TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 257, Number 1, January 1980

DIOPHANTINE SETS OVER ALGEBRAIC INTEGER RINGS. II

BY

J. DENEF[1]

ABSTRACT. We prove that $\mathbf{Z}$ is diophantine over the ring of algebraic integers in any totally real number field or quadratic extension of a totally real number field.

1. Introduction.[2] Let B be a commutative ring with unit and let $R(x_1, \ldots, x_n)$ be a relation in B (in the sense of set theory). We say that $R(x_1, \ldots, x_n)$ is *diophantine over* B if there exists a polynomial $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ with coefficients in B such that, for all $x_1, \ldots, x_n$ in B,

$$R(x_1, \ldots, x_n) \leftrightarrow \exists y_1, \ldots, y_m \in B: P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

We call a subset S of B *diophantine over* B if the 1-ary relation "$x \in S$" is diophantine over B.

Let K be a number field (i.e., a field of finite degree over $\mathbf{Q}$); we denote the *ring of algebraic integers* in K by $\mathcal{O}_K$. Suppose $\mathbf{Z}$ (as a subset of $\mathcal{O}_K$) is diophantine over $\mathcal{O}_K$, then it is easy to see (using the fundamental result of [2]) that a relation R is diophantine over $\mathcal{O}_K$ if and only if R is recursively enumerable. Moreover, if $\mathbf{Z}$ is diophantine over $\mathcal{O}_K$, then the diophantine problem for $\mathcal{O}_K$ is recursively unsolvable.

In Denef and Lipshitz [6], we conjectured that $\mathbf{Z}$ is diophantine over $\mathcal{O}_K$, for every number field K. We proved this for $[K : \mathbf{Q}] = 2$ in [4], and for some $[K: \mathbf{Q}] = 4$ in [6]. A number field K is called *totally real* if every embedding of K into $\mathbf{C}$ maps K into $\mathbf{R}$. In the present paper we prove the following:

THEOREM. *If K is a totally real number field, then $\mathbf{Z}$ is diophantine over $\mathcal{O}_K$.*

Combining the above theorem with Theorem (c) of [6] we obtain:

COROLLARY. *If K is a quadratic extension of a totally real number field, then $\mathbf{Z}$ is diophantine over $\mathcal{O}_K$.*

For related questions and more references, see [6].

Received by the editors January 30, 1978 and, in revised form, November 9, 1978.

AMS (MOS) subject classifications (1970). Primary 02G05, 10N05, 10B99.

Key words and phrases. Hilbert's tenth problem, unsolvable problems, diophantine equations.

[1]This work was supported by the Belgian "Nationaal Fonds voor Wetenschappelijk Onderzoek". It was done at Princeton University whose generous hospitality I greatly appreciated.

[2]We use the following notations: $\mathbf{N}$ is the set of natural numbers; $\mathbf{N}_0$ is the set of positive natural numbers; $\mathbf{Z}$ is the ring of integers; $\mathbf{Q}$ is the field of rationals; $\mathbf{R}$ is the field of real numbers; and $\mathbf{C}$ is the field of complex numbers.

0002-9947/80/0000-0011/$03.50

The theorem is proved in §3. In §2 we define sequences $x_m(a), y_m(a) \in \mathcal{O}_K$, $m = 0, 1, 2, \ldots$. If K is a totally real number field, then, for certain $a \in \mathcal{O}_K$, the $\pm x_m(a)$, $\pm y_m(a)$ are exactly the solutions in $\mathcal{O}_K$ of the equation $x^2 - (a^2 - 1)y^2 = 1$ (Lemma 3). Since these solutions are not rational integers, we cannot use the methods of [**4**] and [**6**]. Instead we use an adaptation of Matijasevič's method [**8**] to obtain m from $y_m(a)$ in a diophantine way. Difficulties arise because we do not know whether or not certain properties of the classical Pell sequences used by Matijasevič are true for our sequences $x_m(a), y_m(a)$. Nevertheless we prove that certain subsequences satisfy all the properties needed (Lemmas 4 and 5). Compare conditions (1), (3), (4), (10), (11), (12), (13) and (14) of the Main Lemma (§3) with conditions (I)–(VII) of Davis [**2**, p. 244]. Condition (2) of the Main Lemma has been added to reach the whole sequence (using Lemma 6).

