Representation of integers by norm forms II.

By KÁLMÁN GYŐRY (Debrecen) and LÁSZLÓ LOVÁSZ (Budapest)

1. Introduction

Let $1, \alpha_2, \ldots, \alpha_m$ be linearly independent algebraic numbers over the field R of rationals, and let n denote the degree of the algebraic number field $K = R(\alpha_1, \ldots, \alpha_m)$ (over R). The conjugates and the norm of an element $\alpha \in K$ will be denoted by $\alpha^{(1)}, \ldots, \alpha^{(n)}$ and $N_{K/R}(\alpha)$, respectively (in the field K). Let further

$$L^{(k)}(\mathbf{x}) = x_1 + \alpha_2^{(k)} x_2 + \ldots + \alpha_m^{(k)} x_m \qquad (k = 1, \ldots, n)$$

It is a question examined by many authors when the Diophantine equation

$$N_{K/R}(L(\mathbf{x})) = a; \qquad a \in R \tag{1}$$

has infinitely many solutions $\mathbf{x} = (x_1, \ldots, x_m)$ among rational integers.

In case $m = n$ the problem is solved. If (1) has a solution then it has infinitely many solutions and these can be represented by help of the units of K ([2] pp. 134—140.).

In case $m \leqq n$ the question is much more difficult, the answer depends on the structure of the module $M = \{1, \alpha_2, \ldots, \alpha_m\}$. The module M is called *degenerated*, if the vector space L over R generated by M has a subspace L' such that, for some $\gamma \in K$, $L'\gamma$ is a (not necessarily proper) subfield of K, different from R and the imaginary number fields of degree 2. Now if M is degenerated then there exists an $a \in R$ such that (1) has infinitely many solutions ([2], p. 322.). In the opposite case — i.e. if M is non-degenerated — by conjecture (1) has only finitely many solutions among rational integers for any $a \in R$.

This conjecture was proved by *A*. THUE ([5]) for $m = 2$ and by W. M. SCHMIDT ([4]) for $m = 3$. However, their method is not effective, it is not suitable to find all the solutions of (1). Recently A. BAKER ([1]) has given an algorithm to find all solutions of (1) in case $m = 2$ by showing that if $\varkappa > n + 1$ then every solution of (1) satisfies

$$\max(|x_1|, |x_2|) < \exp\{n^{v^2} H^{vn^2} + (\log|a| \cdot H)^n\} = \varphi(a, n, H, \varkappa)$$

where $H = H(\alpha_2)$ is the height[1]) of α_2 and $v = 32\varkappa/(\varkappa - u - 1)$ (supposing naturally that M is non-degenerated).

[1]) The maximum of absolute values of the relatively prime integer coefficients in the defining polynomial of α_2. In knowledge of $N(x_1 + \alpha_2 x_2)$, $H(\alpha_2)$ can be considered to be known too.

In [3] one of the authors proved the conjecture for $m=4$ and non-real Abelian number fields of degree not divisible by 3 and 4.

In the present paper we investigate the problem for those number fields K which are contained in a Galois field F (a normal extension of R) whose maximal real subfield is also a Galois field. These fields we be called *allowed*; thus allowed fields are the subfields of the non-real normal extensions (over R) of degree 2 of the real Galois fields, E.g. all Abelian number fields are allowed. We are going to show that in the case of allowed number fields K any solution $\mathbf{x} = (x_1, \dots, x_m)$ of (1) satisfies both

$$(2) \qquad \left|N_{F/R}(\operatorname{Re} L(\mathbf{x}))\right| \leqq |a|^{[F:K]} \quad \text{and} \quad \left|N_{F/R}(i \operatorname{Im} L(\mathbf{x}))\right| \leqq |a|^{[F:K]}$$

Using this and the above mentioned result of Baker we give an explicite bound for $\max(|x_1|, |x_2|, |x_3|)$ in case $m=3$, if K is a non-real allowed number field. Furthermore, we prove the conjecture [2]) in case $m=4$ for non-real allowed Galois fields of degree not divisible by 3 and 4. We give a second proof of this latter proposition too, using Dirichlet's theorem concerning units of algebraic number fields instead of (2).

