Notre Dame Journal of Formal Logic
Volume 33, Number 3, Summer 1992

A Diophantine Definition of Rational Integers over Some Rings of Algebraic Numbers

ALEXANDRA SHLAPENTOKH

Abstract The author considers the rings of algebraic numbers integral at all but finitely many primes in the number fields, where it has been previously shown that Hilbert's Tenth Problem is undecidable in the rings of algebraic integers, and proves that the problem is still undecidable in the bigger rings by constructing a diophantine definition of rational integers there.

1 Introduction Hilbert's Tenth Problem can be phrased as the following question. Is there an algorithm to determine, given an integer polynomial equation $f(x_1, \ldots, x_n) = 0$, whether this equation has integer solutions? This question was answered negatively by Davis, Robinson, Matijasevich, and Putnam. (See Davis et al. [2] and Davis [1].) One of the major and still unresolved problems in the area is the same question applied to rings of algebraic integers of a general number field as well as number field itself. The problem is also still unresolved for $\mathbb{Q}$.

The present paper can be a step in the direction of resolving the problem for some number fields. Instead of the rings of algebraic integers, the author considers the Diophantine problem over the rings of algebraic numbers where finitely many primes are allowed to appear in the denominators. Using the Pell equation technique similar to the one introduced in a proof of the original problem (see [1]) and extended by Denef in [5], the author shows that in all the fields where Hilbert's Tenth Problem is known to have no solution in the rings of algebraic integers, with the exception of the case of the extensions of degree 4 with no real subfield, the problem is still unsolvable in the bigger rings described above.

Besides the ring of rational integers, the Diophantine problem is known to be undecidable in the rings of algebraic integers of all the totally real fields, fields of degree 2 over totally real fields, fields with one pair of complex conjugate embeddings, fields of degree 4 with a subfield of degree 2, and all the subfields of the above-mentioned fields. These subfields include all the abelian extensions

Received September 23, 1991; revised February 24, 1992

of the rationals. (For proofs of these results see Denef [3],[5], Denef and Lipschitz [4], Pheidas [8], Shlapentokh [10], Shapiro and Shlapentokh [9].)

In a preceding paper the author has constructed a Diophantine definition of rational integers over subrings of $\mathbb{Q}$ where only finitely many primes are allowed to appear in the denominators (see Shlapentokh [11]). The present paper extends the result to the analogous rings of all the other above-described fields.

The notion of a Diophantine relation between two sets is central to the discussion. It is defined as follows.

Definition 1.1 Given K, M rings, $K \subset M$, we will say that M *is Diophantine over* K (Dioph(M/K)) if there exists a polynomial equation $f(t, x_1, \ldots, x_n) = 0$ with coefficients in M, which has solutions $t, x_1, \ldots, x_n$ in M if and only if t is in K. The polynomial $f(t, x_1, \ldots, x_n)$ is called a *Diophantine definition* of K over M.

It is not hard to show that if M is not algebraically closed a Diophantine definition can be allowed to consist of finitely many polynomials without changing the relation, and expressions like "$h(x_1, \ldots, x_n) = 0$ AND $g(y_1, \ldots, y_m) = 0$" and "$h(x_1, \ldots, x_n) = 0$ OR $g(y_1, \ldots, y_m) = 0$" can be substituted by a single polynomial equation (see [2]). Finally, for any integral domain M containing $\mathbb{Z}$, Dioph($M/\mathbb{Z}$) implies that there is no solution to Hilbert's Tenth Problem in M (see [2]).

2 The Pell equation over number fields with one pair of complex conjugate embeddings

Definition 2.1 Let K be a number field and let $S = \{p_1, \ldots, p_s\}$ be a set of its finite primes. Then define a ring $O_{K,S} \subset K$ to be

$$O_{K,S} = \{x \in K \mid \forall q \notin S \ \mathrm{ord}_q x \geq 0\}. \tag{2.1.1}$$

In other words $O_{K,S}$ is the ring of all the elements of K integral at all the finite primes of K outside S.

Notation Let $O_K \subset O_{K,S}$ denote the ring of algebraic integers of K. In this paper we shall often refer to divisibility conditions in O_K and $O_{K,S}$. To distinguish the two, we will reserve the symbol "$|$" for the regular divisibility in O_K. Divisibility in $O_{K,S}$ will be denoted by "$|_S$". We will use the same notational scheme with respect to modular equivalencies: "$\equiv_S$" will denote equivalence in $O_{K,S}$ and "$\equiv$" will denote equivalence in O_K.

As has been mentioned in the introduction, the Pell equation plays a prominent role in the proofs presented in this paper. What follows is the examination of properties of the Pell equation in the rings $O_{K,S}$.

Definition 2.2 Let $d \in O_{K,S}$, be a nonsquare of K and define $H_{K,d,S}$ to be a following subset of $M = K(d^{1/2})$

$$H_{K,d,S} = \{x - d^{1/2}y,\ x, y \in O_{K,S} \mid x^2 - dy^2 = 1\}.$$

Lemma 2.3 *$H_{K,d,S}$ is a group under multiplication. Moreover, if $x - d^{1/2}y \in H_{K,d,S}$ and $(x_k - d^{1/2}y_k) = (x - d^{1/2}y)^k$ then the following statements are true:*

(2.3.1) $x_{m\pm k} = x_m x_k \pm d y_m y_k$, $y_{m\pm k} = x_k y_m \pm y_k x_m$;

(2.3.2) *if $m = kj$ then $y_j |_S y_m$;*

(2.3.3) *if* $m = 2kj$ *then* $x_j |_S y_m$;
(2.3.4) *if* $m = 2jk$ *and* $m = rx_j$ *then* $x_j^2 |_S y_m$;
(2.3.5) *if* $m = (2k+1)j$ *then* $x_j |_S x_m$;
(2.3.6) $x_{(2k+1)j} \cong_S -(2k+1)x_j \bmod (x_j^2)$;
(2.3.7) $\forall \eta \in O_{K,S}\ \exists m \in \mathbb{N}$ *such that* $\eta |_S y_m$.

Proof: For the proof of the fact that $H_{K,d,S}$ is a group, see Lemma 2.1 of [11]. (2.3.1)–(2.3.6) follow from binomial theorem, and for the proof of (2.3.7) see Lemma 1 of [5].

Lemma 2.4 *Let* $\tau_1, \ldots, \tau_k$ *be all the real embeddings of* K, *such that* $\tau_i(d) < 0$. *Then, assuming* $x - d^{1/2}y$ *is not a root of unity*:

a. *given any constant* $0 < C_1 < 1$ *and* $x - d^{1/2}y \in H_{K,d,S}$, $\forall z \in \mathbb{N}\ \exists m \in \mathbb{N}$ *such that* $(x_m - d^{1/2}y_m) = (x - d^{1/2}y)^m$, $m \cong 0 \bmod z$ *and* $\exists C_2 < 1$, *depending on* C_1 *and* $x - d^{1/2}y$, *such that* $\forall \tau_i$

$$C_1 < |\tau_i(x_m)| < C_2;$$

b. *if* K *is totally real,* $k < n$, $\forall i = 1, \ldots, k\, |\tau_i(x)| > \frac{1}{2}$, $|\tau_i(d)| \geq \frac{3}{4}$, *and for all the other embeddings of* K *into* $\mathbb{C}$, $\tau(d) > 2^{2n}$ *then* $|N_{K/\mathbb{Q}}(x)| \geq |N_{K/\mathbb{Q}}(y)|$.

