DIOPHANTINE SETS OVER ALGEBRAIC INTEGER RINGS. II

BY

J. DENEF

ABSTRACT. We prove that 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. 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 $\mathbb{Q}$); we denote the ring of algebraic integers in $K$ by $\mathfrak{o}_K$. Suppose $\mathbb{Z}$ (as a subset of $\mathfrak{o}_K$) is diophantine over $\mathfrak{o}_K$, then it is easy to see (using the fundamental result of [2]) that a relation $R$ is diophantine over $\mathfrak{o}_K$ if and only if $R$ is recursively enumerable. Moreover, if $\mathbb{Z}$ is diophantine over $\mathfrak{o}_K$, then the diophantine problem for $\mathfrak{o}_K$ is recursively unsolvable.

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

THEOREM. If $K$ is a totally real number field, then $\mathbb{Z}$ is diophantine over $\mathfrak{o}_K$.

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 $\mathbb{Z}$ is diophantine over $\mathfrak{o}_K$.

For related questions and more references, see [6].
The theorem is proved in §3. In §2 we define sequences \( x_m(a), y_m(a) \in \mathbb{O}_K \), \( m = 0, 1, 2, \ldots \). If \( K \) is a totally real number field, then, for certain \( a \in \mathbb{O}_K \), the \( \pm x_m(a), \pm y_m(a) \) are exactly the solutions in \( \mathbb{O}_K \) 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, \( a \in \mathbb{O}_K \). Set \( \delta(a) = \sqrt{a^2 - 1} \), \( \epsilon(a) = a + \delta(a) \). Suppose \( \delta(a) \not\in \mathbb{O}_K \). We define the sequences \( x_m(a), y_m(a) \in \mathbb{O}_K, m \in \mathbb{N} \), by

\[
x_m(a) + \delta(a)y_m(a) = \epsilon(a)^m
\]

Where the context permits, the dependence on \( a \) is not explicitly shown, writing \( \delta, \epsilon, x_m, y_m \).

**Lemma 1.** Let \( K \) be any number field, and \( a, b, c \in \mathbb{O}_K \). Suppose \( \delta(a), \delta(b) \not\in \mathbb{O}_K \). Let \( m, h, k, j \in \mathbb{N} \). We have:

1. \( \epsilon \) is a unit in \( \mathbb{O}_K^{*} \), \( \epsilon^{-1} = a - \delta \), and \( x_m, y_m \) satisfy the Pell equation \( x^2 - (a^2 - 1)y^2 = 1 \);
2. \( x_m = (\epsilon^m + \epsilon^{-m})/2, y_m = (\epsilon^m - \epsilon^{-m})/2\delta \);
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. \( y_{hk} \equiv k x_h y_{k-1} \mod y_h^3 \);
6. \( x_{m+1} = 2ax_m - x_{m-1}, y_{m+1} = 2ay_m - y_{m-1} \);
7. \( y_m(a) \equiv m \mod (a - 1) \);
8. if \( a \equiv b \mod c \), then \( x_m(a) \equiv x_m(b) \mod c \) and \( y_m(a) \equiv y_m(b) \mod c \);
9. \( x_{m+j} \equiv x_j \mod x_m \);
10. if \( \eta \in \mathbb{O}_K \) and \( \eta \not= 0 \), then there exists an \( m \in \mathbb{N}_0 \) 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 \( \mathbb{O}_K^{*}/(2\delta \eta) \), where \( (2\delta \eta) \) denotes the ideal generated by \( 2\delta \eta \). Then \( \epsilon^m \equiv 1 \mod 2\delta \eta \). Hence \( \eta (\epsilon^m - \epsilon^{-m})/2\delta = y_m \). Q.E.D.