2. Results

To state our results we need the following constants. Let

$$c(n, m, H) = [(m-1)!^6 n^{14(m-1)^2} H^{6m(m-1)^2}]^{n^{5m(m-1)^2}},$$

$$H_1(n, m, H) = [(m-1)c(n, m, H)n^{m-1} H^m]^{n^{m-1}},$$

$$b(a, n, H) = (2H_1(n, 3, H)^3)^{n^2} |a|^n c(n, 3, H)^{4n},$$

$$H_2(n, H) = [2H_1(n, 3, H)]^{5n^2}, \quad H_3(n, H) = [4n^4 H_2(n, H)]^{n^4},$$

$$\psi(a, n, H, \varkappa) = b^2 H_3^2 \varphi(b^{n^4}, n^3, H_3, \varkappa).$$

Then we have

Theorem 1. *Let $\{1, \alpha_2, \alpha_3\}$ be a non-degenerated module with linearly independent generators such that the field $K = R(\alpha_2, \alpha_3)$ is a non-real allowed number field of degree n. If the height of α_1 and α_2 is $\leqq H$ and $\varkappa > n^6+1$, then any solution (x_1, x_2, x_3) of the equation*

$$(1') \qquad N_{K/R}(x_1+\alpha_2 x_2+\alpha_3 x_3) = a \qquad (a \in R)$$

satisfies

$$\max(|x_1|, |x_2|, |x_3|) \leqq \psi(a, n, H, \varkappa)$$

Theorem 2. *Let F be a non-real allowed Galois field of degree not divisible by 3 and 4. Let further $1, \alpha_2, \alpha_3, \alpha_4$ be linearly independent generators of F. Then the equation*

$$(1'') \qquad N_{F/R}(x_1+\alpha_2 x_2+\alpha_3 x_3+\alpha_4 x_4) = a \qquad (a \in R)$$

has only finitely many solutions (x_1, x_2, x_3, x_4) in rational integers.

[2]) Added in pxoof: Recently Prof W. Schmidt proved the conjecture for all m.

3. Lemmas

Lemma 1. *If the coefficients of the linear form $L(\mathbf{x})$ are linearly independent elements of an allowed field K and $F \supseteq K$ is an allowed Galois-field, then any solution of* (1) *satisfies* (2).

PROOF. If K is real we have nothing to proof; assume that K and consequently F are non-real. Let G be the Galois group of F (over R). Since in our assumption the maximal real subfield S of F is normal, the cyclic group $\{\psi\}$ (of order 2) generated by the complex conjugation ψ (as automorphism) is a normal subgroup. Hence ψ belongs to the center of G.

Now if H is the subgroup corresponding to K then all isomorphisms of K in F can be described by the right cosets of H. Let $H\varphi_1, \ldots, H\varphi_n$ be these cosets. Since $\psi \in Z(G)$, we have for any $\varphi \in H\varphi_k$ $(1 \leqq k \leqq n)$

$$(\operatorname{Re} L(\mathbf{x}))\varphi = \frac{1}{2}(L(\mathbf{x}) + L(\mathbf{x})\psi)\varphi = \frac{1}{2}(L(\mathbf{x})\varphi_k + L(\mathbf{x})\varphi_k\psi) = \operatorname{Re}(L(\mathbf{x})\varphi_k)$$

Hence

$$N_{F/R}(\operatorname{Re} L(\mathbf{x})) = \prod_{\varphi}(\operatorname{Re} L(\mathbf{x}))\varphi = \left[\prod_{k=1}^{n} \operatorname{Re}(L(\mathbf{x})\varphi_k)\right]^{[F:K]}$$

and since

$$|L(\mathbf{x})\varphi_k| \geqq |\operatorname{Re}(L(\mathbf{x})\varphi_k)|$$

we have

$$|a|^{[F:K]} = |N_{F/R}(L(\mathbf{x}))| \geqq \left|\prod_{k=1}^{n} \operatorname{Re}(L(\mathbf{x})\varphi_k)^{[F:K]}\right| = |N_{F/R}(\operatorname{Re} L(\mathbf{x}))|$$

The second statement of (2) follows similarly.

