Sur l'irréductibilité d'une classe des polynômes, I.

Par K. GYŐRY (Debrecen)

A la mémoire de I. Seres

Introduction

I. SCHUR a conjecturé [10], [2] que si $f(x) = \prod_{i=1}^{m} (x-a_i)$ est un polynôme avec des entiers différents a_i, alors $(f(x))^{2^n}+1$ est irréductible sur le corps rationnel Q (sauf pour $n=0$, $m\leqq 4$). Cette conjecture a été prouvée pour $n=0$ par W. FLÜGEL [4], pour $n=1$ dans le livre de G. PÓLYA et G. SZEGŐ [9], pour $n=2$ par H. ILLE [7] et pour $n\leqq 3$, dans une forme plus générale, par A. BRAUER, R. BRAUER et H. HOPF [1]. Dans [1] les auteurs ont posé la question de l'irréductibilité des polynômes de la forme $g(f(x))$ généralement, les $f(x)$ étant des polynômes du type précédent. Pour des polynômes $g(x)$ de degré $\leqq 3$ et pour certains polynôms $g(x)$ du quatrième et sixième degré ils ont résolu le problème, en montrant que si $g(x)$ est fixé et irréductible, alors $g(f(x))$ est également irréductible sur Q, sauf pour un nombre fini de polynômes $f(x)$ essentiellement différents (du point de vue de l'irréductibilité $f(x)$ et $f(x+a)$ ne sont pas essentiellement différents), et toutes les exceptions peuvent être déterminées. Pour des polynômes linéaires $g(x)$ cette proposition s'obtient déjà d'un théorème général de G. PÓLYA [8]. H. L. DORWART et O. ORE [3] ont obtenu des résultats analogues pour certains polynômes $g(x)$ du deuxième et du quatrième degré et pour des polynômes $f(x)$ ayant des racines entières différentes dans un corps quadratique imaginaire. U. WEGNER [15] a prouvé que si $g(x) = x^4+d$, $d>0$ entier et $d\not\equiv 3 \pmod 4$, et si $f(x)$ est de la forme précédente avec $m>5$, alors $g(f(x))$ est irréductible. Les méthodes, utilisées dans les travaux cités, ne peuvent pas être appliquées dans le cas de polynômes $g(x)$ de degré supérieur.

En utilisant le théorème de Kronecker concernant les unités des corps cyclotomiques, I. SERES [11], [12] a démontré que si les racines de $g(x)$ sont des unités non réelles d'un corps cyclotomique et si $f(x)$ a plus de $\max\left(\frac{\deg f}{2}, 5\right)$ racines entières différentes, alors $g(f(x))$ est irréductible sur Q. De plus, pour des polynômes cyclotomiques $g(x)$I. SERES [13] a déterminé tous les polynômes exceptionnels de la forme $f(x) = \prod_{i=1}^{m} (x-a_i)$ avec des entiers différents a_i pour lesquels $g(f(x))$ est réductible. Il a prouvé que dans ce cas $g(f(x))$ est réductible sur Q si et seulement

si l'on a $g(x) = x^4 - x^2 + 1$ et $f(x) = (x+a)(x+a+1)(x+a+2)$. Avec cela I. Seres a démontré la conjecture de I. Schur dans une forme plus générale.

Dans la suite nous traitons le problème de Brauer—Hopf dans le cas plus général où les racines de $f(x)$ ne sont pas nécessairement entières mais il y a un polynôme normé $f_1(x) \mid f(x)$ à coefficients entiers ayant des racines réelles différentes, et le corps de décomposition de $g(x)$ est non réel tel que son sous-corps réel maximal est normal sur Q (voir 2.). Soit L le corps de décomposition de $f_1(x)g(x)$. En développant progressivement la méthode de I. Seres et en utilisant les inégalités de norme (1), (2) et (3), nous prouvons, entre autres, que si des paires (α_i, α_k) des racines de $f_1(x)$, satisfaisant à $N_{L/Q}(\alpha_i - \alpha_k) > \{2^n g^2(0)\}^{[L:Q]/n}$ $(n = \deg g)$ forment un graphe connexe à s éléments, alors les degrés des facteurs irréductibles de $g(f(x))$ sur Q sont $\geqq sn$ et par conséquent le nombre de ses diviseurs irréductibles est $\leqq \frac{\deg f}{s}$. Nous démontrons cette proposition dans une forme p-adique. Il en résulte immédiatement, par exemple, que si les racines de $f(x)$ sont réelles et différentes et si pour ses racines on a $\min_{i \neq k} |\alpha_i - \alpha_k| > 2\{g(0)\}^{2/n}$, alors $g(f(x))$ est irréductible sur Q.

Nous remarquons qu'on ne peut pas étendre ces résultats aux polynômes arbitraires $f(x)$ et $g(x)$. En utilisant que $g(x) \mid g(x + h(x)g(x))$, on peut construire des polynômes $f(x)$ et $g(x)$, satisfaisant aux conditions de nos théorèmes sauf que le corps de décomposition de $g(x)$ soit un corps non réel du type précédent ou les racines de $f(x)$ soient des nombres réels différents, pour lesquels $g(f(x))$ est réductible sur Q (voir 3.).

De nos résultats mentionnés on déduit la solution du problème original de Brauer—Hopf pour chaque $g(x)$ et nous obtenons une généralisation des théorèmes cités de I. SERES [11], [12]. De plus, nous résolvons plusieurs problèmes diophantiens et nous déterminons tous les polynômes 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, en généralisant le résultat cité de I. SERES [13] concernant le problème de I. Schur. Dans [6] et dans la partie II. nous donnons plusieurs autres applications et extensions de nos résultats. Par exemple, en considérant tous les polynômes $f(x)$ ayant des racines différentes dans un corps réel fixé, nous prouvons la généralisation du problème de Brauer—Hopf pour chaque $g(x)$ et nous donnons la solutions de ce problème pour chaque $g(x)$ aussi dans le cas où le degré des polynômes $f(x)$ ayant des racines differentes réeles est fixé.

2. Résultats préliminaires

Les corps algébriques satisfaisants à la condition $(a) \Leftrightarrow (b)$ sont souvent utilisés dans la théorie des nombers. Nous appelons ces corps kroneckeriens ou simplement des K-corps, puisque on peut étendre à leurs unités le théorème de Kronecker concernant les unités des corps cyclotomiques.*) Nous étudions ces corps et leurs

*) Le 31 octobre 1971 Prof. A. SCHINZEL m'a informé que dans le cas spécial $S = S_\infty$ $(a) \Leftrightarrow (c)$ est démomtré par R. REMAK (*Comp. Math.* **10** (1952), 245—285)

applications en détail dans [6], ici nous énumerons seulement nos résultats, utilisés dans la suite.

Soit L_0 le sous-corps maximal réel du corps algébrique L et soit $L\psi$ ou $\bar{L}$ le corps conjugué complexe de L dans le corps complexe. Si S^0 est un système de valuations non équivalentes de L_0, alors désignons par S le système de toutes les continuations de ces valuations dans L. Enfin soit S_∞ le système des valuations archimédiennes non équivalentes de L.

Théorème. *Pour un corps algébrique L les assertions suivantes sont équivalentes:*

(a) *L est totalement réel ou bien une extension quadratique totalement imaginaire d'un corps totalement réel (c'est-à-dire $L = L_0(\sqrt{-\mu})$, où $\mu \in L_0$ est totalement positif).*

(b) *$L\psi = L$ et $\sigma\psi = \psi\sigma$ pour chaque isomorphisme σ de L dans le corps complexe.*

(c) *$L = L_0$ est totalement réel ou bien $L \neq L_0$. Dans ce cas soit $S \supseteq S_\infty$ un système de valuations de L tel que chaque valuation de $S^0 \setminus S_\infty^0$ ait continuation unique dans L. Désignons par V, U_s et U_s^0 le groupe des racines d'unité, le groupe des S-unités et le groupe des S-unités réelles dans L respectivement. Alors $U_s/\{V, U_s^0\}$ est fini et dans le cas spécial $S = S_\infty$ on a $[U_s : \{V, U_s^0\}] \leqq 2$.*

(d) *Il existe un corps algébrique $F \supseteq L$ tel que F/Q et F_0/Q sont normales.**)

Dans [5] nous avons appelé les corps algebriques à propriété (d) „allowed".

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

Dans la suite soit L un K-corps. Alors α et $\bar{\alpha}$ appartiennent simultanément à L, et par conséquent $\operatorname{Re}\alpha$, $i \operatorname{Im}\alpha \in L$. Si φ est une valuation normée non archimédienne dans L, alors $\bar{\varphi}(\alpha) = \varphi(\bar{\alpha})$ est également une valuation normée non achimédienne dans L. Nous appelons φ simplement „réelle", si l'on a $\bar{\varphi}(\alpha) = \varphi(\alpha)$ pour chaque $\alpha \in L$, dans le cas contraire soit φ appelé „non réelle".

Nous avons trouvé l'inégalité suivante en collaboration avec L. Lovász [5] dans la forme $|N_{F/Q}(\alpha)| \geqq |N_{F/Q}(\operatorname{Re}\alpha)|$, $|N_{F/Q}(i \operatorname{Im}\alpha)|$, où F désigne un corps galoisien à propriété (*d*).

Lemme 2. *Soit L un K-corps de degré n, et soient S_1 et S_2 des systèmes de ses valuations normées non archimédiennes „réelles" et „non réelles" respectivement. Alors pour tout $\alpha \in L$ on a*

$$\Big\{N_{L/Q}(\alpha) \prod_{\varphi \in S_1} \varphi(\alpha) \prod_{\varphi \in S_2} \max\big(\varphi(\alpha), \varphi(\bar{\alpha})\big)\Big\}^{2/n} \geqq$$

$$\geqq \Big\{\prod_{\varphi \in S_1 \cup S_2} \varphi(2)\Big\}^{2/n} \Big[\Big\{N_{L/Q}(\operatorname{Re}\alpha) \prod_{\varphi \in S_1 \cup S_2} \varphi(\operatorname{Re}\alpha)\Big\}^{2/n} + \tag{1}$$

$$+ \Big\{N_{L/Q}(i \operatorname{Im}\alpha) \prod_{\varphi \in S_1 \cup S_2} \varphi(i \operatorname{Im}\alpha)\Big\}^{2/n}\Big]$$

et en particulier dans le cas $S_1, S_2 = \emptyset$

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

*) Si le corps algébrique L est donné par le polynôme caractéristique $g(x)$ d'un élément primitif de L, on peut décider à l'aide d'un algorithme si L est kroneckerien ou non (voir, par ex. [6]).