For the remainder of §2, we suppose that \( K \) is a totally real number field of degree \( n \) over \( \mathbb{Q} \). Let \( \sigma_1, \ldots, \sigma_n \) be the embeddings of \( K \) into \( \mathbb{R} \). Suppose \( a \in \mathbb{O}_K \) satisfies
\begin{align*}
\sigma_i(a) &> 2^{2n}, \quad |\sigma_i(a)| < \frac{1}{2}, \quad \text{for } i = 2, 3, \ldots, n. 
\end{align*}
\hfill (\ast)

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

\begin{align*}
\sigma_{i,1}(\delta) &= \pm \sqrt{\sigma_i(a)^2 - 1} \quad \text{and} \quad \sigma_{i,2}(\delta) = - \sigma_{i,1}(\delta).
\end{align*}

Only two embeddings \( \sigma_{i,1} \) and \( \sigma_{i,2} \) map \( L \) into \( \mathbb{R} \). Choose \( \sigma_{i,1} \) such that

\begin{align*}
0 < \sigma_{i,1}(\delta) = + \sqrt{\sigma_i(a)^2 - 1} \in \mathbb{R}.
\end{align*}

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

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

\begin{enumerate}
\item \( a/2 < \delta < a, \sigma_j(\delta) \in \sqrt{-1} \mathbb{R} \) and \( \frac{1}{2} < |\sigma_j(\delta)| < 1 \);
\item \( e^m/2 < \delta < e^m/a, |\sigma_j(e^m/a)| = 1 \);
\item \( e^m/2 < \gamma_m < e^m/a, |\sigma_j(\gamma_m)| < 2 \);
\item \( e^m/2 < \gamma_m < e^m, |\sigma_j(\gamma_m)| < 1 \).
\end{enumerate}

**Proof.** Straightforward calculations using \((\ast)\) and Lemma 1(2) yield the lemma. Q.E.D.

**Lemma 3.** Suppose \( K \) is totally real and \( a \) satisfies \((\ast)\); then all solutions in \( \Theta_K \) of the Pell equation

\begin{align*}
x^2 - (a^2 - 1)y^2 &= 1 \quad (1)
\end{align*}

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

**Proof.** Let \( U_K \) be the group of units in \( \Theta_K \), and \( U_L \) the group of units in \( \Theta_L \). Set

\begin{align*}
S &= \{ x + \delta y : x, y \in \Theta_K \text{ satisfy } (1) \}.
\end{align*}

Obviously \( S \) is a subgroup of the kernel of the norm map \( N_{L/K} : U_L \to U_K : u \mapsto N_{L/K}(u) \). Moreover \( N_{L/K} \) maps \( U_L \) onto a subgroup (containing \( U_K^2 \)) of finite index in \( U_K \). Hence \( \text{rk } S < \text{rk } U_L - \text{rk } U_K \), where \( \text{rk} \) denotes the torsion free rank. From the Dirichlet-Minkowski theorem on units (see, e.g., Borevich and Shafarevich [1]) we obtain \( \text{rk } U_K = n - 1, \text{rk } U_L = n. \) Hence \( \text{rk } S = 1 \) (notice that \( e \in S \)). Since \( S \subset \mathbb{R} \), the torsion subgroup of \( S \) is \( \{ \pm 1 \} \). Let \( e_0 \) be a generator for \( S \) modulo torsion, such that \( e_0 > 1 \). We shall prove that \( e_0 = e \), and this implies the lemma.

We have

\begin{align*}
e &= e_0^e \quad \text{for some } e \in \mathbb{N}_0. \quad (2)
\end{align*}

Notice that \( e_0 = x_0 + \delta y_0 \), for some \( x_0, y_0 \in \Theta_K \); hence \( y_0 = (e_0 - e_0^{-1})/2\delta \) and \( 2\delta|e_0 - e_0^{-1}| \). Thus

\begin{align*}
|N(2\delta)| < |N(e_0 - e_0^{-1})|, \quad (3)
\end{align*}

where \( N \) denotes the norm from \( L \) to \( \mathbb{Q} \).
We have
\[ |N(2\delta)| = 2^n \left| \delta (\delta - \delta) \prod_{i \neq j} \sigma_i(\delta) \right| > 2^{2n} \left( \frac{1}{2} \right)^{2n-2} > a^2 \text{ (Lemma 2(1))}, \]
\[ |N(e_0 - e_0^-)| = \left| (e_0 - e_0^-)(e_0^- - e_0) \prod_{i \neq j} \sigma_i(e_0) - \sigma_i(e_0^-)^{-1} \right| \]
\[ < \left( e_0 - e_0^- \right)^2 2^{2n-2} < e_0^2 2^{2n-2} \text{ (Lemma 2(2))}. \]
Combining these inequalities with (3) yields
\[ a^2 < e_0^2 2^{2n-2}. \text{(4)} \]
Suppose \( e \neq 1 \), then (2) gives \( e > e_0^2 \), hence \( 2a > e \) implies \( 2a > e_0^2 \). The last inequality and (4) yield \( a < 2^{2n-1} \), which contradicts \( (\star) \). Q.E.D.

