $\mathscr{G}(f)$ est connexe. Enfin, si l'on a même $\max\limits_{i} |x_i - a_1| \leqq \bar{c} + c'$, alors on peut obtenir un f^* équivalent à f (par exemple en choisissant $a_1 = 0$) tel que $\| f^* \| \leqq c_2'$ avec une constante c_2' calculable explicitement et dépendant seulement de G et de d.

Ensuite soit $k \geqq 2$ et $a_k - a_1 \leqq 4(2G^2)^2$. Nous allons distinguer plusieurs cas.

a) D'abord supposons que (pour $l>1$) $\max\limits_{i,k} |x_i - x_k| \leqq \bar{c}' = \max(c', 13(2G^2)^2 + 1)$ et $\max\limits_{1 \leqq i \leqq l} |y_i| \leqq \bar{c}'' = \max(c'', 4\bar{c}')$ avec les constantes obtenues dans le cas $k=0$. On peut évidemment supposer que $|x_1| \leqq \frac{1}{2}$. Si maintenant $|a_1| > 2(\bar{c}' + d\bar{c}''^2 + 3(2G^2)^2 + 1)$, alors d'après $|a_j| + |a_1 - a_j| \geqq |a_1|$ on a $|a_j| \geqq |a_1| - |a_1 - a_j| > 2(\bar{c}' + d\bar{c}''^2 + (2G^2)^2 + 1)$ pour tout j et

$$|N_{K/Q}(\alpha_i^{(1)} - a_j)| = |N_{K/Q}(\alpha_i^{(2)} - a_j)| = |(x_i - a_j)^2 - dy_i^2| \geqq$$

$$\geqq \frac{1}{2}|a_j - x_i| - dy_i^2 \geqq \frac{1}{2}|a_j| - |x_i| - dy_i^2 \geqq \frac{1}{2}|a_j| - \bar{c}' - d\bar{c}''^2 - 1 > (2G^2)^2.$$

Par conséquent, $(\alpha_i^{(1)}, a_j)$, $(\alpha_i^{(2)}, a_j) \in \mathscr{G}(f)$ pour tout i et j, c'est-à-dire $\mathscr{G}(f)$ est connexe. Si l'on a même $|a_1| \leqq 2(\bar{c}' + d\bar{c}''^2 + 3(2G^2)^2 + 1)$, alors d'après $a_j - a_1 \leqq a_k - a_1 \leqq 4(2G^2)^2$ on a $|a_j| \leqq 2(\bar{c}' + d\bar{c}''^2 + 5(2G^2)^2 + 1)$ pour tout j. On en déduit qu'on peut donner pour $\| f \|$ une borne supérieure calculable explicitement et dépendant seulement de G et de d.

b) Si $\max\limits_{1 \leqq i \leqq l} |y_i| > \bar{c}''$ ou (pour $l>1$) $\max\limits_{i,k} |x_i - x_k| > \bar{c}'$, alors en conséquence de la première partie de notre démonstration (cas $k=0$), et d'après $\bar{c}' \geqq c'$, $\bar{c}'' \geqq c''$, $\mathscr{G}(f_1)$ est connexe.

Supposons d'abord que $l>1$ et $|x_i - x_{i'}| > \bar{c}'$ pour une couple $x_i, x_{i'}$. En choisissant $|x_{i'}| \leqq \frac{1}{2}$, $\mathscr{G}(f)$ ne change pas et $|x_i| > \bar{c}' - 1$.

Si maintenat $|a_j| \leqq 8(2G^2)^2$ pour un j, alors d'après $a_h - a_j$, $a_j - a_h \leqq a_k - a_1 \leqq 4(2G^2)^2$ on a $|a_h| \leqq 12(2G^2)^2$ pour tout h et ainsi $|a_s + a_h| \leqq 24(2G^2)^2$ pour tout

couple s, h $(s \neq h)$. Ici $(\alpha_i^{(1)}, a_s)$ et $(\alpha_i^{(2)}, a_s)$ ou bien $(\alpha_i^{(1)}, a_h)$ et $(\alpha_i^{(2)}, a_h) \in \mathcal{G}(f)$, parce que dans le cas contraire la valeur absolue de

$$N_{K/Q}(\alpha_i^{(1)} - a_s) = N_{K/Q}(\alpha_i^{(2)} - a_s) = (x_i - a_s)^2 - dy_i^2 \tag{4.48}$$

