J. Math. Soc. Japan
Vol. 27, No. 3, 1975

On the best possible exponent in norm form inequalities

By Masahiko Fujiwara

(Received Oct. 15, 1973)

§1. Let K be an algebraic number field of degree k and let $\theta_1, \cdots, \theta_n$ be elements of K where $3 \leqq n < k$. We consider solutions in integers $x_1, \cdots, x_n$ of the following inequality

$$|N(x_1\theta_1 + \cdots + x_n\theta_n)| \leqq c\|x\|^{\eta} \tag{1}$$

where N denotes the norm from K to $\boldsymbol{Q}$, $\|x\| = \max|x_i|$ and c, η are positive constants. Our problem is: How large can we take η and still have the condition that (1) has only finitely many integer solutions? Recently W. M. Schmidt has obtained a number of theorems concerning this problem ([**4**], [**5**]). Minkowski theorem on linear form shows, for suitable c, that there always exist infinitely many integer solutions provided $\eta \geqq k-n$ (see p. 1 [**3**]). Thus the best possible exponent would be at most $k-n-\varepsilon$. Our aim in the present paper is to give a sufficient condition for the norm inequality (1) in which $k-n-\varepsilon$ is actually the best possible exponent.

In Theorem 1, we prove a rather general theorem, and we get Theorem 3 of Schmidt [**4**] as a corollary.

In Theorem 2 and 3, we apply Theorem 1 to a somewhat special type of norm inequalities and get simple conditions for those inequalities to have $k-n-\varepsilon$ as the best possible exponents.

First of all we introduce the notion of complete linear independence.

DEFINITION. Let K be an algebraic number field of degree k over $\boldsymbol{Q}$ and let $\theta_1, \cdots, \theta_n$ be elements of K. We call $\{\theta_1, \cdots, \theta_n\}$ completely linearly independent over $\boldsymbol{Q}$ if, in the $k \times n$ matrix

$$\begin{pmatrix} \theta_1^{(1)} & \cdots & \theta_n^{(1)} \\ & \cdots & \\ \theta_1^{(k)} & \cdots & \theta_n^{(k)} \end{pmatrix} \tag{2}$$

all the $t \times t$ minors in any fixed $t \times n$ submatrix with $t \leqq n$ are linearly independent over $\boldsymbol{Q}$.

Clearly, complete linear independence implies linear independence.

THEOREM 1. *Let K be an algebraic number field of degree k over $\boldsymbol{Q}$ and*

let $\theta_1, \cdots, \theta_n$ *be elements in* K. *Suppose* $\{\theta_1, \cdots, \theta_n\}$ *is completely linearly independent over* $\boldsymbol{Q}$. *Then for every pair of constants* $\varepsilon > 0$ *and* $c > 0$, *the inequality*

$$|N_{k/\boldsymbol{Q}}(x_1\theta_1 + \cdots + x_n\theta_n)| \leqq c\|x\|^{k-n-\varepsilon} \tag{3}$$

has only finitely many solutions in integers $x_1, \cdots, x_n$.

We note here that the condition of the complete linear independence in the theorem is not only sufficient but also necessary in case $n=3$. This fact can be shown, though we shall not do it in this paper, by using the theory of successive minima of pseudocompound.

From Theorem 1, immediately follows the following

COROLLARY 1. *Suppose* K *and* $\theta_1, \cdots, \theta_n$ *are as above and suppose* $f(x_1, \cdots, x_n)$ *is a polynomial of total degree* $\nu < k-n$. *Then the equation*

$$N(x_1\theta_1 + \cdots + x_n\theta_n) = f(x_1, \cdots, x_n)$$

has only finitely many integer solutions.

COROLLARY 2 (Schmidt [4], Theorem 3). *Let* K *be an algebraic number field of degree* k *over* $\boldsymbol{Q}$ *and let* $\theta_1, \cdots, \theta_n$ *be elements in* K. *Suppose* K *is* $n-1$ *times transitive, i.e., the Galois group of the Galois closure of* K *over* $\boldsymbol{Q}$ *is* $n-1$ *times transitive. Further assume any* n *conjugates of the linear form* $x_1\theta_1 + \cdots + x_n\theta_n$ *are linearly independent. Then, for every pair of constants* $\varepsilon > 0$ *and* $c > 0$, (3) *has only finitely many solutions in integers* $x_1, \cdots, x_n$.