Proof: Let $\omega_i = \tau_i(x - d^{1/2}y)$ and note that $|\omega_i| = 1$. Further, consider the multiplicative group Ω generated by $\{\omega_1, \ldots, \omega_k\}$. Renumber ω's so that $\{\omega_j\}$, $j = 1, \ldots, t$ is the smallest subset of $\{\omega_1, \ldots, \omega_k\}$ such that the multiplicative group generated by $\{\omega_j\}_{j=1,\ldots,t}$ is of finite index in Ω. Then $\forall i = 1, \ldots, k$ we have the following equality:

$$\omega_i^{b_i} = \prod_{j=1}^{t} \omega_j^{b_{ij}}, \tag{2.4.1}$$

where $b_i > 0$, and not all b_{ij}'s are zero. To get the construction under way, let $0 < \theta_{\max} < \frac{1}{2}\Pi$ be such that $\mathrm{Re}(e^{i\theta_{\max}}) = \cos\theta_{\max} > C_1$. Let $c_1, \ldots, c_k \in \mathbb{N} - \{0\}$ be such that $\forall i = 1, \ldots, k$, $j = 1, \ldots, t\ \sum c_i b_{ij} \neq 0$. Next if for some $i\ \sum c_i b_{ij} < 0$, then substitute ω_i^{-1} for ω_i and replace b_{ij} by $-b_{ij}$. Thus, without loss of generality, we can assume that $\sum c_i b_{ij} > 0$. Let

$$B = \max_{i,j} |b_{ij}|; \tag{2.4.2}$$

$$C = \max_{i,j} c_{ij}; \tag{2.4.3}$$

$$\theta_j = \frac{c_j \theta_{\max}}{2BCt}. \tag{2.4.4}$$

Then

$$\sum b_{ij}\theta_j = \theta_{\max} \sum \frac{b_{ij}c_j}{2BCt}.$$

Since $\sum b_{ij}c_j > 0$, $\sum b_{ij}\theta_j > 0$, and by definition of B and C,

$$\left| \frac{b_{ij}c_j}{2BCt} \right| < \frac{1}{2t},$$

so that

$$\sum b_{ij}\theta_j < \sum |b_{ij}\theta_j| < \tfrac{1}{2}\theta_{\max},$$

and consequently,

$$0 < b_i^{-1} \sum b_{ij}\theta_j < \tfrac{1}{2}\theta_{\max}.$$

Finally, consider the following family of linear functions

$$f_i(x_1, \ldots, x_t) = b_i^{-1} \sum b_{ij} x_j. \tag{2.4.5}$$

If $|x_j' - x_j| < \varepsilon$ then $|f_i(x_1, \ldots, x_t) - f_i(x_1', \ldots, x_t')| < Bt\varepsilon$. Let

$$\varepsilon_{\min} = \min\left(\min_i (\theta_{\max} - b_i^{-1} \sum b_{ij}\theta_j), \min_i (b_i^{-1} \sum b_{ij}\theta_j)\right) \tag{2.4.6}$$

$$\theta_{\min} = \tfrac{1}{2} \min_i (b_i^{-1} \sum b_{ij}\theta_j), \tag{2.4.7}$$

and denote $\theta_j' = \theta_j + \varepsilon_{\min}/4BT$.

By Kronecker's Theorem (see Hardy and Wright [6]) $\exists m \in \mathbb{N}$, $m \cong 0 \bmod z$ such that $\forall j = 1, \ldots, t\ \omega_j^m = e^{i\varphi_j}$, where $|\varphi_j - \theta_j'| < \varepsilon_{\min}/4BT$. Then by (2.4.1), $\forall i = 1, \ldots, k$, $\arg(\omega_i^m) = \Theta_i$, where $\Theta_i = f_i(\varphi_1, \ldots, \varphi_t)$, and

$$\varphi_j - \theta_j = \varphi_j - \theta_j' + \theta_j' - \theta_j < \epsilon_{\min}/4BT + \epsilon_{\min}/4BT = \epsilon_{\min}/2BT.$$

Therefore, we have the following sequence of inequalities:

$$|\Theta_i - b_i^{-1} \sum b_{ij}\theta_j| < \varepsilon_{\min}/2;$$

$$b_i^{-1} \sum b_{ij}\theta_j - (\varepsilon_{\min}/2) < \Theta_i < b_i^{-1} \sum b_{ij}\theta_j + (\varepsilon_{\min}/2);$$

$$b_i^{-1} \sum b_{ij}\theta_j - \tfrac{1}{2}(\min_i b_i^{-1} \sum b_{ij}\theta_j) < \Theta_i < b_i^{-1} \sum b_{ij}\theta_j$$

$$+ \tfrac{1}{2} \min_i (\theta_{\max} - b_i^{-1} \sum b_{ij}\theta_j);$$

$$\theta_{\max} > \Theta_i > \theta_{\min}.$$

Let $C_2 = \cos\theta_{\min}$, part 1 is proved.

For the proof of part 2 note the following.

$$\forall i = 1, \ldots, k\, |\tau_i(dy^2)| < \tfrac{3}{4},$$

and consequently,

$$\forall i = 1, \ldots, k\, \tfrac{1}{2}|\tau_i(y)| < |\tau_i(x)|.$$

On the other hand, if τ is any other embedding of K into $\mathbb{R}$, then by assumption, $\tau(d) > 2^{2n}$, and $\tau(x^2) = \tau(dy^2) + 1 \geq \tau(dy^2) \geq 2^{2n}\tau(y^2)$. Therefore,

$$|N_{K/\mathbb{Q}}(x)| \geq (\tfrac{1}{2})^k 2^{2n(n-k)} |N_{K/\mathbb{Q}}(y)| \geq (\tfrac{1}{2})^k 2^{2n} |N_{K/\mathbb{Q}}(y)| \geq (\tfrac{1}{2})^k 2^{2n}.$$

Lemma 2.5 *Let d, K, M be as in Definition 2.2, let $x, y \in K$, and let $\omega = x - d^{1/2}y \in M$ be such that $N_{L/K}(\omega) = 1$. Then:*

a. *$\forall$ prime β of M, $\operatorname{ord}_\beta \omega \neq 0$ implies β has a distinct conjugate over K;*
b. *assuming $\omega \in H_{K,d,S}$ and all primes of S are either ramified or do not split in M, ω is integral;*
c. *assuming $d = d_0 d_1$, where $\operatorname{ord}_p d$ is odd positive, $\forall p \in S\ 0 \leq \operatorname{ord}_p d_0 \leq 1$, and $x - d^{1/2}y \in H_{K,d,S}$, we can conclude that $x, y^2 d_1 \in O_K$, $yd^{1/2}$, $x - d^{1/2}y \in O_M$.*

Proof: Let $\prod \beta_i^{a_i}$ be the divisor of ω. Then $(1) = N_{M/K}(\prod \beta_i^{a_i}) = \prod q_i^{f_i a_i}$, where β_i lies above q_i – a prime of K, and $f_i = f(\beta_i/q_i)$ is the degree of β_i over q_i. Unless each q_i occurs twice in the product, the equality cannot hold. Therefore, each q_i must split and each β_i has a distinct conjugate.

If all the primes of S ramify or do not split, by the preceding argument, ω cannot have a nonzero order at any of the primes of M above the primes of S. On the other hand, if for some prime β of M $\operatorname{ord}_\beta \omega < 0$, then $0 > \operatorname{ord}_\beta(\omega + \omega^{-1}) = \operatorname{ord}_\beta 2x$. But $x \in O_{K,S}$ and hence β must lie above a prime of S. Therefore we have a contradiction with the first part of the proof.