et de

$$N_{K/Q}(\alpha_i^{(1)} - a_h) = N_{K/Q}(\alpha_i^{(2)} - a_h) = (x_i - a_h)^2 - dy_i^2 \tag{4.49}$$

serait $\leqq (2G^2)^2$, c'est-à-dire pour leur différence on obtiendrait

$$2(2G^2)^2 \leqq 2\bar{c}' - 2 - 24(2G^2)^2 < |2x_i| - |a_s + a_h| \leqq |a_s - a_h|\,|a_s + a_h - 2x_i| \leqq 2(2G^2)^2,$$

ce qui est impossible. Donc, en considérant les couples (a_1, a_2), (a_3, a_4), ... le nombre de ces couples est $\geqq \frac{k-1}{2}$ et il y a dans toutes les couples au moins un élément a_s tel que $(\alpha_i^{(1)}, a_s), (\alpha_i^{(2)}, a_s) \in \mathcal{G}(f)$. Vu que $\mathcal{G}(f_1)$ est connexe, il en résulte que $\mathcal{G}(f)$ a un sous-graphe connexe ayant au moins $2l + \frac{k-1}{2}$ sommets, où $2l + \frac{k-1}{2} > \frac{2l+k}{2} = \frac{m}{2}$.

D'autre part, si $|a_j| > 8(2G^2)^2$ pour tout $1 \leqq j \leqq k$, alors d'après $a_k - a_1 \leqq 4(2G^2)^2$ les a_j ont le même signe, c'est-à-dire $|a_s + a_h| > 16(2G^2)^2$ pour tout couple a_s, a_h $(s \neq h)$. De plus, si (a_s, a_h) est une couple arbitraire, alors par exemple $(a_s, \alpha_{i'}^{(1)})$, $(a_s, \alpha_{i'}^{(2)}) \in \mathcal{G}(f)$. En effet, dans le cas contraire en remplaçant i par i' dans (4. 48) et (4. 49) la valeur de ces nombres serait $\leqq (2G^2)^2$ et pour leur différence on obtiendrait

$$16(2G^2)^2 - 1 \leqq |a_s + a_h| - |2x_{i'}| \leqq |a_s - a_h|\,|a_s + a_h - 2x_{i'}| \leqq 2(2G^2)^2,$$

ce qui entraîne une contradiction. Donc, $\mathcal{G}(f)$ a un sous-graphe connexe ayant au moins $2l + \frac{k-1}{2}$ sommets, où $2l + \frac{k-1}{2} > \frac{m}{2}$.

Ensuite supposons qu'en plus des hypothèses originaires on a $|y_i| > \bar{c}''$ pour un i et (pour $l > 1$) $\max\limits_{i,k} |x_i - x_k| \leqq \bar{c}'$, c'est-à-dire, par exemple, $|x_1| \leqq \frac{1}{2}$ et $\max\limits_{1 \leqq j \leqq l} |x_j| \leqq \bar{c}' + 1$. Si pour tout $1 \leqq h \leqq k$ on a $(\alpha_i^{(1)}, a_h)$ et $(\alpha_i^{(2)}, a_h) \in \mathcal{G}(f)$, alors $\mathcal{G}(f_1)$ étant connexe, $\mathcal{G}(f)$ est également connexe. Dans le cas contraire, si pour un h on a $(\alpha_i^{(1)}, a_h)$ et $(\alpha_i^{(2)}, a_h) \notin \mathcal{G}(f)$, c'est-à-dire

$$|N_{K/Q}(\alpha_i^{(1)} - a_h)| = |N_{K/Q}(\alpha_i^{(2)} - a_h)| = |(x_i - a_h)^2 - dy_i^2| \leqq (2G^2)^2,$$

alors d'après $(2G^2)^2 \leqq (d-1)\bar{c}''^2 < (d-1)y_i^2$ on déduit

$$\bar{c}'' < |y_i| \leqq \sqrt{dy_i^2 - (2G^2)^2} \leqq |x_i - a_h| \leqq |x_i| + |a_h|,$$

d'où

$$|a_h| > \bar{c}'' - |x_i| \geqq \bar{c}'' - \bar{c}' - 1 \geqq \frac{3}{4}\bar{c}'' - 1.$$