I would like to thank L. Lipshitz for inspiring conversations on this subject.

2. The sequences $x_m(a), y_m(a)$.

DEFINITION. Let K be a number field, $a \in \mathcal{O}_K$. Set $\delta(a) = \sqrt{a^2 - 1}$, $\varepsilon(a) = a + \delta(a)$. Suppose $\delta(a) \notin K$. We define the sequences $x_m(a), y_m(a) \in \mathcal{O}_K$, $m \in \mathbf{N}$, by

$$x_m(a) + \delta(a)y_m(a) = (\varepsilon(a))^m.$$

Where the context permits, the dependence on a is not explicitly shown, writing δ, ε, x_m, y_m.

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

(1) *ε is a unit in $\mathcal{O}_{K(\delta)}$, $\varepsilon^{-1} = a - \delta$, 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) $h | m \Rightarrow y_h | y_m$;

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

(6) $x_{m+1} = 2ax_m - x_{m-1}, y_{m+1} = 2ay_m - y_{m-1}$;

(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 $\eta \in \mathcal{O}_K$ and $\eta \neq 0$, then there exists an $m \in \mathbf{N}_0$ such that $\eta | y_m(a)$.*

PROOF. The proofs of (1)–(9) are exactly the same as for the classical Pell sequences, see, e.g., Lemmas 2.5, 2.8, 2.10, 2.13–2.15 and 2.20 of Davis [**2**]. We now prove (10): Let m be the order of the group of units in the finite ring $\mathcal{O}_{K(\delta)}/(2\delta\eta)$, where $(2\delta\eta)$ denotes the ideal generated by $2\delta\eta$. Then $\varepsilon^{\pm m} \equiv 1 \bmod 2\delta\eta$. Hence $\eta | (\varepsilon^m - \varepsilon^{-m})/2\delta = y_m$. Q.E.D.

For the remainder of §2, we suppose that K is a totally real number field of degree n over $\mathbf{Q}$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbf{R}$. Suppose $a \in \mathcal{O}_K$ satisfies

$$\sigma_1(a) \geqslant 2^{2n}, \qquad |\sigma_i(a)| < \tfrac{1}{2}, \quad \text{for } i = 2, 3, \ldots, n. \tag{$*$}$$

(Hence $a \notin \mathbf{Z}$.) Set $L = K(\delta) \neq K$. Every embedding σ_i of K into $\mathbf{R}$ extends to two embeddings $\sigma_{i,1}$ and $\sigma_{i,2}$ of K into $\mathbf{C}$. We have

$$\sigma_{i,1}(\delta) = \pm\sqrt{\sigma_i(a)^2 - 1} \quad \text{and} \quad \sigma_{i,2}(\delta) = -\sigma_{i,1}(\delta).$$

Only two embeddings $\sigma_{1,1}$ and $\sigma_{1,2}$ map L into $\mathbf{R}$. Choose $\sigma_{1,1}$ such that

$$0 < \sigma_{1,1}(\delta) = +\sqrt{\sigma_1(a)^2 - 1} \in \mathbf{R}.$$

We *identify* L with a subfield of $\mathbf{R}$ by the embedding $\sigma_{1,1}$; thus we write z instead of $\sigma_{1,1}(z)$.

LEMMA 2. *Suppose K is totally real and a satisfies* ($*$); *then for $m \in \mathbf{N}_0$, $i = 2, 3, \ldots, n$ and $j = 1, 2$ we have*:

(1) $a/2 < \delta < a$, $\sigma_{i,j}(\delta) \in \sqrt{-1}\,\mathbf{R}$ *and* $\frac{1}{2} < |\sigma_{i,j}(\delta)| < 1$;

(2) $a < \varepsilon < 2a$, $|\sigma_{i,j}(\varepsilon)| = 1$;

(3) $\varepsilon^m/4a < y_m < \varepsilon^m/a$, $|\sigma_i(y_m)| < 2$;

(4) $\varepsilon^m/2 < x_m < \varepsilon^m$, $|\sigma_i(x_m)| < 1$.

PROOF. Straightforward calculations using ($*$) and Lemma 1(2) yield the lemma. Q.E.D.