THEOREM 2. *Let* ξ *be a primitive* n*-th root of unity where* n *is an odd positive integer greater than* 1. *Let* $K = \boldsymbol{Q}(\xi)$. *Let* i_1, i_2, i_3 *be rational integers with* $0 \leqq i_1 < i_2 < i_3 < n$ *such that* $i_2 - i_1$, $i_3 - i_2$, $i_1 - i_3$ *are different modulo* n *and* $(i_2 - i_1, i_3 - i_2, i_1 - i_3, n) = 1$. *Then for every pair of constants* $\varepsilon > 0$ *and* $c > 0$, *the inequality*

$$|N(x_1\xi^{i_1} + x_2\xi^{i_2} + x_3\xi^{i_3})| \leqq c\|x\|^{\varphi(n)-3-\varepsilon} \tag{4}$$

has only finitely many solutions in integers.

THEOREM 3. *Let* a *and* n *be positive integers greater than* 1 *so that* $\theta = \sqrt[n]{a}$ *is of degree* n *and let* $K = \boldsymbol{Q}(\theta)$. *Let* j_1, j_2, j_3 *be rational integers with* $0 \leqq j_1 < j_2 < j_3 < n$, $(j_2 - j_1, n) = (j_3 - j_2, n) = (j_3 - j_1, n) = 1$. *Then for every pair of constants* $\varepsilon > 0$ *and* $c > 0$, *the inequality*

$$|N(x_1\theta^{j_1} + x_2\theta^{j_2} + x_3\theta^{j_3})| \leqq c\|x\|^{n-3-\varepsilon} \tag{5}$$

has only finitely many solutions in integers x_1, x_2, x_3.

In the final Remark, we show that in each of Theorem 2 and 3, all the conditions are not only sufficient but also necessary in the sense that, if any one of these conditions fails to hold, the conclusion of the theorem is no longer true. Our proofs depend primarily on the remarkable theorem of W. M. Schmidt (Satz 1 [3]) which will be written here in a convenient form for our purpose:

Let K be an algebraic number field of degree k and let δ be a positive constant. Let L be a linear form in $x_1, \cdots, x_n$ with coefficients in K. Then the following two conditions are equivalent. (a) *There exists a constant $C=C(L, \delta)>0$ such that $|N(L)| \leqq C\|x\|^{k-\delta}$ has infinitely many integer solutions in $x_1, \cdots, x_n$.* (b) *There exists a non-null rational subspace S^t (i.e., linear subspace defined over $\boldsymbol{Q}$) of $\boldsymbol{R}^n$ of dimension t and a symmetric system $L_{i_1}, \cdots, L_{i_m}$ of conjugates of L (i.e., stable under taking complex conjugates) whose rank r on S^t satisfies both $r \leqq tm/\delta$ and $r<t$.*

§2. Proof of Theorem 1.