By assumption, $x^2 - dy^2 = 1$. Let $p \in S$, then $\operatorname{ord}_p dy^2 = \operatorname{ord}_p d + 2\operatorname{ord}_p y$ is an odd number, because for all $p \in S$ $\operatorname{ord}_p d$ is an odd positive number. Therefore,

$$\operatorname{ord}_p(dy^2 + 1) = \begin{cases} 0 \text{ if } \operatorname{ord}_p dy^2 > 0, \\ \text{odd negative integer, if } \operatorname{ord}_p dy^2 < 0. \end{cases}$$

But $2\operatorname{ord}_p x = \operatorname{ord}_p(dy^2 + 1)$, and therefore, $\operatorname{ord}_p x = 0$, and $\operatorname{ord}_p dy^2 \geq 0$.

Letting $d = d_0 d_1$, we also deduce $0 \leq \operatorname{ord}_p dy^2 < \operatorname{ord}_p d_0 + \operatorname{ord}_p d_1 y^2$. Next, suppose that $\operatorname{ord}_p d_1 y^2 < 0$, then $|\operatorname{ord}_p d_0| > |\operatorname{ord}_p d_1 y^2| \geq 1$. But $\operatorname{ord}_p d_0 \leq 1$, so the previous double inequality implies that $\operatorname{ord}_p d_0 = 1$, and $\operatorname{ord}_p d_1 y^2 = -1$. These two equalities in turn imply that $\operatorname{ord}_p d_1$ is odd and $\operatorname{ord}_p d = \operatorname{ord}_p d_0 d_1$ is even. The last statement is of course in contradiction with our assumption on d.

Notation From here to the end of this section let K be a number field with one pair of complex conjugate embedding and assume K is of degree $n > 2$ over $\mathbb{Q}$. (We will consider the case of a complex extension of degree 2 later.) Let $\sigma_1 =$ identity, $\sigma_2, \ldots, \sigma_n$ be all the embeddings of K into $\mathbb{C}$. Assume σ_1, σ_2 are the complex embeddings, and $\sigma_{i,1}$ and $\sigma_{i,2}$ are the two extensions of σ_i to M, $i = 1, \ldots, n$.

Let $a \in O_K$, and consider $a - (a^2 - 1)^{1/2} \in M = K((a^2 - 1)^{1/2})$. Since $(a - (a^2 - 1)^{1/2})(a + (a^2 - 1)^{1/2}) = 1$, either $|a - (a^2 - 1)^{1/2}| \geq 1$ or $|a + (a^2 - 1)^{1/2}| \geq 1$. Let $\varepsilon(a) = a \pm (a^2 - 1)^{1/2}$, with the sign chosen to ensure that $|\varepsilon(a)| \geq 1$. Also denote by ω a generic element of $H_{K,d,S}$.

Lemma 2.6 *Suppose $a \in O_K$, and $\forall i = 3, \ldots, n |\sigma_i(a)| < 1$. Then $\forall i = 1, \ldots, n$ $\sigma_{i,j}(M)$ is not real and*

$$3|a| > |\sigma_{1,1}(\varepsilon)| = |\sigma_{2,1}(\varepsilon)| > |a|, \tag{2.6.1}$$

$$\forall \omega \in H_{K,d,S}\ \forall i = 3, \ldots, n,\ \forall j = 1,2 |\sigma_{i,j}(\omega)| = 1, \tag{2.6.2}$$

where $d = a^2 - 1$.

Proof: We will show $3|a| > |\varepsilon|$. The rest will follow from Lemma 12 of [10].

It is enough to show $2|a| > |(a^2 - 1)^{1/2}|$, which is equivalent to $4|a|^2 > |a^2 - 1|$, and the last inequality clearly holds since $|a| > 1$, by the product formula.

Lemma 2.7 *Let $c, b \in O_K$ and assume $\forall p \in S \operatorname{ord}_p c = 0$. Then*

$$c |_S b \Leftrightarrow c | b.$$

Proof: The fact that $\forall c, b \in O_K c | b \Rightarrow c |_S b$ is obvious.

To prove the converse assume $c|_S b$ and consider b/c. $\forall q \notin S$ $\operatorname{ord}_q b/c \geq 0$. On the other hand, $\forall p \in S$ $\operatorname{ord}_p(b/c) = \operatorname{ord}_p b - \operatorname{ord}_p c = \operatorname{ord}_p b \geq 0$ because b is integral by assumption. Hence b/c is integral.

Lemma 2.8 *Let $a \in O_K$ satisfy the following conditions*:

a. *for all $p \in S$ which are not factors of* 2 $\operatorname{ord}_p(a-1)$ *is an odd positive integer*;
b. *for all $p \in S$ which are factors of* 2 $\operatorname{ord}_p(a-1)$ *is equal to the ramification degree of p plus an odd number*;
c. *for $i > 2$ $|\sigma_i(a)| < 2^{-12}$ (the product formula will imply that $|a| > 2^{6(n-2)}$)*;
d. *$(a^2-1) = d_1 d_0$, where $\forall p \in S$ $\operatorname{ord}_p d_0 = 0$, and $|d_1| < 2^{-n}(|a|-1)$, $|\sigma_i(d_1)| \leq 1$.*

Set $d = a^2 - 1$. Then as a group under multiplication, $H_{K,d,S}$ is generated by $\varepsilon(a)$ modulo the roots of unity of M.

Proof: First of all we want to show that for all $p \in S$ $\operatorname{ord}_p(a^2-1)$ is odd. It is obviously true for all p which are not factors of 2. Next let $p^{e(p/2)} | 2$, $p^{e(p/2)+1} \nmid 2$. Then by construction, $\operatorname{ord}_p(a-1) = e(p/2)$ + positive odd number,

$$\operatorname{ord}_p(a+1) = \operatorname{ord}_p(a-1+2) = \min(\operatorname{ord}_p(a-1), \operatorname{ord}_p 2) = e(p/2).$$

Therefore,

$$\operatorname{ord}_p(a^2-1) = 2e(p/2) + \text{posit. odd number} = \text{a positive odd integer}.$$

Hence by Lemma 2.5, $H_{K,d,S}$ contains only integral units ω of M such that $N_{M/K}(\omega) = 1$. Since the difference between the ranks of the integral unit groups of K and M is 1, by Dirichlet Unit Theorem (see O'Meara [7], p. 77), the rank of $H_{K,d,S}$ under multiplication is at most one. On the other hand $\varepsilon(a) \in H_{K,d,S}$, so the rank is at least one and consequently is one.

Next it is easy to see that rank one implies that the group is generated by a single element modulo the group of roots of unity of M. We have to show that this element is $\varepsilon(a)$. Assume

$$a - (a^2-1)^{1/2} = \rho \varepsilon_0^e, \tag{2.8.1}$$

where ρ is a root of unity, $\varepsilon_0 \in H_{K,d,S}$, and therefore is integral. Next let

$$\varepsilon_0 = x_0 - (a^2-1)^{1/2} y_0.$$

By Lemma 2.5, $d_1 y_0^2, x_0$ are integral, and, therefore,

$$d_0 = [(a^2-1)/d_1] \mid (x_0^2 - 1),$$

$$N_{K/\mathbb{Q}}((a^2-1)/d_1) \mid N_{K/\mathbb{Q}}(x_0^2 - 1),$$

$$|N_{K/\mathbb{Q}}((a^2-1)/d_1)| \leq |N_{K/\mathbb{Q}}(x_0^2-1)|.$$

On one hand,

$$\begin{aligned} |N_{K/\mathbb{Q}}((a^2-1)/d_1)| &= \prod_{i=1}^{n} |(\sigma_i(a)^2 - 1)/\sigma_i(d_1)| \\ &\geq (|a^2-1|/|d_1|)^2 \prod (1 - |\sigma_i(a)|^2) \\ &\geq (\tfrac{1}{2})^{n-2}(|a^2-1|/|d_1|)^2. \end{aligned} \tag{2.8.2}$$