**Lemma 4.** Suppose \( K \) is totally real, \( a \) satisfies \( (\ast) \), \( h, m \in \mathbb{N} \), and
\[ |\eta_i(\eta_h)| > \frac{1}{2} \text{ for } i = 2, 3, \ldots, n. \text{(1)} \]

Then we have
(i) \( \eta_h|\eta_m \Rightarrow h|m \),
(ii) \( \eta_h^2|\eta_m \Rightarrow h^2|m \).

**Proof.** (i) Suppose \( \eta_h|\eta_m \), but \( h \nmid m \). Set \( m = hq + k \) with \( q, k \in \mathbb{N} \) and \( 0 < k < h \). Lemma 1(3) yields \( \eta_m = x_h \eta_q + x_q \eta_h \). Notice that \( \eta_h|\eta_q \), hence \( \eta_h|x_h \eta_h \). Since \( x_h^2 - (a^2 - 1)y_q^2 = 1 \), the elements \( \eta_h \) and \( x_h \) are relatively prime. Thus \( \eta_h \) and \( \eta_k \) and
\[ |N(\eta_h)| < |N(\eta_k)|, \text{(2)} \]
where \( N \) denotes the norm from \( K \) to \( \mathbb{Q} \). We have
\[ |N(\eta_h)| = |\eta_h| \prod_{i \neq 1} |\sigma_i(\eta_h)| > |\eta_h|(\frac{1}{2})^{n-1} \text{ (by (1))} \]
\[ > \frac{e^h}{4a} (\frac{1}{2})^{n-1} \text{ (Lemma 2(3))}, \]
\[ |N(\eta_k)| = |\eta_k| \prod_{i \neq 1} |\sigma_i(\eta_k)| < \frac{e^k}{a} 2^{n-1} \text{ (Lemma 2(3))}. \]
Combining these inequalities with (2) yields \( e^{h-k} < 2^n \). Since \( k < h \) we obtain \( a < e < 2^n \), which contradicts \( (\ast) \). This proves (i).

(ii) Suppose \( \eta_h^2|\eta_m \). Then (i) implies \( h|m \), and \( m = hk \), with \( k \in \mathbb{N} \). Lemma 1(5) yields \( \eta_m \equiv kx_h^{k-1} \eta_h \mod y_h^k \). Hence \( y_h^2 | kx_h^{k-1} \eta_h \). 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 \( (\ast) \), \( k, j \in \mathbb{N}, m \in \mathbb{N}_0 \), and
\[ |\sigma_i(\eta_m)| > \frac{1}{2} \text{ for } i = 2, 3, \ldots, n. \text{(1)} \]

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 \( q, h, k_0, j_0 \in \mathbb{N} \), and \( k_0 < m, j_0 < m \). Lemma 1(9) implies

\[
x_k \equiv \pm x_{k_0}, \quad x_j \equiv \pm x_{j_0} \mod x_m.
\]

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

\[
|N(x_m)| < |N(x_k \pm x_j)|, \tag{2}
\]

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

\[
|N(x_m)| = x_m \prod_{i \neq 1} |\sigma_i(x_m)| > x_m \left( \frac{1}{2} \right)^n \quad \text{(by (1))}
\]

\[
> e^m \left( \frac{1}{2} \right)^n \quad \text{(Lemma 2(4))},
\]

\[
|N(x_k \pm x_j)| < (|x_k| + |x_j|) \prod_{i \neq 1} (|\sigma_i(x_k)| + |\sigma_i(x_j)|)
\]

\[
< 2x_k 2^{n-1} < e^k 2^n \quad \text{(Lemma 2(4))}.
\]

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

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

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

\[
|N(x_m)| < |N(x_j)| \quad \text{(4)}
\]