By virtue of Schmidt's theorem (see the last part of §1; in our case $\delta = n+\varepsilon$ and $L=x_1\theta_1+\cdots+x_n\theta_n$), we have only to show the non-existence of a rational subspace S^t of the type mentioned there. Assume to the contrary that there exists such S^t; that is, we assume that there exist a rational subspace S^t of $\boldsymbol{R}^n$ and a symmetric system $L^{(i_1)}, \cdots, L^{(i_m)}$, whose rank on S^t satisfies $r \leqq tm/(n+\varepsilon)$ and $r<t$. We are going to get to a contradiction in the end of the proof. First, as a basis for S^t, we take $\alpha_i = {}^t(a_{1i}, \cdots, a_{ni})$ $(i=1, \cdots, t)$ where a_{kl} $(1 \leqq k \leqq n,\ 1 \leqq l \leqq t)$ are rationals. Let A be the $n \times t$ matrix (a_{kl}). It is of rank t. Then any $x={}^t(x_1, \cdots, x_n)$ in S^t can be written as $x=Ay$ where $y={}^t(y_1, \cdots, y_t)$ ranges over $\boldsymbol{R}^t$. $L^{(i)}=(\theta_1^{(i)}, \cdots, \theta_n^{(i)})x=(\theta_1^{(i)}, \cdots, \theta_n^{(i)})Ay$. Therefore the rank of a system of linear forms $L^{(i_1)}, \cdots, L^{(i_s)}$ on S^t is equal to the rank of $(\theta_1^{(i_1)}, \cdots, \theta_n^{(i_1)})Ay, \cdots, (\theta_1^{(i_s)}, \cdots, \theta_n^{(i_s)})Ay$ on $\boldsymbol{R}^t$ and this is obviously equal to the rank of

$$\begin{pmatrix} \theta_1^{(i_1)}, & \cdots, & \theta_n^{(i_1)} \\ \vdots & & \\ \theta_1^{(i_s)}, & \cdots, & \theta_n^{(i_s)} \end{pmatrix} A .$$

We can see easily that there exists a system of t linear forms $L^{(i_1)}, \cdots, L^{(i_t)}$ whose rank on S^t is less than t; if $m \geqq t$, pick up any t linear forms from $L^{(i_1)}, \cdots, L^{(i_m)}$, then its rank $\leqq r<t$. If $m<t$, enlarge $L^{(i_1)}, \cdots, L^{(i_m)}$ to a set of t linear forms, then its rank $\leqq r+(t-m)=t+(r-m)<t$. Thus we have proved our assertion. Therefore, the rank of $L^{(i_1)}, \cdots, L^{(i_t)}$ on S^t is less than t and consequently, by the above argument, the rank of

$$\begin{pmatrix} \theta_1^{(i_1)}, & \cdots, & \theta_n^{(i_1)} \\ \vdots & & \\ \theta_1^{(i_t)}, & \cdots, & \theta_n^{(i_t)} \end{pmatrix} A$$

is less than t.

This is a $t \times t$ matrix and hence its determinant must be 0. But by the well-known formula,

$$(6)\qquad \left|\begin{pmatrix}\theta_1^{(i_1)}, & \cdots, & \theta_n^{(i_1)}\\ \vdots & & \\ \theta_1^{(i_t)}, & \cdots, & \theta_n^{(i_t)}\end{pmatrix}A\right| = \sum_{1\leqq\alpha_1<\alpha_2<\cdots<\alpha_t\leqq n}\begin{vmatrix}\theta_{\alpha_1}^{(i_1)}, & \cdots, & \theta_{\alpha_t}^{(i_1)}\\ \vdots & & \\ \theta_{\alpha_1}^{(i_t)}, & \cdots, & \theta_{\alpha_t}^{(i_t)}\end{vmatrix}\begin{vmatrix}a_{\alpha_1,1}, & \cdots, & a_{\alpha_1,t}\\ \vdots & & \\ a_{\alpha_t,1}, & \cdots, & a_{\alpha_t,t}\end{vmatrix}$$

where $\{\alpha_1, \alpha_2, \cdots, \alpha_t\}$ range over all the t-tuples of natural numbers satisfying $1\leqq\alpha_1<\alpha_2<\cdots<\alpha_t\leqq n$. As the rank of A is t, the second factors of the right hand side of (6) are not all 0. This means the linear dependence of the first factors of the right hand side over $\boldsymbol{Q}$ and hence contradicts the complete linear independence of $\theta_1, \cdots, \theta_n$.