We are going to apply Baker's result onto one of the inequalities (2). This can be done only if one of the forms $\operatorname{Re} L(\mathbf{x})$, $\operatorname{Im} L(\mathbf{x})$ has two variables at the most, its coefficients are linearly independent and generate a non-generated module. This is not the case in general but it can be reached by multiplying (1′) by the norm of an appropriate element of F and by applying a linear transformation. In lemmas 2. and 3. this will be carried out.

Before stating them we remark that the heights of α, $\bar{\alpha}$ and $1/\alpha$ are equal and the same holds for their degrees. Furthermore, if $d(\alpha)$ is the degree of α then $|\alpha| \leqq d(\alpha)H(\alpha)$. Using this one easily verifies that $d(\alpha\beta), d(\alpha+\beta) \leqq d(\alpha)d(\beta)$, and if f is a polynomial of degree l having integer coefficients and $s \geqq l$ variables, $H(\alpha_i) \leqq H$ and $d(\alpha_i) \leqq d (1 \leqq i \leqq s)$, then

$$d(f(\alpha_1, \ldots, \alpha_s)) \leqq d^s,$$

$$H(f(\alpha_1, \ldots, \alpha_s)) \leqq (\|f\| \cdot d^s H^{l(s+1)})^{d^s} \tag{3}$$

(here $\|f\|$ means the sum of absolute values of the coefficients of f).

Lemma 2. *One can find a linear, non-singular transformation $Y = CX$ with integer coefficients transforming* (1) *into an equation*

$$N_{K/R}(y_1 + \alpha_2' y_2 + \ldots + \alpha_m' y_m) = a_1 \tag{4}$$

of the following properties:

(a) *the non-zero imaginary parts of* $1, \alpha_2', \ldots, \alpha_m'$ *are linearly independent*;

(b) $\max H(\alpha_i') \leqq H_1(n, m, H)$

$$|a_1| \leqq |a| \cdot c(n, m, H)^{(m-1)2n}$$

(c) *If* $\mathbf{x}$ *is a solution of* (1) *and* $\mathbf{y} = C\mathbf{x}$ *is the corresponding solution of* (4) *then*

$$\max_i |x_i| \leqq (m-1) c(n, m, H) \max_i |y_i|$$

Remark: The systems $\{1, \alpha_2, \ldots, \alpha_m\}$ and $\{1, \alpha_2', \ldots, \alpha_m'\}$ are both linearly dependent or linearly independent and since they generate the same vector space over R they are both degenerated or non-degenerated.

PROOF. Let, say, $\operatorname{Im} \alpha_2, \ldots, \operatorname{Im} \alpha_l$ be a maximal independent subsystem of the imaginary parts $(2 \leqq l \leqq m)$. Then

$$\begin{aligned} \operatorname{Im} \alpha_{l+1} &= c'_{l+1,2} \operatorname{Im} \alpha_2 + \ldots + c'_{l+1,l} \operatorname{Im} \alpha_l \\ &\vdots \\ \operatorname{Im} \alpha_m &= c'_{m,2} \operatorname{Im} \alpha_2 + \ldots + c'_{m,l} \operatorname{Im} \alpha_l \end{aligned} \tag{5}$$

where the $c'_{r,s}$-s are rational. Let c denote the l. c. m. of the denominators of the $c'_{r,s}$-s. Put $c_{r,s} = c \cdot c'_{r,s}$ and consider the substitution

$$\begin{aligned} y_1 &= cx_1 \\ y_2 &= \quad cx_2 \quad + c_{l+1,2} x_{l+1} + \ldots + c_{m,2} x_m \\ &\vdots \qquad \ddots \qquad \vdots \qquad \vdots \\ y_l &= \qquad cx_l + c_{l+1,l} x_{l+1} + \ldots + c_{m,l} x_m \\ y_{l+1} &= \qquad cx_{l+1} \\ &\vdots \qquad \ddots \\ y_m &= \qquad cx_m \end{aligned} \tag{6}$$