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 \( k \in \mathbb{N}_0 \). Then there exist multiples \( m, h \in \mathbb{N}_0 \) of \( k \) such that

\[
|\sigma_i(x_m)| \geq \frac{1}{2} \quad \text{for } i = 2, 3, \ldots, n,
\]

\[
|\sigma_i(y_h)| \geq \frac{1}{2} \quad \text{for } i = 2, 3, \ldots, n.
\]

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., \( T = \mathbb{R}/\mathbb{Z} \), and \( e, k \in \mathbb{N}_0 \), \( \bar{e} = (v_1, \ldots, v_n) \in T^n \). If \( v_1, \ldots, v_n \) are linearly independent in \( T \), then \( \{m \cdot \bar{e}: m \in \mathbb{N}_0, k|m\} \) is everywhere dense in \( T^n \).

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

\[
\bar{e} = (\sigma_{2,1}(e), \sigma_{3,1}(e), \ldots, \sigma_{n,1}(e))
\]
Lemma 2(2) gives \( \bar{\theta} \in T^{n-1} \). Since
\[
\sigma_i(x_m) = \frac{1}{2} (\sigma_{i,1}(\epsilon)^m + \sigma_{i,1}(\epsilon)^{-m}) \quad \text{(Lemma 1(2))},
\]
\[
|\sigma_i(y_h)| > \frac{1}{2} (\sigma_{i,1}(\epsilon)^m - \sigma_{i,1}(\epsilon)^{-m}) \quad \text{(Lemma 1(2) and 2(1))},
\]
for \( i = 2, 3, \ldots, n \), it is easy to see that Kronecker’s theorem implies the lemma. Thus we only have to prove
\[
\prod_{i \neq 1} \sigma_{i,1}(\epsilon)^{a_i} = 1 \Rightarrow a_2 = a_3 = \cdots = a_n = 0, \quad (1)
\]
for \( a_2, a_3, \ldots, a_n \in \mathbb{Z} \).

Let us show, e.g., that \( a_2 = 0 \). Let \( \tau \) be an automorphism of \( \mathbb{C} \) such that
\[
\tau \sigma_{2,1} = \sigma_{1,1}.
\]
When \( \tau \) acts on (1), we obtain
\[
\epsilon^{a_2} \prod_{i \neq 1, 2} \tau \sigma_{i,1}(\epsilon)^{a_i} = 1.
\]
If \( i \neq 2 \), then \( \tau \sigma_{i,1} \neq \sigma_{1,1}, \sigma_{1,2} \) and \( |\tau \sigma_{i,1}(\epsilon)| = 1 \) (Lemma 2(2)). Hence \( |\epsilon^{a_2}| = 1 \), and \( a_2 = 0 \). Q.E.D.

**Lemma 7.** Suppose \( K \) is totally real, \( a \) satisfies (\( * \)), and \( |\sigma_i(a)| < \frac{1}{2} \) for \( i = 2, 3, \ldots, n \). Let \( m \in \mathbb{N}_0 \). Then there exists an element \( b \) in \( \Theta_K \) such that:

(i) \( b \equiv 1 \mod y_m(a) \),
(ii) \( b \equiv a \mod y_m(a) \),
(iii) \( b \) satisfies (\( * \)).

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

3. Diophantine definition of \( \mathbb{Z} \).

**Lemma 8.** Let \( K \) be any number field of degree \( n \) over \( \mathbb{Q} \), and let \( \sigma_1, \sigma_2, \ldots, \sigma_n \) be the embeddings of \( K \) into \( \mathbb{C} \). Let \( \xi, z \in \Theta_K \) 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 also [6, Lemma 1].) Let \( j = 0, 1, \ldots, n - 1 \). We have \( 2^{n+1}(\xi + j)^n |z| \), thus
\[
|N(2^{n+1}(\xi + j)^n)| < |N(z)| \quad \text{and} \quad |N(\xi + j)| < |N(z/2^{n+1})|^{1/n},
\]
where \( N \) denotes the norm from \( K \) to \( \mathbb{Q} \). Set \( c = |N(z/2^{n+1})|^{1/n} > 1 \). We have
\[
\prod_i |\sigma_i(\xi) + j| < c.
\]
We only give a hint for the proof of the following claim: If \( a_1, \ldots, a_n \in \mathbb{C} \), \( c \in \mathbb{R}, c > 1 \) and if \( \prod_j |a_i + j| < c \) for all \( j = 0, 1, \ldots, n - 1 \), then we have
\[ |a_i| < 2^c \text{ for all } i = 1, \ldots, n. \text{ Hint: Consider two cases: } \exists \forall i: |a_i + j| > \frac{1}{2} \text{ and } \forall \exists i: |a_i + j| < \frac{1}{2}, \text{ where } i \text{ runs over } 1, 2, \ldots, n \text{ and } j \text{ over } 0, 1, \ldots, n - 1. \text{ Notice that the second case implies } \forall \exists i: |a_i + j| < \frac{1}{2}. \]