Mais d'après $a_k - a_1 \leqq 4(2G^2)^2$ les signes des a_s sont égaux et, en conséquence de $4(2G^2)^2 \geqq |a_h - a_s| \geqq |a_h| - |a_s|$, c'est-à-dire de $|a_s| \geqq |a_h| - 4(2G^2)^2 \geqq \frac{3}{4}\bar{c}'' - 1 -$

$-\frac{\bar{c}''-4}{13} > \frac{3}{8}\bar{c}''$, on obtient $|a_s+a_h| > \frac{3}{4}\bar{c}''$ pour tout s. Ainsi $(\alpha_i^{(1)}, a_s)$ et $(\alpha_i^{(2)}, a_s) \in$ $\in \mathcal{G}(f)$ pour chaque $s \neq h$, parce que dans le cas contraire la valeur absolue de (4. 48) et celle de (4. 49) seraient $\leqq (2G^2)^2$, c'est-à-dire pour leur différence on obtiendrait

$$13(2G^2)^2 - 2 \leqq \frac{1}{4}\bar{c}'' - 2 \leqq \frac{3}{4}\bar{c}'' - 2\bar{c}' - 2 < |a_s+a_h| - |2x_i| \leqq$$

$$\leqq |a_h-a_s|\,|a_h+a_s-2x_i| \leqq 2(2G^2)^2,$$

ce qui est impossible. Donc, $\mathcal{G}(f)$ a un sous-graphe connexe ayant $2l+(k-1) > > \frac{2l+k}{2} = \frac{m}{2}$ sommets.

Enfin, soit $k \geqq 2$ et $a_k - a_1 > 4(2G^2)^2$. Alors $a_k - a_j$ ou $a_j - a_1 > 2(2G^2)^2$ pour tout $1 \leqq j \leqq k$, par conséquent $\mathcal{G}(f_2)$ est connexe.

Soit $1 \leqq i \leqq l$ un indice arbitraire, mais fixé et considérons un indice $1 \leqq s \leqq k$ tel que $a_k + a_s \neq 2x_i$ $(s \neq k)$ ou $a_s + a_1 \neq 2x_i$ $(s \neq 1)$. Dans le cas $k \geqq 3$ il y a un tel s, mais dans le cas $k=2$ il n'y en a pas nécessairement. Si $a_1 + a_k \neq 2x_i$, on peut choisir par exemple $s=1$, et si $a_1 + a_k = 2x_i$ et $k \geqq 3$, on peut prendre $s=2$. Maintenant, en choisissant convenablement l'indice 1 ou k, on peut même assurer $|a_1 - a_s|$ ou $|a_s - a_k| > 2(2G^2)^2$. Donc, pour $h=1$ ou pour $h=k$ on a simultanément $a_h + a_s \neq$ $\neq 2x_i$ et $|a_h - a_s| > 2(2G^2)^2$. On en déduit que, pour ces indices s, h et pour i, la valeur absolue de (4. 48) et de (4. 49) n'est pas simultanément $\leqq (2G^2)^2$, car dans le cas contraire pour la valeur absolue de leur différence on obtiendrait

$$2(2G^2)^2 < |a_h-a_s| \leqq |a_h-a_s| \cdot |a_h+a_s-2x_i| \leqq 2(2G^2)^2,$$

ce qui est impossible. Par conséquent, il y a un sommet de $\mathcal{G}(f_2)$, par exemple a_s, tel que $(\alpha_i^{(1)}, a_s)$, $(\alpha_i^{(2)}, a_s) \in \mathcal{G}(f)$, ce qui est vrai pour tou i dans le cas $k \geqq 3$. Il en résulte que $\mathcal{G}(f)$ est connexe.

Finalement prenons le cas $k=2$ (et $a_2 - a_1 > 4(2G^2)^2$). Si $\max\limits_{1 \leqq i \leqq l} |y_i| \leqq c''$ et (pour $l>1$) $\max\limits_{i,k} |x_i - x_k| \leqq c'$, alors en choisissant par exemple $|x_1| \leqq \frac{1}{2}$, on déduit $\max\limits_{1 \leqq i \leqq l} |x_i| \leqq c' + 1$. D'abord supposons que $|a_1|$ ou $|a_2| > 2(c' + dc''^2 + (2G^2)^2 + 1)$. En prenant par exemple le premier cas, de (4. 47) il résulte que $(\alpha_j^{(1)}, a_1)$ et $(\alpha_j^{(2)}, a_1) \in$ $\in \mathcal{G}(f)$ pour tout j, c'est-à-dire $\mathcal{G}(f)$ est connexe. Ensuite, en supposant que $|a_1|$ et $|a_2| \leqq 2(c' + dc''^2 + (2G^2)^2 + 1)$, on peut donner pour $\|f\|$ une borne supérieure calculable explicitement et dépendant seulement de G et de d.

