PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 104, Number 2, October 1988

HILBERT'S TENTH PROBLEM FOR A CLASS OF RINGS OF ALGEBRAIC INTEGERS

THANASES PHEIDAS

(Communicated by Thomas J. Jech)

ABSTRACT. We show that $\mathbf{Z}$ is diophantine over the ring of algebraic integers in any number field with exactly two nonreal embeddings into $\mathbf{C}$ of degree ≥ 3 over $\mathbf{Q}$.

Introduction. Let R be a ring. A set $S \subset R^m$ is called diophantine over R if it is of the form $S = \{x \in R^m : \exists y \in R^n \ p(x,y) = 0\}$, where p is a polynomial in $R[x,y]$. A number field is a finite extension of the field $\mathbf{Q}$ of rational numbers. If K is a number field, we denote by O_K the ring of elements of K which are integral over the ring $\mathbf{Z}$ of rational integers.

$\mathbf{N}$ is the set $\{0,1,2,\dots\}$ and $\mathbf{N}_0$ is the set $\{1,2,3,\dots\}$.

In this paper we prove

THEOREM. *Let K be a number field of degree $n \geq 3$ over $\mathbf{Q}$ with exactly two nonreal embeddings into the field $\mathbf{C}$ of complex numbers. Then $\mathbf{Z}$ is diophantine over O_K.*

An example of such a number field is $\mathbf{Q}(d)$ where d^3 is a rational number which does not have a rational cube root.

In order to prove the theorem, we use the methods of J. Denef in [**3**]. The terminology and enumeration of the lemmas is kept the same as in [**3**] so that the similarities and differences of the proofs are clear. The theorem implies

COROLLARY. *Let K be as in the theorem. Then Hilbert's Tenth Problem in O_K is undecidable.*

The results of [**3**] and the present paper are the maximum that can be achieved using the present methods. Hence the general conjecture made in [**4**], namely that Hilbert's Tenth Problem for the integers of any number field is undecidable, remains open.

Let K be a number field of degree $n \geq 3$ over $\mathbf{Q}$ with exactly two nonreal embeddings into $\mathbf{C}$. Let σ_i, $i = 1,2,\dots,n$, be all the embeddings of K into $\mathbf{C}$, enumerated in such a way that σ_{n-1} and σ_n are nonreal. Then the embedding $\sigma\colon K \to \mathbf{C}$ such that $\sigma(x) = \overline{\sigma_n(x)}$ is distinct from σ_n and from all σ_i, $i \leq n-2$,

Received by the editors July 16, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 03B25; Secondary 12B99.

I would like to thank Professor Leonard Lipschitz for his encouragement and help during the preparation of this work.

In the process of publication of this paper I was informed that Alexandra Shlapentokh obtained the same results as part of her thesis at Courant Institute of Mathematical Sciences.

This paper has been supported in part by NSF Grant #DMS 8605-198.

since σ_n is nonreal (i.e. for at least an $x \in K$, $\sigma_n(x) \notin \mathbf{R}$, hence $\sigma(x) \neq \overline{\sigma_n(x)}$ and $\sigma(x) \notin \mathbf{R}$). Hence $\sigma = \sigma_{n-1}$ and therefore, for every $x \in K$, $\sigma_{n-1}(x) = \overline{\sigma_n(x)}$. In the rest of the paper we identify K with $\sigma_1(K)$.

There are two cases: $\sigma_{n-1}(K) = \sigma_n(K)$ or $\sigma_{n-1}(K) \neq \sigma_n(K)$. In the first case, let b be an element of K such that $K = \mathbf{Q}(b)$. We have that $\operatorname{Re}\sigma_n(b) \in \sigma_n(K)$ and $(\operatorname{Im}\sigma_n(b))^2 \in \sigma_n(K)$ where $\operatorname{Re} x$ and $\operatorname{Im} x$ are the real and imaginary parts of x, respectively. So, since $\sigma_n(K) = \mathbf{Q}(\sigma_n(b))$, $[\sigma_n(K) : \sigma_n(K) \cap \mathbf{R}] = 2$ and so $\sigma_n(K)$ is nontotally real of degree 2 over $\sigma_n(K) \cap \mathbf{R}$ which is totally real. By [**3**] $\mathbf{Z}$ is diophantine over $\sigma_n(O_K) \cap \mathbf{R}$ and by the results of [**4**] this implies that $\mathbf{Z}$ is diophantine over $\sigma_n(O_K)$. Hence $\mathbf{Z}$ is diophantine over O_K. Therefore, we will consider only the case where $\sigma_{n-1}(K) \neq \sigma_n(K)$.

Let $a \in O_K$ be such that

$$(*) \qquad |\sigma_i(a)| < 1/2^{4n} \quad \text{for } i = 1, 2, \ldots, n-2 \text{ and } a \neq 0.$$

For each $x \in O_K$, let $\delta(x) \in C$ be a number so that $\delta^2(x) = x^2 - 1$. Let $\delta = \delta(a)$ and call $L = K(\delta)$. By $(*)$ a may not be a rational integer and therefore $\delta \notin K$. So $[L : K] = 2$ and each embedding σ_i of K into $\mathbf{C}$ extends to two embeddings $\sigma_{i,1}$ and $\sigma_{i,2}$ of L into $\mathbf{C}$. The relations $\sigma_{i,2}(\delta) = -\sigma_{i,1}(\delta)$ are obvious. Call $\varepsilon = \delta + a$ and x_m and y_m the solutions in O_K of the equation $x_m + \delta y_m = (a+\delta)^m$ for $m \in \mathbf{Z}$. Clearly $\varepsilon^m = x_m + \delta y_m$, $\varepsilon^{-m} = x_m - \delta y_m$, and ε is a unit in O_L.