On the other hand,

$$(2.8.3) \qquad |N_{K/\mathbb{Q}}(x_0^2 - 1)| = \left| \prod_{i=1}^{n} \left(\frac{1}{4} (\sigma_{i1}(\varepsilon_0)^2 + \sigma_{i1}(\varepsilon_0)^{-2}) - \frac{1}{2} \right) \right| \leq |\varepsilon_0^4|.$$

Therefore, by combining (2.8.2) and (2.8.3) and applying Lemma 2.6, we obtain

$$(2.8.4) \qquad (\tfrac{1}{2})^{n-2}(|a^2 - 1|/|d_1|)^2 \leq |\varepsilon_0^4|,$$

$$(2.8.5) \qquad (|a^2 - 1|/|d_1|)^{2e} \leq 2^{(n-2)e}|\varepsilon|^4 \leq 3 \cdot 2^{(n-2)e}|a|^4,$$

and assuming $e \geq 2$, we further derive

$$(2.8.6) \qquad (|a^2 - 1|/|d_1|) \leq 2^n |a|$$

$$(2.8.7) \qquad 2^{-n}(|a| - 1) \leq |d_1|.$$

This contradicts the assumption on d_1, so $e = 1$.

Lemma 2.9 *Let q be a prime of K such that for any root unity ξ of degree $2n$ or less over $\mathbb{Q}$, no prime lying above q in $K(\xi)$ divides $\xi^2 \pm 1$. Then if $\operatorname{ord}_q(a - 1)$ is odd, M contains no roots of unity except $\{\pm 1\}$.*

Proof: K contains no complex roots of unity, since it has real embeddings. Therefore, if ξ is a root of unity which belongs to M, $N_{M/K}(\xi) = \pm 1$, that is $\sigma_{1,2}(\xi) = \pm\xi^{-1}$. Therefore, $(\xi \pm \xi^{-1})^2 = (\xi^{-1}(\xi^2 \pm 1))^2 \in K$, and, hence, $a^2 - 1 = c^2((\xi^{-1}(\xi^2 \pm 1))^2)$. Therefore, $\operatorname{ord}_q(\xi^{-1}(\xi^2 \pm 1))^2$ is odd, but by assumption we must have $\operatorname{ord}_q(\xi^{-1}(\xi^2 \pm 1))^2 = 0$. Consequently, M contains no complex roots of unity.

Notation From now on we will assume that a satisfies the conditions of Lemma 2.8 and Lemma 2.9, and we will let $(a - (a^2 - 1)^{1/2})^m = x_m(a) - (a^2 - 1)^{1/2} y_m(a)$, where $x_m(a), y_m(a) \in O_{K,S}$. If the value of a is clear from the context of the discussion we will sometimes substitute x_m, y_m for $x_m(a)$ and $y_m(a)$ respectively.

Lemma 2.10 *The following statements are true in O_K (the ring of algebraic integers of K) for $j, m, k \geq 0$:*

$$(2.10.1) \qquad y_m(a) \cong m \bmod a - 1; \; x_m(a) \cong 1 \bmod a - 1;$$

$$(2.10.2) \qquad \text{if } a \cong b \bmod c \text{ then} \begin{cases} x_m(a) \cong x_m(b) \bmod c, \\ y_m(a) \cong y_m(b) \bmod c; \end{cases}$$

$$(2.10.3) \qquad x_{2m \pm j} \cong -x_j \bmod x_m.$$

Proof: See Lemma 1 of [5].

Lemma 2.11 *Let a satisfy conditions of Lemmata 2.8 and 2.9. Furthermore, assume that the prime q described in Lemma 2.9 is not in S. Then $x^2 - (a^2 - 1)y^2 = 1$ and $x \cong_s 1 \bmod a - 1$ implies $\exists m \in \mathbb{Z}$ such that $x = x_m(a)$, $y = y_m(a)$.*

Proof: We have two alternatives: $x - (a^2 - 1)^{1/2}y = (a - (a^2 - 1)^{1/2})^m$ or $x - (a^2 - 1)^{1/2}y = -(a - (a^2 - 1)^{1/2})^m$. The second alternative is excluded by the equivalence.

Lemma 2.12 *Suppose $k, j \in \mathbb{N}$, $m \in \mathbb{N}$, $m > 0$, and $\forall i = 2, \ldots, n \, |\sigma_i(x_m(a))| \geq \frac{1}{2}$. Then $x_k(a) \cong \pm x_j(a) \bmod x_m(a)$ implies $k \cong \pm j \bmod m$.*

Proof: See Lemma 15 of [10].

Lemma 2.13 *Suppose* $|\sigma_i(x_j(a))| > \frac{1}{2}$ then
(i) *if* $x_j(a) \,|\, y_m(a)$ *then* $m = 2kj$, $k \in \mathbb{N}$;
(ii) *if* $x_j^2(a) \,|\, y_m(a)$ *then* $jx_j(a) \,|\, m$ *in* O_K.

Proof: (i) Let $m = zj + r$, where $0 \leq r < j$. Then, by Lemma 2.3, $y_m = x_{zj}y_r + y_{zj}x_r$. By the same lemma, $z \cong 0 \bmod 2$ implies $x_j \,|\, x_{zj}$, and $z \cong 1 \bmod 2$ implies $x_j \,|\, y_{zj}$. Therefore, either $x_j \,|\, x_r$ or $x_j \,|\, y_r$. We will show that this is impossible for $j > r > 0$.

The divisibility conditions above imply that either $N_{K/\mathbb{Q}}(x_j) \,|\, N_{K/\mathbb{Q}}(x_r)$ or $N_{K/\mathbb{Q}}(x_j) \,|\, N_{K/\mathbb{Q}}(y_r)$, and unless $N_{K/\mathbb{Q}}(x_r) = 0$ or $N_{K/\mathbb{Q}}(y_r) = 0$, $|N_{K/\mathbb{Q}}(x_j)| \leq |N_{K/\mathbb{Q}}(x_r)|$ or $|N_{K/\mathbb{Q}}(x_j)| \leq |N_{K/\mathbb{Q}}(y_r)|$. The last two inequalities imply

$$\prod_{i=1}^{n} |\sigma_i(x_j)| \leq \prod_{i=1}^{n} |\sigma_i(x_r)| \tag{2.13.1}$$

OR

$$\prod_{i=1}^{n} |\sigma_i(x_j)| \leq \prod_{i=1}^{n} |\sigma_i(y_r)|. \tag{2.13.2}$$

On the other hand, for $i > 2$, $|\sigma_i(x_j)| \geq \frac{1}{2}$, by assumption, and $|\sigma_i(\varepsilon_r)| = 1$, by Lemma 2.6. Hence from (2.13.1) and (2.13.2) we derive

$$(\tfrac{1}{2})^{n-2}|x_j^2| \leq |x_r^2|, \tag{2.13.3}$$

OR

$$(\tfrac{1}{2})^{n-2}|x_j^2| \leq 2^{n-2}|y_r^2|, \tag{2.13.4}$$

$$|\varepsilon^j + \varepsilon^{-j}| \leq 2^{2(n-2)}|(\varepsilon^r \pm \varepsilon^{-r})|; \tag{2.13.5}$$

$$|\varepsilon|^j \leq 2^{2(n-1)}|\varepsilon|^r; \tag{2.13.6}$$

$$|a| < |\varepsilon| \leq 2^{2(n-1)}. \tag{2.13.7}$$

This is impossible, by our assumptions on a. Therefore $N_{K/\mathbb{Q}}(x_r) = 0$ or $N_{K/\mathbb{Q}}(y_r) = 0$. Hence $r = 0$.