D'autre part, si l'on a $\max\limits_{1 \leqq i \leqq l} |y_i| > c''$ ou (pour $l>1$) $\max\limits_{i,k} |x_i - x_k| > c'$, alors $\mathcal{G}(f_1)$ est connexe (voir le cas $k=0$) et ainsi dans le cas $l>1$ $\mathcal{G}(f)$ contient un sous-graphe connexe ayant $2l > \frac{2l+2}{2} = \frac{m}{2}$ sommets. Si $l=1$ et $a_1 + a_2 \neq 2x_1$, alors pour l'un des a_i on a $(\alpha_1^{(1)}, a_i)$, $(\alpha_1^{(2)}, a_i) \in \mathcal{G}(f)$ (voir le cas $k \geqq 2$), et par conséquent $\mathcal{G}(f)$ est également connexe.

Enfin, il suffit de considérer le cas où $k=2$, $a_2 - a_1 > 4(2G^2)^2$, $l=1$, $a_1 + a_2 = 2x_1$ (où on peut choisir $2x_1 = 0, \pm 1$) et $|y_1| > c''$. Dans ce cas $a_1 - x_1 = x_1 - a_2$, ainsi

pour $i=1$, $s=1$ et $h=2$ les nombres (4. 48) et (4. 49) sont égaux, c'est-à-dire leurs valeurs absolues sont simultanément $>(2G^2)^2$ ou $\leqq(2G^2)^2$. Dans le premier cas $\mathcal{G}(f)$ est connexe. Quant au deuxième cas, de l'égalité de (4. 48) et de (4. 49) il résulte

$$(a_1-x_1)^2-dy_1^2=(x_1-a_2)^2-dy_1^2=t \tag{4.50}$$

avec un nombre entier rationnel t tel que $0<|t|\leqq(2G^2)^2$. Vu que $f_1(x)=$ $=(x-\alpha_1^{(1)})(x-\alpha_1^{(2)})=x^2-2x_1x+(x_1^2-dy_1^2)$ et $f_2(x)=(x-a_1)(x-a_2)=x^2-$ $-2x_1x+a_1(2x_1-a_1)$, en vertu de (4. 50) on déduit

$$f_1(x)-f_2(x)=t. \tag{4.51}$$

Supposons que pour un $f(x)$ à cette propriété et pour un $g(x)\in P(G)$, $g(f(x))$ est réductible sur Q, c'est-à-dire $f(x)-\alpha$ est réductible sur $Q(\alpha)$, α étant une des racines de $g(x)$ dans le corps des nombres complexes. Alors on peut écrire

$$f(x)-\alpha=\pi_1(x)\pi_2(x) \tag{4.52}$$

avec des polynômes normés $\pi_1(x)$, $\pi_2(x)$ à coefficients entiers de $Q(\alpha)$. Vu que $\mathcal{G}(f_1)$ et $\mathcal{G}(f_2)$ sont connexes, d'après les lemmes 7, 8 et 9 on a nécessairement $\deg\pi_1=\deg\pi_2=2$. Ainsi $\pi_1(x)$ et $\pi_2(x)$ peuvent être représentés sous la forme

$$\pi_1(x)=f_1(x)+\varphi_1(x)=f_2(x)+\varphi_1'(x) \tag{4.53}$$

et

$$\pi_2(x)=f_1(x)+\varphi_2(x)=f_2(x)+\varphi_2'(x) \tag{4.54}$$

avec des polynômes $\varphi_1(x)$, $\varphi_1'(x)$, $\varphi_2(x)$, $\varphi_2'(x)$ à coefficients entiers de $Q(\alpha)$ et de degré $\leqq 1$. Mais (4. 51), (4. 52) et (4. 53) sont de la même forme que (4. 21), (4. 22) et (4. 23). Ainsi, en appliquant le procédé de la démonstration du théorème 1a, on peut prouver que