Multiplying both sides of (1) by c^n and carrying out this substitution we obtain the equality (4), where

$$\begin{aligned} \alpha_2' &= \alpha_2 \\ &\vdots \qquad \ddots \\ \alpha_l' &= \qquad \alpha_l \\ \alpha_{l+1}' &= -c'_{l+1,2} \alpha_2 - \ldots - c'_{l+1,l} \alpha_l + \alpha_{l+1} \\ &\vdots \qquad \vdots \qquad \vdots \qquad \ddots \\ \alpha_m' &= -c'_{m,2} \alpha_2 - \ldots - c'_{m,l} \alpha_l \qquad + \alpha_m \end{aligned} \tag{7}$$

Here $\operatorname{Im} \alpha'_{l+1} = \ldots = \operatorname{Im} \alpha_m' = 0$ and $\operatorname{Im} \alpha_2', \ldots, \operatorname{Im} \alpha_l'$ are linearly independent.

Now we deal with the necessary estimations. First let us consider the heights of the $c'_{r,s}$-s. Since in our assumption $i\operatorname{Im}\alpha_2, \ldots, i\operatorname{Im}\alpha_l$ are linearly independent, we can find certain indices $i_1, \ldots, i_{l-1}$ such that

$$\beta = \begin{vmatrix} (i\operatorname{Im}\alpha_2)^{(i_1)} & \ldots (i\operatorname{Im}\alpha_l)^{(i_1)} \\ \vdots & \vdots \\ (i\operatorname{Im}\alpha_2)^{(i_{l-1})} & \ldots (i\operatorname{Im}\alpha_l)^{(i_{l-1})} \end{vmatrix}$$

Then $c'_{r,s}$ $(l+1 \leqq r \leqq m,\ 2 \leqq s \leqq l)$ can be determined from the system of equalities

$$\begin{aligned} (i\operatorname{Im}\alpha_r)^{(i_1)} &= c'_{r,2}(i\operatorname{Im}\alpha_2)^{(i_1)} + \ldots + c'_{r,l}(i\operatorname{Im}\alpha_l)^{(i_1)} \\ &\ \vdots \\ (i\operatorname{Im}\alpha_r)^{(i_{l-1})} &= c'_{r,2}(i\operatorname{Im}\alpha_2)^{(i_{l-1})} + \ldots + c'_{r,l}(i\operatorname{Im}\alpha_l)^{(i_{l-1})} \end{aligned}$$

as a quotient where the denominator is the determinant β and the numerator is a determinant of similar type. Now by (3),

$$d(i\operatorname{Im}\alpha_k) = d\left(\frac{\alpha_k - \bar{\alpha}_k}{2}\right) \leqq n^2, \quad H(i\operatorname{Im}\alpha_k) \leqq (4n^2H^3)^{n^2},$$

$$d\left(\frac{1}{\beta}\right) = d(\beta) \leqq n^{2(m-1)^2}, \quad H\left(\frac{1}{\beta}\right) = H(\beta) \leqq [(m-1)!\, n^{2(m-1)^2} H^{m(m-1)^2}]^{n^{(m-1)^2}}$$

hence, applying (3) again,

$$H(c'_{r,s}) \leqq c(n, m, H).$$

c being the l. c. m. of the denominators of the $c'_{r,s}$-s,

$$\max(|c|, |c_{r,s}|) \leqq c(n, m, H)^{(m-1)^2}$$

Hence

$$|a_1| = |ac^n| \leqq |a| \cdot c(n, m, H)^{(m-1)^2 n}$$

Since

$$|c'_{r,s}| \leqq H(c'_{r,s}) \leqq c(n, m, H),$$

(6) gives

$$\max_i |x_i| \leqq (m-1)\, c(n, m, H) \max_i |y_i|$$

and, finally, (7) implies

$$H(\alpha'_i) \leqq H_1(n, m, H),$$

which was to be proved.