(ii) $x_j^2 \,|\, y_m$ implies $\exists q \in \mathbb{N}$ such that $m = 2qj$. By the Binomial theorem,

$$y_m = \sum_{k \cong 1 \bmod 2} \binom{2q}{k} x_j^k y_j^{2q-k}(a^2 - 1)^{q-((k-1)/2)}; \tag{2.13.8}$$

$$y_m \cong 2qy_j^{2q-1}x_j(a^2 - 1)^q \bmod(x_j^2); \tag{2.13.9}$$

since $(x_j, y_j(a^2 - 1)) = 1$, $x_j \,|\, 2q$, and consequently $jx_j \,|\, m$.

Lemma 2.14
(a) *If for all* $i = 3, \ldots, k$ $\sigma_i(x_k(a)) \geq \frac{1}{2}$ *then*
  (i) $\forall i = 3, \ldots, k$ $|\sigma_i(y_k(a))| < 1$,
  (ii) $|N_{K/\mathbb{Q}}(x_k(a))| \geq |N_{K/\mathbb{Q}}(y_k(a))|$;
(b) $k < |x_k(a)|$.

Proof: (a) is similar to the proof of Lemma 2.4. For (b) see the proof of Lemma 21 of [10].

3 A bound equation In this section K is any number field of degree n over $\mathbb{Q}$, and $\sigma_1, \ldots, \sigma_n$ are all the embeddings of K into $\mathbb{C}$.

Lemma 3.1 *Let $x, z \neq 0$ be algebraic integers, let $N \neq 0$, $N \in \mathbb{Z}$, let $s_1, \ldots, s_n$ be rational integers such that for $i \neq j$, $s_i \neq s_j$. Assume also that the following divisibility conditions are true in O_K.*

$$(x + s_i N) \mid Nz, \; i = 1, \ldots, n. \tag{3.1.1}$$

Then $\forall i = 1, \ldots, n$

$$\left|\sigma_i\left(\frac{x}{N}\right)\right| < C(s_1, \ldots, s_n) \cdot |N_{K/\mathbb{Q}}(z)|,$$

where $C(s_1, \ldots, s_n)$ is a natural number depending only on $s_1, \ldots, s_n$.

Proof: From 3.1.1 we obtain

$$N_{K/\mathbb{Q}}(x + s_i N) \mid N_{K/\mathbb{Q}}(Nz). \tag{3.1.2}$$

Let $f(T) = T^n + a_{n-1}T^{n-1} + \ldots$ be the characteristic polynomial of x over $\mathbb{Q}$. Then $N_{K/\mathbb{Q}}(x + s_i N) = f(-s_i N)$. Therefore, from (3.1.2) we can obtain the following linear system:

$$\begin{pmatrix} 1 & -s_1 N & (s_1 N)^2 & \cdots & (-s_1 N)^{n-1} \\ 1 & -s_2 N & (s_2 N)^2 & \cdots & (-s_2 N)^{n-1} \\ \cdots & & & & \\ 1 & -s_n N & (s_n N)^2 & & (-s_n N)^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \\ a_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} c_1 & N_{K/\mathbb{Q}}(Nz) - (-s_1 N)^n \\ c_2 & N_{K/\mathbb{Q}}(Nz) - (-s_2 N)^n \\ & \cdots \\ c_{n-1} & N_{K/\mathbb{Q}}(Nz) - (-s_n N)^n \end{pmatrix},$$

where $|c_1|, \ldots, |c_n| \leq 1$. Our plan is to solve for the polynomial coefficients using Cramer's rule. Therefore we will start by estimating the determinant of the system which is a nonzero Van-Der-Monde determinant and is actually equal to

$$\det \begin{pmatrix} 1 & -s_1 N & (s_1 N)^2 & \cdots & (-s_1 N)^{n-1} \\ 1 & -s_2 N & (s_2 N)^2 & \cdots & (-s_2 N)^{n-1} \\ \cdots & & & & \\ 1 & -s_n N & (s_n N)^2 & \cdots & (-s_n N)^{n-1} \end{pmatrix}$$

$$= N^{1+2+\ldots+n-1} \det \begin{pmatrix} 1 & -s_1 & (s_1)^2 & \cdots & (-s_1)^{n-1} \\ 1 & -s_2 & (s_2)^2 & \cdots & (-s_2)^{n-1} \\ \cdots & & & & \\ 1 & -s_n & (s_n)^2 & \cdots & (-s_n)^{n-1} \end{pmatrix}$$

$$= N^{n(n-1)/2} \det(s_1, \ldots, s_n),$$

where $\det(s_1, \ldots, s_n)$ is the determinant of the above matrix and depends only on $\{s_i\}$. Next we will evaluate the determinants corresponding to the unknowns.

$$|a_r N^{n(n-1)/2} \det(s_1, \ldots, s_n)|$$

$$= \left| \det \begin{pmatrix} 1 & -Ns_1 & (Ns_1)^2 & \cdots & c_1 N_{K/\mathbb{Q}}(Nz) - (-Ns_1)^n & \cdots & (-Ns_1)^{n-1} \\ 1 & -Ns_2 & (Ns_2)^2 & \cdots & c_2 N_{K/\mathbb{Q}}(Nz) - (-Ns_2)^n & \cdots & (-Ns_2)^{n-1} \\ \cdots & & & & & & \\ 1 & -Ns_n & (Ns_n)^2 & \cdots & c_n N_{K/\mathbb{Q}}(Nz) - (-Ns_n)^n & \cdots & (-Ns_n)^{n-1} \end{pmatrix} \right| \quad \downarrow r\text{th column}$$

$$\leq \left| \det \begin{pmatrix} 1 & -Ns_1 & (Ns_1)^2 & \cdots & c_1 N_{K/\mathbb{Q}}(Nz) & \cdots & (-Ns_1)^{n-1} \\ 1 & -Ns_2 & (Ns_2)^2 & \cdots & c_2 N_{K/\mathbb{Q}}(Nz) & \cdots & (-Ns_2)^{n-1} \\ \cdots & & & & & & \\ 1 & -Ns_n & (Ns_n)^2 & \cdots & c_n N_{K/\mathbb{Q}}(Nz) & \cdots & (-Ns_n)^{n-1} \end{pmatrix} \right| \quad \downarrow r\text{th column}$$

$$+ \left| \det \begin{pmatrix} 1 & -Ns_1 & (Ns_1)^2 & \cdots & (-Ns_1)^n & \cdots & (-Ns_1)^{n-1} \\ 1 & -Ns_2 & (Ns_2)^2 & \cdots & (-Ns_2)^n & \cdots & (-Ns_2)^{n-1} \\ \cdots & & & & & & \\ 1 & -Ns_n & (Ns_n)^2 & \cdots & (-Ns_n)^n & \cdots & (-Ns_n)^{n-1} \end{pmatrix} \right| \quad \downarrow r\text{th column}$$

$$\leq \left| N^{n(n-1)/2-r} N_{K/\mathbb{Q}}(Nz) \det \begin{pmatrix} 1 & -s_1 & (s_1)^2 & \cdots & c_1 & \cdots & (-s_1)^{n-1} \\ 1 & -s_2 & (s_2)^2 & \cdots & c_2 & \cdots & (-s_2)^{n-1} \\ \cdots & & & & & & \\ 1 & -s_n & (s_n)^2 & \cdots & c_n & \cdots & (-s_n)^{n-1} \end{pmatrix} \right| \quad \downarrow r\text{th column}$$