PROOF OF COROLLARY 2. By Theorem 1, we have only to show the complete linear independence of $\{\theta_1, \cdots, \theta_n\}$ over $\boldsymbol{Q}$ under our assumptions. Assume, to the contrary, that it is not completely linearly independent. Then there exists, by definition, a natural number $t\leqq n$ and a $t\times n$ submatrix S of (2) where $t\times t$ minors are linearly dependent over $\boldsymbol{Q}$. Here, note that $t<n$ since any $n\times n$ minors of (2) are not 0 by the assumption. Let us take an $n\times n$ matrix

$$\begin{pmatrix}\theta_1^{(1)}, & \cdots, & \theta_n^{(1)}\\ \vdots & & \\ \theta_1^{(n)}, & \cdots, & \theta_n^{(n)}\end{pmatrix}$$

containing S in (2) and denote it by T. Here $\det T\neq 0$ by the assumption.

Let $C(n, t)$ consist of all t-tuples of integers $i_1, \cdots, i_t$ with $1\leqq i_1<i_2<\cdots<i_t\leqq n$. The number of elements of $C(n, t)$ is $\binom{n}{t}$. Let us fix a lexicographic order in $C(n, t)$ and make a $\binom{n}{t}\times\binom{n}{t}$ matrix $T'=(\theta_{\tau\sigma})_{\tau,\sigma\in C(n,t)}$. Here $\theta_{\tau\sigma}$ is determined as follows. Let $\tau=\{j_1<j_2<\cdots<j_t\}$ and $\sigma=\{k_1<k_2<\cdots<k_t\}$, then $\theta_{\tau\sigma}$ is the determinant of the $t\times t$ matrix which is the intersection of j_1-th, $\cdots, j_t$-th rows and k_1-th, $\cdots, k_t$-th columns. As T contains S, at least one row of T' is linearly dependent over $\boldsymbol{Q}$ and hence, by the t-transitivity of K, the columns of T' are linearly dependent over $\boldsymbol{Q}$. Therefore $\det T'=0$. On the other hand, as is well-known, $\det T'=(\det T)^{\frac{t}{n}\binom{n}{t}}\neq 0$. This is a contradiction.

REMARK. For the actual application of the Theorem 1 to some type of norm form inequality, we don't always have to check the complete linear independence of $\theta_1, \cdots, \theta_n$. As is clear from the proof of Theorem 1, we have only to consider, for the validity of the theorem, those $t\times n$ matrices whose rows are symmetric or symmetric except for one row. This fact will be used in the proof of Theorem 2.

§ 3. Proof of Theorem 2.

We need the following lemma, in whose proof we use the idea of the proof of Theorem 1 in [2].

LEMMA 1. *Let ξ be a primitive n-th root of* 1 *where n is a positive integer greater than* 1 *and prime to* 2. *Let s, t be integers such that s, $-s$, t, $-t$, $t-s$ and $s-t$ are different modulo n. Then $\xi^s-\xi^{-s}$, $\xi^t-\xi^{-t}$, $\xi^{t-s}-\xi^{s-t}$ are linearly independent over $\boldsymbol{Q}$.*

PROOF OF LEMMA 1. Without loss of generality we can assume $g.c.d(s, t, n)=1$, since, if $(s, t, n)=d>1$, we have only to replace ξ^d by a new ξ which is a primitive (n/d)-th root of 1. Now, assume the numbers are linearly dependent over $\boldsymbol{Q}$, say

$$a_1(\xi^s-\xi^{-s})+a_2(\xi^t-\xi^{-t})+a_3(\xi^{t-s}-\xi^{s-t})=0 \tag{7}$$

where a_1, a_2, a_3 are rational numbers which are not all 0. We are going to derive a contradiction. Denote s, $-s$, t, $-t$, $t-s$, $s-t$ by $\nu_1, \cdots, \nu_6$ respectively. These are distinct mod n. Let p be a prime divisor of n, say $n=p^jn'$ where $(p, n')=1$. Let ρ be a primitive p^j-th root of 1 and ξ_* be a primitive $p^{j-1}n'$-th root of 1. We fix these two primitive roots of 1 once for all in this proof. Then the n numbers $\rho^\sigma\xi_*^\lambda(0\leqq\sigma\leqq p-1, 0\leqq\lambda\leqq p^{j-1}n'-1)$ are all n-th roots of 1. It is easily seen that these n numbers are all distinct. Hence, $\rho^\sigma\xi_*^\lambda$ ranges over all the n-th roots of 1 just for once and every ξ^{ν_i} $(i=1, \cdots, 6)$ can be represented uniquely in the form $\xi^{\nu_i}=\rho^{\sigma_i}\xi_*^{\lambda_i}$, where $0\leqq\sigma_i\leqq p-1$, $0\leqq\lambda_i\leqq p^{j-1}n'-1$. Therefore, if we collect terms with the same value of σ_i as $\alpha_\mu=\sum_{\sigma_i=\mu}a_i\xi_*^{\lambda_i}$, we obtain from (7)