Lemma 3. *Let $1, \alpha_2, \alpha_3$ be linearly independent algebraic numbers and assume that $M = \{1, \alpha_2, \alpha_3\}$ is non-real and non-degenerated. Then there exists a linear, non-singular transformation $Z = AX$ with integer coefficients, such that the application of A and appropriate expontation of both sides of* (1′) *tranforms* (1′) *into an equation*

$$N_{K'/R}(\alpha'_1 z_1 + \alpha'_2 z_2 + \alpha'_3 z_3) = a_2 \tag{8}$$

where $K \subseteqq K' = R(\alpha'_1, \alpha'_2, \alpha'_3)$ is of degree $\leqq n^2$, the module $\{i\operatorname{Im}\alpha'_1, i\operatorname{Im}\alpha'_2, i\operatorname{Im}\alpha'_3\}$

has at most two generators different from 0, *these are linearly independent and generate a non-degenerated module, furthermore*

$$|a_2| \leqq |a|^n c(n, 3, H)^{4n}$$
$$H(\alpha_i') \leqq H_1(n, 3, H)$$

and the corresponding solutions of (1′) *and* (8) *satisfy*

$$\max_i |x_i| \leqq 2c(n, 3, H) \max_i |y_i|$$

Remark: The proof shows that if K is allowed then so is K'.

PROOF. Put $\alpha_k = \beta_k + i\gamma_k$ $(k=2, 3)$ in (1′). If γ_2 and γ_3 are linearly dependent then by lemma 2 (1′) can be transformed into a form like (8), where $K' = \boldsymbol{K}$ and then the required inequalities follow trivially.

Thus we may assume that γ_2, γ_3 are linearly independent. Put $i\gamma_3 = \gamma \cdot i\gamma_2$. If γ is of degree $\geqq 3$ we have nothing to prove since (1′) itself satisfies the requirements. Thus we may confine ourselves to the case $d(\gamma) = 2$.

Put $\delta = \beta_3 - \gamma\beta_2 = \alpha_3 - \gamma\alpha_2$. Now $\delta \notin R(\gamma)$, since otherwise we would have $\alpha_3 - \gamma\alpha_2 = r_1\gamma - r_2$ with some rational coefficients r_1, r_2, which would imply

$$\gamma = \frac{\alpha_3 - r_2}{\alpha_2 + r_1},$$

i.e. that $\{1, \alpha_2, \alpha_3\}$ is degenerated, which is a contradiction. Hence either $\gamma - \delta$ or $\gamma + \delta$, say $\gamma - \delta$ is of degree $\geqq 3$.

Put $K' = K(\bar{\alpha}_2) \subseteqq F$. Consider the $[K':K]$-th power of both sides of (1′), multiply by $N_{K'/R}(1+\bar{\alpha}_2)$ and substitute $z_1 = x_1 - x_2, z_2 = x_2, z_3 = x_3$

$$N_{K'/R}\big((1+\bar{\alpha}_2)z_1 + (1+\bar{\alpha}_2)(1+\alpha_2)z_2 + (1+\bar{\alpha}_2)\alpha_3 z_3\big) = a^{[K':K]} N_{K'/R}(1+\bar{\alpha}_2).$$

Here $\operatorname{Im}(1+\bar{\alpha}_2) = \gamma_2$, $\operatorname{Im}(1+\bar{\alpha}_2)(1+\alpha_2) = 0$, $\operatorname{Im}(1+\bar{\alpha}_2)\alpha_3 = \gamma_2(\gamma - \delta)$, i.e. we have obtained an equality of the required type. The necessary estimations are trivial.

4. Proofs of the theorems

Proof of theorem 1. By lemma 3, it is enough to find an upper bound for the solutions of equality (8). We may assume that $\operatorname{Im} \alpha_1' = 0$ and either $\operatorname{Im} \alpha_2' = 0$, $\operatorname{Im} \alpha_3' \neq 0$ or $\operatorname{Im} \alpha_2', \operatorname{Im} \alpha_3'$ are linearly independent and $\{i \operatorname{Im} \alpha_2', i \operatorname{Im} \alpha_3'\}$ is non-degenerated.