LEMMA 1. *Let K be any number field, and $a, b, c \in O_K$. Suppose $\delta(a)$, $\delta(b) \notin K$. Let $m, h, k, j \in N$. We have:*

(1) *ε is a unit in $O_{K(\delta)}$, $\varepsilon^{-1} = a - \delta$, and x_m, y_m satisfy the Pell equation $x^2 - (a^2-1)y^2 = 1$;*

(2) $x_m = (\varepsilon^m + \varepsilon^{-m})/2$, $y_m = (\varepsilon^m - \varepsilon^{-m})/2\delta$;

(3) $x_{m\pm k} = x_m x_k \pm (a^2-1) y_m y_k$, $y_{m\pm k} = x_k y_m \pm x_m y_k$;

(4) $h \mid m \Rightarrow y_m \mid y_h$;

(5) $y_{hk} \equiv k x_h^{k-1} y_h \bmod y_h^3$;

(6) $x_{m+1} = 2a x_m - x_{m-1}, y_{m+1} = 2a y_m - y_{m-1}$;

(7) $y_m(a) \equiv m \bmod (a-1)$;

(8) *if $a \equiv b \bmod c$, then $x_m(a) \equiv x_m(b) \bmod c$ and $y_m(a) \equiv y_m(b) \bmod c$;*

(9) $x_{2m\pm j} \equiv -x_j \bmod x_m$;

(10) *if $n \in O_K$ and $n \neq 0$, then there exists an $m \in N_0$ such that $n \mid y_m(a)$.*

PROOF. See [**3**].

LEMMA 2. *Let a be as above. Then:*

(1) *for $i \leq n-2$, $0 < |\sigma_i(a)| < 1/2^{4n}$ and $|\sigma_n(a)| = |\sigma_{n-1}(a)| > 2^{2n}$;*

(2) *for $i \leq n-2$, $j = 1, 2$, $|\sigma_{i,j}(\varepsilon)| = 1$;*

(3) *$|\sigma_{n-1,j}(\varepsilon)| \neq 1$ and $|\sigma_{n,j}(\varepsilon)| \neq 1$ and*

$$\max\{|\sigma_{n,1}(\varepsilon)|, |\sigma_{n,2}(\varepsilon)|\} = \max\{|\sigma_{n-1,1}(\varepsilon)|, |\sigma_{n-1,2}(\varepsilon)|\} > 2^{2n}.$$

PROOF. (1) Since $\sigma_{n-1}(a) = \overline{\sigma_n(a)}$, $|\sigma_{n-1}(a)| = |\sigma_n(a)|$. Moreover $N_{K/\mathbf{Q}}(a)$ is a rational integer different from zero and hence $\prod_{i=1}^n |\sigma_i(a)| = |N_{K/\mathbf{Q}}(a)| \geq 1$. Since for $i \leq n-2$, $|\sigma_i(a)| < 1/2^{4n}$ we get $|\sigma_{n-1}(a)| \cdot |\sigma_n(a)| = |\sigma_n(a)|^2 > 2^{4n(n-2)}$ and since $n \geq 3$, $4n(n-2) \geq 4n$ and so $|\sigma_n(a)|^2 > 2^{4n}$, i.e. $|\sigma_n(a)| > 2^{2n}$.

(2) Since, for $i \le n-2$, $\sigma_i(a) \in R$ and $|\sigma_i(a)| < 1$, we get that $\sigma_{i,j}(\delta) \in iR$. So

$$|\sigma_{i,j}(\varepsilon)|^2 = |\sigma_i(a) + \sigma_{i,j}(\delta)|^2 = \sigma_i(a)^2 + |\sigma_{i,j}(\delta)|^2 = 1.$$

(3) $\sigma_{n,1}(\varepsilon) + \sigma_{n,2}(\varepsilon) = 2\sigma_n(a)$, so that we have that

$$\begin{aligned} |\sigma_{n,1}(\varepsilon)| + |\sigma_{n,2}(\varepsilon)| &= |\sigma_{n,1}(\varepsilon)| + |\sigma_{n,1}(\varepsilon)|^{-1} \\ &\ge |\sigma_{n,1}(\varepsilon) + \sigma_{n,2}(\varepsilon)| = 2|\sigma_n(a)| > 2^{2n+1} \quad \text{(by (1))}. \end{aligned}$$

So either $|\sigma_{n,1}(\varepsilon)| > 2^{2n}$ or $|\sigma_{n,1}(\varepsilon)^{-1}| = |\sigma_{n,2}(\varepsilon)| > 2^{2n}$. Similarly for σ_{n-1}.

NOTATIONAL REMARK. From now on we adopt the convention that $\sigma_{n-1,1}$ and $\sigma_{n,1}$ are such that$|\sigma_{n-1,1}(\varepsilon)| > 1$ and $|\sigma_{n,1}(\varepsilon)| > 1$.

REMARK. It is well known that if $\varphi(n)$ is the Euler function of n then

$$\lim_{n\to\infty} \varphi(n) = \infty$$

and hence there is only a finite number of roots of unity such that their degrees over $\mathbf{Q}$ is less than or equal to $2n$. Call d the least common multiple of their orders. It is then obvious that for any root of unity $J \in L$, $J^d = 1$.

LEMMA 3. *Let K, a, δ be as above. Let d be as in the last remark. Then all the solutions (x, y) in O_K of the equation $x^2 - \delta^2 y^2 = 1$, for which there are x^* and y^* in O_K such that $x + \delta y = (x^* + \delta y^*)^{6d}$ and $x^{*2} - \delta^2 y^{*2} = 1$, are given by $x = \pm x_m$ and $y = \pm y_m$ for some $m \in \mathbf{Z}$.*