$$\sum_{\mu=0}^{p-1}\rho^\mu\alpha_\mu=0 \qquad \alpha_\mu\in\boldsymbol{Q}[\xi_*]\,. \tag{8}$$

Clearly at most 6 of the α_μ are non-zero.

Suppose first that $\alpha_\mu=0$ for $\mu=0, \cdots, p-1$. From the representation of $\xi^{\nu_i}=\rho^{\sigma_i}\xi_*^{\lambda_i}$, it is obviously impossible for some α_μ either to be a rational multiple of a $p^{j-1}n'$-th root of unity or to be a linear combination of two different $p^{j-1}n'$-th roots of unity. Therefore if α_μ is a non-empty sum of $p^{j-1}n'$-th roots of unity, it must be a linear combination of three or six different $p^{j-1}n'$-th roots of unity. Suppose a complex conjugate term, $a_1\xi^s$ and $a_1\xi^{-s}$ say, appear with some ρ^μ factor, say $\rho^\mu\alpha_\mu$, then $2\mu=0 \bmod p$, hence $\mu=0$ and therefore p divides s. Now that $\rho^\mu\alpha_\mu$ contains another term, it easily follows that p also divides t, which contradicts $(s, t, n)=1$. Similarly if $a_2\xi^t$, $a_2\xi^{-1}$ or $a_3\xi^{t-s}$, $a_3\xi^{s-t}$ have the same ρ^μ factor we get a contradiction. Therefore non-empty $\rho^\mu\alpha_\mu$ must contain $a_1\xi^{\delta_1 s}$, $a_2\xi^{\delta_2 t}$ and $a_3\xi^{\delta_3(t-s)}$ where δ_i are -1 or 1, and no other terms. As the ρ-parts of these three numbers are ρ^μ, uniqueness of ρ-parts

shows $\mu=0$, from which p divides s and t. This contradicts $(s, t, n)=1$. We have thus seen that $\alpha_\mu=0$ for $\mu=0, \cdots, p-1$ leads to a contradiction.

(Case 1) n: not square free.

In this case we choose the prime p above so that p^2 divides n. Then ρ is of degree $\varphi(n)/\varphi(n/p)=p$ over $\boldsymbol{Q}(\xi_*)$. Hence $\alpha_\mu=0$ for $\mu=0, \cdots, p-1$. This is a contradiction as seen above.

(Case 2) n: square free and divisible by a prime $p\geqq 7$.

In this case we choose p to be the largest prime divisor of n. Then ρ is of degree $p-1$ over $\boldsymbol{Q}(\xi_*)$, hence $\alpha_0=\cdots=\alpha_{p-1}$. As $p\geqq 7$ one of α_i's, consequently all α_i's must be 0. This is a contradiction.

(Case 3) n: square free and divisible only by primes $\leqq 5$.

Our conditions on s and t show $n\geqq 6$. Since 2 does not divide n, in this case n is 15. So, we choose $p=5$ and $n'=3$. In this case, as in case 2, $\alpha_0=\cdots=\alpha_{p-1}$. Since we can assume that none of α_i's are 0, four of α_i's must consist of just one term. It is easy to obtain a contradiction by considering the ξ_*-parts this time. Q. E. D.