LEMMA 3. *Suppose K is totally real and a satisfies* ($*$); *then all solutions in $\mathcal{O}_K$ of the Pell equation*

$$x^2 - (a^2 - 1)y^2 = 1 \tag{1}$$

are given by $x = \pm x_m(a)$, $y = \pm y_m(a)$.

PROOF. Let U_K be the group of units in $\mathcal{O}_K$, and U_L the group of units in $\mathcal{O}_L$. Set

$$S = \{x + \delta y : x, y \in \mathcal{O}_K \text{ satisfy (1)}\}.$$

Obviously S is a subgroup of the kernel of the norm map $N_{L/K}\colon U_L \to U_K$: $u \mapsto N_{L/K}(u)$. Moreover $N_{L/K}$ maps U_L onto a subgroup (containing U_K^2) of finite index in U_K. Hence $\operatorname{rk} S \leqslant \operatorname{rk} U_L - \operatorname{rk} U_K$, where rk denotes the torsion free rank. From the Dirichlet-Minkowski theorem on units (see, e.g., Borevich and Shafarevich [1]) we obtain $\operatorname{rk} U_K = n - 1$, $\operatorname{rk} U_L = n$. Hence $\operatorname{rk} S = 1$ (notice that $\varepsilon \in S$). Since $S \subset \mathbf{R}$, the torsion subgroup of S is $\{\pm 1\}$. Let ε_0 be a generator for S modulo torsion, such that $\varepsilon_0 > 1$. We shall prove that $\varepsilon_0 = \varepsilon$, and this implies the lemma.

We have

$$\varepsilon = \varepsilon_0^e \quad \text{for some } e \in \mathbf{N}_0. \tag{2}$$

Notice that $\varepsilon_0 = x_0 + \delta y_0$, for some $x_0, y_0 \in \mathcal{O}_K$; hence $y_0 = (\varepsilon_0 - \varepsilon_0^{-1})/2\delta$ and $2\delta \mid (\varepsilon_0 - \varepsilon_0^{-1})$. Thus

$$|N(2\delta)| \leqslant |N(\varepsilon_0 - \varepsilon_0^{-1})|, \tag{3}$$

where N denotes the norm from L to $\mathbf{Q}$.

We have

$$|N(2\delta)| = 2^{2n}\left|(\delta)(-\delta)\prod_{\substack{i\neq 1\\ j}}(\sigma_{i,j}(\delta))\right| > 2^{2n}\delta^2\left(\tfrac{1}{2}\right)^{2n-2} > a^2 \quad \text{(Lemma 2(1))},$$

$$|N(\varepsilon_0 - \varepsilon_0^{-1})| = \left|(\varepsilon_0 - \varepsilon_0^{-1})(\varepsilon_0^{-1} - \varepsilon_0)\prod_{\substack{i\neq 1\\ j}}\left(\sigma_{i,j}(\varepsilon_0) - \sigma_{i,j}(\varepsilon_0)^{-1}\right)\right|$$

$$< \left(\varepsilon_0 - \varepsilon_0^{-1}\right)^2 2^{2n-2} < \varepsilon_0^2 2^{2n-2} \quad \text{(Lemma 2(2))}.$$

Combining these inequalities with (3) yields

$$a^2 < \varepsilon_0^2 2^{2n-2}. \tag{4}$$

Suppose $e \neq 1$, then (2) gives $\varepsilon \geqslant \varepsilon_0^2$, hence $2a > \varepsilon$ implies $2a > \varepsilon_0^2$. The last inequality and (4) yield $a < 2^{2n-1}$, which contradicts (*). Q.E.D.

LEMMA 4. *Suppose K is totally real, a satisfies (*), $h, m \in \mathbf{N}$, and*

$$|\sigma_i(y_h)| \geqslant \tfrac{1}{2} \quad \textit{for } i = 2, 3, \ldots, n. \tag{1}$$

Then we have

(i) $y_h | y_m \Rightarrow h | m$,
(ii) $y_h^2 | y_m \Rightarrow h y_h | m$.