$$+ \left| (N)^{n(n+1)/2-r} \det \begin{pmatrix} 1 & -s_1 & (s_1)^2 & \cdots & (-s_1)^n & \cdots & (-s_1)^{n-1} \\ 1 & -s_2 & (s_2)^2 & \cdots & (-s_2)^n & \cdots & (-s_2)^{n-1} \\ \cdots & & & & & & \\ 1 & -s_n & (s_n)^2 & \cdots & (-s_n)^n & \cdots & (-s_n)^{n-1} \end{pmatrix} \right|$$

$$\leq |N^{n(n+1)/2-r} N_{K/\mathbb{Q}}(z)| \cdot \sum_{i=1}^{n} |C_{ir}| + |N^{n(n+1)/2-r}| \sum_{i=1}^{n} |s_i|^b |C_{ir}|$$

where C_{ir} are cofactors of the matrix

$$\det \begin{pmatrix} 1 & -s_1 & (s_1)^2 & \cdots & (-s_1)^{n-1} \\ 1 & -s_2 & (s_2)^2 & \cdots & (-s_2)^{n-1} \\ \cdots & & & & \\ 1 & -s_n & (s_n)^2 & \cdots & (-s_n)^{n-1} \end{pmatrix}.$$

Let $C_1(s_1, \ldots, s_n) = n \cdot \max_{i,r}(|s_i|^n |C_{ir}|)$, then

$$\begin{aligned} &|a_r(-N)^{n(n-1)/2} \det(s_1, \ldots, s_n)| \\ &\quad \leq N^{n(n+1)/2-r} C_1(s_1, \ldots, s_n)|(N_{K/\mathbb{Q}}(z) + 1)| \\ &\quad \leq 2 \cdot N^{n(n+1)/2-r} C_1(s_1, \ldots, s_n)|N_{K/\mathbb{Q}}(z)|. \end{aligned}$$

Therefore,

$$|a_r| \leq 2C_1(s_1, \ldots, s_n)\det(s_1, \ldots, s_n)^{-1} N^{n-r} |N_{K/\mathbb{Q}}(z)|.$$

We can assume that for some j $|\sigma_j(x/N)| > 1$, otherwise we are done. Then for such a j consider $x^n + a_{n-1}x^{n-1} + \ldots a_0 = 0$, and derive

$$\begin{aligned} |\sigma_j(x)| &\leq \sum_{i=1}^{n} |a_{n-i}/\sigma_j(x^{i-1})| \\ &\leq \sum_{i=1}^{n} |N^i 2C_1(s_1, \ldots, s_n)\det(s_1, \ldots, s_n)^{-1} N_{K/\mathbb{Q}}(z)| / |\sigma(x^{i-1})| \\ &\leq \sum_{i=1}^{n} 2C_1(s_1, \ldots, s_n)\det(s_1, \ldots, s_n)^{-1} |N_{K/\mathbb{Q}}(z)| N. \end{aligned}$$

Let $C(s_1, \ldots, s_n) = [2nC_1(s_1, \ldots, s_n)\det(s_1, \ldots, s_n)^{-1}] + 1$. (Here "[ ]" denotes the integer part of the number.) Then

$$\left|\sigma_j\left(\frac{x}{N}\right)\right| \leq C(s_1, \ldots, s_n)|N_{K/\mathbb{Q}}(z)|.$$

Lemma 3.2 *Let $\omega \in O_{K,S}$, let $h = h(K)$ be the class number of K. Then $\omega^h = \omega_1/\omega_2$, where $\omega_i \in O_K$, $(\omega_1, \omega_2) = 1$ in O_K and ω_2 is divisible by primes of S only.*

Proof: Let $\prod q_i^{a_i}/\prod p_i^{b_i}$ be the divisor of ω, with $a_i, b_i \geq 0$ and no prime appearing simultaneously in the numerator and the denominator with a positive exponent. Then ideals $(\prod q_i^{a_i})^h$ and $(\prod p_i^{b_i})^h$ are principal and relatively prime. Let $\tilde{\omega}_1$ correspond to the first one and ω_2 correspond to the second one. Then $\omega(\tilde{\omega}_2/\tilde{\omega}_1)$ is an integral unit ξ. Let $\omega_1 = \xi\tilde{\omega}_1$, and we are done.

Lemma 3.3 *Let $P \in \mathbb{N}$ be the product of all rational primes below primes of S, let $w \in O_{K,S}$, and let*

$$k = \max_{p \in S}(\mathrm{ord}_p P).$$

Then $(Pw^{2k}+1)^h$ *can be written as* j/t, *where* $j, t \in O_K$, j *is prime to every prime in* S, *and* t *is divisible by primes of* S *only.*

Proof: Let $q \in S$ and let $\operatorname{ord}_q w < 0$. Then $\operatorname{ord}_q P + 2k \operatorname{ord}_q w < 0$. On the other hand, if $\operatorname{ord}_q w \geq 0$ then $\operatorname{ord}_q(Pw^{2k}+1) = 0$. Therefore, the result follows by the previous lemma.

Lemma 3.4 *Suppose* $w \in O_{K,S}$, *is such that* $\forall p \in S$ $\operatorname{ord}_p w \leq 0$. *Assume additionally that the following condition holds in* $O_{K,S}$:

$$w^h \ldots (w^h + (n-1)P) \mid_S z. \tag{3.4.1}$$

Then for all $1 \leq i \leq n |\sigma_i(w^h)| \leq B_1 \cdot |N_{K/\mathbb{Q}}(z)|$, *where* $B_1 = C(0, P, \ldots, (n-1)P)$ *is a constant of the type defined in Lemma* 3.1.

Proof: First of all, by Lemma 3.2, $w^h = j/t$, where $j, t \in O_{K,S}$ and $\forall p \in S$ $\operatorname{ord}_p j = 0$. Next, to examine implications of divisibility condition (3.4.1) we will rewrite $w^h = j/t$ as k/D, where $D = N_{K/\mathbb{Q}}(t) \in \mathbb{Z}$. We can no longer claim that k is not divisible by any prime of S, but if $k = jC$, then $C \mid D$. Next consider $w^h + Pi$, where $i \in \mathbb{Z}$, and P was defined in Lemma 3.3.

$$w^h + Pi = \frac{k + PiD}{D} = \frac{jC + PiD}{D} = \frac{C(j + (D/C)Pi)}{D}. \tag{3.4.2}$$

We want to show that $w^h + Pi \mid_S z$ implies $k + PiD \mid Dz$. Let $y = Dz/(k + PiD)$. We need to prove that $y \in O_K$. Since $w + Pi \mid_S z$, $\forall p \notin S$ $\operatorname{ord}_p(w^h + Pi) \leq \operatorname{ord}_p z$ and $\operatorname{ord}_p(k + PiD) = \operatorname{ord}_p D(w^h + Pi) \leq \operatorname{ord}_p(Dz)$. Consequently, it is enough to show that $\forall p \in S$ $\operatorname{ord}_p y \geq 0$. So let $p \in S$, then $p \mid P$, and $\operatorname{ord}_p(j + (D/C)Pi) = 0$. Therefore, $\operatorname{ord}_p y = \operatorname{ord}_p(Dz) - \operatorname{ord}_p(k + PiD) = \operatorname{ord}_p D + \operatorname{ord}_p z - \operatorname{ord}_p(j + (D/C)Pi) - \operatorname{ord}_p C \geq \operatorname{ord}_p D - \operatorname{ord}_p C \geq 0$.