PROOF OF THEOREM 2. Dividing the left hand side of (4) by $|N(\xi)^{i_1}|=1$, we have $|N(x_1+x_2\xi^{i_2-i_1}+x_3\xi^{i_3-i_1})|$. Putting $i_2-i_1=s$ and $i_3-i_1=t$, our assumptions on i_1, i_2, i_3 imply that $0<s<t<n$, $\{s, -t, t-s\}$ are different mod n and $(s, -t, t-s, n)=1$. From these, it follows easily that $\{s, -s, t, -t, t-s, s-t\}$ are all different mod n and $(s, t, n)=1$. To prove our theorem, owing to Theorem 1 and the remark after its proof, we have only to show (a) the non-degeneracy of the following matrix

$$\begin{pmatrix} 1 & \xi^s & \xi^t \\ 1 & \xi^{-s} & \xi^{-t} \\ 1 & (\xi^m)^s & (\xi^m)^t \end{pmatrix}$$

where $m\neq\pm 1$, (b) the linear independence over Q of all the 2×2 minors of the following matrix

$$\begin{pmatrix} 1 & \xi^s & \xi^t \\ 1 & \xi^{-s} & \xi^{-t} \end{pmatrix}$$

and (c) the linear independence of 1, ξ^s, ξ^t over $\boldsymbol{Q}$.

PROOF OF (a). The determinant of the matrix is

$$(\xi^{-s+mt}-\xi^{ms-t})-(\xi^{s+mt}-\xi^{ms+t})+(\xi^{s-t}-\xi^{t-s}).$$

Suppose this is 0, then

$$\xi^{-s+mt}+\xi^{ms+t}+\xi^{s-t}=\xi^{ms-t}+\xi^{s+mt}+\xi^{t-s}. \tag{9}$$

Denote these six numbers ξ^{-s+mt}, ξ^{ms+t}, ξ^{s-t}, ξ^{ms-t}, ξ^{s+mt} and ξ^{t-s} by α_1, β_1, γ_1, α_2, β_2, and γ_2 respectively. Then clearly

$$\alpha_1+\beta_1+\gamma_1=\alpha_2+\beta_2+\gamma_2 \tag{10}$$

$$\alpha_1\beta_1\gamma_1=\alpha_2\beta_2\gamma_2\,. \tag{11}$$

Also on applying the automorphism which sends ξ to ξ^2 to both sides of (9), we have

$$\alpha_1^2+\beta_1^2+\gamma_1^2=\alpha_2^2+\beta_2^2+\gamma_2^2\,. \tag{12}$$

From (10) and (12) we have

$$\alpha_1\beta_1+\beta_1\gamma_1+\gamma_1\alpha_1=\alpha_2\beta_2+\beta_2\gamma_2+\gamma_2\alpha_2\,. \tag{13}$$

Furthermore (10), (11) and (13) show that $\{\alpha_1, \beta_1, \gamma_1\}$ and $\{\alpha_2, \beta_2, \gamma_2\}$ are the three roots of the same cubic equation. Therefore $\{\alpha_1, \beta_1, \gamma_1\}=\{\alpha_2, \beta_2, \gamma_2\}$ as a set.

(Subcase 1) $\alpha_1=\alpha_2$.

In this case, if $\gamma_1=\gamma_2$ then $2(s-t)=0 \bmod n$, contradiction. If $\gamma_1=\beta_2$ then $-t=mt \bmod n$ and $\beta_1=\gamma_1$ i.e., $-s=ms$; these two mean $(s, t, n)\neq 1$ and we get a contradiction.

(Subcase 2) $\alpha_1=\beta_2$.

In this case $-s=s \bmod n$, a contradiction.

(Subcase 3) $\alpha_1=\gamma_2$.

This implies $tm=t$. If $\beta_1=\alpha_2$ then $t=-t$ and we have a contradiction. If $\beta_1=\beta_2$ then $\gamma_1=\alpha_2$ and $sm=s$. These two mean $(s, t, n)\neq 1$, a contradiction.