On peut aisément donner (1) aussi dans une forme p-adique (voir par exemple le théorème 1').

Lemme 3. *Si L est un K-corps non réel et si $\alpha, \beta \in L$ sont des entiers non réels et non purement imaginaires tels que $\alpha \pm \beta$ est réel ou purement imaginaire, alors on a*

$$N_{L/Q}\left(\frac{\alpha \pm \beta}{2}\right) \leqq N_{L/Q}(\alpha\beta) \leqq \frac{N^2_{L/Q}(\alpha) + N^2_{L/Q}(\beta)}{2} \tag{3}$$

Dans la suite soit L un K-corps normal non réel sur Q et soit P un idéal premier dans l'anneau des entiers de L. Nous appelons P „réel", si son groupe de décomposition contient la conjugation complexe (c'est-à-dire la valuation φ_P est „réelle"), dans le cas contraire P soit appelé „non réel". Appelons le nombre premier rationnel p „réel" ou „non réel" dans L, si tous les idéaux premiers $P|p$ sont „réels" ou bien „non réels" dans L.

Lemme 4. *Dans L chaque nombre premier rationnel p est ou „réel" ou „non réel" et le nombre des premiers „réels" dans L est infini.*

Par conséquent dans un K-corps non réel il y a une infinité de valuations non équivalentes „réelles". Dans les corps abéliens on peut aisément caractériser les premiers „réels" à l'aide de la théorie du corps de classes.

Lemme 5. *Si $L = L_0(\sqrt{-\mu})$ ($\mu \in L_0$ est un entier totalement positif) est normal sur Q et si p est un nombre premier rationnel tel que $p \nmid 2D_{L/Q}$, $p \nmid N_{L_0/Q}(-\mu)$, alors p est „réel" dans L si et seulement si $-\mu$ est un quadratique non-résidu* (mod p) *dans L_0. Par conséquent, si $N_{L_0/Q}(-\mu)$ est un quadratique non-résidu* (mod p), *alors p est „réel" dans L.*

3. Résultats

a) *Irréductibilité des polynômes sur K-corps non réels*

Dans la suite soit L un K-corps non réel, S_1 et S_2 des systèmes de valuations normées non archimédiennes „réelles" et „non réelles" respectivement. Si $f(x) = \beta_0 x^k + \cdots + \beta_k \in L[x]$ et $\operatorname{Re} f(x) = \operatorname{Re}\beta_0 x^k + \cdots + \operatorname{Re}\beta_k$, $i \operatorname{Im} f(x) = i \operatorname{Im}\beta_0 x^k + \cdots + i \operatorname{Im}\beta_k$, alors on a $\operatorname{Re} f(x), i \operatorname{Im} f(x) \in L[x]$. De plus, si $f(x)$ est irréductible sur L et non réel, alors on a nécessairement $(\operatorname{Re} f(x), i \operatorname{Im} f(x)) = 1$.

Théorème 1. *Soit $f(x) \in L[x]$ normé avec des coefficients entiers tel que $(\operatorname{Re} f(x), i \operatorname{Im} f(x)) = 1$. S'ils existent des entiers réels α_i dans L tels que pour des paires (α_i, α_k) convenablement choisies*

$$N^2_{L/Q}(\alpha_i - \alpha_k) \prod_{\varphi \in S_1} \varphi^2(\alpha_i - \alpha_k) \prod_{\varphi \in S_2} \varphi(\alpha_i - \alpha_k) > \tag{4}$$

$$> 2^{2[L:Q]} N^2_{L/Q}\big(f(\alpha_i) f(\alpha_k)\big) \prod_{\varphi \in S_1} \varphi^2\big(f(\alpha_i) f(\alpha_k)\big) \prod_{\varphi \in S_2} \max\big(\varphi(f(\alpha_i) \times$$

$$\times \overline{f(\alpha_k)}),\ \varphi\big(\overline{f(\alpha_i)} f(\alpha_k)\big)\big) > 0$$

et si ces paires forment un graphe connexe à s éléments, alors $f(x)$ n'a aucun diviseur

irréductible de degré $<s$*) *sur* L. *Par conséquent, si* $s>\frac{\deg f}{2}$, *alors* $f(x)$ *est irréductible sur* L.

En choisissant convenablement les α_i, α et $f_1(x)$, les polynômes de la forme $f(x)=f_1(x)\prod_{i=1}^{s}(x-\alpha_i)+\alpha$, par exemple, satisfont aux conditions du théorème.

Nous remarquons qu'on ne peut pas étendre le théorème aux K-corps réels. Soit, par exemple, L un corps quadratique réel et soit $\varepsilon>1$ son unité fondamentale. Si maintenant n est un nombre naturel „grand" et $f(x)=x[(x-1)(x-\varepsilon^n)+(\varepsilon-1)\varepsilon^n]$, alors $N^2_{L/Q}(1-\varepsilon^n)$ et $N^2_{L/Q}(\varepsilon^n-\varepsilon)$ sont „grands", $N^2_{L/Q}(f(1))=N^2_{L/Q}(f(\varepsilon))=N^2_{L/Q}(f(\varepsilon^n))=$ $=N^2_{L/Q}(1-\varepsilon)$ sont „petits" et $f(x)$ est réductible sur L.

Dans le cas de polynômes spéciaux on peut encore un peu améliorer le théorème 1.

Théorème 2. *Soit* $f(x)=\prod_{i=1}^{m}(x-\alpha_i)+\alpha$, $\alpha_1, \ldots, \alpha_m$ *et* α *étant des entiers réels et non réels dans* L *respectivement. Si pour des paires* (α_i, α_k) *convenablement choisies on a*

$$N^2_{L/Q}(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi^2(\alpha_i-\alpha_k)>2^{2[L:Q]}N_{L/Q}(\alpha\bar{\alpha})\prod_{\varphi\in S_1}\varphi(\alpha\bar{\alpha})>0 \tag{5}$$

et si ces paires forment un graphe connexe à m *éléments***), *alors* $f(x)$ *est irréductible sur* L.

b) *Irréductibilité des polynômes sur* Q.

Dans la suite soient $f(x)$ et $g(x)$ des polynômes à coefficients entiers rationnels. Pour que $g(f(x))$ soit irréductible sur Q il faut que $g(x)$ soit également irréductible sur Q. De plus, évidemment on peut se réduire aux polynômes normés. Dans la suite soit $g(x)$ irréductible sur Q et soient $g(x)$ et $f(x)$ normés.

Dans ce point nous supposons que le corps de décomposition de $g(x)$ est un K-corps non réel et supposons qu'il existe un polynôme $f_1(x)|f(x)$ à coefficients entiers, ayant seulement des racines réelles différentes. Désignons par L le corps de décomposition de $f_1(x)g(x)$ et par $\mathscr{P}_1$, $\mathscr{P}_2$ des systémes convenablement formés (peut être vides) des nombres premiers rationnels „réels" et „non réels" dans L respectivement.

Théorème 1′. *Si pour des paires* (α_i, α_k) *convenablement choisies des racines de* $f_1(x)$ *on a*

$$N^2_{L/Q}(\alpha_i-\alpha_k)\prod_{p\in P_1}|N^2_{L/Q}(\alpha_i-\alpha_k)|_p\prod_{p\in P_2}|N_{L/Q}(\alpha_.-\alpha_k)|_p> \tag{6}$$

$$>\{2^n g^2(0)\prod_{p\in S_1}|g^2(0)|_p\prod_{p\in P_2}|g(0)|_p\}^{\frac{2[L:Q]}{n}};\qquad n=\deg g$$

*) En général, dans le théorème 1. et 1′. ces inégalités ne peuvent pas être déjà améliorées.

**) Addendum. Si les paires (α_i, α_k) satisfaisant à (5) (à (7)) forment un graphe connexe à s éléments, alors l'assertion du théorème 1 (1') est également vrai. Par conséquent nos théorèmes 1', 2', 3, 4 et 5 peuvent être encore améliorés.

et si ces paires forment un graphe connexe à s éléments, 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.

Considérons maintenant le cas spécial où $f_1(x)=f(x)$.

Théorème 2′. *Supposons que toutes les racines de* $f(x)$ *sont réelles et différentes. Si pour des paires* (α_i, α_k) *convenablement choisies des racines de* $f(x)$ *on a*

$$N_{L/Q}(\alpha_i-\alpha_k) \prod_{p\in P_1} |N_{L/Q}(\alpha_i-\alpha_k)|_p > \{2^n g(0) \prod_{p\in P_1} |g(0)|_p\}^{\frac{[L:Q]}{n}} \tag{7}$$

et si ces paires forment un graphe connexe à $\deg f$ *éléments***), *alors* $g(f(x))$ *est irréductible sur* Q.

On peut bien appliquer les formes p-adiques ($\mathscr{P}_1$ ou $\mathscr{P}_2 \neq \emptyset$) des théorèmes 1′ et 2′ par exemple dans le cas où $g(0)$ est divisible par beaucoup de nombres premiers „réels", premiers à $D(f_1)$ ou $D(f)$ respectivement. Par exemple, si les polynômes $f(x)$ et $g(x) = \Pi(x-\alpha)$ satisfont aux conditions du théorème 1′ ou 2′ et si dans $g^*(x) = \Pi(x-a\alpha)$ tous les diviseurs premiers de a sont „réels" et premiers à $D(f_1)$ ou $D(f)$, alors $g^*(f(x))$ est également irréductible. Dans le cas $g(x) = x^4+1$ il en résulte un théorème de U. WEGNER [15].