PROOF. By the Dirichlet-Minkowski theorem on units (see [**1**]), there are $n-2$ fundamental units in K. Also L has no real embeddings into $\mathbf{C}$ and so L has $2n/2 - 1 = n-1$ fundamental units. Consider the set $S = \{x + \delta y \mid x^2 - \delta^2 y^2 = 1, x, y \in O_K\}$. S is clearly in the kernel of the map $N_{L/K}\colon O_L\backslash\{0\} \to O_K\backslash\{0\}$ considered as a multiplicative homomorphism. For any unit u of O_K, $N_{L/K}(u) = u^2$ and hence the image of $N_{L/K}$ has torsion-free rank at least equal to $n-2$. Therefore, the torsion-free rank of S is at most $(n-1) - (n-2) = 1$. Since ε is in S and ε is torsion free, $\operatorname{rank} S = 1$. Hence there is a unit $\varepsilon_0 = x' + \delta y' \in S$ such that every $u \in S$ can be written in the form $u = J\varepsilon_0^m$ where $m \notin \mathbf{Z}$ and J is a root of unity in L. In particular $\varepsilon = J_0 \varepsilon_0^e$ for some $e \notin \mathbf{Z}$, $e \ne 0$ and a root of unity $J_0 \in L$ (so $J_0^d = 1$). Clearly we may assume that $e > 0$ interchanging ε_0 with ε_0^{-1} if necessary. Then $\varepsilon_0 - \varepsilon_0^{-1} = 2\delta y'$ and $\varepsilon - \varepsilon^{-1} = 2\delta$, so $\varepsilon - \varepsilon^{-1} \mid \varepsilon_0 - \varepsilon_0^{-1}$. So $|N(2\delta)| \le |N(\varepsilon_0 - \varepsilon_0^{-1})|$, where $N = N_{L/Q}$. We have

$$|N(2\delta)| = 2^{2n}|N(\delta)| = \left|\prod_{i=1}^{n-2} (\sigma_i(a)^2 - 1)\right| \cdot |\sigma_n(a)^2 - 1|^2 \cdot 2^{2n}$$

since $\sigma_n(a)^2 - 1 = \overline{\sigma_{n-1}(a)^2 - 1}$. Hence

$$\begin{aligned} |N(2\delta)| &\ge 2^{2n} \cdot (1 - 1/2^{16n^2})^{n-2} \cdot |\sigma_n(a)^2 - 1|^2 > 2^{2n} \cdot (1/2^2)^{n-2} \cdot |\sigma_n(a)^2 - 1|^2 \\ &= 2^4 |\sigma_n(a)^2 - 1|^2 \ge 2^4 \cdot \left| |\sigma_n(a)|^2 - 1 \right| \ge 2^3 |\sigma_n(a)|^2, \end{aligned}$$

using $(*)$. Finally

$$|N(2\delta)| > 2^2 \cdot |\sigma_n(a)|^2 (i).$$

Now observe that $\sigma_{n-1,1}(\varepsilon_0) = \sigma_{n-1}(x') + \sigma_{n-1,1}(\delta)\sigma_{n-1}(y')$ and $\sigma_{n-1,2}(\varepsilon_0) = \sigma_{n-1}(x') + \sigma_{n-1,2}(\delta)\sigma_{n-1}(y') = \sigma_{n-1}(x') - \sigma_{n-1,1}(\delta)\sigma_{n-1}(y')$. So $\sigma_{n-1,2}(\varepsilon_0) = \sigma_{n-1,1}(\varepsilon_0^{-1})$ and hence

$$|\sigma_{n-1,1}(\varepsilon_0)-\sigma_{n-1,1}(\varepsilon_0^{-1})|\cdot|\sigma_{n-1,2}(\varepsilon_0)-\sigma_{n-1,2}(\varepsilon_0^{-1})| = |\sigma_{n-1,1}(\varepsilon_0)-\sigma_{n-1,1}(\varepsilon_0^{-1})|^2.$$

Similarly for $\sigma_{n,1}(\varepsilon_0)$ and $\sigma_{n,2}(\varepsilon_0)$. Moreover,

$$(\sigma_{n,1}(\varepsilon_0) - \sigma_{n,1}(\varepsilon_0^{-1}))^2 = 4(\sigma_n(a)^2 - 1)\sigma_n(y')^2$$

and

$$(\sigma_{n-1,1}(\varepsilon_0) - \sigma_{n-1,1}(\varepsilon_0^{-1}))^2 = 4(\sigma_{n-1}(a)^2 - 1)\sigma_{n-1}(y')^2$$

and since $\sigma_n(a)^2 = \overline{\sigma_{n-1}(a)^2}$ and $\sigma_n(y')^2 = \overline{\sigma_{n-1}(y')^2}$, we get

$$(\sigma_{n,1}(\varepsilon_0) - \sigma_{n,1}(\varepsilon_0^{-1}))^2 = \overline{(\sigma_{n-1,1}(\varepsilon_0) - \sigma_{n-1,1}(\varepsilon_0^{-1}))^2}.$$

Also since $|\sigma_{n,1}(\varepsilon_0)|^e = |\sigma_{n,1}(\varepsilon)|$ and $|\sigma_{n,1}(\varepsilon)| > 1$, we get $|\sigma_{n,1}(\varepsilon_0)| > 1$, using the convention $e > 0$. Similarly $|\sigma_{n-1,1}(\varepsilon_0)| > 1$. So we get

$$\begin{aligned}|N(\varepsilon_0 - \varepsilon_0^{-1})| &= \prod_{\substack{i=1\\ j=1,2}}^{n} |\sigma_{i,j}(\varepsilon_0) - \sigma_{i,j}(\varepsilon_0)^{-1}| \le 2^{2n-4} \\ &\qquad \prod_{\substack{i=n-1,n\\ j=1,2}} |\sigma_{i,j}(\varepsilon_0) - \sigma_{i,j}(\varepsilon_0^{-1})| \\ &= 2^{2n-4} \cdot |\sigma_{n,1}(\varepsilon_0) - \sigma_{n,1}(\varepsilon_0^{-1})|^4\end{aligned}$$

and finally we get

$$|N(\varepsilon_0 - \varepsilon_0^{-1})| \le 2^{2n-4}|\sigma_{n,1}(\varepsilon_0) - \sigma_{n,1}(\varepsilon_0)^{-1}|^4.$$