There exists a rational integer c with $|c| \leqq 2H_2^3$ such that $\alpha_k'' = c\alpha_k'$, $i \operatorname{Im} \alpha_k''$ $(k = 1, 2, 3)$ are algebraic integers. Multiplying both sides of (8) by $N_{K'/R}(c) = c^{(K':R)}$,

$$N_{K'/R}(\alpha_1'' z_1 + \alpha_2'' z_2 + \alpha_3'' z_3) = a_3 \tag{9}$$

where $\quad |a_3| = |a_2 c^{[K':R]}| \leqq b(a, n, H)$ and $H(\alpha_k'') \leqq H_2(n, H)$.

Assume first that in (8) we have $\operatorname{Im} \alpha_1'' = \operatorname{Im} \alpha_2'' = 0$. Let F be an allowed Galois extension of K, then, as we have noticed after lemma 3, $K' \subseteqq F$ and similarly $K''=K'(\bar{\alpha}_3'')\subseteq F$ where K'' is of degree $\leqq n^4$. Applying now lemma 1 onto the equality (9), we obtain

$$|a_3|^{[F:K']}\geqq|N_{K''/R}(i\operatorname{Im}\alpha_3''z_3)|^{[F:K'']}\geqq|z_3|^{[F:R]},$$

hence

$$|z_3|\leqq|a_3|\leqq b(a,n,H).$$

Now if $z_3=0$, then (9) gives, by the mentioned result of Baker, that

$$\max(|z_1|,|z_2|)\leqq\varphi(b,n^2,H_2,\varkappa).$$

If $z_3\neq 0$, (9) gives

$$|a_3|^{[F:K']}\geqq\left|\frac{L^{(k)}(z)}{i\operatorname{Im}L^{(k)}(z)}\right|^{[F:K']}|N_{K''/R}(i\operatorname{Im}\alpha_3''z_3)|^{[F:K'']}\geqq\left|\frac{L^{(k)}(z)}{i\operatorname{Im}\alpha_3''^{(k)}}\right|^{[F:K']}$$

hence we have for every $1\leqq k\leqq n$

$$|L^{(k)}(z)|\leqq|a_3|\,|i\operatorname{Im}\alpha_3''^{(k)}|\leqq bn^4H_3$$

Now $\alpha_1'',\alpha_2'',\alpha_3''$ are linearly independent, therefore we can find a pair j,k of indices such that

$$\beta=\begin{vmatrix}\alpha_1''^{(j)} & \alpha_2''^{(j)}\\ \alpha_1''^{(k)} & \alpha_2''^{(k)}\end{vmatrix}\neq 0$$

Expressing z_1,z_2 from the equalities

$$\alpha_1''^{(j)}z_1+\alpha_2''^{(j)}z_2=L^{(j)}(z)-\alpha_3''^{(j)}z_3$$

$$\alpha_1''^{(k)}z_1+\alpha_2''^{(k)}z_2=L^{(k)}(z)-\alpha_3''^{(k)}z_3$$

we can find an upper bound for them with the help of an upper bound for the height of β, which can be obtained similarly as in the proof of lemma 2. The upper bound for $|x_1|,|x_2|,|x_3|$ deduced from this is much better than the upper bound given in the theorem.