Nous remarquons qu'on peut appliquer les théorèmes 1′—6 aussi pour les autres substitutions entières x_0 ($x_0=0$ ou $x_0\neq 0$), en supposant que $g(x_0)$ et les racines de $f(x)-x_0$ satisfont aux conditions. En effet, si $g^*(x) = g(x+x_0)$ et $f^*(x) = f(x)-x_0$, alors $g(f(x))=g^*(f^*(x))$ est irréductible d'après nos théorèmes.

Dans la suite nous donnons quelques conséquences des théorèmes 1′ et 2′.

Pour un polynôme $f(x) = \prod_{i=1}^{m} (x-\alpha_i)$ à coefficients entiers avec le discriminant $D(f)\neq 0$ nous introduisons la notation

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

Théorème 3. *Supposons que* $\deg f_1 > \frac{\deg f}{2}$, $(D(f_1), p)=1$ *pour tout* $p\in\mathscr{P}_1$, $\mathscr{P}_2$ *et supposons qu'on a*

$$c(f_1) > 2\{g^2(0) \prod_{p\in P_1} |g^2(0)|_p \prod_{p\in P_1} |g(0)|_p\}^{1/n}, \qquad n = \deg g \tag{8}$$

$$c(f) > 2\{g(0) \prod_{p\in P_1} |g(0)|_p\}^{1/n} \tag{9}$$

selon que $f_1(x)\neq f(x)$ *ou* $f_1(x)=f(x)$. *Alors* $g(f(x))$ *est irréductible sur* Q. *Par conséquent si l'on a en particulier*

$$c(f_1) > 2g^{2/n}(0) \quad \textit{ou} \quad c(f) > 2g^{1/n}(0) \quad (f_1(x)=f(x)), \tag{10}$$

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

Donc, pour un polynôme fixé $g(x)$ et pour une classe assez large des polynômes $f(x)$ on obtient l'irréductibilité de $g(f(x))$. D'un autre côté, fixons un polynôme normé $f(x)$ à coefficients entiers, ayant des racines réelles différentes. En supposant que le corps de décomposition d'un polynôme $g(x)$ est un K-corps non réel et $2\{g(0)\}^{1/\deg g} < c(f)$, de 1′ irréductibilité de $g(f(x))$ dans $Q[f(x)]$ il résulte son irréductibilité aussi dans $Q[x]$.

Nous remarquons qu'on ne peut pas étendre nos théorèmes 1′, 2′ et 3 aux polynômes arbitraires $f(x)$ et $g(x)$. Plus exactement on peut aisément construire des polynômes $f(x)$ et $g(x)$ pour lesquels le corps de décomposition de $g(x)$ n'est pas de K-corps non réel ou les racines de $f(x)$ ne sont pas tous réelles différentes, $f(x)$ et $g(x)$ satisfont aux conditions supplémentaires des théorèmes, pourtant $g(f(x))$ est réductible sur Q.

Pour construire des polynômes convenables, considérons, par exemple, un corps quadratique réel avec une unité fondamentale $\varepsilon > 1$ de norme $+1$ et soit n un nombre naturel „grand". Alors $a = \varepsilon^n + \varepsilon^{-n}$ et $a' = \varepsilon^{2n} + \varepsilon^{-2n}$ sont des nombres naturels „grands".

Prenons maintenant, par exemple, les polynômes $g(x) = x^2 - ax + 1 = (x-\varepsilon^n)(x-\varepsilon^{-n})$ et $f(x) = x + g(x) = x^2 - (a-1)x + 1 = (x-\alpha_1)(x-\alpha_2)$ ayant des racines réelles différentes. Alors $N_{L/Q}(\alpha_1 - \alpha_2)$ et $|\alpha_1 - \alpha_2|$ sont „grands" par rapport à $2^{[L:Q]}\{g(0)\}^{\frac{[L:Q]}{2\deg g}}$ et $2\{g(0)\}^{2/\deg g}$ respectivement, pourtant $g(x) | g(f(x))$, c'est-à-dire $g(f(x))$ est réductible sur Q.

D'autre part, considérons les polynômes $f(x) = x^4 + a'x^2 + 1 = (x - i\varepsilon^n) \cdot (x + i\varepsilon^n)(x - i\varepsilon^{-n})(x + i\varepsilon^{-n})$ et $g(x) = f(x) - x$ ayant des racines non réelles ($g(x)$ est irréductible sur Q). Alors on peut également vérifier que $g(x)$ et $f(x)$ satisfont aux conditions supplémentaires des théorèmes 1′ et 2′, mais $g(x) | g(f(x))$, c'est-à-dire $g(f(x))$ est réductible sur Q.

Du théorème 1′ on obtient la généralisation suivante des théorèmes de I. Seres concernant les polynômes cyclotomiques $g(x)$ [11] et les polynômes minimales $g(x)$ des unités non réelles des corps cyclotomiques [12].

Théorème 4. *Si $f(x)$ a plus de $\frac{\deg f}{2}$ racines entières différentes et si $\deg f \geqq 2[4\{g(0)\}^{2/\deg g} + 1]$, alors $g(f(x))$ est irréductible sur Q.*

Ensuite nous donnons la solution du problème original de Brauer—Hopf [1] pour tous les polynômes $g(x)$ ayant des corps de décomposition kroneckeriens non réels.

Théorème 5. *Soit $f(x) = \prod_{i=1}^{m} (x - a_i)$ avec des entiers différents a_i. Alors $g(f(x))$ est irréductible sur Q, sauf certains cas où $\max_{i \neq j} |a_i - a_j| \leqq 4\{g(0)\}^{1/\deg g}$, c'est-à-dire $m \leqq 4\{g(0)\}^{1/\deg g} + 1$. Par conséquent, pour $g(x)$ fixé il y a seulement un nombre fini de polynômes $f(x)$ essentiellement différents*) du type précédent tels que $g(f(x))$ est réductible sur Q et ces exceptions peuvent être déterminées.*

*) Les polynômes $f(x)$ et $f(x+a)$ ne sont pas essentiellement différents du point de vue d'irréductibilité.

Enfin, en généralisant les résultats de I. Seres concernant les polynômes cyclotomiques $g(x)$ ([13]), nous déterminons tous les polynômes $f(x)$, $g(x)$ tels que $f(x) = \prod_{i=1}^{m}(x-a_i)$, $g(0)=1$ pour lesquels $g(f(x))$ est réductible. Pour démontrer ce théorème nous résolvons plusieurs problèmes diophantiens.

Théorème 6. *Dans le théorème précédent soit $g(0)=1$ et désignons par ε une des racines de $g(x)$. Alors $g\left(\prod_{i=1}^{m}(x-a_i)\right)$ est réductible sur Q si et seulement si les a_i sont des entiers consécutifs et*

$m=4$, $\varepsilon=\zeta^2-1$, où ζ est une racine d'unité primitive de degré n ou $2n$, $2\nmid n$, $n\neq p^\alpha$ ($p\geqq 3$ nombre premier $\alpha\geqq 0$).

$m=3$, $\varepsilon=\pm\zeta(1-\zeta^2)$, où ζ est une racine d'unité primitive de degré $\neq p^\alpha, 2p^\alpha$ ($p\geqq 2$ nombre premier, $\alpha\geqq 0$).

$m=2$, $\varepsilon=\dfrac{(1-\zeta_1)(1-\zeta_2)}{(\zeta_1-\zeta_2)^2}$, où $\zeta_1, \zeta_2 (\neq\zeta_1, \bar{\zeta}_1)$ ζ_1/ζ_2 sont des racines d'unité primitives de degré p^α simultanément (p nombre premier) ou bien aucun de leurs degrés n'est une puissance de premiers, et il n'y a aucune racine d'unité ζ de degré $q\neq p^\alpha$ ($p\geqq 3$ nombre premier) telle que $\zeta_1=\zeta^a$, $\zeta_2=\zeta^b$, $\zeta_1^a=\zeta_2^b$ et $(a, q)=(b, q)=1$,

ou $m=2$, $a_2-a_1=2$, $\varepsilon=\zeta^2-1$, où ζ est une racine d'unité primitive de degré n ou $2n$, $2\nmid n$, $n\neq p^\alpha$ ($p\geqq 3$ nombre premier).

Si $m=3$ et ε est une racine d'unité, de notre théorème on obtient l'exception $g(x)=x^4-x^2+1$, $f(x)=(x+a)(x+a+1)(x+a+2)$, donnée par I. Seres [13].

4. Démonstrations

Dans la suite soit L un K-corps non réel et soient S_1, S_2 des systèmes de ses valuations normées non archimédiennes „réelles" et „non réelles" respectivement.

Lemme 6. *Si α, β sont entiers dans L et $\alpha|\beta$, alors les nombres ci-dessous sont entiers rationnels et on a*

(11)

$$N_{L/Q}^2(\alpha)\prod_{\varphi\in S_1}\varphi^2(\alpha)\prod_{\varphi\in S_2}\max\left(\varphi(\alpha),\varphi(\bar{\alpha})\right)\Big|N_{L/Q}^2(\beta)\prod_{\varphi\in S_1}\varphi^2(\beta)\prod_{\varphi\in S_2}\max\left(\varphi(\beta),\varphi(\bar{\beta})\right)$$

Démonstration. Considérons les décompositions de α et β en produits d'idéaux premiers. Si l'on a φ_P, $\varphi_P\notin S_2$ pour chaque idéal premier „non réel" $P|\alpha$, alors notre proposition est évidente. Donc, soit $P|\alpha$ un idéal premier „non réel" tel que φ_P ou $\varphi_P\in S_2$ et désignons par $a(P, \bar{P})$ et $a'(P, \bar{P})$ la somme des exposants de $N(P)$ et $N(\bar{P})$ dans le côté gauche et droit de (11) respectivement. Il suffit de montrer qu'on a $0\leqq a(P, \bar{P})\leqq a'(P, \bar{P})$. Supposons que $P^k\|\alpha$, $P^l\|\bar{\alpha}\Rightarrow\bar{P}^l\|\alpha$ et $P^{k'}\|\beta$, $P^{l'}\|\bar{\beta}\Rightarrow$ $\Rightarrow\bar{P}^{l'}\|\beta$, où $k\leqq k'$, $l\leqq l'$ d'aprés $\alpha|\beta$. Si maintenant φ_P et $\varphi_P\in S_2$, alors on a $a(P, \bar{P})=$ $=2k+2l-2\min(k, l)$, $a'(P, \bar{P})=2k'+2l'-2\min(k', l')$, dans le cas contraire $a(P, \bar{P})=2k+2l-\min(k, l)$, $a'(P, \bar{P})=2k'+2l'-\min(k', l')$. L'inégalité nécessaire en résulte aisément dans tous les deux cas.