$$\varphi_1(x)=\varphi_1,\quad \varphi_1'(x)=\varphi_1',\quad \varphi_2(x)=\varphi_2,\quad \varphi_2'(x)=\varphi_2'$$

sont des constantes et $\varphi_1=-\varphi_2'$, $\varphi_2=-\varphi_1'$, $\alpha=-\varphi_1'\varphi_2'$. Par conséquent, de (4. 51) et (4. 53) on déduit

$$t=f_1(x)-f_2(x)=\varphi_1'+\varphi_2', \tag{4.55}$$

et en choisissant $\varphi_1'=\varphi$ ($\varphi\in Q(\alpha)$ est un entier), on a $\alpha=\varphi(\varphi-t)$. Donc, si $g(f(x))$ est réductible sur Q, alors $f_1(x)$ et $f_2(x)$ sont nécessairement de la forme précédente, de plus, on a (4. 50) et on obtient $\alpha=\varphi(\varphi-t)$ pour un entier $\varphi\in Q(\alpha)$ et pour un t entier rationnel tel que $0<|t|\leqq(2G^2)^2$. Mais alors, d'après la Proposition 5, il y a une infinité de polynômes $f(x)$ du quatrième degré et ayant la propriété précédente, pour lesquels $g(f(x))$ est donc réductible sur Q et tous ces $f(x)$ peuvent être représentés par des formules récurrentes. Enfin, $n_0>1$ étant donné, d'après la Proposition 4 il n'existe qu'un nombre fini de polynômes $g(x)\in P(G)$ de degré $\leqq n_0$ tels que pour une racine α de $g(x)$ et pour un $t\in Z$ $(0<|t|\leqq(2G^2)^2)$ $\alpha=\varphi(\varphi-t)$ soit résoluble pour φ en entiers de $Q(\alpha)$ et ces $g(x)$ peuvent être déterminés par un nombre fini d'opérations. Ainsi nous avons caractérisé tous les polynômes normés

$f(x)$, $g(x)$ $(g(x)\in P(G)$; $f(x)\in Z[x]$ ayant des racines différentes dans $K)$ pour lesquels $g(f(x))$ peut être réductible sur Q, et notre théorème est démontré.

DÉMONSTRATION *du théorème 1c.* Soient $a_1<\cdots<a_m$ et supposons que $a_m-a_1>$ $>4G-1$. Dans le cas $m>2$ on a

$$a_m-a_i \quad \text{ou} \quad a_i-a_1 \geqq \frac{a_m-a_1}{2}+\frac{1}{2} > 2G$$

sauf, peut être, pour un $i\,(1<i<m)$. Alors, d'après $a_m-a_1 > 2G$ le graphe des couples (a_i, a_k) satisfaisant à

$$|a_i-a_k| > 2G$$

a un sous-graphe connexe ayant $m-1 > m/2$ sommets. Par conséquent, du lemme 9 il résulte l'irréductibilité de $g(f(x))$ sur Q pour tout $g(x)\in P(G)$.

D'autre part, dans le cas $m=2$ d'après

$$a_2-a_1 > 4G-1 > 2G$$

nous obtenons de nouveau l'irréductibilité de $g(f(x))$ pour tout $g(x)\in P(G)$. Donc, si $g(f(x))$ est réductible sur Q pour un $g(x)\in P(G)$, alors on a nécessairement $a_m-a_1 \leqq$ $\leqq 4G-1$, d'où on obtient $m\leqq 4G$.

Pour la démonstration des théorèmes 2a et 2b nous aurons besoin encore de quelques lemmes.

Lemme 18. *Soit $G\geqq 1$ une constante et soit $f(x)\in Z[x]$ un polynôme normé irréductible sur Q avec des racines réelles et soit α un des racines de $f(x)$. Si le corps $Q(\alpha)$ est primitif, c'est-à-dire, par exemple, si $m=\deg f$ est un nombre premier et*

$$D(f) > (2G)^{m(m-1)}, \tag{4.56}$$

alors $g(f(x))$ est irréductible sur Q pour tout $g(x)\in P(G)$.

Ensuite considérons le cas où $\deg f\leqq 3$.

Lemme 19. *Soit $G\geqq 1$ une constante. Si $f(x)\in Z[x]$ est un polynôme normé de degré $m\leqq 3$ ayant des racines réelles différentes et si*

$$D(f) > (2G)^{m(m-1)}, \tag{4.57}$$

alors $g(f(x))$ est irréductible sur Q pour tout $g(x)\in P(G)$.