Assume now that in (8) $\operatorname{Im}\alpha_1''=0$, $\operatorname{Im}\alpha_2'',\operatorname{Im}\alpha_3''$ are linearly independent and $\{i\operatorname{Im}\alpha_2'',i\operatorname{Im}\alpha_3''\}$ is non-degenerated. Consider the field $K'''=K'(\bar{\alpha}_2'',\bar{\alpha}_3'')\subset F$ of degree $\leqq n^6$ and apply lemma 1. Then (9) gives the inequality

$$|a_3|^{n^4}\geqq|a_3|^{[F:K']/[F:K''']}\geqq|N_{K'''/R}(i\operatorname{Im}\alpha_2''z_2+i\operatorname{Im}\alpha_3''z_3)|$$

which implies by Baker

$$\max(|z_1|,|z_2|)\leqq\varphi(b^{n^4},n^3,H_3,\varkappa)$$

Now if $z_2=z_3=0$ then (9) gives

$$b\geqq|a_3|=|N_{K'/R}(\alpha_1''z_1)|\geqq|z_1|$$

which is not larger than the upper bound given above. On the other hand, if one of z_2 and z_3 is non-zero, then by

$$|a_3|^{[F:K']}\geqq\left|\frac{L^{(k)}(z)}{i\operatorname{Im}L^{(k)}(z)}\right|^{[F:K']}|N_{K'''/R}(i\operatorname{Im}\alpha_2''z_2+i\operatorname{Im}\alpha_3''z_3)|^{[F:K''']}\geqq\frac{|L^{(k)}(z)|^{[F:K']}}{|i\operatorname{Im}L^{(k)}(z)|^{[F:K']}}$$

and

$$\alpha_1'' z_1 = L^{(k)}(z) - \alpha_2'' z_2 - \alpha_3'' z_3$$

we can deduce

$$|z_1| \leqq 4n^6 b H_2 H_3 \varphi(b^{n^4}, n^3, H_3, \varkappa)$$

which proves the theorem.

1ST PROOF OF THEOREM 2. By our assumption $\alpha_2, \alpha_3, \alpha_4$ are not all real. Moreover, by lemma 2 we may suppose that the non-zero imaginary parts of $\alpha_1, \alpha_2, \alpha_3$, say $\operatorname{Im}\alpha_k, \dots, \operatorname{Im}\alpha_4$, are linearly independent. Obviously we may assume that they are algebraic integers. Now by lemma 1,

$$|a| \geqq |_{F/R}(i \operatorname{Im}\alpha_k x_k + \dots + i \operatorname{Im}\alpha_4 x_4)|$$

By our assumption concerning the degree of F, F has no real subfield of degree 2 and no subfield of degree 3, hence the module $\{i \operatorname{Im}\alpha_k, \dots, i \operatorname{Im}\alpha_4\}$ is non-degenerated. By Thue's and Schmidt's mentioned results this inequality has only finitely many solutions. Thus it is enough to show that for fixed $x_k, \dots, x_4$ (1″) has only finitely many solutions in $x_1, \dots, x_{k-1}$.

If $x_k = \dots = x_4 = 0$, then (1″) gives

$$N_{F/R}(x_1 + \alpha_2 x_2 + \dots + \alpha_{k-1} x_{k-1}) = a$$

and here $\{1, \alpha_2, \dots, \alpha_{k-1}\}$ is non-degenerated, consequently $x_1, \dots, x_{k-1}$ can have only finitely many different values. On the other hand, if there is an x_j $(k \leqq j \leqq 4)$ different from 0, then because of the linear independence of $\operatorname{Im}\alpha_k, \dots, \operatorname{Im}\alpha_4$,

$$|a| \geqq \left| \frac{L^{(r)}(\mathbf{x})}{i \operatorname{Im} L^{(r)}(\mathbf{x})} \right| \cdot \left| N_{F/R}\big(i \operatorname{Im} L(\mathbf{x})\big) \right| \geqq \frac{|L^{(r)}(\mathbf{x})|}{|i \operatorname{Im} L^{(r)}(\mathbf{x})|} \quad (r = 1, \dots [F:R])$$

and this gives an upper bound for $L^{(r)}(\mathbf{x})$ independently from the value of $x_1, \dots, x_{k-1}$. Since $1, \alpha_1, \dots, \alpha_{k-1}$ are linearly independent, there exist indices $i_1, \dots, i_{k-1}$ such that

$$\begin{vmatrix} 1 & \alpha_2^{(i_1)} & \dots \alpha_{k-1}^{(i_1)} \\ \vdots & & \\ 1 & \alpha_2^{(i_{k-1})} & \dots \alpha_{k-1}^{(i_{k-1})} \end{vmatrix} \neq 0$$