Lemme 7. *Soit $\pi(x)$ un polynôme à coefficients entiers sur L et soient α_i, α_k des entiers réels dans L. Si l'on a*

$$(12)\qquad N_{L/Q}^2(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi^2(\alpha_i-\alpha_k)\prod_{\varphi\in S_2}\varphi(\alpha_i-\alpha_k) > 2^{2[L:Q]}N_{L/Q}^2\big(\pi(\alpha_i)\pi(\alpha_k)\big)\times$$

$$\times\prod_{\varphi\in S_1}\varphi^2\big(\pi(\alpha_i)\pi(\alpha_k)\big)\prod_{\varphi\in S_2}\max\big(\varphi(\pi(\alpha_i)\overline{\pi(\alpha_k)}),\,\varphi(\overline{\pi(\alpha_i)}\pi(\alpha_k))\big) > 0,$$

alors

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

DÉMONSTRATION. D'après l'hypothèse

$$\alpha_i-\alpha_k\,|\,\pi(\alpha_i)-\pi(\alpha_k)\quad\text{et}\quad\alpha_i-\alpha_k\,|\,\overline{\pi(\alpha_i)}-\overline{\pi(\alpha_k)},$$

par conséquent

$$\alpha_i-\alpha_k\,|\,\pi(\alpha_i)\overline{\pi(\alpha_k)}-\overline{\pi(\alpha_i)}\pi(\alpha_k) = 2i\,\mathrm{Im}\,\pi(\alpha_i)\overline{\pi(\alpha_k)} = \gamma_{ik}.$$

Il en résulte

$$(13)\qquad N_{L/Q}(\alpha_i-\alpha_k)\prod_{\varphi\in S_1\cup S_2}\varphi(\alpha_i-\alpha_k)\,|\,N_{L/Q}(\gamma_{ik})\prod_{\varphi\in S_1\cup S_2}\varphi(\gamma_{ik})$$

et

$$(14)\qquad N_{L/Q}(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi(\alpha_i-\alpha_k)\,|\,N_{L/Q}(\gamma_{ik})\prod_{\varphi\in S_1}\varphi(\gamma_{ik}).$$

En utilisant maintenant l'inégalité de norme (1), nous obtenons

$$(15)\qquad N_{L/Q}(\gamma_{ik})\prod_{\varphi\in S_1\cup S_2}\varphi(\gamma_{ik}) \leqq 2^{[L:Q]}N_{L/Q}\big(\pi(\alpha_i)\pi(\alpha_k)\big)\prod_{\varphi\in S_1}\varphi\big(\pi(\alpha_i)\pi(\alpha_k)\big)\times$$

$$\times\prod_{\varphi\in S_2}\max\big(\varphi(\pi(\alpha_i)\overline{\pi(\alpha_k)}),\,\varphi(\overline{\pi(\alpha_i)}\pi(\alpha_k))\big)$$

et

$$(16)\qquad N_{L/Q}(\gamma_{ik})\prod_{\varphi\in S_1}\varphi(\gamma_{ik}) \leqq 2^{[L:Q]}N_{L/Q}\big(\pi(\alpha_i)\pi(\alpha_k)\big)\prod_{\varphi\in S_1}\varphi\big(\pi(\alpha_i)\pi(\alpha_k)\big)$$

Si l'on a $\gamma_{ik}\neq 0$, c'est-à-dire $\overline{\pi(\alpha_i)}\pi^{-1}(\alpha_i)\neq\overline{\pi(\alpha_k)}\pi^{-1}(\alpha_k)$, alors en comparant le produit de (13) et de (14) avec le produit de (15) et de (16), on déduit

$$N_{L/Q}^2(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi^2(\alpha_i-\alpha_k)\prod_{\varphi\in S_2}\varphi(\alpha_i-\alpha_k) \leqq 2^{2[L:Q]}N_{L/Q}^2\big(\pi(\alpha_i)\pi(\alpha_k)\big)\times$$

$$\times\prod_{\varphi\in S_1}\varphi^2\big(\pi(\alpha_i)\pi(\alpha_k)\big)\prod_{\varphi\in S_2}\max\big(\varphi(\pi(\alpha_i)\overline{\pi(\alpha_k)}),\,\varphi(\overline{\pi(\alpha_i)}\pi(\alpha_k))\big),$$

contrairement à l'hypothèse (12).

Lemme 8. *Soit $\pi(x)$ un polynôme à coefficients entiers sur L. S'ils existent des entiers réels $\alpha_1,\ldots,\alpha_s$ ($s>\deg\pi$) dans L tels que leurs paires (α_i,α_k) satisfaisant à* (12) *forment un graphe connexe à s éléments, alors on a $\overline{\pi(x)}=\varrho\pi(x)$ avec un certain $\varrho\in L$.*

DÉMONSTRATION. Si le graphe des paires (α_i, α_k) satisfaisant à (12) est connexe, alors d'après le lemme 7. on déduit $\overline{\pi(\alpha_i)}\pi^{-1}(\alpha_i)=\varrho\in L$ $(i=1, \ldots, s)$. Soit

$$\pi(x) = \beta_0 x^k + \cdots + \beta_k$$

et substituons les $\alpha_1, \ldots, \alpha_s$ dans $\pi(x)$. Alors du système d'équation obtenu il résulte

$$\beta_j = \sum_{l=1}^{k+1} \sigma_{jl}\pi(\alpha_l) \qquad (j = 0, \ldots, k)$$

avec des nombres réels $\sigma_{jl}\in L$. On en déduit nécessairement $\overline{\beta_j}/\beta_j = \varrho$ $(j=0, \ldots, k)$ c'est-à-dire $\overline{\pi(x)}=\varrho\pi(x)$.

Lemme 9. *Soit $f(x)$ un polynôme sur L tel que* $(\operatorname{Re} f(x), i \operatorname{Im} f(x))=1$. *Alors $f(x)$ n'a aucun diviseur $\pi(x)$ du type $\overline{\pi(x)}=\varrho\pi(x)$ $(\varrho\in L)$.*

DÉMONSTRATION. Pour chaque diviseur $\pi(x)$ de $f(x)$ on a $\overline{\pi(x)}\,|\,\overline{f(x)}$ dans $L[x]$. Si l'on a maintenant $\overline{\pi(x)}=\varrho\pi(x)$ $(\varrho\in L)$, alors on conclut $\pi(x)\,|\,\overline{f(x)}$, $\pi(x)\,|\,f(x)\pm$ $\pm\overline{f(x)}$, c'est-à-dire $\pi(x)\,|\,(\operatorname{Re} f(x), i \operatorname{Im} f(x))$ dans $L[x]$, ce qui est contraire à l'hypothèse.

DÉMONSTRATION DU THÉORÈME 1. Supposons que $f(x)$ a un diviseur $\pi(x)\in L[x]$ à coefficients entiers de degré $<s$. Alors pour les paires convenables (α_i, α_k) on a $0\neq\pi(\alpha_i)\overline{\pi(\alpha_k)}\,|\,f(\alpha_i)\overline{f(\alpha_k)}$ d'après (4), c'est-à-dire $f(\alpha_i)f(\alpha_k)\neq 0$. En utilisant le lemme 6., de (4) il résulte

$$N_{L/Q}^2(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi^2(\alpha_i-\alpha_k)\prod_{\varphi\in S_2}\varphi(\alpha_i-\alpha_k) > 2^{2[L:Q]}N_{L/Q}^2\big(f(\alpha_i)f(\alpha_k)\big)\times$$

$$\times\prod_{\varphi\in S_1}\varphi^2\big(f(\alpha_i)f(\alpha_k)\big)\prod_{\varphi\in S_2}\max\big(\varphi(f(\alpha_i)\overline{f(\alpha_k)}), \varphi(\overline{f(\alpha_i)}f(\alpha_k))\big) \geqq$$

$$\geqq 2^{2[L:Q]}N_{L/Q}^2\big(\pi(\alpha_i)\pi(\alpha_k)\big)\prod_{\varphi\in S_1}\varphi^2\big(\pi(\alpha_i)\pi(\alpha_k)\big)\times$$

$$\times\prod_{\varphi\in S_2}\max\big(\varphi(\pi(\alpha_i)\overline{\pi(\alpha_k)}), \varphi(\overline{\pi(\alpha_i)}\pi(\alpha_k))\big) > 0.$$

Mais par l'hypothèse le graphe de ces paires est connexe et elle a $s>\deg\pi$ éléments, ainsi d'après le lemme 8. on en déduit $\overline{\pi(x)}=\varrho\pi(x)$ avec une constante $\varrho\in L$, ce qui entraîne une contradiction d'après le lemme 9.

