SOME APPLICATIONS OF A THEOREM OF W. M. SCHMIDT

Masahiko Fujiwara

1. INTRODUCTION

A module $\mathfrak{M}$ in an algebraic number field K is called *degenerate* if $\mathfrak{M}$ has a submodule $\mathfrak{N}$ such that for some $\alpha \in K$, $\alpha\mathfrak{N}$ is a full module in some subfield K' of K, where K' is neither the field of rational numbers nor an imaginary quadratic field. In [3, Satz 2], W. M. Schmidt obtained the following remarkable generalization of Thue's theorem:

Let K *be an algebraic number field of degree at least* 3, *and let* $\alpha_1, \cdots, \alpha_n$ *be linearly independent elements of* K. *If the module generated by* $\alpha_1, \cdots, \alpha_n$ *over the integers* Z *is nondegenerate, then the equation*

$$N(\alpha_1 x_1 + \cdots + \alpha_n x_n) = C,$$

where N *denotes the norm from* K *to the rational field* Q *and where* C *is a rational number, has only finitely many solutions in integers* $x_1, \cdots, x_n$.

In the present paper, we shall make certain applications of Schmidt's theorem. Among other things, we shall generalize and improve certain theorems of Siegel and of Nagell. Our results are as follows.

THEOREM 1. *Let* h *be a positive integer, and let* θ *be an algebraic number of degree* $n > 2h$. *Let* N *be the norm from* $Q(\theta)$ *to* Q. *Then for each rational number* C, *the equation*

$$N(x_0 + \theta x_1 + \cdots + \theta^h x_h) = C$$

has only a finite number of integral solutions $x_0, x_1, \cdots, x_h$.

Siegel [4] had proved a result of this type, with the stronger hypothesis that

$$n > h^2\left(\frac{n}{s+1} + s\right), \quad \text{where } 2s = \sqrt{4n+1} - 1.$$

We note that the present hypothesis $n > 2h$ is in a certain sense best possible. For if $n = 2h$, let α be a real quadratic irrational with the property that $\theta = \sqrt[h]{\alpha}$ is of degree n. Then the equation $N(x_0 + x_h\alpha) = N(x_0 + x_h\theta^h) = C$ does have infinitely many solutions x_0, x_h for suitable values of C, and hence the equation $N(x_0 + \theta x_1 + \cdots + \theta^h x_h) = C$ has infinitely many solutions.

THEOREM 2. *Let* n *be an integer greater than* 1 *that is not divisible by* 2, 3, *or* 5. *Let* ξ *be a primitive* nth *root of unity, and let* r, s, t *be rational integers with* $0 \le r < s < t < n$. *Let* N *be the norm from* $Q(\xi)$ *to* Q. *Then, for each rational constant* C, *the equation*

$$N(\xi^r x + \xi^s y + \xi^t z) = C$$

Received October 19, 1971.

Michigan Math. J. 19 (1972).

has only finitely many solutions in integers x, y, z.

The case where n is a prime has been treated by Nagell [2]. The following example shows that our conditions on n cannot all be omitted. Suppose $n = 5a$ for some $a > 0$, and let ξ be a primitive nth root of unity. Then it is easily seen that

$$\eta = \xi^a + \xi^{4a} = \frac{1}{2}(1 \pm \sqrt{5}) \in Q(\sqrt{5}).$$

The equation $N_{Q(\sqrt{5})/Q}(x + \eta y) = 1$ has infinitely many solutions in integers x, y, and hence the equation $N(x + \xi^a y + \xi^{4a} z) = 1$ has infinitely many solutions in integers x, y, z.

THEOREM 3. *Suppose* m *and* n *are integers greater than* 1 *such that* $\theta = \sqrt[n]{m}$ *is of degree* n. *Let* $S = \{i_1, \cdots, i_h\}$ *be a set of positive integers with* $0 \le i_1 < i_2 < \cdots < i_h < n$. *Assume that for each positive divisor* d *of* n, S *does not contain an arithmetic progression of common difference* n/d *and consisting of* d *terms. Then the Diophantine equation*

$$N(\theta^{i_1} x_1 + \cdots + \theta^{i_h} x_h) = C,$$

where N *denotes the norm from* $Q(\theta)$ *to* Q *and where* C *is a constant, has only finitely many solutions.*

2. PROOF OF THEOREM 1

Let $K = Q(\theta)$, and let $\mathfrak{M}$ be the module generated by $1, \theta, \cdots, \theta^h$. By Schmidt's theorem, we have only to show that $\mathfrak{M}$ is not degenerate. Assume $\mathfrak{M}$ to be degenerate. Then, by the definition, there exists a submodule $\mathfrak{N}$ of $\mathfrak{M}$ such that, for some $\alpha \in K$ and some subfield K' of K, $\alpha\mathfrak{N}$ is a full module in K'. Let $K' = Q(\eta)$ be of degree $s \ge 2$. Denoting by $\mathfrak{M}^Q$ the vector space generated by $\mathfrak{M}$ over Q, we see that there exist $w_1, \cdots, w_s, w_{s+1}$ in $\mathfrak{M}^Q$ such that

$$\alpha w_1 = 1, \quad \alpha w_2 = \eta, \quad \cdots, \quad \alpha w_s = \eta^{s-1}, \quad \alpha w_{s+1} = \eta^s.$$