PROOF OF (b). The 2×2 minors are the following: $\xi^{-s}-\xi^s$, $\xi^{-t}-\xi^t$ and $\xi^{s-t}-\xi^{t-s}$. As we noted at the beginning of this proof, our assumptions on s and t satisfy those of Lemma 1. Hence these three are linearly independent over $\boldsymbol{Q}$.

PROOF OF (c). Suppose 1, ξ^s and ξ^t are linearly dependent over $\boldsymbol{Q}$. Then for some rationals a_1, a_2 and a_3, $a_1+a_2\xi^s+a_3\xi^t=0$. Hence $a_1+a_2\xi^{-s}+a_3\xi^{-t}=0$. Therefore $a_2(\xi^s-\xi^{-s})+a_3(\xi^t-\xi^{-t})=0$, which contradicts Lemma 1.

§ 4. Proof of Theorem 3.

By our Theorem 1, we have only to prove the complete linear independence of θ^{j_1}, θ^{j_2} and θ^{j_3} over $\boldsymbol{Q}$. By dividing these by θ^{j_1} and putting $s=j_2-j_1$, $t=j_3-j_1$ we have to show the complete linear independence of 1, θ^s and θ^t under the assumptions $0<s<t<n$ and $(s, n)=(t, n)=(t-s, n)=1$. For this purpose, by Theorem 1, we must show (a) the non-degeneracy of

$$\begin{pmatrix} 1 & \theta^s & \theta^t \\ 1 & (\theta\xi^m)^s & (\theta\xi^m)^t \\ 1 & (\theta\xi^l)^s & (\theta\xi^l)^t \end{pmatrix} \tag{14}$$

where 1, m and l are different natural numbers less than n, (b) that all 2×2 minors in the matrix

$$\begin{pmatrix} 1 & (\theta\xi^m)^s & (\theta\xi^m)^t \\ 1 & (\theta\xi^l)^s & (\theta\xi^l)^t \end{pmatrix}$$

are linearly independent over $\boldsymbol{Q}$, and (c) the linear independence of 1, θ^s and θ^t.

PROOF OF (a).

$$\text{det of (14)} = \theta^s\theta^t \begin{pmatrix} 1 & 1 & 1 \\ 1 & \xi^{ms} & \xi^{mt} \\ 1 & \xi^{ls} & \xi^{lt} \end{pmatrix} = \theta^{s+t}(\xi^{ms+lt} - \xi^{ls+mt} - \xi^{lt} + \xi^{mt} + \xi^{ls} - \xi^{ms}).$$

Suppose this is 0. Then

$$\xi^{ms+lt} + \xi^{mt} + \xi^{ls} = \xi^{ls+mt} + \xi^{lt} + \xi^{ms}. \tag{15}$$

As our assumptions on s and t imply that n is not divisible by 2, we can use the same technique as in the proof of Theorem 2 and we see that the terms on both sides are pairwise equal.

(Subcase 1) $\xi^{ms+lt} = \xi^{ls+mt}$.

Then $\xi^{mt} = \xi^{lt}$ or $\xi^{mt} = \xi^{ms}$. If $mt = lt \bmod n$ then $m = l$, a contradiction. If $mt = ms \bmod n$ then $m = 0$, a contradiction.

(Subcase 2) $\xi^{ms+lt} = \xi^{lt}$.

Then $ms = 0 \pmod n$ and hence $m = 0$, a contradiction.

(Subcase 3) $\xi^{ms+lt} = \xi^{ms}$.

Then $lt = 0 \bmod n$ and hence $l = 0$, again a contradiction.

PROOF OF (b). All the 2×2 minors are $\theta^s(\xi^{ls} - \xi^{ms})$, $\theta^t(\xi^{lt} - \xi^{mt})$ and $\theta^{s+t}(\xi^{ms+lt} - \xi^{ls+mt})$. It is easily seen that $\xi^{ls} - \xi^{ms}$, $\xi^{lt} - \xi^{mt}$ and $\xi^{ms+lt} - \xi^{ls+mt}$ are not 0. As $\boldsymbol{Q}(\theta) \cap \boldsymbol{Q}(\xi) = \boldsymbol{Q}$, θ is of degree n over $\boldsymbol{Q}(\xi)$. Since $n \geqq 3$, it follows that θ^s, θ^t and θ^{s+t} are linearly independent over $\boldsymbol{Q}(\xi)$, which proves our assertion.