Hence, we have the following divisibility conditions in O_K:

$$k + PiD \mid Dz,\ i = 0, \ldots, n-1. \tag{3.4.3}$$

Apply Lemma 3.1, with $s_i = Pi$ to conclude that $|\sigma_j(w^h)| \leq C(0, P, \ldots, (n-1)P)|N_{K/\mathbb{Q}}(z)|$.

Lemma 3.5 *Let* P *be defined as in the previous lemmas, and suppose* $z \in O_K$ *and* $w \in O_{K,S}$ *is such that* $\forall$ *prime* $p \mid P$ $\operatorname{ord}_p w \leq 0$. *Assume additionally that the following conditions hold in* $O_{K,S}$:

$$(w^h + P)((P+1)w^h + P) \ldots (((n-1)P + 1)w^h + P) \mid_S z. \tag{3.5.1}$$

Then $\forall i = 1, \ldots, n |\sigma_i(w^h)| \geq B_2^{-1} N_{K/\mathbb{Q}}(z^{-1})$, *where*

$$B_2 = \frac{C(1, \ldots, (n-1)P + 1)}{P},$$

and $C(1, \ldots, (n-1)+1)$ *is the constant of the type defined in Lemma* 3.1.

Proof: As in the previous lemma $w^h = j/t$, where $j, t \in O_{K,S}$ and $\forall p \in S$ $\operatorname{ord}_p j = 0$, t divisible by primes of S only. Let $J = N_{K/\mathbb{Q}}(j)$, and let $C = N_{K/\mathbb{Q}}(j)/j$, and let $T = tC$, so that $w^h = J/T$.

Next we will show that $(iP+1)w^h + P \mid_S z$ implies $(J(iP+1) + TP) \mid Jz$. Indeed, $(iP+1)w^h + P \mid_S z$ implies $\forall p \notin S$ $\operatorname{ord}_p z + \operatorname{ord}_p J \geq \operatorname{ord}_p((iP+1)w^h +$

$P) + \operatorname{ord}_p J = \operatorname{ord}_p [(J(iP+1) + TP)/T] + \operatorname{ord}_p J = \operatorname{ord}_p (J(iP+1) + TP) - \operatorname{ord}_p T + \operatorname{ord}_p J = \operatorname{ord}_p (J(iP+1) + TP) - \operatorname{ord}_p t + \operatorname{ord}_p j \geq \operatorname{ord}_p (J(iP+1) + TP)$, since $\forall p \notin S \operatorname{ord}_p t = 0$.

Next let $p \in S$ and consider $\operatorname{ord}_p (J(iP+1) + TP) = \operatorname{ord}_p C + \operatorname{ord}_p (j(iP + 1) + tP) = \operatorname{ord}_p C \leq \operatorname{ord}_p jC \leq \operatorname{ord}_p Jz$.

Hence, we can apply Lemma 3.1 with $s_i = iP + 1$, $N = J$, and $x = TP$ to conclude

$$\left| \sigma_i \left(\frac{TP}{J} \right) \right| < C(1, \ldots, (n-1)P + 1) |N_{K/\mathbb{Q}}(z)|,$$

or

$$|\sigma_i(w^h)| > (P[C(1, \ldots, (n-1)P + 1) |N_{K/\mathbb{Q}}(z)|]^{-1}).$$

4 A Diophantine definition of $\mathbb{Z}$ for number fields with one pair of complex conjugate embedding

Lemma 4.1 *$\exists a \in O_K$ satisfying all the requirements of Lemma 2.8 and Lemma 2.9.*

Proof: Let q be a prime described in Lemma 2.9 such that $N_{K/\mathbb{Q}}(q)$ has no factors in S and not a factor of 2. Next $\forall p \in S$, $p \nmid 2$ let $b(p)$ be an element of K such that $\operatorname{ord}_p b(p) = 1$. $\forall p \in S$ such that $p \mid 2$ and $\forall p \notin S$, $p \mid 2$, p has a conjugate in S, let $b(p)$ be an element of K such that $\operatorname{ord}_p b(p) = e(p/2)$ (ramification degree of p). Additionally, let $b(q) \in K$ be such that $\operatorname{ord}_q b(q) = 1$. By the "very strong" approximation theorem (see [7], p. 77), $\exists a \in K$ such that

$$|a - 1 - b(p)|_p < |b(p)|_p, \tag{4.1.1}$$

for the above described primes p of K, and

$$|\sigma_i(a)| = |a|_i < 2^{-12},\ i = 3, \ldots, n, \tag{4.1.2}$$

$$|a|_t \leq 1 \text{ for all } t \notin S,\ t \neq q, \tag{4.1.3}$$

$$|a - 1 - b(q)|_q < |b(q)|_q, \tag{4.1.4}$$

where $|\ |_t$ is the valuation generated by a prime t, and $|\ldots|_i$ is an extension of the archimedean valuation of $\mathbb{Q}$ to K.

From (4.1.1) and (4.1.4) we can conclude that $|a - 1|_q = |b(q)| < 1$, $|a - 1|_p = |b(p)|_p < 1$, since otherwise,

$$|a - 1 - b(p)|_p = \max(|a-1|_p, |b(p)|_p) = \begin{cases} 1, & \text{if } |a-1|_p > |b(p)|_p \\ |b(p)|_p, & \text{if } |a-1| < |b(p)|_p \end{cases} \geq |b(p)|_p.$$

Moreover, $|a|_p = |a - 1 + 1|_p \leq \max(|a-1|_p, 1) = 1$. Next note that, by the product formula, (4.1.1)-(4.1.4) imply as before that $|a| > 2^{6(n-2)}$.

Finally, $\forall p \in S \operatorname{ord}_p (a^2 - 1) > 1$ only if $p \mid 2$. In this case $\operatorname{ord}_p (a^2 - 1) = 2e(p/2) + 1$, and $4 \mid a - 1$. Therefore, $|d_1| \leq 4 < 2^{-n}(|a| - 1)$.

Lemma 4.2 *Assume a has been constructed using Lemma* 4.1. *Assume additionally that* $(\forall i > 2)\ \frac{1}{2} \leq |\sigma_i(x_m(a))| \leq C_2(\frac{1}{2}, a) < 1$, *and* $Q, r \in \mathbb{N}$ *satisfy the following conditions*:
(a) $\forall p \in S$, p *not a factor of* 2, $Q \cong 0 \bmod p$ and $Q \cong 0 \bmod q$.
(b) *If* S *contains factors of* 2 *then* $Qr \cong 3 \bmod 4$;
(c) $r > -13 \ln 2/(2Q \ln C_2)$.

Let

$$b = (x_m(a))^{2(Qr)} + a(1 - (x_m(a))^2). \tag{4.2.1}$$

Then b *satisfies all the requirements of Lemmata* 2.8 *and* 2.9, *and*

$$b \cong 1 \bmod y_m(a), \tag{4.2.2}$$

$$b \cong a \bmod x_m(a). \tag{4.2.3}$$

Proof: Let $i > 2$. Then

$$|\sigma_i(b)| \leq |\sigma_i(x_m)|^{2(Qr)} + 2^{-12}(1 - \tfrac{1}{2}) < C_2^{2Qr} + (\tfrac{1}{2})^{13}. \tag{4.2.4}$$

It is enough to arrange for $C_2^{2Qr} < (\frac{1}{2})^{13}$, i.e., $r > (-13 \ln 2/2Q \ln C_2)$ to ensure that $|\sigma_i(b)| < (\frac{1}{2})^{12}$. Since, b is an algebraic integer, the product formula will ensure for b, as in the previous lemma for a, that

$$|\sigma_1(b)| > 2^{6(n-2)} \tag{4.2.5}$$

holds. Next consider

$$\begin{aligned} b - 1 &= x_m^{2(Qr)} + a(1 - x_m^2) - 1 \\ &= (x_m^2 - 1)\left(\sum_{i=1}^{Qr} (x_m^2)^{Qr-i} - a\right) \\ &= (a - 1)(a + 1)y_m^2\left(\left(\sum_{i=1}^{Qr} (x_m^2)^{Qr-i}\right) - a\right). \end{aligned} \tag{4.2.6}$$