DÉMONSTRATION DU THÉORÈME 2. Supposons qu'il existe une décomposition

$$f(x)=\pi_1(x)\pi_2(x)$$

avec des polynômes $\pi_1(x)$, $\pi_2(x)$ à coefficients entiers sur L. De $f(\alpha_k) = -\alpha\neq 0$ on déduit $\pi_1(\alpha_k)\pi_2(\alpha_k)\neq 0$ $(k=1, \ldots, m)$ et $\alpha\bar{\alpha}=f(\alpha_i)\overline{f(\alpha_k)}=\pi_1(\alpha_i)\,\pi_2(\alpha_i)\overline{\pi_1(\alpha_k)\pi_2(\alpha_k)}=$ $=\pi_1(\alpha_i)\overline{\pi_1(\alpha_k)}\cdot\pi_2(\alpha_i)\overline{\pi_2(\alpha_k)}$. Mais $N_{L/Q}\big(\overline{\pi_j(\alpha_k)}\big)=N_{L/Q}\big(\pi_j(\alpha_k)\big)$ et $\varphi\big(\overline{\pi_j(\alpha_k)}\big)=\varphi\big(\pi_j(\alpha_k)\big)$

($j=1, 2$; $\varphi \in S_1$, $k=1, \ldots, m$), par conséquent de (5) il résulte

$$N_{L/Q}^2(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi^2(\alpha_i-\alpha_k) > 2^{2[L:Q]}N_{L/Q}\big(\pi_1(\alpha_i)\pi_1(\alpha_k)\big)\prod_{\varphi\in S_1}\varphi\big(\pi_1(\alpha_i)\pi_1(\alpha_k)\big)\times$$
$$\times N_{L/Q}\big(\pi_2(\alpha_i)\pi_2(\alpha_k)\big)\prod_{\varphi\in S_1}\varphi\big(\pi_2(\alpha_i)\pi_2(\alpha_k)\big) > 0$$

pour chaque paire convenable (α_i, α_k). On en déduit que

$$N_{L/Q}(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi(\alpha_i-\alpha_k) > 2^{[L:Q]}N_{L/Q}\big(\pi_1(\alpha_i)\pi_1(\alpha_k)\big)\prod_{\varphi\in S_1}\varphi\big(\pi_1(\alpha_i)\pi_1(\alpha_k)\big) > 0$$

ou

$$N_{L/Q}(\alpha_i-\alpha_k)\prod_{\varphi\in S_1}\varphi(\alpha_i-\alpha_k) > 2^{[L:Q]}N_{L/Q}\big(\pi_2(\alpha_i)\pi_2(\alpha_k)\big)\prod_{\varphi\in S_1}\varphi\big(\pi_2(\alpha_i)\pi_2(\alpha_k)\big) > 0$$

est vrai. Donc, d'après le lemme 7. ($S_2=\varnothing$), on obtient $\overline{\pi_1(\alpha_i)}/\pi_1(\alpha_i)=\overline{\pi_1(\alpha_k)}/\pi_1(\alpha_k)$ ou $\overline{\pi_2(\alpha_i)}/\pi_2(\alpha_i)=\overline{\pi_2(\alpha_k)}/\pi_2(\alpha_k)$, c'est-à-dire $i\,\mathrm{Im}\,\pi_1(\alpha_i)\overline{\pi_1(\alpha_k)}=0$ ou $i\,\mathrm{Im}\,\pi_2(\alpha_i)\overline{\pi_2(\alpha_k)}=0$. Mais le produit

$$\pi_1(\alpha_i)\overline{\pi_1(\alpha_k)}\cdot\pi_2(\alpha_i)\overline{\pi_2(\alpha_k)} = f(\alpha_i)\overline{f(\alpha_k)} = \alpha\bar{\alpha} \neq 0$$

est réel, ainsi $\pi_1(\alpha_i)\overline{\pi_1(\alpha_k)}$ et $\pi_2(\alpha_i)\overline{\pi_2(\alpha_k)}$ sont simultanément réels. Vu que le graphe des paires (α_i, α_k) est connexe, il en résulte $\overline{\pi_j(\alpha_i)}=\varrho_j\pi_j(\alpha_i)$ ($j=1, 2$; $i=1, \ldots, m$), d'où $\overline{\pi_j(x)}=\varrho_j\pi_j(x)$ ($j=1, 2$) d'après $m>\deg\pi_1, \deg\pi_2$ (voir la démonstration du lemme 8.). Mais c'est une contradiction d'après le lemme 9 et l'hypothèse.

Lemme 10. (CAPELLI [14]*). *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. Si $f(x)-\alpha = \pi_1^{k_1}(x)\ldots\pi_r^{k_r}(x)$ est une décomposition en facteurs normés irréductibles sur $Q(\alpha)$, alors*

$$g\big(f(x)\big) = \prod_{i=1}^{r} N_{Q(\alpha)/Q}^{k_i}\big(\pi_i(x)\big) \tag{17}$$

est également une décomposition en facteurs irréductibles sur Q.

Il en résulte que le degré de chaque facteur irréductible de $g\big(f(x)\big)$ est divisible par $\deg g$ et le nombre des facteurs irréductibles de $f(x)-\alpha$ sur $Q(\alpha)$ et de $g\big(f(x)\big)$ sur Q est égal.

DÉMONSTRATION DU THÉORÈME 1′. 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 de $f_1(x)g(x)$, c'est-à-dire le corps L, est également un K-corps. Désignons par S_1 et S_2 toutes les continuations ns L des valuations p-adiques correspondant aux nombres premiers $p\in P_1$ et $p\in$ _ respectivement. D'après le lemme 4 les éléments de S_1 et de S_2 sont ous „réels" et „non réels" respectivement.

Étant donné un nombre premier p et un entier $\beta\in L$, on a

$$|N_{L/Q}(\beta)|_p = \prod_{\substack{\varphi\\ \varphi(p)\neq 1}}\varphi(\beta), \tag{18}$$

*) Dans [14] on trouve une forme moins générale de ce théorème. *Addendum.* Dans le livre de L. Rédei (Algebra, Akadémiai Kiadó, Budapest, 1967) on trouve une forme plus générale du lemme 10.

où les valuations normées φ sont tous „réelles" ou bien „non réelles" d'après le lemme 4.

Soit $g(x) = \Pi(x-\alpha)$ et $F(x) = f(x)-\alpha$. Alors on a

$$\{g(0)\}^{\frac{2[L:Q]}{n}} = \{N_{Q(\alpha)/Q}\}^{\frac{2[L:Q]}{[Q(\alpha):Q]}} = N^2_{L/Q}(\alpha) = N_{L/Q}(\alpha\bar{\alpha}).$$

De (6) on déduit

$$N^2_{L/Q}(\alpha_i-\alpha_k) \prod_{\varphi\in S_1} \varphi^2(\alpha_i-\alpha_k) \prod_{\varphi\in S_2} \varphi(\alpha_i-\alpha_k) = N^2_{L/Q}(\alpha_i-\alpha_k) \prod_{p\in P_1} \{ \prod_{\substack{\varphi \\ \varphi(p)\neq 1}} \varphi^2(\alpha_i-\alpha_k)\} \times$$

$$\times \prod_{p\in P_2} \{ \prod_{\substack{\varphi \\ \varphi(p)\neq 1}} \varphi(\alpha_i-\alpha_k)\} = N^2_{L/Q}(\alpha_i-\alpha_k) \prod_{p\in P_1} |N^2_{L/Q}(\alpha_i-\alpha_k)|_p \prod_{p\in P_2} |N_{L/Q}(\alpha_i-\alpha_k)|_p >$$

$$> \{2^n g^2(0) \prod_{p\in P_1} |g^2(0)|_p \prod_{p\in P_2} |g(0)|_p\}^{\frac{2[L:Q]}{n}} = 2^{2[L:Q]} N^2_{L/Q}(\alpha\bar{\alpha}) \times$$

$$\times \prod_{p\in P_1} |N^2_{L/Q}(\alpha\bar{\alpha})|_p \prod_{p\in P_2} |N_{L/Q}(\alpha\bar{\alpha})|_p = 2^{2[L:Q]} N^2_{L/Q}(\alpha\bar{\alpha}) \prod_{p\in P_1} \{ \prod_{\substack{\varphi \\ \varphi(p)\neq 1}} \varphi^2(\alpha\bar{\alpha})\} \times$$

$$\times \prod_{p\in P_2} \{ \prod_{\substack{\varphi \\ \varphi(p)\neq 1}} \max(\varphi(\alpha\bar{\alpha}), \varphi(\alpha\bar{\alpha}))\} = 2^{2[L:Q]} N^2_{L/Q}(F(\alpha_i)F(\alpha_k)) \times$$

$$\times \prod_{\varphi\in S_1} \varphi^2(F(\alpha_i)F(\alpha_k)) \prod_{\varphi\in S_2} \max(\varphi(F(\alpha_i)\overline{F(\alpha_k)}), \varphi(\overline{F(\alpha_i)}F(\alpha_k)) > 0$$

pour chaque paire considérée (α_i, α_k). Si ces paires forment un graphe connexe à s éléments, alors d'après le théorème 1 $F(x) = f(x)-\alpha$ n'a aucun facteur irréductible de degré $< s$ sur L et par conséquent sur $Q(\alpha)$ non plus. Enfin, du lemme 10. il résulte 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 $\leqq \frac{\deg f}{s}$. Donc, en particulier, de $s > \frac{\deg f}{2}$ déduit que $g(f(x))$ est irréductible sur Q.

Démonstration du théorème 2'. Elle s'obtient du théorème 2. (voir la démonstration précédente).

Démonstration du théorème 3. Vu que les nombres premiers $p \in P_1$, P_2 ne divisent pas

$$D^{[L:Q]}(f_1) = N_{L/Q}(D(f_1)) = \prod_{1\leqq k<i\leqq \deg f_1} N^2_{L/Q}(\alpha_i-\alpha_k),$$

on obtient $|N_{L/Q}(\alpha_i-\alpha_k)|p = 1$ pour chaque paire (α_i, α_k) $(i\neq k)$ de racines de $f_1(x)$. De (8) il résulte

$$N^2_{L/Q}(\alpha_i-\alpha_k) \geqq \{c(f_1)\}^{2[L:Q]} > 2^{2[L:Q]} \{g^2(0) \prod_{p\in P_1} |g^2(0)|_p \prod_{p\in P_2} |g(0)|_p\}^{\frac{2[L:Q]}{n}}.$$

Par conséquent le graphe de toutes les racines de $f_1(x)$ et connexe. En appliquant

maintenant le théorème 1′, d'après l'hypothèse $\deg f_1 > \frac{\deg f}{2}$ il résulte l'irréductibilité de $g(f(x))$ sur Q. On peut prouver de la même façon la deuxième partie de notre théorème.