Now clearly we have

$$\begin{aligned}|\sigma_{n,1}(\varepsilon_0) - \sigma_{n,1}(\varepsilon_0)^{-1}|^2 &= |\sigma_{n,1}(\varepsilon_0)^2 + \sigma_{n,1}(\varepsilon_0)^{-2} - 2| \\ &\le |\sigma_{n,1}(\varepsilon_0)|^2 + |\sigma_{n,1}(\varepsilon_0)|^{-2} + 2 \\ &\le 2(|\sigma_{n,1}(\varepsilon_0)|^2 + |\sigma_{n,1}(\varepsilon_0)|^{-2})\end{aligned}$$

and so

$$|\sigma_{n,1}(\varepsilon_0) - \sigma_{n,1}(\varepsilon_0)^{-1}|^4 \le 4(|\sigma_{n,1}(\varepsilon_0)|^2 + |\sigma_{n,1}(\varepsilon_0)|^{-2})^2,$$

and hence

$$|N(\varepsilon_0 - \varepsilon_0^{-1})| \le 2^{2n-2}(|\sigma_{n,1}(\varepsilon_0)^2| + |\sigma_{n,1}(\varepsilon_0)|^{-2})^2.$$

If $|\varepsilon| = |\varepsilon_0|^e$ and $e \ge 4$ then $|\sigma_{n,1}(\varepsilon)| \ge |\sigma_{n,1}(\varepsilon_0)|^4 > 1$ and so

$$\begin{aligned}|N(\varepsilon_0 - \varepsilon_0^{-1})| &\le 2^{2n-2}(|\sigma_{n,1}(\varepsilon_0)|^2 + |\sigma_{n,1}(\varepsilon_0)|^{-2})^2 \\ &= 2^{2n-2}(|\sigma_{n,1}(\varepsilon_0)|^4 + |\sigma_{n,1}(\varepsilon_0)|^{-4} + 2) \le 2^{2n-1}(|\sigma_{n,1}(\varepsilon_0)|^4 + |\sigma_{n,1}(\varepsilon_0)|^{-4}) \\ &\le 2^{2n}|\sigma_{n,1}(\varepsilon_0)|^4 \le 2^{2n}|\sigma_{n,1}(\varepsilon)| = 2^{2n}|\sigma_n(a) + \sigma_{n,1}(\delta)| \\ &\le 2^{2n}(|\sigma_n(a)| + |\sigma_{n,1}(\delta)|) = 2^{2n}(|\sigma_n(a)| + \sqrt{|\sigma_n(a) - 1|}) \\ &\le 2^{2n}(|\sigma_n(a)| + 2|\sigma_n(a)|) \le 2^{2n+2}|\sigma_n(a)|.\end{aligned}$$

Combining the last inequality with (i) above gives $|\sigma_n(a)| < 2^{2n}$ which contradicts Lemma 2(1). So $e \le 3$. Therefore, if $x^{*2} + \delta^2 y^{*2} = 1$ and $x + \delta y = (x^* + \delta y^*)^{6d}$, since for some $n \in \mathbf{Z}$, $x^* + \delta y^* = J\varepsilon_0^n$ and $J^d = 1$ then $x + \delta y = \varepsilon_0^{6nd} = \varepsilon^{n_1}$ and hence $x = \pm x_{n_1}$ and $y = \pm y_{n_1}$ where $n_1 = 6n/e$.

LEMMA 4. *Assume that* K, a *are as above,* $h, m \in \mathbf{N}$ *and*

$$|\sigma_i(y_h)| \geq \tfrac{1}{2} \quad \textit{for} \;\; i = 1, 2, \ldots, n-2 \quad (\textit{condition } (1)).$$

Then

(1) $|\sigma_n(y_h)| > |\sigma_{n,1}(\varepsilon)|^h / 4|\sigma_{n,1}(\delta)|$ *and* $|\sigma_{n,1}(\varepsilon)| > 2^{2n}$,
(2) $y_h \mid y_m \Rightarrow h \mid m$ (the first divisibility is meant in O_K, the second in Z),
(3) $y_h^2 \mid y_m \Rightarrow y_h \mid m$ in O_K.

PROOF. (1) We have proved that $|\sigma_{n,1}(\varepsilon)| > 2^{2n}$. It is trivial to see that from this fact the following immediately follows: $|\sigma_{n,1}(\varepsilon)|^h - |\sigma_{n,1}(\varepsilon)|^{-h} \geq |\sigma_{n,1}(\varepsilon)|^h/\sqrt{2}$ for $h \in N_0$. So

$$|\sigma_n(y_h)| = \frac{|\sigma_{n,1}(\varepsilon)^h - \sigma_{n,1}(\varepsilon)^{-h}|}{2|\sigma_{n,1}(\delta)|} > \frac{|\sigma_{n,1}(\varepsilon)|^h}{2\sqrt{2}|\sigma_{n,1}(\delta)|} \geq \frac{|\sigma_{n,1}(\varepsilon)|^h}{4|\sigma_{n,1}(\delta)|}.$$

(2) Suppose $y_h \mid y_m$ but $h \nmid m$. Set $m = hq + k$, with $q, k \leq \mathbf{N}$ and $0 < k < h$. Lemma 1 yields $y_m = x_k y_{hq} + x_{hq} y_k$. Notice that $y_h \mid y_{hq}$, hence $y_h \mid x_{hq} y_k$. Since $x_{hq}^2 - (a^2-1) y_{hq}^2 = 1$, the elements y_h and x_{hq} are relatively prime. Thus $y_h \mid y_k$ and $|N_{K/\mathbf{Q}}(y_h)| \leq |N_{K/\mathbf{Q}}(y_k)|$. From the Introduction we have that $\sigma_{n-1}(y_h) = \overline{\sigma_n(y_h)}$. Also from condition 1 and (1),

$$\begin{aligned} |N_{K/\mathbf{Q}}(y_h)| &= |\sigma_{n-1}(y_n)| \cdot |\sigma_n(y_h)| \cdot \prod_{i \leq n-2} |\sigma_i(y_h)| \geq |\sigma_n(y_h)|^2 \cdot \left(\frac{1}{2}\right)^{n-2} \\ &> \left(\frac{|\sigma_{n,1}(\varepsilon)|^h}{4|\sigma_{n,1}(\delta)|}\right)^2 \cdot \left(\frac{1}{2}\right)^{n-2}. \end{aligned}$$