DÉMONSTRATION *du lemme 18.* Soient les racines de $f(x)$ $\alpha^{(1)}=\alpha$, $\alpha^{(2)}, \ldots, \alpha^{(m)}$ et soit $K=Q(\alpha^{(1)}, \ldots, \alpha^{(m)})$. En conséquence de l'hypothèse K est réel. De plus, désignons par $\mathcal{G}(f, G)=\mathcal{G}(f)$ le graphe des couples $(\alpha^{(i)}, \alpha^{(k)})$ satisfaisants à

$$|N_{K/Q}(\alpha^{(i)}-\alpha^{(k)})| > (2G)^{[K:Q]}. \tag{4.58}$$

Soient $\{\alpha^{(1)}, \ldots, \alpha^{(s)}\}$ les sommets d'un sous-graphe connexe maximal de $\mathcal{G}(f)$. En conséquence de (4.56) et de

$$D(f) = \prod_{1\leqq i<j\leqq m} (\alpha^{(j)}-\alpha^{(i)})^2$$

on a

$$\prod_{1\leqq i<j\leqq m} N^2_{K/Q}(\alpha^{(j)}-\alpha^{(i)}) = \{D(f)\}^{[K:Q]} > (2G)^{[K:Q]m(m-1)}$$

Il en résulte que pour au moins une couple $j \neq i$

$$|N_{K/Q}(\alpha^{(j)} - \alpha^{(i)})| > (2G)^{[K:Q]},$$

c'est-à-dire $s \geqq 2$. De plus, en dèsignant par Γ le groupe de Galois de $f(x)$, Γ est un sous-groupe du groupe d'automorphismes de $\mathcal{G}(f)$. Par conséquent, $\varphi\{\alpha^{(1)}, \ldots, \alpha^{(s)}\}$ et $\chi\{\alpha^{(1)}, \ldots, \alpha^{(s)}\}$ sont identiques ou bien disjoints pour tout $\varphi, \chi \in \Gamma$. Ainsi on peut écrire $m = t \cdot s$ et il y a des automorphismes $\varphi_1, \ldots, \varphi_t$ tels que $\varphi_1\{\alpha^{(1)}, \ldots, \alpha^{(s)}\}, \ldots, \varphi_t\{\alpha^{(1)}, \ldots, \alpha^{(s)}\}$ soient disjoints deux à deux. Alors tout $\chi \in \Gamma$ permute ces ensembles entre eux. Soient $\beta_1, \ldots, \beta_s$ les fonctions symétriques élémentaires de $\alpha^{(1)}, \ldots, \alpha^{(s)}$ et soit β un élément primitif de $K' = Q(\beta_1, \ldots, \beta_s)$, c'est-à-dire soit $\beta = k(\beta_1, \ldots, \beta_s) = h(\alpha^{(1)}, \ldots, \alpha^{(s)})$ avec des polynômes h, k à coefficients rationnels. Il en résulte que $\beta\chi = h(\alpha^{(1)}\varphi_i, \ldots, \alpha^{(s)}\varphi_i) = \beta\varphi_i$ pour tout χ et pour un φ_i convenablement choisi. Par conséquent, le nombre des conjugués de β est $\leqq t$, d'où $[K':Q] \leqq t$. Mais, en conséquence de la construction de K', les nombres $\alpha^{(1)}, \ldots, \alpha^{(s)}$ sont des nombres algébriques de degré $\leqq s$ sur K' et $\alpha^{(1)}$ est de degré $m = t \cdot s$ sur Q. Il en résulte que K' est un sous-corps de $Q(\alpha)$ et $1 \leqq [K':Q] = t < m$. Vu que le corps $Q(\alpha)$ est primitif d'après l'hypothèse, on a nécessairement $K' = Q$, $t = 1$. Donc, on déduit $s = m$, c'est-à-dire $\mathcal{G}(f)$ est connexe, et ainsi d'après le lemme 9 $g(f(x))$ est irréductible sur Q pour tout $g(x) \in P(G)$.

Démonstration *du lemme 19*. D'après le lemme 18 il suffit de considérer le cas où $f(x)$ est réductible sur Q.