DÉMONSTRATION DU THÉORÈME 4. Soient $a_1 < \cdots < a_m$ les racines entières différentes de $f(x)$. D'après $m > \frac{\deg f}{2}$ on a $m > 4g^{2/n}(0) + 1$ ($n = \deg g$). Par conséquent il existe un nombre entier v tel que $2g^{2/n}(0) < v-1 < m-2g^{2/n}(0)$. Il en résulte

$$2g^{2/n}(0) < v-1 \leqq a_v - a_1 < \cdots < a_m - a_1,$$

et

$$2g^{2/n}(0) < m-(v-1) \leqq a_m - a_{v-1} < \cdots < a_m - a_1.$$

Désignons par L le corps de décomposition de $g(x)$. Alors pour les différences précédentes $a_i - a_k$ on a

$$|a_i - a_k|^{2[L:Q]} = N^2_{L/Q}(a_i - a_k) > \{2^n g^2(0)\}^{\frac{2[L:Q]}{n}}$$

et le graphe de ces paires (a_i, a_k) est connexe. En appliquant maintenant le théorème 1′ dans la forme spéciale P_1, $P_2 = \varnothing$, nous obtenons l'irréductibilité de $g(f(x))$ sur Q.

DÉMONSTRATION DU THÉORÈME 5. Soient $a_1 < \cdots < a_m$ et soit $a_m - a_1 = \max_{i,j} |a_i - a_j| > 4g^{1/n}(0)$. Alors on a $a_i - a_1$ ou $a_m - a_i \geqq \frac{a_m - a_1}{2} > 2g^{1/n}(0)$ pour chaque $i (\neq 1, m)$. Par conséquent ils existent des paires (a_i, a_k) telles que $|a_i - a_k| > 2g^{1/n}(0)$, c'est-à-dire

$$|a_i - a_k|^{[L:Q]} = N_{L/Q}(a_i - a_k) > \{2^n g(0)\}^{\frac{[L:Q]}{n}}$$

et ces paires (a_i, a_k) forment un graphe connexe à m éléments. D'après le théorème 2′ on en déduit l'irréductibilité de $g(f(x))$ sur Q. Si maintenant $g(x)$ est fixé et $\max_{i,j} |a_i - a_j| \leqq 4g^{1/n}(0)$, alors on peut supposer que $0 \leqq a_i \leqq 4g^{1/n}(0)$ pour chaque i. Donc, du point de vue de l'irréductibilité de $g(f(x))$ il y a seulement un nombre fini d'exceptions essentiellement différentes et ces ecxeptions peuvent être déterminées.

Lemme 11. *Soient $f(x)$ et $g(x)$ des polynômes satisfaisant aux conditions du théorème 5, et supposons que $g(0) = 1$. S'ils existent des paires (a_i, a_k) des $a_1, \ldots, a_m$ telles que $|a_i - a_k| > 2$ et si ces paires forment un graphe connexe ayant plus de $m/2$ éléments, alors $g(f(x))$ est irréductible sur Q.*

DÉMONSTRATION. Ce lemme est un cas particulier du théorème 1′, mais dans la suite il sera utilisé toujours dans cette forme.

Lemme 12. *Si ε_1 et ε_2 sont des unités non réelles dans un K-corps et*

$$\varepsilon_1 + \varepsilon_2 = 1, \tag{19}$$

alors on a nécessairement

$$\varepsilon_1 = \frac{1-\zeta_2}{\zeta_1-\zeta_2}, \quad \varepsilon_2 = \frac{\zeta_1-1}{\zeta_1-\zeta_2}, \tag{20}$$

où chacun des $\zeta_1, \zeta_2 (\neq \zeta_1)$, ζ_1/ζ_2 *est une racine d'unité primitive de degré* p^α *avec le même* p^α *(p nombre premier) ou bien aucune des degrés des racines d'unité* $\zeta_1, \zeta_2, \zeta_1/\zeta_2$ *n'est une puissance de nombres premiers.*

DÉMONSTRATION. Si ε_1 et ε_2 sont des solutions de (19) dans un K-corps, alors d'après le théorème du point 2 on peut écrire $\bar{\varepsilon}_1 = \zeta_1 \varepsilon_1$, $\bar{\varepsilon}_2 = \zeta_2 \varepsilon_2$ avec des racines d'unité ζ_1, ζ_2. En effet, si dans le théorème nous choisissons $S = S_\infty$ et si, par exemple, $\varepsilon_1 \in \{V, U_s^\circ\}$, alors $\varepsilon_1 = \zeta_1 \varepsilon_0$ et $\bar{\varepsilon}_1 = \zeta_1^{-1} \varepsilon_0$ avec une racine d'unité ζ_1 et avec une unité réelle ε_0. Par conséquent $\bar{\varepsilon}_1 = \zeta_1^{-2} \varepsilon_1$, où ζ_1^{-2} est une racine d'unité. Dans le cas contraire, si $\varepsilon_1 \notin \{V, U_s^\circ\}$, alors $\bar{\varepsilon}_1 \notin \{V, U_s^\circ\}$ et d'après $[U_s: \{V, U_s^\circ\}] \leqq 2$ on a $\bar{\varepsilon}_1/\varepsilon_1 \in \{V, U_s^\circ\}$, c'est-à-dire $\bar{\varepsilon}_1 = \varepsilon_1 \zeta \varepsilon_0$ avec une racine d'unité ζ et avec une unité réelle ε_0. Il en résulte $\varepsilon_1 = \bar{\varepsilon}_1 \zeta^{-1} \varepsilon_0$, d'où $\varepsilon_0 = \pm 1$ et $\bar{\varepsilon}_1 = \pm \zeta \varepsilon_1$, $\zeta_1 = \pm \zeta$. De plus de (19) on obtient $\bar{\varepsilon}_1 + \bar{\varepsilon}_2 = 1$ et il en résulte (20).

Soient maintenant $\zeta_1 = e^{2\pi i \frac{a_1}{q_1}}$, $(a_1, q_1) = 1$ et $\zeta_2 = e^{2\pi i \frac{a_2}{q_2}}$, $(a_2, q_2) = 1$ et prenons le corps $Q(\zeta_1, \zeta_2)$. Alors $\varepsilon_1, \varepsilon_2$ sont des unités aussi dans $Q(\zeta_1, \zeta_2)$. En considérant la décomposition $x^{q_1 q_2} - 1 = \prod_{d | q_1 q_2} F_d(x)$ en polynômes cyclotomiques $F_d(x)$, on peut montrer par induction que $1 - \zeta_1$ et $1 - \zeta_2$ sont des unités simultanément si et seulement si aucun des q_1, q_2 n'est de la forme p^α. Pour que $\varepsilon_1, \varepsilon_2$ soient des unités dans $Q(\zeta_1, \zeta_2)$ il faut et il suffit que $1 - \zeta_1, 1 - \zeta_2$ et $1 - \zeta_1/\zeta_2$ soient associés entre eux. Si $1 - \zeta_1$, $1 - \zeta_2$ ne sont pas des unités, alors on a $q_1 = p^{\alpha_1}$, $q_2 = p^{\alpha_2}$ avec le même premier p, parce que dans le cas contraire on aurait $((1 - \zeta_1), (1 - \zeta_2)) = 1$ et $\varepsilon_1, \varepsilon_2$ ne seraient pas des unités. Si maintenant $\alpha_1 < \alpha_2$, alors on déduit $1 - \zeta_2 | 1 - \zeta_1$ et $1 - \zeta_1 \nmid 1 - \zeta_2$, ce qui est impossible. Donc, on a $\alpha_1 = \alpha_2 = \alpha$. Enfin il faut que ζ_1/ζ_2 soit également une p^α-ième racine primitive de l'unité. Si $1 - \zeta_1$, $1 - \zeta_2$ sont des unités simultanément, alors il faut que $1 - \zeta_1/\zeta_2$ soit également une unité, par conséquent dans ce cas aucun des degrés de $\zeta_1, \zeta_2, \zeta_1/\zeta_2$ n'est une puissance de nombres premiers.

On peut aisément vérifier que dans ces cas les nombres $\varepsilon_1, \varepsilon_2$ sont des unités non réelles dans le K-corps $Q(\zeta_1, \zeta_2)$ (et par conséquent dans tous les K-corps $L \supseteq Q(\zeta_1, \zeta_2)$) et ils satisfont à l'équation (19).

Lemme 13. *Soit* $\varepsilon = \dfrac{(1-\zeta_1)(1-\zeta_2)}{(\zeta_1-\zeta_2)^2}$ *avec des racines d'unité* ζ_1, ζ_2 $(\zeta_2 \neq \zeta_1, \bar{\zeta}_1)$ *satisfaisant aux conditions du lemme 12. Alors* $\zeta_1, \zeta_2 \in Q(\varepsilon)$ *si et seulement s'il n y a aucune q-ième racine d'unité primitive* ζ *telle que* $\zeta_1 = \zeta^a$, $\zeta_2 = \zeta^b$, $(a, q) = (b, q) = 1$, $a^2 \equiv b^2 \pmod{q}$ *et* $q \neq p^\alpha$ $(p \geqq 3$ *nombre premier).*

DÉMONSTRATION. ε étant non réel, $Q(\varepsilon)$ est un K-corps non réel et $\bar{\varepsilon} \in Q(\varepsilon)$, c'est-à-dire $\zeta_1 \zeta_2 = \dfrac{\bar{\varepsilon}}{\varepsilon} \in Q(\varepsilon)$. D'après $\varepsilon = \dfrac{1 - (\zeta_1 + \zeta_2) + \zeta_1 \zeta_2}{(\zeta_1 + \zeta_2)^2 - 4\zeta_1 \zeta_2}$ on a $[Q(\zeta_1 + \zeta_2): Q(\varepsilon)] \leqq 2$ et $[Q(\zeta_1, \zeta_2): Q(\varepsilon)] \leqq 4$.