PROOF OF (c). 1, θ^s, θ^t are linearly independent over $\boldsymbol{Q}$ since $n \geqq 3$.

REMARK. We will show that the conditions in Theorem 2 and 3 are necessary in the sense that, without any one of them, the theorems are no longer true even if all the other conditions are fulfilled.

In the case of Theorem 2. If $(2, n) \neq 1$, then set $n = 14$ and $i_1 = 0$, $i_2 = 1$, $i_3 = 7$. Let $L_1 = x_1 + x_2\xi + x_3\xi^7$ and $L_2 = x_1 + x_2\xi^2 + x_3\xi^7$. Then it is easily seen

that L_1 $\bar{L}_1$, L_2 and $\bar{L}_2$ make a symmetric system of rank 2 on $\boldsymbol{R}^3$. Therefore, by Schmidt's theorem, $|N(x_1+x_2\xi+x_3\xi^7)| \leqq C\|x\|^{1-\varepsilon}$ has infinitely many solutions in integers x_1, x_2, x_3 for some constant c and $\varepsilon>0$. If $i_2-i_1=i_3-i_2$, then set $n=5$ and $i_1=0$, $i_2=1$, $i_3=2$. Let S^2 be the rational subspace of $\boldsymbol{R}^3$ defined by $x_1=x_3$. Then $L=x_1+x_2\xi+x_3\xi^2$ and $\bar{L}=x_1+x_2\xi^4+x_3\xi^3$ has rank 1 on S^2. Therefore $|N(x_1+x_2\xi+x_3\xi^2)| \leqq C\|x\|^{1-\varepsilon}$ has infinitely many solutions in integers for some constant $c>0$ and $\varepsilon>0$. If $(i_2-i_1, i_3-i_2, i_1-i_3, n)=d>1$, then set $i_1=0$, $i_2=3$, $i_3=9$ and $n=15$. Then $d=3$. Put $\xi'=\xi^3$. Then $N(x_1+x_2\xi^3+x_3\xi^9)=(N'(x_1+x_2\xi'+x_3\xi'^3))^2$ where N' denotes the norm from $\boldsymbol{Q}(\xi')$. There are infinitely many solutions of $|N'(x_1+x_2\xi'+x_3\xi'^3)| \ll \|x\|^{\varphi(5)-3}=\|x\|$, hence of $|N(x_1+x_2\xi^3+x_3\xi^9)| \ll \|x\|^2$.

In the case of Theorem 3 if $(j_3-j_2, n)\neq 1$, then set $n=15$, $j_1=0$, $j_2=2$ and $j_3=7$. Let S be the rational subspace of $\boldsymbol{R}^3$ defined by $x_1=0$, and $L=x_1+x_2(\theta\xi^3)^2+x_3(\theta\xi^3)^7$. Then L and $\bar{L}$ has rank 1 on S^2. Therefore $|N(x_1+x_2\theta^2+x_3\theta^7)| \leqq c\|x\|^{5-\varepsilon}$ has infinitely many solutions in integers for some constant c and $\varepsilon>0$.

References

[1] M. Fujiwara, Some applications of a theorem of W.M. Schmidt, Michigan Math. J., 19 (1972), 315-319.
[2] H.B. Mann, On linear relations between the roots of unity, Mathematika, 12 (1965), 107-117.
[3] W.M. Schmidt, Linearformen mit algebraischen Koeffizienten II, Math. Ann. 191 (1971), 1-20.
[4] W.M. Schmidt, Norm form equations, Ann. of Math., 96, No. 3 (1972), 526-551.
[5] W.M. Schmidt, Inequalities for resultants and for decomposable forms, Diophantine Approximation and its Applications, Academic Press, 1973.

Masahiko FUJIWARA
Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Fukazawa, Setagaya-ku
Tokyo, Japan