Si $f(x) = \prod_{i=1}^{m} (x - a_i)$ avec des nombres entiers rationnels différents a_i, alors de (4. 57) on déduit

$$|a_j - a_i| > 2G$$

pour au moins une couple $i < j$. Il en résulte que le graphe $\mathcal{G}(f)$ défini par (4. 58) contient un sous-graphe connexe ayant plus de $\frac{\deg f}{2}$ sommets, c'est-à-dire d'après le lemme 9 $g(f(x))$ est irréductible sur Q pour tout $g(x) \in P(G)$.

D'autre part, si $f(x)$ est réductible sur Q et si ses racines ne sont pas tous entières rationnelles, alors on a nécessairement $f(x) = (x - \alpha^{(1)})(x - \alpha^{(2)})(x - a)$, où $a \in Z$ et $f_1(x) = (x - \alpha^{(1)})(x - \alpha^{(2)}) \in Z[x]$ est irréductible sur Q. Maintenant $D(f) = D(f_1) f_1^2(a)$ et il y a deux possibilités. Si

$$D(f_1) > (2G)^2$$

alors, en désignant par K le corps $Q(\alpha^{(1)}, \alpha^{(2)})$, on a

$$N_{K/Q}^2(\alpha^{(1)} - \alpha^{(2)}) = \{D(f_1)\}^{[K:Q]} > (2G)^{2[K:Q]}.$$

Par conséquent, $\mathcal{G}(f)$ contient un sous-graphe ayant plus de degf/2 sommets, ainsi d'après le lemme 9 $g(f(x))$ est irréductible sur Q pour tout $g(x) \in P(G)$. Enfin, si $D(f_1) \leqq (2G)^2$, alors de (4. 57) on obtient $f_1^2(a) > (2G)^4$, c'est-à-dire

$$N_{K/Q}(f_1(a)) = N_{K/Q}^2(a - \alpha^{(1)}) = N_{K/Q}^2(a - \alpha^{(2)}) > (2G)^{2[K:Q]}.$$

On en déduit que $\mathcal{G}(f)$ est connexe et ainsi $g(f(x))$ est irréductible sur Q aussi dans ce cas pour tout $g(x) \in P(G)$.

Le lemme suivant est au fait une généralisation de notre résultat concernant les nombres algébriques entiers de discriminant donné (voir [11]):

Lemme 20. *Soit* $D \geqq 1$ *une constante et soit* $f(x) \in Z[x]$ *un polynôme normé tel que* $0 < |D(f)| \leqq D$. *Il y a des constantes* $c_1(D)$, $c_2(D)$ *calculables explicitement et dépendant seulement de* D *telle que* $\deg f \leqq c_1(D)$ *et* $\| f^* \| \leqq c_2(D)$ *pour un* f^* *équivalent à* f.

DÉMONSTRATION: voir [11].

Nous démontrerons simultanément les théorèmes 2a et 2b.

DÉMONSTRATION *des théorèmes 2a et 2b.* Soient $f(x)$, $g(x)$ des polynômes arbitraires, satisfaisant aux conditions du théorème 2a ou 2b (c'est-à-dire dans le cas $p \geqq 5$ $f(x)$ soit irréductible sur Q).

Si

$$D(f) > (2G)^{p(p-1)}$$

alors d'après les lemmes 18 et 19 $g(f(x))$ est irréductible sur Q.

D'autre part, si

$$0 < D(f) \leqq (2G)^{p(p-1)},$$

alors d'après le lemme 20 il y a une constante $c_1(G, p)$, calculable explicitement et dépendant seulement de G et de p (plus précisément de $(2G)^{p(p-1)}$), telle que $\| f^* \| \leqq$ $\leqq c_1(G, p)$ pour un f^* équivalent à f. Dans le cas $\deg f \leqq 3$, c'est-à-dire dans le théorème 2b on peut prendre $c_2(G) = \max\left(c_1(G, 2), c_1(G, 3)\right)$ et ainsi nos théorèmes sont démontrés.

DÉMONSTRATION *du corollaire.* Si $f(x), g(x) \in Z[x]$ sont des polynômes normés tels que l'irréductibilité de $g(f(x))$ s'obtient d'un de nos théorèmes, alors, en conséquence de nos démonstrations, le graphe défini par (4. 6) contient un sous-graphe connexe ayant $s > \dfrac{\deg f}{2}$ sommets. Ainsi, d'après le lemme 10, le nombre des diviseurs irréductibles de $g(f(x))$ sur un K-corps arbitraire est en effet $\leqq \deg g \cdot \left[\dfrac{\deg f}{s}\right] =$ $= \deg g$.