Supposons que ζ_1 ou $\zeta_2 \notin Q(\varepsilon)$. Alors, il en résulte $[Q(\zeta_1, \zeta_2): Q(\varepsilon)] \geqq 2$. Soit $\zeta_1 = e^{2\pi i \frac{a_1}{q_1}}$, $(a_1, q_1) = 1$ et $\zeta_2 = e^{2\pi i \frac{a_2}{q_2}}$, $(a_2, q_2) = 1$. Alors on peut écrire $Q(\zeta_1, \zeta_2) =$

$=Q(\zeta)$, où $\zeta=e^{\frac{2\pi i}{q}}$, $q=[q_1, q_2]$ (voir, par exemple, S. Lang, Algebraic Number, New York—London, 1964.) Soit $a=a_1q_2(q_1, q_2)^{-1}$, $b=a_2q_1(q_1, q_2)^{-1}$ et $\zeta_1=\zeta^a$, $\zeta_2=\zeta^b$, où $a\not\equiv\pm b \pmod q$ par hypothèse. Considérons $\beta=\dfrac{1-\zeta^b}{\zeta^a-\zeta^b}$, $\gamma=\dfrac{\zeta^a-1}{\zeta^a-\zeta^b}$, où $-\gamma\beta=\varepsilon$. Nous montrons que β et γ sont des éléments primitifs dans $Q(\zeta)$. Dans le cas contraire on aurait $\beta=\dfrac{1-\zeta^b}{\zeta^a-\zeta^b}=\dfrac{1-\zeta^{lb}}{\zeta^{la}-\zeta^{lb}}=\beta^{(l)}$ pour un automorphisme $\zeta\to\zeta^l$, $(l, q)=1$, $l\not\equiv 1 \pmod q$ et il en résulterait $\dfrac{1-\zeta^{-b}}{\zeta^{-a}-\zeta^{-b}}=$ $=\dfrac{1-\zeta^{-lb}}{\zeta^{-la}-\zeta^{-lb}}$, d'où $\dfrac{\zeta^a(1-\zeta^b)}{\zeta^a-\zeta^b}=\dfrac{\zeta^{la}(1-\zeta^{lb})}{\zeta^{la}-\zeta^{lb}}$, c'est-à-dire $\zeta_1^{(l)}=\zeta^{la}=\zeta^a=\zeta_1$. Mais alors de $\beta=\beta^{(l)}$ on obtient $\zeta^a(\zeta^{lb}-\zeta^b)=\zeta^{lb}-\zeta^b$ et, d'après $\zeta_1=\zeta^a\neq 1$, $\zeta_2^{(l)}=\zeta^{lb}=$ $=\zeta^b=\zeta_2$. En appliquant l'automorphisme $\zeta\to\zeta^{(l)}$, tous les éléments de $Q(\zeta_1, \zeta_2)=$ $=Q(\zeta)$ seraient fixés. Par conséquent $l\equiv 1 \pmod q$ et β est primitif dans $Q(\zeta)$. On peut démontrer de la même manière que γ est également primitif dans $Q(\zeta)$. Vu que $\beta+\gamma=1$, on peut écrire le polynôme $x(x+1)-\varepsilon$ sous la forme

$$x(x+1)-\varepsilon=(x+\beta)(x+\gamma)$$

d'où

$$N_{Q(\varepsilon)/Q}^{[Q(\zeta):Q(\varepsilon)]}\big(x(x+1)-\varepsilon\big)=N_{Q(\zeta)/Q}\big(x(x+1)-\varepsilon\big)=N_{Q(\zeta)/Q}(x+\beta)N_{Q(\zeta)/Q}(x+\gamma).$$

Mais les polynômes $N(x+\beta)$ et $N(x+\gamma)$ sont irréductibles sur Q, par conséquent $N_{Q(\zeta)/Q}(x+\beta)=N_{Q(\zeta)/Q}(x+\gamma)=N_{Q(\varepsilon)/Q}\big(x(x+1)-\varepsilon\big)$ et $[Q(\zeta):Q(\varepsilon)]=2$. Il en résulte que β et γ sont conjugués entre eux sur Q, c'est-à-dire avec un automorphisme $\zeta\to\zeta^k$ $(k, q)=1$ on a

$$\beta=\frac{1-\zeta^b}{\zeta^a-\zeta^b}=\frac{\zeta^{ka}-1}{\zeta^{ka}-\zeta^{kb}}=\gamma^{(k)}, \tag{21}$$

où $k\not\equiv 1 \pmod q$, parce que dans le cas contraire de $\beta+\gamma=1$ on obtiendrait $2\gamma=1$, mais γ est une unité dans $Q(\zeta)$ d'après le lemme 12. De (21) on déduit

$$\frac{1-\zeta^{-b}}{\zeta^{-a}-\zeta^{-b}}=\frac{\zeta^{-ka}-1}{\zeta^{-ka}-\zeta^{-kb}} \quad \text{et} \quad \frac{\zeta^a(1-\zeta^b)}{\zeta^a-\zeta^b}=\frac{\zeta^{kb}(\zeta^{ka}-1)}{\zeta^{ka}-\zeta^{kb}},$$

et finalement $\zeta^a=\zeta^{kb}$. D'après (21) on en conclut $\zeta^b(\zeta^a-1)=\zeta^{ka}(\zeta^a-1)$ et $\zeta^b=\zeta^{ka}$. Donc, on a

$$ak\equiv b \pmod q \quad \text{et} \quad bk\equiv a \pmod q \tag{22}$$

et par conséquent $(a, q)|b$ et $(b, q)|a$. Il en résulte

$$\left(\frac{a_1q_2}{(q_1, q_2)}, [q_1, q_2]\right)\Bigg|\frac{a_2q_1}{(q_1, q_2)}\Rightarrow(a_1q_2, q_1q_2)\,|\,a_2q_1\Rightarrow q_2(a_1, q_1)\,|\,a_2q_1\Rightarrow q_2|q_1$$

et de la même manière $q_1|q_2$, c'est-à-dire $q_1=q_2=q$, d'où $a=a_1$, $b=a_2$ et $(a, q)=$ $=(b, q)=1$. De (22) on obtient $k\equiv ba^{-1}\equiv ab^{-1} \pmod q$, d'où $a^2\equiv b^2 \pmod q$. Enfin,

si $q=p^\alpha$ ($p\geqq 3$ nombre premier), alors $Q(\zeta)$ est cyclique et le corps réel $Q(\zeta+\zeta^{-1})$ est sous-corps unique de degré $[Q(\zeta):Q]/2$ dans $Q(\zeta)$. D'après $[Q(\zeta_1,\zeta_2):Q(\varepsilon)]=2$ on en déduit $\varepsilon\in Q(\zeta+\zeta^{-1})$. Mais d'après $\zeta_2\neq\bar{\zeta}$, ε n'est pas réel. Par conséquent $q\neq p^\alpha$ ($p\geqq 3$ nombre premier).

Réciproquement supposons que dans $\varepsilon=\dfrac{(1-\zeta_1)(1-\zeta_2)}{(\zeta_1-\zeta_2)^2}$ $(\zeta_2\neq\zeta_1,\bar{\zeta}_1)$ on a $\zeta_1=\zeta^a$, $\zeta_2=\zeta^b$ avec une racine d'unité ζ de degré $q\neq p^\alpha$ ($p\geqq 3$ nombre premier) telle que $(a,q)=(b,q)=1$, $a^2\equiv b^2 \pmod q$ et $a\not\equiv\pm b \pmod q$ d'après $\zeta_2\neq\zeta_1,\bar{\zeta}_1$. Soit $k\equiv ba^* \pmod q$, où $aa^*\equiv 1 \pmod q$. Alors $(k,q)=1$ et $k^2\equiv 1 \pmod q$, mais $k\not\equiv\pm 1 \pmod q$. Considérons l'automorphisme non identique $\zeta\to\zeta^k=\zeta^{ba^*}$ dans $Q(\zeta)$. D'après $a^2\equiv b^2 \pmod q$ on a

$$\varepsilon^{(k)}=\frac{(1-\zeta^{ka})(1-\zeta^{kb})}{(\zeta^{ka}-\zeta^{kb})^2}=\frac{(1-\zeta^b)(1-\zeta^a)}{(\zeta^b-\zeta^a)^2}=\varepsilon,$$

par conséquent ε n'est pas primitif dans $Q(\zeta)$, c'est-à-dire $[Q(\zeta):Q(\varepsilon)]\geqq 2$. Il en résulte que $\zeta_1,\zeta_2\notin Q(\varepsilon)$. Avec cela notre lemme est démontré.

Lemme 14. *Si ε_1 et ε_2 sont des unités non réelles dans un K-corps et*

$$\varepsilon_1+\varepsilon_2=2, \tag{23}$$

alors on a nécessairement

$$\varepsilon_1=1-\zeta,\quad \varepsilon_2=1+\zeta \tag{24}$$

où ζ est une racine d'unité et son degré $\neq p^\alpha$, $2p^\alpha$ (p nombre premier, $\alpha\geqq 0$).

DÉMONSTRATION. Si ε_1 et ε_2 sont des solutions de (23) et $\bar{\varepsilon}_1=\zeta_1\varepsilon_1$, $\bar{\varepsilon}_2=\zeta_2\varepsilon_2$, alors on en déduit que $\varepsilon_1=\dfrac{2(1-\zeta_2)}{\zeta_1-\zeta_2}$, $\varepsilon_2=\dfrac{2(\zeta_1-1)}{\zeta_1-\zeta_2}$, $\zeta_1\neq\zeta_2$ (voir la démonstration du lemme 12). De plus on a nécessairement $2|(\zeta_1-\zeta_2)|(1-\zeta_1/\zeta_2)$, c'est-à-dire $N_{Q(\zeta_1,\zeta_2)/Q}(2)|N_{Q(\zeta_1,\zeta_2)/Q}(1-\zeta_1/\zeta_2)$, d'où il résulte $\zeta_2=-\zeta_1$ et finalement (24) avec des unités $(1+\zeta)$ et $(1-\zeta)$. On en conclut (voir aussi la démonstration du lemme 12) que le degré de ζ n'est pas de la forme p^α ou $2p^\alpha$ (p nombre premier).

DÉMONSTRATION DU THÉORÈME 6. Pour $m\geqq 5$ notre proposition s'obtient du théorème 5.

Dans la suite nous supposons que $a_1<\cdots<a_m$. Dans le cas $m=5$ $g(f(x))$ est irréductible d'après $a_5-a_1>a_4-a_1>2$ et le lemme 11.