PROOF. (i) Suppose $y_h | y_m$, but $h \nmid m$. Set $m = hq + k$ with $q, k \in \mathbf{N}$ and $0 < k < h$. Lemma 1(3) yields $y_m = x_k y_{hq} + x_{hq} y_k$. Notice that $y_h | y_{hq}$, hence $y_h | x_{hq} y_k$. Since $x_{hq}^2 - (a^2 - 1) y_{hq}^2 = 1$, the elements y_h and x_{hq} are relatively prime. Thus $y_h | y_k$ and

$$|N(y_h)| \leqslant |N(y_k)|, \tag{2}$$

where N denotes the norm from K to $\mathbf{Q}$. We have

$$|N(y_h)| = |y_h| \prod_{i\neq 1} |\sigma_i(y_h)| \geqslant |y_h|\left(\tfrac{1}{2}\right)^{n-1} \quad \text{(by (1))}$$

$$> \frac{\varepsilon^h}{4a}\left(\tfrac{1}{2}\right)^{n-1} \quad \text{(Lemma 2(3))},$$

$$|N(y_k)| = |y_k| \prod_{i\neq 1} |\sigma_i(y_k)| < \frac{\varepsilon^k}{a} 2^{n-1} \quad \text{(Lemma 2(3))}.$$

Combining these inequalities with (2) yields $\varepsilon^{h-k} < 2^{2n}$. Since $k < h$ we obtain $a < \varepsilon < 2^{2n}$, which contradicts (*). This proves (i).

(ii) Suppose $y_h^2 | y_m$. Then (i) implies $h | m$, and $m = hk$, with $k \in \mathbf{N}$. Lemma 1(5) yields $y_m \equiv k x_h^{k-1} y_h \mod y_h^3$. Hence $y_h^2 | k x_h^{k-1} y_h$. Since x_h and y_h are relatively prime, we obtain $y_h | k$. Q.E.D.

LEMMA 5. *Suppose K is totally real, a satisfies (*), $k, j \in \mathbf{N}$, $m \in \mathbf{N}_0$, and*

$$|\sigma_i(x_m)| \geqslant \tfrac{1}{2} \quad \textit{for } i = 2, 3, \ldots, n. \tag{1}$$

Then we have

$$x_k \equiv \pm x_j \mod x_m \Rightarrow k \equiv \pm j \mod m.$$

(*The two $\pm$'s 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 $k_0 \leqslant m$, $j_0 \leqslant m$. Lemma 1(9) implies

$$x_k \equiv \pm x_{k_0}, \qquad x_j \equiv \pm x_{j_0} \mod x_m.$$

Hence, it is sufficient to prove the lemma for $k \leqslant m, j \leqslant m$. Thus suppose $x_k \equiv \pm x_j \mod x_m$, $k \leqslant m$ and $j \leqslant m$. We shall prove that $x_k = x_j$. Assume $x_k \neq x_j$, then

$$|N(x_m)| \leqslant |N(x_k \pm x_j)|, \tag{2}$$

where N denotes the norm from K to $\mathbf{Q}$. We may suppose that $x_k > x_j$. We have

$$|N(x_m)| = x_m \prod_{i \neq 1} |\sigma_i(x_m)| \geqslant x_m\left(\tfrac{1}{2}\right)^{n-1} \quad \text{(by (1))}$$
$$> \varepsilon^m\left(\tfrac{1}{2}\right)^n \quad \text{(Lemma 2(4))},$$
$$|N(x_k \pm x_j)| \leqslant (|x_k| + |x_j|) \prod_{i \neq 1} (|\sigma_i(x_k)| + |\sigma_i(x_j)|)$$
$$< 2x_k 2^{n-1} \leqslant \varepsilon^k 2^n \quad \text{(Lemma 2(4))}.$$

From these inequalities, and (2) it follows that $\varepsilon^{m-k} < 2^{2n}$. Hence

$$a^{m-k} < 2^{2n}. \tag{3}$$

Combining (3) with (*) yields $k = m$. Thus the given congruence takes the simpler form $x_m | x_j$. Whence

$$|N(x_m)| \leqslant |N(x_j)|. \tag{4}$$

Using the same estimates as in the proof of (3) we obtain from (4) that $a^{m-j} < 2^n$. Since $j < m$ we are in contradiction with (*). Thus $x_k = x_j$. But the sequence x_k is strictly increasing in k, hence $k = j$. Q.E.D.

REMARK. Condition (1) in Lemmas 4 and 5 may not be necessary.