With each $w_i = a_{i0} + a_{i1}\theta + \cdots + a_{ih}\theta^h$, where the a_{ij} are rational numbers, we associate a polynomial

$$f_i(X) = a_{i0} + a_{i1}X + \cdots + a_{ih}X^h.$$

Here we can assume that the $f_i(X)$ $(i = 1, \cdots, s)$ have no common factor except constants; for if f(X) is a nonconstant common factor, we can choose a suitable rational integer m such that $\frac{\alpha f(\theta)}{m}$ and the submodule

$$\left\{ \frac{mw_1}{f(\theta)}, \cdots, \frac{mw_s}{f(\theta)} \right\}_Z$$

of $\mathfrak{M}$ play the same role as α and $\mathfrak{N}$ in the arguments above. Eliminating α from the relations above, we obtain the equation

$$w_i^2 = w_{i-1} w_{i+1} \quad \text{for } i = 2, \cdots, s.$$

Since $2h < n$,

$$f_i(X)^2 = f_{i-1}(X) f_{i+1}(X) \quad \text{for } i = 2, \cdots, s$$

as polynomials in $Q[X]$.

It follows that if $f(X)$ is an irreducible factor of $f_{i-1}(X)$ in $Q[X]$, then $f(X)$ divides $f_i(X)$. This implies that each irreducible factor of $f_1(X)$ is a common factor of all the $f_i(X)$ for $i = 1, \cdots, s$. On account of our choice of $f_i(X)$, $f_1(X)$ must be a rational number; that is, w_1 is rational and hence α is rational. This means that $\mathfrak{M}^Q$ contains K'. This is absurd, because it implies that there exists an element β in K' of the form

$$\beta = a_0 + a_1\theta + \cdots + a_t\theta^t \quad \text{with } 1 \leq t \leq h,\ a_t \neq 0.$$

But there is an integer k with $h < tk \leq 2h < n$, and β^k does not lie in $\mathfrak{M}^Q$.

3. PROOF OF THEOREM 2

LEMMA. *Suppose* n, ξ, r, s, t *are as in Theorem* 2. *Then* ξ^r, ξ^s, ξ^t *are linearly independent over each real quadratic field.*

Proof of the lemma. We may divide each of ξ^r, ξ^s, ξ^t by ξ^r, and hence it will suffice to prove the lemma for $r = 0$. We have to show the linear independence of $1, \xi^s, \xi^t$ over each real quadratic field K'. Suppose

$$\text{g.c.d. } (s, t) = a \quad \text{and} \quad s = s'a,\ t = t'a,\ n' = n/(n, a).$$

Put $\eta = \xi^a$. Then $\xi^s = \eta^{s'}$, $\xi^t = \eta^{t'}$. The number η is a primitive root of unity of order n', and $0 < s' < t' < n'$. Note that n' is not divisible by 2, 3, or 5. We have to show that $1, \eta^{s'}, \eta^{t'}$ are linearly independent over K'. Since $(s', t') = 1$, we change the notation back to ξ, n, s, t, and see that *it will suffice to show the linear independence of* $1, \xi^s, \xi^t$ *if* $0 < s < t < n$ *and* $(s, t) = 1$.

We shall do this by induction on t. The least possible value for t is 2; then $s = 1$. In this case we have to show the linear independence of $1, \xi, \xi^2$ over K'. If these three elements were linearly dependent over K', ξ would have degree at most 2 over K', hence degree at most 4 over the rationals. On the other hand, since ξ is a primitive nth root of unity, the degree of ξ is $\phi(n) \geq 6$ since 2, 3, and 5 do not divide n.

Suppose now that we have proved our assertion for values of t less than h, where $h \geq 3$, and we wish to prove it for $t = h$. Suppose we had a relation

$$a + b\xi^s + c\xi^h = 0, \tag{1}$$

where $a, b, c \in K'$ are not all zero, and where $0 < s < h < n$, $(s, h) = 1$. The automorphism of $Q(\xi)$ that maps ξ into ξ^{-1} may be extended to an automorphism of $K'(\xi)$. If we apply this automorphism to (1), we obtain the equation

$$a' + b'\xi^{-s} + c'\xi^{-h} = 0, \tag{2}$$

where $a', b', c' \in K'$ are the images of a, b, c. Multiplying (2) by ξ^h and combining (1) and (2), we obtain the relation

$$cc' - aa' - a'b\xi^s + b'c\xi^{h-s} = 0. \tag{3}$$

Clearly, $0 < s < h$ and $0 < h - s < h$. If we had the relation $s = h - s$, it would imply that $h = 2s$ and $(h, s) = s$, whence $s = 1$, $h = 2$, a contradiction. Thus s and $h - s$ are distinct positive numbers less than h, with $(s, h - s) = 1$. Since K' is real and n is odd, ξ^s and ξ^h do not lie in K', so that in (1) $b \neq 0$ and $c \neq 0$, which implies that $b'c \neq 0$. Thus (3) is a relation of linear dependence of $1, \xi^s, \xi^{h-s}$. Since both s and $h - s$ are less than h, our inductive assumption gives the desired contradiction.