Now observe that, for $i \leq n-2$, $\sigma_i(x_k)^2 - (\sigma_i(a)^2 - 1) \cdot \sigma_i(y_k)^2 = 1$ and $\sigma_i(a)^2 < 1$. So $|\sigma_i(y_k)| < 1$ for $i \leq n-2$. Therefore,

$$\begin{aligned} |N_{K/\mathbf{Q}}(y_k)| &= |\sigma_{n-1}(y_k)| \cdot |\sigma_n(y_k)| \cdot \prod_{i \leq n-2} |\sigma_i(y_k)| < |\sigma_n(y_k)|^2 \\ &= \frac{|\sigma_{n,1}(\varepsilon^k) - \sigma_{n,1}(\varepsilon)^{-k}|^2}{(2|\sigma_{n,1}(\delta)|)^2} \leq \left(\frac{2|\sigma_{n,1}(\varepsilon)|^k}{2|\sigma_{n,1}(\delta)|}\right)^2 \\ &= \frac{|\sigma_{n,1}(\varepsilon)|^{2k}}{|\sigma_{n,1}(\delta)|^2}. \end{aligned}$$

Hence

$$\left(\frac{1}{2}\right)^{n-2} \frac{|\sigma_{n,1}(\varepsilon)|^{2h}}{4^2 |\sigma_{n,1}(\delta)|^2} < \frac{|\sigma_{n,1}(\varepsilon)|^{2k}}{|\sigma_{n,1}(\delta)|^2},$$

i.e. $|\sigma_{n,1}(\varepsilon)|^{2h-2k} < 2^n$ which contradicts (1) since $h - k \geq 1$. Hence $h \mid m$.

(3) is obvious since $(\varepsilon^{lh} - \varepsilon^{-lh})/(\varepsilon^h - \varepsilon^{-h}) \equiv 1 \cdot u \bmod (\varepsilon^h - \varepsilon^{-h})$ where u is a unit and hence if $y_h^2 \mid y_m$, by (2) $h \mid m$, i.e. $m = lh$ for some $l \in \mathbf{N}$, and so $y_m / y_h \equiv 0 \bmod y_h$ which means that $m/h \equiv 0 \bmod y_h$, i.e. $m \equiv 0 \bmod y_h$.

LEMMA 5. *If* K, a *are as above and* $k, j \in \mathbf{N}$, $m \in \mathbf{N}_0$ *and* $|\sigma_i(x_m)| \geq \frac{1}{2}$ *for* $i = 1, \ldots, n-2$, *then if* $x_k \equiv \pm x_j \bmod x_m$ *we get that* $k \equiv \pm j \bmod m$ (*the two* $\pm$ *do not have to correspond*).

PROOF. Set $k = 2mq \pm k_0$, $j = 2mh \pm j_0$ with $q, h, k_0, j_0 \in \mathbf{N}$ and $k_0 \leq m$, $j_0 \leq m$. Lemma 1(9) implies $x_k \equiv \pm x_{k_0} \bmod x_m$, $x_j \equiv \pm x_{j_0} \bmod x_m$. Hence, it is sufficient to prove the lemma for $k \le m$, $j \le m$. Thus suppose $x_k \equiv \pm x_j \bmod x_m$, $k \le m$ and $j \le m$. We shall prove that $x_k = \pm x_j$. Assume $x_k \ne \pm x_j$; then $|N_{K/\mathbf{Q}}(x_m)| \le |N_{K/\mathbf{Q}}(x_k \pm x_j)|$. We may assume without loss of generality that $|\sigma_n(x_k)| \ge |\sigma_n(x_j)|$. Then by the hypothesis of the lemma,

$$\begin{aligned}|N_{K/\mathbf{Q}}(x_m)| &= |\sigma_n(x_m)|^2 \cdot \prod_{i\le n-2} |\sigma_i(x_m)| \ge |\sigma_n(x_m)|^2 \cdot (\tfrac{1}{2})^{n-2} \\ &= (\tfrac{1}{2})^{n-2} \cdot \frac{|\sigma_{n,1}(\varepsilon)^m + \sigma_{n,1}(\varepsilon)^{-m}|^2}{4} \ge (\tfrac{1}{2})^n \left(|\sigma_{n,1}(\varepsilon)|^m - |\sigma_{n,1}(\varepsilon)|^{-m}\right)^2 \\ &> (\tfrac{1}{2})^{n+1} |\sigma_{n,1}(\varepsilon)|^{2m}.\end{aligned}$$

The last inequality holds by Lemma 4(1). Also

$$\begin{aligned}|N_{K/\mathbf{Q}}(x_k \pm x_j)| &\le (|\sigma_n(x_k)| + |\sigma_n(x_j)|)^2 \cdot \prod_{i\le n-2} (|\sigma_i(x_k)| + |\sigma_i(x_j)|) \\ &< (2|\sigma_n(x_k)|)^2 \cdot 2^{n-2} = |\sigma_n(x_k)|^2 \cdot 2^n \le |\sigma_{n,1}(\varepsilon)|^{2k} \cdot 2^n.\end{aligned}$$

So $|\sigma_{n,1}(\varepsilon)|^{2m-2k} < 2^{2n+1}$, i.e. $|\sigma_{n,1}(\varepsilon)|^{m-k} < 2^{n+1} < 2^{2n}$ which contradicts Lemma 4(1), if $m \ne k$. So we get $x_m = x_k$ and hence $x_m \mid x_j$. So we conclude that $|N_{K/\mathbf{Q}}(x_m)| \le |N_{K/\mathbf{Q}}(x_j)|$. As we proved above,

$$|N_{K/\mathbf{Q}}(x_m)| \ge (\tfrac{1}{2})^{n+1} |\sigma_{n,1}(\varepsilon)|^{2m}.$$