LEMMA 6. *Suppose K is totally real and a satisfies* (*). *Let $k \in \mathbf{N}_0$. Then there exist multiples $m, h \in \mathbf{N}_0$ of k such that*

$$|\sigma_i(x_m)| \geqslant \tfrac{1}{2} \quad \textit{for } i = 2, 3, \ldots, n,$$
$$|\sigma_i(y_h)| \geqslant \tfrac{1}{2} \quad \textit{for } i = 2, 3, \ldots, n.$$

PROOF. We recall a theorem of Kronecker (see, e.g., Hardy and Wright [7, Chapter 23, Theorem 442, p. 370], although we use another formulation): Let T, + be a 1-dimensional torus, i.e., $T \cong \mathbf{R}/\mathbf{Z}$, and $e, k \in \mathbf{N}_0$, $\bar{v} = (v_1, \ldots, v_e) \in T^e$. If $v_1, \ldots, v_e$ are linearly independent in T, then $\{m \cdot \bar{v}: m \in \mathbf{N}_0, k|m\}$ is everywhere dense in T^e.

Set $T = \{z \in \mathbf{C}: |z| = 1\}$ (now we use multiplicative notation). Set

$$\bar{v} = (\sigma_{2,1}(\varepsilon), \sigma_{3,1}(\varepsilon), \ldots, \sigma_{n,1}(\varepsilon)).$$

Lemma 2(2) gives $\bar{v} \in T^{n-1}$. Since

$$\sigma_i(x_m) = \tfrac{1}{2}\left(\sigma_{i,1}(\varepsilon)^m + \sigma_{i,1}(\varepsilon)^{-m}\right) \qquad \text{(Lemma 1(2))},$$
$$|\sigma_i(y_h)| \geqslant \left|\tfrac{1}{2}\left(\sigma_{i,1}(\varepsilon)^m - \sigma_{i,1}(\varepsilon)^{-m}\right)\right| \qquad \text{(Lemma 1(2) and 2(1))},$$

for $i = 2, 3, \ldots, n$, it is easy to see that Kronecker's theorem implies the lemma. Thus we only have to prove

$$\prod_{i \neq 1} \sigma_{i,1}(\varepsilon)^{a_i} = 1 \Rightarrow a_2 = a_3 = \cdots = a_n = 0, \tag{1}$$

for $a_2, a_3, \ldots, a_n \in \mathbf{Z}$.

Let us show, e.g., that $a_2 = 0$. Let τ be an automorphism of $\mathbf{C}$ such that $\tau\sigma_{2,1} = \sigma_{1,1}$. When τ acts on (1), we obtain

$$\varepsilon^{a_2} \prod_{i \neq 1,2} \tau\sigma_{i,1}(\varepsilon)^{a_i} = 1.$$

If $i \neq 2$, then $\tau\sigma_{i,1} \neq \sigma_{1,1}, \sigma_{1,2}$ and $|\tau\sigma_{i,1}(\varepsilon)| = 1$ (Lemma 2(2)). Hence $|\varepsilon^{a_2}| = 1$, and $a_2 = 0$. Q.E.D.

LEMMA 7. *Suppose K is totally real, a satisfies* (*), *and* $|\sigma_i(a)| \leqslant \frac{1}{8}$ *for* $i = 2, 3, \ldots, n$. *Let $m \in \mathbf{N}_0$. Then there exists an element b in $\mathcal{O}_K$ such that*:

(i) $b \equiv 1 \bmod y_m(a)$,
(ii) $b \equiv a \bmod x_m(a)$,
(iii) b *satisfies* (*),

PROOF. Set $b = x_m^{2s} + a(1 - x_m^2)$, with $s \in \mathbf{N}_0$ to be determined. Obviously (ii) is satisfied. Since $x_m^2 - (a^2 - 1)y_m^2 = 1$, we have $x_m^2 \equiv 1 \bmod y_m$; hence (i) holds. Lemma 2(4) gives $x_m > 1$ and $|\sigma_i(x_m)| < 1$ for $i \neq 1$. Thus we can choose s large enough that $b \geqslant 2^{2n}$ and $|\sigma_i(x_m^{2s})| \leqslant \frac{1}{4}$, for $i \neq 1$. Then (iii) is also satisfied. Q.E.D.