The proof of Theorem 2 is now accomplished as follows. By Schmidt's theorem, we have to show that the module $\mathfrak{M}$ generated by ξ^r, ξ^s, ξ^t over Z is nondegenerate. Otherwise there would be a submodule $\mathfrak{N}$ of $\mathfrak{M}$, such that either rank $\mathfrak{N} = 3$ and $\mathfrak{N}$ is proportional to a full module in a cubic field $K' \subset K = Q(\xi)$, or rank $\mathfrak{N} = 2$ and $\mathfrak{N}$ is proportional to a full module in a real quadratic field $K' \subset K$.

In the first case, $\mathfrak{M}$ itself is proportional to a full module in K', and the quotient $\xi^r/\xi^s = \xi^{r-s}$ lies in K'. Thus ξ^{r-s} would be a root of unity of degree $3 = \deg K'$. But since there is no integer q whose Euler quotient function equals $\phi(q) = 3$, there is no root of unity of degree 3. In the second case, suppose

$$\eta = a_1\xi^r + a_2\xi^s + a_3\xi^t \quad \text{and} \quad \mu = b_1\xi^r + b_2\xi^s + b_3\xi^t$$

were a basis of $\mathfrak{N}$. Then $\eta/\mu \in K'$, say $\eta = \kappa'\mu$ with $\kappa' \in K'$. Thus

$$(a_1 - b_1\kappa')\xi^r + (a_2 - b_2\kappa')\xi^s + (a_3 - b_3\kappa')\xi^t = 0,$$

and the lemma implies that $a_i = b_i\kappa'$, so that κ' is rational and $\eta = \kappa'\mu$, and μ cannot be a basis of $\mathfrak{N}$.

4. PROOF OF THEOREM 3

Suppose the conditions of Theorem 3 are satisfied and $\mathfrak{M}$ is the module generated over Z by $\theta^{i_1}, \cdots, \theta^{i_h}$. We must show that $\mathfrak{M}$ is nondegenerate. Without loss of generality, we may assume that θ is real.

Let K' be a subfield of $K = Q(\theta)$ of degree d, say. Then $d \mid n$. We see that $N_{K/K'}(\theta) = \xi\theta^{n/d}$, where ξ is a root of unity, and since $\xi \in K$ and K is real, we conclude that $\xi = \pm 1$. Thus $\theta^{n/d} \in K'$, and since $\theta^{n/d}$ is of degree d, it follows that $K' = Q(\theta^{n/d})$. We must show that $\mathfrak{M}$ contains no submodule that is proportional to a full K'-module.

Otherwise, there would exist a $\mu \neq 0$ such that

$$\mu, \mu\theta^{n/d}, \mu\theta^{2(n/d)}, \cdots, \mu\theta^{(d-1)(n/d)}$$

all lie in $\mathfrak{M}$. Suppose $\mu = \sum_{k=1}^{h} b_{i_k}\theta^{i_k}$, and suppose $b_{i_g} \neq 0$, say. Then $\mu\theta^{i(n/d)}$ $(i = 0, 1, \cdots, d - 1)$ is a unique linear combination with rational coefficients of $1, \theta, \cdots, \theta^{n-1}$, and if $i_g + i\left(\frac{n}{d}\right) < n$, the coefficient of $\theta^{i_g+i(n/d)}$ is $b_{i_g} \neq 0$, while if $i_g + i\left(\frac{n}{d}\right) \geq n$, then the coefficient of $\theta^{i_g+(i-d)(n/d)}$ is $b_{i_g} \neq 0$. Thus all the

elements $\theta^{i_g+j(n/d)}$ where j satisfies the condition

$$0 \leq i_g + j(n/d) < n$$

lie in $\mathfrak{M}$, and the corresponding exponents $i_g + j(n/d)$ form an arithmetic progression in S with common difference n/d and consisting of d elements. This contradicts our hypothesis on S.

REFERENCES

1. L. J. Mordell, *Diophantine equations*. Academic Press, New York, 1969.
2. T. Nagell, *Remarques sur les formes à plusieurs variables décomposables en facteurs linéaires*. Ark. Math. 7 (1968), 313-329.
3. W. M. Schmidt, *Linearformen mit algebraischen Koeffizienten. II*. Math. Ann. 191 (1971), 1-20.
4. C. L. Siegel, *Approximation algebraischer Zahlen*. Math. Z. 10 (1921), 173-213.

Tokyo Metropolitan University
Tokyo, Japan