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 \( \mathbb{Q} \), and let \( \sigma_1, \ldots, \sigma_n \) be the embeddings of \( K \) into \( \mathbb{R} \). Suppose \( a \in \Theta_K \) satisfies

\[ \sigma_1(a) \geq 2^{2n} \quad \text{and} \quad |\sigma_i(a)| < \frac{1}{8} \quad \text{for } i = 2, 3, \ldots, n. \quad (**) \]

Define the subset \( S \) of \( \Theta_K \) by

\[ \xi \in S \iff \xi \in \Theta_K \land \exists x, y, w, z, u, v, s, t, b \in \Theta_K: \]

\[ \begin{align*}
x^2 - (a^2 - 1)y^2 &= 1, \\
w^2 - (a^2 - 1)z^2 &= 1, \\
u^2 - (a^2 - 1)v^2 &= 1, \\
v^2 - (b^2 - 1)t^2 &= 1, \\
\sigma_i(b) &> 2^{2n}, \\
|\sigma_i(b)| &< \frac{1}{2} \quad \text{for } i = 2, 3, \ldots, n, \\
|\sigma_i(x)| &> \frac{1}{2} \quad \text{for } i = 2, 3, \ldots, n, \\
|\sigma_i(u)| &> \frac{1}{2} \quad \text{for } i = 2, 3, \ldots, n, \\
v &\neq 0, \\
z &\neq 0, \\
b &\equiv 1 \mod z, \\
b &\equiv a \mod u, \\
s &\equiv x \mod u, \\
t &\equiv \xi \mod z, \\
2^{n+1}x^n(\xi + 1)^n \ldots (\xi + n - 1)^n x^n(x + 1)^n \ldots (x + n - 1)^n \xi. \quad (15)
\end{align*} \]

Then \( N_0 \subset S \subset \mathbb{Z} \).

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

\[ \begin{align*}
x &= \pm x_k(a), & y &= \pm y_k(a), \\
w &= \pm x_h(a), & z &= \pm y_h(a), \\
u &= \pm x_m(a), & v &= \pm y_m(a), \\
s &= \pm x_j(b), & t &= \pm y_j(b).
\end{align*} \]
Thus (7)–(14) become

\[
\begin{align*}
|\sigma_i(y_h(a))| &> \frac{1}{2} \quad \text{for } i = 2, 3, \ldots, n, \quad (7') \\
|\sigma_i(x_m(a))| &> \frac{1}{2} \quad \text{for } i = 2, 3, \ldots, n, \quad (8') \\
y_m(a) &\neq 0, \quad (9') \\
y_m(a) | y_m(a), \quad (10') \\
b &\equiv 1 \mod y_h(a), \quad (11') \\
b &\equiv a \mod x_m(a), \quad (12') \\
x_j(b) &\equiv \pm x_k(a) \mod x_m(a), \quad (13') \\
y_j(b) &\equiv \pm \xi \mod y_h(a). \quad (14')
\end{align*}
\]