3. Diophantine definition of Z.

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 $\xi, z \in \mathcal{O}_K$ and $z \neq 0$. If*

$$2^{n+1}\xi^n(\xi + 1)^n \ldots (\xi + n - 1)^n | z,$$

then $|\sigma_i(\xi)| < \frac{1}{2}|N(z)|^{1/n}$ *for all* $i = 1, 2, \ldots, n$.

PROOF. (See also [**6**, Lemma 1].) Let $j = 0, 1, \ldots, n - 1$. We have $2^{n+1}(\xi + j)^n | z$, thus

$$|N(2^{n+1}(\xi + j)^n)| \leqslant |N(z)| \quad \text{and} \quad |N(\xi + j)| \leqslant |N(z/2^{n+1})|^{1/n},$$

where N denotes the norm from K to $\mathbf{Q}$. Set $c = |N(z/2^{n+1})|^{1/n} \geqslant 1$. We have

$$\prod_i |\sigma_i(\xi) + j| \leqslant c.$$

We only give a hint for the proof of the following claim: If $a_1, \ldots, a_n \in \mathbf{C}$, $c \in \mathbf{R}$, $c \geqslant 1$ and if $\prod_i |a_i + j| \leqslant c$ for all $j = 0, 1, \ldots, n - 1$, then we have

$|a_i| < 2^n c$ for all $i = 1, \ldots, n$. Hint: Consider two cases: $\exists j \forall i$: $|a_i + j| \geq \frac{1}{2}$ and $\forall j \exists i$: $|a_i + j| < \frac{1}{2}$, where i runs over $1, 2, \ldots, n$ and j over $0, 1, \ldots, n - 1$. Notice that the second case implies $\forall i \exists j$: $|a_i + j| < \frac{1}{2}$.

Applying the claim for $a_i = \sigma_i(\xi)$ yields the lemma. Q.E.D.

MAIN LEMMA. *Let K be a totally real number field of degree n over $\mathbf{Q}$, and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbf{R}$. Suppose $a \in \mathcal{O}_K$ satisfies*

$$\sigma_1(a) \geqslant 2^{2n} \quad \textit{and} \quad |\sigma_i(a)| \leqslant 1/8 \quad \textit{for } i = 2, 3, \ldots, n. \tag{**}$$

Define the subset S of $\mathcal{O}_K$ by

$$\xi \in S \leftrightarrow \xi \in \mathcal{O}_K \wedge \exists x, y, w, z, u, v, s, t, b \in \mathcal{O}_K:$$

$$x^2 - (a^2 - 1)y^2 = 1, \tag{1}$$
$$w^2 - (a^2 - 1)z^2 = 1, \tag{2}$$
$$u^2 - (a^2 - 1)v^2 = 1, \tag{3}$$
$$s^2 - (b^2 - 1)t^2 = 1, \tag{4}$$
$$\sigma_1(b) \geqslant 2^{2n}, \tag{5}$$
$$|\sigma_i(b)| \leqslant \tfrac{1}{2} \quad \textit{for } i = 2, 3, \ldots, n, \tag{6}$$
$$|\sigma_i(z)| \geqslant \tfrac{1}{2} \quad \textit{for } i = 2, 3, \ldots, n, \tag{7}$$
$$|\sigma_i(u)| \geqslant \tfrac{1}{2} \quad \textit{for } i = 2, 3, \ldots, n, \tag{8}$$
$$v \neq 0, \tag{9}$$
$$z^2 | v, \tag{10}$$
$$b \equiv 1 \mod z, \tag{11}$$
$$b \equiv a \mod u, \tag{12}$$
$$s \equiv x \mod u, \tag{13}$$
$$t \equiv \xi \mod z, \tag{14}$$
$$2^{n+1}\xi^n(\xi + 1)^n \ldots (\xi + n - 1)^n x^n (x + 1)^n \ldots (x + n - 1)^n | z. \tag{15}$$

Then $\mathbf{N}_0 \subset S \subset \mathbf{Z}$.