Also

$$\begin{aligned}|N_{K/\mathbf{Q}}(x_j)| &= \prod_{i\le n-2} |\sigma_i(x_j)| \cdot |\sigma_n(x_j)|^2 \le |\sigma_n(x_j)|^2 \\ &= \frac{|\sigma_{n,1}(\varepsilon)^j + \sigma_{n,1}(\varepsilon)^{-j}|^2}{4} \le |\sigma_{n,1}(\varepsilon)|^{2j}.\end{aligned}$$

Hence $|\sigma_{n,1}(\varepsilon)|^{2m-2j} \le 2^{n+1}$, which by Lemma 4(1) can happen only if $2m-2j = 0$, i.e. $m = j$. So $x_k = \pm x_j$. If $x_k = x_j$, then $\varepsilon^k + \varepsilon^{-k} = \varepsilon^j + \varepsilon^{-j}$, i.e. $\varepsilon^k - \varepsilon^j = \varepsilon^{-j} - \varepsilon^{-k}$, i.e. $\varepsilon^{-k}(1 - \varepsilon^{j-k}) = \varepsilon^j(\varepsilon^{k-j} - 1)$, i.e. $(\varepsilon^{k+j} + 1)(\varepsilon^{k-j} - 1) = 0$, i.e. $k = \pm j$. Similarly, if $x_k = -x_j$, $\varepsilon^k + \varepsilon^{-k} = -\varepsilon^j - \varepsilon^{-j}$, i.e. $(\varepsilon^k + \varepsilon^j)(1 + \varepsilon^{-k-j}) = 0$, i.e. $k = \pm j$.

LEMMA 6. *Suppose that K and a are as above with the additional hypothesis that $\sigma_{n,1}(\varepsilon)/\sigma_{n-1,1}(\varepsilon)$ is not a root of unity. Let $k \in \mathbf{N}_0$. Then there exist multiples m, h of k such that $|\sigma_i(x_m)| > \frac{1}{2}$ for $i = 1, 2, \ldots, n-2$ and $|\sigma_i(y_h)| > \frac{1}{2}$ for $i = 1, 2, \ldots, n-2$.*

PROOF. We shall prove that if

$$\sigma_{1,1}(\varepsilon)^{k_1} \sigma_{2,1}(\varepsilon)^{k_2} \cdots \sigma_{n-2,1}(\varepsilon)^{k_{n-2}} = 1, \tag{1}$$

then $k_1 = k_2 = \cdots = k_{n-2} = 0$. Let K_1 be the least normal extension of K and L_1 the least normal extension of L, so $K_1 \subset L_1$. It is enough to prove that for each σ_i, $i \le n-2$, there is an automorphism τ of K_1 such that $\tau\sigma_i = \sigma_{n-1}$ and $\tau\sigma_{n-1} = \sigma_i$ and for all $j \ne i, n-1$, $\tau\sigma_j = \sigma_j$, where by $\tau\sigma_j$ we mean the restriction of τ on $\sigma_j(K)$ composition σ_j. This is enough because for each $i \le n-2$, applying the corresponding τ extended to L_1 on both sides of (1) and taking absolute values, we get $|\sigma_{n,j}(\varepsilon)^{k_i}| = 1$ where $j = 1$ or 2; hence $k_i = 0$ and hence the result follows by the theorem of Kronecker (see [**5**]).

Notice that every automorphism of K_1 determines a permutation of the embeddings of K and conversely every permutation of these embeddings determines at most one automorphism of K_1. So when we write $\tau = (\sigma_i, \sigma_j)$ we mean that τ is the unique automorphism of K_1 which transposes σ_i and σ_j. Since $\sigma_{n-1}(K) \neq \sigma_n(K)$, the degree of the extension $\sigma_{n-1}(K)\sigma_n(K)$ over $\sigma_n(K)$ is at least 2, so the identity embedding of $\sigma_n(K)$ into $\mathbf{C}$ extends to at least one nonidentity embedding of $\sigma_{n-1}(K)\sigma_n(K)$ into $\mathbf{C}$. This embedding extends to an automorphism τ_1 of K_1. Since τ_1 is not the identity on $\sigma_{n-1}(K)\sigma_n(K)$ and is the identity on $\sigma_n(K)$, it can not be the identity on $\sigma_{n-1}(K)$. So, since $\tau_1\sigma_{n-1} \neq \sigma_{n-1}$ and $\tau_1\sigma_{n-1} \neq \sigma_n$, $\tau_1\sigma_{n-1}$ is a real embedding of K, say $\tau_1\sigma_{n-1} = \sigma_{i_0}$. Let τ_0 be the automorphism of K_1 such that $\tau_0(x) = \bar{x}$. Then $\tau_1\tau_0\tau_1^{-1} = (\sigma_{i_0}, \sigma_n)$, since τ_0 is a transposition $(\tau_0 = (\sigma_n, \sigma_{n-1}))$.