We have

\[
\begin{align*}
y_j(b) &\equiv j \mod (b - 1) \quad \text{(Lemma 1(7))}, \\
y_j(b) &\equiv j \mod y_h(a) \quad \text{(by (11'))}, \\
j &\equiv \pm \xi \mod y_h(a) \quad \text{(by (14'))}, \\
x_j(b) &\equiv x_j(a) \mod x_m(a) \quad \text{(by (12')) and Lemma 1(8))}, \\
x_j(a) &\equiv \pm x_k(a) \mod x_m(a) \quad \text{(by (13'))}, \\
k &\equiv \pm j \mod m \quad \text{(by (8'), (9') and Lemma 5),} \\
y_h(a) | m \quad \text{(by (7'), (10') and Lemma 4(ii))}, \\
k &\equiv \pm j \mod y_h(a) \quad \text{(by (17))}, \\
k &\equiv \pm \xi \mod z \quad \text{(by (16))}, \\
|\sigma_i(\xi)| &< \frac{1}{2} |N(z)|^{1/n} \quad \text{for } i = 1, 2, \ldots, n \quad \text{(by (15) and Lemma 8),} \\
k &< |\sigma_i(x_k(a))| < \frac{1}{2} |N(z)|^{1/n} \quad \text{(by (15) and Lemma 8),} \\
|\sigma_i(k \pm \xi)| &< |N(z)|^{1/n} \quad \text{for } i = 1, 2, \ldots, n, \\
|N(k \pm \xi)| &< |N(z)|, \\
k &\equiv \pm \xi \quad \text{(by (18))}.
\end{align*}
\]

Thus \( \xi \in \mathbb{Z} \).

(ii) Conversely, suppose \( \xi \in \mathbb{N}_0 \). We shall prove that there are \( x, y, \ldots, b \in \mathbb{C}_K \) satisfying (1)–(15). Set \( k = \xi \in \mathbb{N}_0, x = x_k(a), \) and \( y = y_k(a) \), then (1) is satisfied. By Lemmas 1(10), 1(4) and 6, there exists an \( h \in \mathbb{N}_0 \) such that the left-hand side of (15) divides \( y_h(a) \) and \( |\sigma_i(y_h(a))| > \frac{1}{2} \) for \( i = 2, 3, \ldots, n \). Set \( w = x_k(a) \) and \( z = y_k(a) \), then (2), (7) and (15) are satisfied. Again by Lemmas 1(10), 1(4) and 6, there exists an \( m \in \mathbb{N}_0 \) such that \( y_m(a) \) divides \( y_m(a) \) and \( |\sigma_i(x_m(a))| > \frac{1}{2} \) for \( i = 2, 3, \ldots, n \). Set \( u = x_m(a) \) and \( v = y_m(a) \), then (3), (8)–(10) are satisfied. From Lemma 7 it follows that there exists \( b \in \mathbb{C}_K \) 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 \( \xi \in \mathbb{S} \). 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 $R_1 \lor R_2$ and $R_1 \land R_2$ 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 $\sigma$ an embedding of $K$ into $\mathbb{R}$. Then the relation $\sigma(x) > 0$ 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 $\mathbb{R}$ is negative. Then we have for all $x \in \mathcal{O}_K$ that

$$\sigma(x) > 0 \iff \exists x_0, x_1, \ldots, x_4 \in \mathcal{O}_K : x_0 \neq 0 \land x_0^2 x = x_1^2 + x_2^2 + x_3^2 + cx_4^2.$$ 

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 $\mathbb{Z}$ is also diophantine over $\mathcal{O}_K$. Q.E.D.

Remarks. From the Main Lemma one easily obtains a $\mathcal{O}_K$-diophantine representation of the relation “$y = y_\xi(a) \land \xi \in \mathbb{N}$” in the variables $y$ and $\xi$.

Let $K$ be a totally real algebraic field. If there exists an elliptic curve over $\mathbb{Q}$ such that its group of rational points over $\mathbb{Q}$ is infinite and of finite index in its group of rational points over $K$, then there exists a diophantine definition of $\mathbb{Z}$ 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

$$\xi \in \mathbb{Z} \iff \exists x, y \in K : (y^2 = x^3 + ax + b \land |\sigma(\xi - y)| < \frac{1}{2},$$

for every embedding $\sigma$ of $K$ into $\mathbb{C}$),

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 $\mathbb{Q}$ is infinite, then it is dense in the group of rational points over $\mathbb{R}$; (ii) if $\xi \in \mathcal{O}_K$, $y \in \mathbb{Q}$ and $|\sigma(\xi - y)| < \frac{1}{4}$ for every embedding $\sigma$ of $K$ into $\mathbb{C}$, then $\xi \in \mathbb{Z}$. (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 $\mathbb{Z}$ 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 $\mathbb{C}$ 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


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LEUVEN, CELESTIJNENLAAN 200B, 3030 HEVERLEE, BELGIUM