PROOF. (i) Suppose there are $x, y, \ldots, b \in \mathcal{O}_K$ satisfying (1)–(15). We shall prove that $\xi \in \mathbf{Z}$. From (**), (5) and (6) it follows that a and b satisfy (*). Hence from (1)–(4) and Lemma 3 it follows that there are $k, h, m, j \in \mathbf{N}$ such that

$$x = \pm x_k(a), \qquad y = \pm y_k(a),$$
$$w = \pm x_h(a), \qquad z = \pm y_h(a),$$
$$u = \pm x_m(a), \qquad v = \pm y_m(a),$$
$$s = \pm x_j(b), \qquad t = \pm y_j(b).$$

Thus (7)–(14) become

$$|\sigma_i(y_h(a))| \geqslant \tfrac{1}{2} \quad \text{for } i = 2, 3, \ldots, n, \tag{7'}$$

$$|\sigma_i(x_m(a))| \geqslant \tfrac{1}{2} \quad \text{for } i = 2, 3, \ldots, n, \tag{8'}$$

$$y_m(a) \neq 0, \tag{9'}$$

$$y_h^2(a) | y_m(a), \tag{10'}$$

$$b \equiv 1 \mod y_h(a), \tag{11'}$$

$$b \equiv a \mod x_m(a), \tag{12'}$$

$$x_j(b) \equiv \pm x_k(a) \mod x_m(a), \tag{13'}$$

$$y_j(b) \equiv \pm \xi \mod y_h(a). \tag{14'}$$

We have

$$y_j(b) \equiv j \mod (b-1) \quad \text{(Lemma 1(7))},$$

$$y_j(b) \equiv j \mod y_h(a) \quad \text{(by (11'))},$$

$$j \equiv \pm \xi \mod y_h(a) \quad \text{(by (14'))}, \tag{16}$$

$$x_j(b) \equiv x_j(a) \mod x_m(a) \quad \text{(by (12') and Lemma 1(8))},$$

$$x_j(a) \equiv \pm x_k(a) \mod x_m(a) \quad \text{(by (13'))},$$

$$k \equiv \pm j \mod m \quad \text{(by (8'), (9') and Lemma 5)}, \tag{17}$$

$$y_h(a) | m \quad \text{(by (7'), (10') and Lemma 4(ii))},$$

$$k \equiv \pm j \mod y_h(a) \quad \text{(by (17))},$$

$$k \equiv \pm \xi \mod z \quad \text{(by (16))}, \tag{18}$$

$$|\sigma_i(\xi)| < \tfrac{1}{2}|N(z)|^{1/n} \quad \text{for } i = 1, 2, \ldots, n \quad \text{(by (15) and Lemma 8)},$$

$$k < |\sigma_1(x_k(a))| < \tfrac{1}{2}|N(z)|^{1/n} \quad \text{(by (15) and Lemma 8)},$$

$$|\sigma_i(k \pm \xi)| < |N(z)|^{1/n} \quad \text{for } i = 1, 2, \ldots, n,$$

$$|N(k \pm \xi)| < |N(z)|,$$

$$k = \pm \xi \quad \text{(by (18))}.$$

Thus $\xi \in \mathbf{Z}$.

(ii) Conversely, suppose $\xi \in \mathbf{N}_0$. We shall prove that there are $x, y, \ldots, b \in \mathcal{O}_K$ satisfying (1)–(15). Set $k = \xi \in \mathbf{N}_0$, $x = x_k(a)$, and $y = y_k(a)$, then (1) is satisfied. By Lemmas 1(10), 1(4) and 6, there exists an $h \in \mathbf{N}_0$ such that the left-hand side of (15) divides $y_h(a)$ and $|\sigma_i(y_h(a))| \geqslant \frac{1}{2}$ for $i = 2, 3, \ldots, n$. Set $w = x_h(a)$ and $z = y_h(a)$, then (2), (7) and (15) are satisfied. Again by Lemmas 1(10), 1(4) and 6, there exists an $m \in \mathbf{N}_0$ such that $y_h^2(a) | y_m(a)$ and $|\sigma_i(x_m(a))| \geqslant \frac{1}{2}$ for $i = 2, 3, \ldots, n$. Set $u = x_m(a)$ and $v = y_m(a)$, then (3), and (8)–(10) are satisfied. From Lemma 7 it follows that there exists $b \in \mathcal{O}_K$ satisfying (11), (12), (5) and (6). Set $s = x_k(b)$ and $t = y_k(b)$, then (4) is satisfied. Lemma 1(8) and (12) imply (13), and Lemma 1(7) and (11) imply (14). Thus all conditions (1)–(15) are satisfied, and $\xi \in S$. Q.E.D.