Now assume that $\sigma_{n-1}(K) \subset \sigma_1(K)\cdots\sigma_{n-2}(K)\sigma_n(K)$. Applying $\tau_1\tau_0\tau_1^{-1}$ to both sides we find $\sigma_{n-1}(K) \subset \sigma_1(K)\cdots\sigma_{n-2}(K)$ which is impossible since $\sigma_{n-1}(K)$ is nonreal and the right-hand side of the relation is real. So

$$\sigma_{n-1}(K) \not\subset \sigma_1(K)\cdots\sigma_{n-2}(K)\sigma_n(K).$$

Let $i \leq n-2$. Consider the extension

$$\sigma_{n-1}(K)\sigma_1(K)\cdots\sigma_{i-1}(K)\sigma_{i+1}(K)\cdots\sigma_{n-2}(K)\sigma_n(K)$$

over $\sigma_1(K)\cdots\sigma_{i-1}(K)\sigma_{i+1}(K)\cdots\sigma_{n-2}(K)\sigma_n(K)$. This extension may not be of degree 1, otherwise $\sigma_{n-1}(K) \subset \sigma_1(K)\cdots\sigma_{i-1}(K)\sigma_{i+1}(K)\cdots\sigma_{n-2}(K)\sigma_n(K)$, contrary to what we proved. So the identity embedding in $\mathbf{C}$ of the ground field extends to at least one nonidentity embedding of the extension field in $\mathbf{C}$. Let τ be an extension of this embedding to an automorphism of K_1. Clearly, since $\tau\sigma_{n-1} \neq \sigma_{n-1}$ and $\tau\sigma_j = \sigma_j$ for $j \neq i, n-1$, we must have $\tau\sigma_{n-1} = \sigma_i$ and hence $\tau = (\sigma_i, \sigma_{n-1})$ and this is what we should prove in order to conclude the lemma.

LEMMA 7. *Suppose that K and a are as above and that $|\sigma_i(a)| < 1/2^{8n}$ for $i = 1, 2, \ldots, n-2$. Let $m \in \mathbf{N}_0$. Then there exists an element b in O_K such that:*

(1) $b \equiv 1 \bmod y_m(a)$;

(2) $b \equiv a \bmod x_m(a)$;

(3) *b satisfies* $(*)$.

PROOF. Set $b = x_m^{2s} + a(1 - x_m^2)$ with $s \in \mathbf{N}_0$ to be determined. Since $x_m^2 - (a^2-1)y_m^2 = 1$, we have $x_m^2 \equiv 1 \bmod y_m$; hence (1) holds. Also (2) holds obviously. Since $|\sigma_i(x_m)| < 1$ for $i = 1, 2, \ldots, n-2$ and $|\sigma_n(x_m)| \cdot |\sigma_{n-1}(x_m)| = |\sigma_n(x_m)|^2 > 1$, we can choose s large enough so that $|\sigma_i(x_m)^{2s}| < 1/2^{8n}$ for $i = 1, 2, \ldots, n-2$. Then for $i = 1, 2, \ldots, n-2$ the following holds:

$$|\sigma_i(b)| \leq |\sigma_i(x_m)^{2s}| + |\sigma_i(a)| \cdot |1 - \sigma_i(x_m)^2| < |\sigma_i(x_m)|^{2s} + \frac{1}{2^{8n}} < \frac{2}{2^{8n}} < \frac{1}{2^{4n}}.$$

LEMMA 8. *Let K be any number field of degree n over $\mathbf{Q}$, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K into $\mathbf{C}$. Let $\xi, z \in O_K$ and $z \neq 0$. If $2^{n+1}\xi^n(\xi+1)^n\cdots(\xi+n-1)^n | z$, then $|\sigma_i(\xi)| < \frac{1}{2}|N(z)|^{1/n}$ for all $i = 1, 2, \ldots, n$.*

PROOF. See [**3**].

MAIN LEMMA. *Let K be as above and $a \in O_K$ satisfying*
$|\sigma_i(a)| < 1/2^{8n}$ *for* $i = 1, 2, \ldots, n-2$. $(**)$
and let d be defined as in the Remark before Lemma 3. Define the subset S of O_K by $\xi \in S \Leftrightarrow \xi \in O_K \wedge \exists x, y, w, z, u, v, s, t, x', y', w', z', u', v', s', t', b$ *in* O_K:

$$x'^2 - (a^2-1)y'^2 = 1, \tag{1}$$
$$w'^2 - (a^2-1)z'^2 = 1, \tag{2}$$
$$u'^2 - (a^2-1)v'^2 = 1, \tag{3}$$
$$s'^2 - (b^2-1)t'^2 = 1, \tag{4}$$
$$x + \delta(a)y = (x' + \delta(a)y')^{6d}, \tag{1*}$$
$$w + \delta(a)z = (w' + \delta(a)z')^{6d}, \tag{2*}$$
$$u + \delta(a)v = (u' + \delta(a)v')^{6d}, \tag{3*}$$
$$s + \delta(b)t = (s' + \delta(b)t')^{6d}, \tag{4*}$$
$$|\sigma_i(b)| < 1/2^{4n}, \qquad i = 1, 2, \ldots, n-2, \tag{5}$$
$$|\sigma_i(z)| \geq \tfrac{1}{2}, \qquad i = 1, 2, \ldots, n-2, \tag{6}$$
$$|\sigma_i(u)| \geq \tfrac{1}{2}, \qquad i = 1, 2, \ldots, n-2, \tag{7}$$
$$v \neq 0, \tag{8}$$
$$z^2 \mid v, \tag{9}$$
$$b \equiv 1 \bmod z, \tag{10}$$
$$b \equiv a \bmod u, \tag{11}$$
$$s \equiv x \bmod u, \tag{12}$$
$$t \equiv \xi \bmod z, \tag{13}$$
$$2^{n+1}\xi^n(\xi+1)^n \cdots (\xi+n-1)^n x^n (x+1)^n \cdots (x+n-1)^n | z. \tag{14}$$

Then $N_0 \subset S \subset \mathbf{Z}$.