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—J. COATES, Integer points on curves of genus 1, *Proc. Cambridge Philos. Soc.*, **67**, (1970), 595—602.

[3] A. BRAUER, Bemerkungen zu einem Satze von Herrn G. Pólya, *Jahresber. Deutsch. Math. Ver.*, **43**, (1933), 124—129.

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

[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—G. EHRLICH, On the irreducibility of certain polynomials, *Bull. Amer. Math. Soc.*, **52**, (1964), 844—856.

[7] H. L. DORWART—O. ORE, Criteria for the irreducibility of polynomials, *Annals of Math.*, **34**, (1933), 81—94.

[8] K. GYŐRY—L. LOVÁSZ, Representation of integers by norm-forms, II. *Publ. Math. Debrecen,* **17**, (1970), 173—181.
[9] K. GYŐRY, Sur une classe des corps algébriques et ses applications, *sous presse.*
[10] K. GYŐRY, Sur l'irréductibilité d'une classe des polynômes, I. *Publ. Math. Debrecen,* **18**, (1971), 289—307.
[11] K. GYŐRY, Sur les nombres algébriques entiers de discriminant donné, *sous presse.*
[12] H. ILLE, Einige Bemerkungen zu einem von G. Pólya herrührenden Irreduzibilitätskriterium, *Jahresber. Deutsch. Math. Ver.,* **35**, (1926), 204—208.
[13] *М. В. Яковкин*, Численная теория приводимости многочленов, *Москва*, 1959.
[14] E. LANDAU, Vorlesungen über Zahlentheorie, III. *Leipzig,* 1927.
[15] T. NAGELL, Sur les discriminants des nombres algébriques, *Arkiv för Mat.,* **7**, (1967), 265—282.
[16] O. ORE, Les corps algébriques et la théorie des idéaux, *Mémorial Sci. Math.,* **64**, Paris, 1934.
[17] G. PÓLYA, Verschidene Bemerkungen zur Zahlentheorie, *Jahresber. Deutsch. Math. Ver.,* **28**, (1919), 31—40.
[18] G. PÓLYA—G. SZEGŐ, Aufgaben und Lehrsätze aus der Analysis, II., *Berlin,* 1925.
[19] L. RÉDEI, Algebra I. *Budapest,* 1967.
[20] R. REMAK, Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers, *Comp. Math.* **10** (1952), 245—285.
[21] W. SCHULZ, Über Reduzibilität bei gewissen Polynomen und das Tarry-Escottsche Problem, Math. Z. **63** (1955/56), 133—144.
[22] I. SCHUR, Aufgabe 275, 259, *Archiv der Math. und Physik,* **15**, (1909).
[23] I. SERES, Lösung und Verallgemeinerung eines Schurschen Irreduzibilitatätsproblems für Polynome, *Acta Math. Acad. Sci. Hung.,* **7**, (1956), 151—157.
[24] I. SERES, Über die Irreduzibilität gewisser Polynome, *Acta Arith.,* **8**, (1963), 321—341.
[25] I. SERES, Irreducibility of polynomials, *J. Algebra,* **2**, (1965), 283—286.
[26] C. SIEGEL, Approximation algebraischer Zahlen, *Math. Z.* **10**, (1921), 173—213.
[27] T. TATUZAWA, Über die Irreduzibilität gewisser ganzzahliger Polynome, *Proc. Imp. Acad. Tokyo,* **15**, (1939), 253—254.
[28] N. TSCHEBOTARÖW—H. SCHWERDTFEGER, Grundzüge der Galois'schen Theorie, *Gröningen—Djakarta,* 1950.
[29] U. WEGNER, Über die Irreduzibilität einer Klasse von ganzen rationalen Funktionen, *Jahresber. Deutsch. Math. Ver.,* **40**, (1931), 239—241.
[30] L. WEISNER, Irreducibility of polynomials of degree n which assume the same value n times, *Bull. Amer. Math. Soc.,* **41**, (1935), 248—252.

(Reçu le 29 mars 1970, et dans une forme modifiée le 12 juillet 1972.)