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

(i) *If R_1 and R_2 are diophantine relations over $\mathcal{O}_K$, then $R_1 \vee R_2$ and $R_1 \wedge R_2$ are also diophantine over $\mathcal{O}_K$.*

(ii) *The relation $x \neq 0$ is diophantine over $\mathcal{O}_K$.*

PROOF. See [**6**, Proposition 1] or [**3**, §11]. Q.E.D.

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

PROOF. We recall a theorem of Hasse-Minkowski (see, e.g., O'Meara [**10**, §66]). Let $y \in K$. A quadratic form represents y in K if and only if it represents y in all completions of K. Moreover every quadratic form in 4 or more variables represents y in every nonarchimedean completion of K.

Choose $c \in \mathcal{O}_K$ such that $\sigma(c) > 0$ and the image of c under every other embedding of K into **R** is negative. Then we have for all x in $\mathcal{O}_K$ that

$$\sigma(x) \geqslant 0 \leftrightarrow \exists x_0, x_1, \ldots, x_4 \in \mathcal{O}_K\colon x_0 \neq 0 \wedge x_0^2 x = x_1^2 + x_2^2 + x_3^2 + c x_4^2.$$

Now apply Lemma 9. Q.E.D.

PROOF OF THE THEOREM. It is easy to see that there exists an $a \in \mathcal{O}_K$ satisfying (**) (this follows, e.g., from Minkowski's lemma on convex bodies [1, Chapter 2, §4.2, Theorem 3, p. 110]). From Lemmas 10 and 9 it follows that the set S of the Main Lemma is diophantine over $\mathcal{O}_K$. Thus **Z** is also diophantine over $\mathcal{O}_K$. Q.E.D.

REMARKS. From the Main Lemma one easily obtains an $\mathcal{O}_K$-diophantine representation of the relation "$y = y_\xi(a) \wedge \xi \in \mathbf{N}$" in the variables y and ξ.

Let K be a *totally real* algebraic field. If there exists an elliptic curve over **Q** such that its group of rational points over **Q** is *infinite* and of *finite index* in its group of rational points over K, then there exists a diophantine definition of **Z** over $\mathcal{O}_K$ which is much simpler than the one given in the Main Lemma. For example if the index is one, then we have for $\xi \in \mathcal{O}_K$ that

$$\xi \in \mathbf{Z} \leftrightarrow \exists x, y \in K\colon \big(y^2 = x^3 + ax + b \wedge |\sigma(\xi - y)| \leqslant \tfrac{1}{4},$$
$$\text{for every embedding } \sigma \text{ of } K \text{ into } \mathbf{C}\big),$$

where $y^2 = x^3 + ax + b$ is the equation of the elliptic curve. Indeed this follows from the following two facts: (i) if the group of rational points over **Q** is infinite, then it is dense in the group of rational points over **R**; (ii) if $\xi \in \mathcal{O}_K$, $y \in \mathbf{Q}$ and $|\sigma(\xi - y)| \leqslant \frac{1}{4}$ for every embedding σ of K into **C**, then $\xi \in \mathbf{Z}$. (See [**5**] for a detailed treatment.) Perhaps for every number field K there exists such an elliptic curve, but I could only prove this in special cases. This method also gives some single examples of algebraic fields K of infinite degree for which **Z** is diophantine over $\mathcal{O}_K$ (by using B. Mazur [**9**]).

The starting point of the present paper is Lemma 3. For number fields having only two nonreal embeddings into **C** a similar statement holds. Probably this case also can be treated by the method of the present paper. But I do not know how to treat the general case.

References

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, "Nauka", Moscow 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966.

2. M. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), 233–269.

3. M. Davis, Yu. Matijasevič and J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R. I., 1976, pp. 323–378.

4. J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220.

5. ______, *Diophantische verzamelingen over ringen van algebraische gehelen*, Thesis, Leuven, 1976.

6. J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), 385–391.

7. G. Hardy and E. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1960.

8. Yu. Matijasevič, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian); improved English translation: Soviet Math. Dokl. **11** (1970), 354–357.

9. B. Mazur, *Rational points on abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

10. O. T. O'Meara, *Introduction to quadratic forms*, 2nd ed., Springer-Verlag, Berlin, New York, 1971.

Department of Mathematics, University of Leuven, Celestijnenlaan 200B, 3030 Heverlee, Belgium