PROOF. (i) Suppose there are $x, y, \ldots, b \in O_K$ satisfying (1)–(14). We shall prove that $\xi \in \mathbf{Z}$. From $(**)$ and (5) it follows that a and b satisfy $(*)$. Hence from (1)–(4), (1*)–(4*) and Lemma 3 it follows that there are $k, h, m, j \in \mathbf{N}$ such that:

$$\begin{aligned} x &= \pm x_k(a), & y &= \pm y_k(a), \\ w &= \pm x_h(a), & z &= \pm y_h(a), \\ u &= \pm x_m(a), & v &= \pm y_m(a), \\ s &= \pm x_j(b), & t &= \pm y_j(b). \end{aligned}$$

So (6)–(13) become

$$|\sigma_i(y_h(a))| \geq \tfrac{1}{2} \quad \text{for } i = 1, 2, \ldots, n-2, \tag{6'}$$
$$|\sigma_i(x_m(a))| \geq \tfrac{1}{2} \quad \text{for } i = 1, 2, \ldots, n-2, \tag{7'}$$
$$y_m(a) \neq 0, \tag{8'}$$
$$y_h^2(a) \mid y_m(a), \tag{9'}$$
$$b \equiv 1 \bmod y_h(a), \tag{10'}$$
$$b \equiv a \bmod x_m(a), \tag{11'}$$

$$(12') \qquad x_j(b) \equiv \pm x_k(a) \bmod x_m(a),$$
$$(13') \qquad y_j(b) \equiv \pm \xi \bmod y_h(a).$$

We have

$$y_j(b) \equiv j \bmod (b-1) \quad \text{(Lemma 1(7))},$$
$$y_j(b) \equiv j \bmod y_h(a) \quad \text{(by (10'))},$$
$$(15) \qquad j \equiv \pm \xi \bmod y_h(a) \quad \text{(by (13'))},$$
$$x_j(b) \equiv x_j(a) \bmod x_m(a) \quad \text{(by (11') and Lemma 1(8))},$$
$$x_j(a) \equiv \pm x_k(a) \bmod x_m(a) \quad \text{(by (12'))},$$
$$(16) \qquad k \equiv \pm j \bmod m \quad \text{(by (7'), (8') and Lemma 5)},$$
$$y_h(a) \mid m \quad \text{(by (6'), (9') and Lemma 4)},$$
$$k \equiv \pm j \bmod y_h(a) \quad \text{(by (16))},$$
$$(17) \qquad k \equiv \pm \xi \bmod z \quad \text{(by (15))},$$
$$|\sigma_i(\xi)| < \tfrac{1}{2}|N(z)|^{1/n} \quad \text{for } i = 1, 2, \ldots, n \quad \text{(by (14) and Lemma 8)},$$
$$k < |\sigma_n(x_k(a))| < \tfrac{1}{2}|N(z)|^{1/n} \quad \text{(by (14) and Lemma 8)},$$
$$|\sigma_i(k \pm \xi)| < |N(z)|^{1/n} \quad \text{for } i = 1, 2, \ldots, n.$$

So $|N(k+\xi)| < |N(z)|$ and so $k = \pm\xi$ (by (17)).

(ii) Conversely, suppose $\xi \in \mathbf{N}_0$. We shall prove that there are $x, y, \ldots, b \in O_K$ satisfying (1)–(14). Set $k = \xi \in \mathbf{N}_0$, $x' = x_k(a)$ and $y' = y_k(a)$; then (1) and (1*) are satisfied. By Lemmas 1(10), (4) and 6 there exists an $h \in \mathbf{N}_0$ such that the left-hand side of (14) divides $y_h(a)$ and $|\sigma_i(y_h(a))| \geq \frac{1}{2}$ for $i = 1, 2, \ldots, n-2$. Set $w' = x_h(a)$ and $z = y_h(a)$, then (2), (6) and (14) are satisfied. Again by Lemmas 1(10), (4) and 6, there exists an $m \in \mathbf{N}_0$ such that $y_h^2(a) \mid y_m(a)$ and $|\sigma_i(x_m(a))| \geq \frac{1}{2}$ for $i = 1, 2, \ldots, n-2$. Set $u' = x_m(a)$ and $v' = y_m(a)$; then (3), (3*) and (7)–(9) are satisfied. From Lemma 7 it follows that there exists $b \in O_K$ satisfying (10), (11) and (5). Set $s' = x_k(b)$ and $t' = y_k(b)$; then (4) is satisfied. Lemma 1(8) and (11) imply (12) and Lemma 1(7) and (10) imply (13). Thus all conditions are satisfied and $\xi \in S$.

LEMMA 9. *Let K be any number field.*

(i) *If R_1 and R_2 are diophantine relations over O_K, then $R_1 \vee R_2$ and $R_1 \wedge R_2$ are also diophantine over O_K.*

(ii) *The relation $x \neq 0$ is diophantine over O_K.*

PROOF. See [**3**].

LEMMA 10. *Let K be any number field, and σ an embedding of K into $\mathbf{R}$. Then the relation $\sigma(x) \geq 0$ is diophantine over O_K.*

PROOF. See [**3**].

THEOREM. *Let K be a number field with exactly two nonreal embeddings into $\mathbf{C}$, of degree $n \geq 3$ over $\mathbf{Q}$. Then $\mathbf{Z}$ is diophantine over O_K.*

PROOF. By Minkowski's lemma on convex bodies it follows that there is an a satisfying (**) of the Main Lemma. By Lemma 10 the relations (5)–(7) are diophantine over O_K and clearly the relations (1^*)–(4^*) can be written so that $\delta(a)$ and $\delta(b)$ do not occur, i.e. (1^*)–(4^*) are diophantine over O_K. So the set S of the Main Lemma is diophantine over L_K and hence $\mathbf{Z}$ is also diophantine over O_K.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, "Nauka", Moskow, 1964; English transl., Pure Appl. Math. 20, Academic Press, New York 1966.
2. J. Denef, *Hilbert's Tenth Problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220.
3. J. Denef, *Diophantine sets over algebraic integer rings.* II, Trans. Amer. Math. Soc. **257** (1980).
4. J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), 385–391.
5. G. Hardy and E. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1960.
6. Yu. Matijasevič, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 272–282; English transl., Soviet Math. Dokl. **11** (1970), 354–357.

COMPUTER TECHNOLOGY INSTITUTE, PATRAS 26110, GREECE

Current address: Department of Mathematics, Florida International University, University Park, Miami, Florida 33199