Soit ensuite $m=4$. Si les entiers a_1, a_2, a_3, a_4 ne sont pas consécutifs, alors $a_4-a_1\geqq 4$, a_3-a_1 ou $a_4-a_2>2$ et il en résulte également notre proposition. Dans le cas contraire on peut prendre $a_1=-1$, $a_2=0$, $a_3=1$, $a_4=2$. Si $g(f(x))$ est réductible sur Q, alors $f(x)-\varepsilon$ est également réductible sur $Q(\varepsilon)=L$, c'est-à-dire on peut écrire

$$f(x)-\varepsilon=(x+1)x(x-1)(x-2)-\varepsilon=\pi_1(x)\pi_2(x) \tag{25}$$

avec des polynômes à coefficients entiers $\pi_1(x)$, $\pi_2(x)$ sur L. D'après les lemmes 8 et 9 on a nécessairement $\deg\pi_1$, $\deg\pi_2>1$, c'est-à-dire $\pi_1(x)=x^2+\beta x+\gamma$, $\pi_2(x)=x^2+\delta x+\sigma$. Les $\pi_1(a_i)=\varepsilon_i$ sont des unités, par conséquent on peut écrire $\varepsilon_i=\zeta_i\varepsilon_i$

avec des racines d'unité ζ_i dans L. En appliquant le lemme 7, de $a_4-a_1>2$ il résulte $\zeta_4=\zeta_1$. De plus, de $a_3-a_1=2$ on déduit $2|\pi_1(a_3)-\pi_1(a_1)=\varepsilon_3-\varepsilon_1$ et $2|\bar{\varepsilon}_3-\bar{\varepsilon}_1=\zeta_3\varepsilon_3-\zeta_1\varepsilon_1$, c'est-à-dire $2|\zeta_3-\zeta_1$. En prenant maintenant les normes de ces nombres, on conclut $\zeta_3=-\zeta_1$ et $\zeta_2=-\zeta_4=-\zeta_1$. Considérons l'égalité

$$-\pi_1(a_1)+3\pi_1(a_2)-3\pi_1(a_3)+\pi_1(a_4)=-\varepsilon_1+3\varepsilon_2-3\varepsilon_3+\varepsilon_4=0$$

et prenons son conjugué complexe. Alors nous obtenons

$$-\varepsilon_1-3\varepsilon_2+3\varepsilon_3+\varepsilon_4=0$$

et finalement $\varepsilon_1=\varepsilon_4$, $\varepsilon_2=\varepsilon_3$. Donc, on a $\pi_1(-1)=\pi_1(2)$, $\pi_1(0)=\pi_1(1)$, d'où $\beta=-1$ et de la même manière $\delta=-1$. De (25) on déduit

$$\gamma+\sigma=-2,\quad \gamma\sigma=-\varepsilon.$$

Par conséquent $-\gamma$, $-\sigma$ sont des unités non réelles satisfaisant à l'équation (23). En conséquence du lemme 14 on a $-\gamma=1+\zeta$, $-\sigma=1-\zeta$ et finalement $\varepsilon=\zeta^2-1$ avec une racine d'unité satisfaisant au lemme 14. Mais $\zeta\in Q(\varepsilon)=Q(\zeta^2)$ si et seulement si le degré ζ est n *ou* $2n$, $n>1$ étant impaire. Dans ces cas $g(f(x))$ est réductible sur Q.

Supposons ensuite que $m=3$ et

$$f(x)-\varepsilon=(x+\beta)(x^2+\gamma x+\delta) \tag{26}$$

avec des polynômes à coefficients entiers sur $Q(\varepsilon)=L$. Si les entiers $a_1<a_2<a_3$ ne sont pas consécutifs, alors d'après les lemmes 8 et 9 $a_3-a_1>2$ entraîne une contradiction. Dans le cas contraire on peut prendre $a_1=-1$, $a_2=0$, $a_3=1$. Maintenant de (26) il résulte

$$\beta+\gamma=0,\quad \beta\gamma+\delta=-1,\quad \beta\delta=-\varepsilon,$$

c'est-à-dire

$$\varepsilon=\beta(1-\beta)(1+\beta).$$

Par conséquent β, $1-\beta$ et $1+\beta$ sont des unités non réelles dans L telles que $\beta+(1-\beta)=1$ et $(1-\beta)+(1+\beta)=2$. Donc, d'après les lemmes 12 et 14 on peut déterminer β et ε, par exemple $\beta=\zeta$, $\varepsilon=\pm(\zeta-\zeta^3)$, ζ étant une racine d'unité convenablement choisie. Mais dans ces cas les conjugués de $\zeta-\zeta^3$ sont différents dans $Q(\zeta)$, par conséquent $\zeta\in Q(\varepsilon)$ et ainsi on obtient les décompositions de la forme (26) dans $Q(\varepsilon)$, c'est-à-dire les polynômes exceptionnels.

Enfin, si $m=2$ et $f(x)-\varepsilon$ est réductible sur $Q(\varepsilon)$, alors on peut écrire

$$f(x)-\varepsilon=(x+\beta)(x+\gamma) \tag{27}$$

où β et γ sont des nombres non réels dans $Q(\varepsilon)$. Dans le cas $a_2-a_1>2$ on obtient une contradiction d'après les lemmes 8 et 9. Dans le cas $a_2-a_1=2$ on peut prendre $a_1=-2$, $a_2=0$. De (27) on déduit

$$\beta+\gamma=2,\quad \beta\gamma=-\varepsilon$$

avec des unités β, γ non réelles. Par conséquent, d'après le lemme 14 $\beta=1-\zeta$, $\gamma=1+\zeta$ et $\varepsilon=\zeta^2-1$ avec une racine d'unité primitive de degré $\neq p^\alpha$, $2p^\alpha$ (p nombre premier, $\alpha\geqq 0$). Mais (voir le cas $m=4$) $\zeta\in Q(\varepsilon)=Q(\zeta^2)$ si et seulement si le degré

de ζ est n *ou* $2n$, $n>1$ étant impaire. Il en résulte que $n \neq p^z$ ($p \geqq 3$ nombre premier). Enfin, si l'on a $a_2 - a_1 = 1$, par exemple $a_2 = 0$, $a_1 = -1$, alors de (27) il résulte

$$\beta + \gamma = 1, \quad \beta\gamma = -\varepsilon. \tag{28}$$

D'après le lemme 12 on a nécessairement

$$\beta = \frac{1-\zeta_2}{\zeta_1 - \zeta_2}, \quad \gamma = \frac{\zeta_1 - 1}{\zeta_1 - \zeta_2}$$

et

$$\varepsilon = \frac{(1-\zeta_1)(1-\zeta_2)}{(\zeta_1 - \zeta_2)^2}$$

avec des racines d'unité ζ_1, ζ_2, déterminées dans le lemme 12. Vu que ε est non réel, on a $\bar{\zeta}_2 \neq \zeta_1$. De plus par hypothèse β, $\gamma \in Q(\varepsilon)$. Mais $Q(\varepsilon)$ est un K-corps, ainsi $\bar{\beta}$, $\bar{\gamma} \in Q(\varepsilon)$, d'où on déduit $\zeta_1 = \frac{\bar{\beta}}{\beta}$, $\zeta_2 = \frac{\bar{\gamma}}{\gamma} \in Q(\varepsilon)$. Par conséquent, d'après le lemme 13 il n'existe pas de racine d'unité ζ de degré $q \neq p^z$ ($p \geqq 3$ nombre premier) telle que $\zeta_1 = \zeta^a$, $\zeta_2 = \zeta^b$, $(a, q) = (b, q) = 1$, $a^2 \equiv b^2 \pmod{q}$. Il en résulte que ε satisfait aux conditions du théorème.

Supposons ensuite que $\varepsilon = \frac{(1-\zeta_1)(1-\zeta_2)}{(\zeta_1 - \zeta_2)^2}$ avec des racines d'unité ζ_1, ζ_2 satisfaisant aux conditions du théorème (le cas $m=2$). Alors

$$\beta = \frac{1-\zeta_2}{\zeta_1 - \zeta_2}, \quad \gamma = \frac{\zeta_1 - 1}{\zeta_1 - \zeta_2}$$

sont des unités non réelles dans $Q(\zeta_1, \zeta_2)$ d'après le lemme 12. De plus, d'après le lemme 13 on a $\zeta_1, \zeta_2 \in Q(\varepsilon)$, c'est-à-dire β, $\gamma \in Q(\varepsilon)$. Par conséquent il existe la décomposition $x(x+1) - \varepsilon = (x+\beta)(x+\gamma)$ dans $Q(\varepsilon)$, et si $g(\varepsilon) = 0$, alors $g(x(x+1))$ est réductible sur Q.

Bibliographie

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

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

[3] H. L. Dorwart—O. Ore, Criteria for the irreducibility of polynomials, *Annals of Math.* **34** (1933), 81—94.

[4] W. Flügel, Lösung der Aufgabe 226, *Archiv. der Math und Phys.* **15** (1909), 271—272.

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

[6] K. Győry, Sur une classe des corps algébrique et ses applications, *sous presse*

[7] H. Ille, Einige Bemerkungen zu einem von G. Pólya herrührenden Irreduzibilitätskriterium, *Jber. Deutsch. Math. Verein.* **35** (1926), 204—208.

[8] G. Pólya, Verschiedene Bemerkungen zur Zahlentheorie, *Jber. Deutsch. Math. Verein.* **28** (1919), 31—40.

[9] G. Pólya und G. Szegő, Aufgaben und Lehrsätze aus der Analysis, Band II, *Berlin* 1964.

[10] I. Schur, Aufgabe 275, 259, *Archiv der Math. und Physik,* **15** (1909).

[11] I. SERES, Lösung und Verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome, *Acta Math. Acad. Sci. Hung.* (1956), 151—157.
[12] I. SERES, Irreducibility of polynomials, *J. Algebra,* **2** (1965), 283—286.
[13] I. SERES, Über die Irreduzibilität gewisser Polynome, *Acta Arithmetica* **8** (1963), 321—341.
[14] N. TSCHEBOTARÖW—H. SCHWERDTFEGER, Grundzüge der Galois'schen Theorie, *Gröningen—Djakarta,* 1950.
[15] U. WEGNER, Über die Irreduzibilität einer Klasse von ganzen rationalen Funktionen, *Jber. Deutschen Math. Verein.* **40** (1931), 239—241.

(Reçu le 3 janvier 1970.)