Hence the system

$$\begin{gathered} x_1 + \alpha_2^{(i_1)} x_2 + \dots + \alpha_{k-1}^{(i_1)} x_{k-1} = L^{(i_1)}(\mathbf{x}) - \alpha_k^{(i_1)} x_k - \dots - \alpha_4^{(i_1)} x_4 \\ \vdots \\ x_1 + \alpha_2^{(i_{k-1})} x_2 + \dots + \alpha_{k-1}^{(i_{k-1})} x_{k-1} = L^{(i_{k-1})}(\mathbf{x}) - \alpha_k^{(i_{k-1})} x_k - \dots - \alpha_4^{(i_{k-1})} x_4 \end{gathered}$$

gives an upper bound for $|x_1|, \dots, |x_{k-1}|$.

2ND PROOF OF THEOREM 2. We start like in the 1st proof: $\alpha_2, \alpha_3, \alpha_4$ are not all real, $\operatorname{Im}\alpha_1 = \dots = \operatorname{Im}\alpha_{k-1} = 0$, while $\operatorname{Im}\alpha_k, \dots, \operatorname{Im}\alpha_4$ are linearly independent algebraic integers.

Assume indirectly that (1″) has infinitely many solutions. Since only finitely many principal ideals of F can have norm a, we can find an appropriate element $\beta \in F$ such that infinitely many solutions of (1″) and units ε of F satisfy

$$x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 = \beta\varepsilon.$$

Since F is a non-real Galois field, it is totally imaginary, hence by Dirichlet's theorem the rank of the group of its units is $\frac{1}{2}[F:R]-1$. On the other hand, F being allowed its maximal real subfield is normal, consequently totally real, thus the rank of the group of the units of S is also $\frac{1}{2}[F:R]-1$. Now the logarithmical representation of the units shows that the units of S form a subgroup of the group of units of F, and the index of this subgroup is a finite number h. Therefore, there are units $\varepsilon_1, \dots, \varepsilon_h$ such that every unity of F is of form $\varepsilon_j\varepsilon$, where ε is a real unity. Consequently we can find a fixed integer j such that

$$x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 = \beta\varepsilon_j\varepsilon$$

has infinitely many solutions in integers x_1, x_2, x_3, x_4 and real units ε. Considering the imaginary parts of both sides,

$$i \operatorname{Im} \alpha_k x_k + \dots + i \operatorname{Im} \alpha_4 x_4 = \gamma\varepsilon$$

where $\gamma = \frac{1}{2}(\beta\varepsilon_j - \overline{\beta\varepsilon_j})$. Taking the norm of both sides,

$$N_{F/R}(i \operatorname{Im} \alpha_k x_k + \dots + i \operatorname{Im} \alpha_4 x_4) = N_{F/R}(\gamma\varepsilon) = N_{F/R}(\gamma) = \text{const.}$$

which has, by our assumption concerning the degree of F, only finitely many solutions $x_k, \dots, x_4$. But then

$$x_1 + \alpha_2 x_2 + \dots + \alpha_{k-1} x_{k-1} = \beta\varepsilon_j\varepsilon - \alpha_k x_k - \dots - \alpha_4 x_4 = \eta$$

or

$$N_{F/R}(x_1 + \alpha_2 x_2 + \dots + \alpha_{k-1} x_{k-1}) = N_{F/R}(\eta)$$

has infinitely many solutions for some fixed $x_k, \dots, x_4$ (and, consequently, for fixed ε), which is a contradiction.

References

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

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

[3] K. Győry, Représentation des nombres par des formes décomposables, I. *Publ. Math. Debrecen* **16** (1969), 253—263.

[4] W. M. Schmidt, Some diophantine equations in three variables with only finitely many solutions, *Mathematika* **14** (1967), 113—120.

[5] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. Reine. Angew. Math.* **135** (1909), 284—305.

(Received July 17, 1968.)