First, we shall show that $\forall p \in S$ such that p is not a factor of 2, $\operatorname{ord}_p[(\sum_{i=1}^{Qr} (x_m^2)^{Qr-i} - a)] = 0$. Since $x_m^2 \cong 1 \bmod (a - 1)$, for all $p_i \in S$ which are not factors of 2

$$\left(\sum_{i=1}^{Qr} (x_m^2)^{Qr-i} - a\right) \cong Qr - 1 \bmod (a - 1) \cong -1 \bmod p_i. \tag{4.2.7}$$

Therefore, for such a p

$$\operatorname{ord}_p(b^2 - 1) = \operatorname{ord}_p(b - 1) = \operatorname{ord}_p(a - 1) + 2 \operatorname{ord}_p y_m = 1 + 2 \operatorname{ord}_p y_m.$$

On the other hand, let $p \mid 2$ and assume either $p \in S$ or $N_{K/\mathbb{Q}}(p)$ has a factor in S. As has been noted in the previous lemma, this implies that $4 \mid a - 1$, and therefore, $(\sum_{i=1}^{Qr} (x_m^2)^{Qr-i} - a) \cong Qr - 1 \cong 2 \bmod 4$. Hence,

$$\operatorname{ord}_p\left(\sum_{i=1}^{Qr} (x_m^2)^{Qr-i} - a\right) = \operatorname{ord}_p\left(\left(\sum_{i=1}^{Qr} (x_m^2)^{Qr-i} - a\right) - 2\right) + 2 = \operatorname{ord}_p 2.$$

$$(4.2.8)\quad \operatorname{ord}_p b - 1 = \operatorname{ord}_p(a^2-1) + 2\operatorname{ord}_p y_m + \operatorname{ord}_p\left(\sum_{i=1}^{Qr}(x_m^2)^{Qr-i} - a\right)$$

$$= 2e(p/2) + 1 + 2\operatorname{ord}_p y_m + e(p/2)$$

$$= 3e(p/2) + 1 + 2\operatorname{ord}_p y_m.$$

$$(4.2.9)\quad \operatorname{ord}_p(b^2-1) = 3e(p/2) + 1 + 2\operatorname{ord}_p y_m + e(p/2)$$

$$= 4e(p/2) + 1 + 2\operatorname{ord}_p y_m.$$

Therefore, $\forall p \in S$, p not a factor of 2, $\operatorname{ord}_p(b^2-1)/y_m^2) = 1$ and if S contains factors of 2, then $b^2 - 1$ is divisible by 16 and $\forall p \in S$, $p|2$, $\operatorname{ord}_p(b^2-1)/(16y_m^2) = 1$. Hence, $|d_1| \leq 16y_m^2 \leq 2^{-n}(|b|-1)|$.

Finally by an argument similar to an argument above, $\operatorname{ord}_q(b-1)$ is a positive odd number.

Lemma 4.3
(a) *If* $\sigma(K) \subset \mathbb{R}$ *then the set* $\{x \in O_{K,S} | \sigma(x) \geq 0\}$ *is Diophantine over* $O_{K,S}$.
(b) *The set* $\{x \in O_{K,S} | x \neq 0\}$ *is Diophantine over* $O_{K,S}$.

Proof: (a) follows with slight modification from Lemma 10 of [5]. (b) follows from section 11 of [2].

Lemma 4.4 (Diophantine definition of O_K over $O_{K,S}$) *Let a be the element constructed in Lemma* 4.1, *with* $d = a^2 - 1$. *Let* $0 < \frac{1}{2} < C_2(\frac{1}{2}, a) < 1$, *let Q be as in Lemma* 4.2, *let P, h, k be as in Lemmata* 3.2 *and* 3.3, *and let* $r > -13 \ln 2/(2Q \ln C_2)$. *Then the following system of equations will have solutions in* $O_{K,S}$ *only if w is integral, and if w is a rational integer these equations can be satisfied in* $O_{K,S}$. (*All the divisibility conditions are over* $O_{K,S}$.)

$$(4.4.1)\quad \xi = (1 + Pw^{2k})^h;$$
$$(4.4.2)\quad x^2 - dy^2 = 1,\ x \cong_S 1 \bmod (a-1);$$
$$(4.4.3)\quad w^2 - dz^2 = 1,\ w \cong_S 1 \bmod (a-1)$$
$$(4.4.4)\quad (\forall i > 2)|\sigma_i(w)| \geq \tfrac{1}{2};$$
$$(4.4.5)\quad u^2 - dv^2 = 1,\ v \neq 0,\ u \cong_S 1 \bmod (a-1);$$
$$(4.4.6)\quad (\forall i > 2)\tfrac{1}{2} \leq |\sigma_i(u)| \leq C_2;$$
$$(4.4.7)\quad b = u^{2(Qr)} + a(1-u^2);$$
$$(4.4.8)\quad f^2 - (b^2-1)t^2 = 1, f \cong_S 1 \bmod b - 1;$$
$$(4.4.9)\quad f \cong_S x \bmod u;$$
$$(4.4.10)\quad w^2 |_S v;$$
$$(4.4.11)\quad t \cong_S \xi \bmod w;$$
$$(4.4.12)\quad R_1 = (P^3 B_1 B_2)^n + 1,$$
$$R_2 = x^{n^2}(x^{n^2} + P)\ldots(x^{n^2} + nP),$$
$$R_3 = \xi^{n^2}(\xi^{n^2} + P)\ldots(\xi^{n^2} + (n-1)P),$$
$$R_1 R_2 R_3 |_S z;$$
$$(4.4.13)\quad (\xi^{n^3} + P)((P+1)\xi^{n^3} + P)\ldots(((n-1)P+1)\xi^{n^3} + P)|_S z.$$

Proof: First suppose (4.4.1)–(4.4.13) are satisfied. From (4.4.1) we can conclude by Lemma 3.2 that $\xi = U/V$, where $U, V \in O_K$, U has no divisors in S, V divisible by primes of S only.

Next we note that by Lemmata 2.11 and 4.1, $\exists e, h, m, j \in \mathbf{N}$ such that

(4.4.14) $x = x_e(a), y = y_e(a);$
(4.4.15) $w = x_h(a), z = y_h(a);$
(4.4.16) $(\forall i > 2)|\sigma_i(x_h)| \geq \frac{1}{2};$
(4.4.17) $u = x_m(a), v = y_m(a), y_m(a) \neq 0;$
(4.4.18) $(\forall i > 2)\frac{1}{2} \leq |\sigma_i(x_m(a))| < C_2.$

Next, by Lemmata 2.11 and 4.2

(4.4.19) $f = x_j(b), t = y_j(b).$

Moreover, we have the following divisibility condition:

(4.4.20) $x_h^2(a) \mid_S y_m(a).$

To begin with, this divisibility condition, as indicated, holds in $O_{K,S}$, but then we note that $\forall p \in S(x_h(a), p) = 1$ since $p \mid a - 1$ and therefore, by Lemma 2.7, the division can actually take place in O_K. Hence, by Lemma 2.13, we can conclude that

(4.4.21) $x_h(a) \mid m$ in O_K.

Also, by Lemma 4.2, we have

(4.4.22) $b \cong 1 \bmod y_m(a),$
(4.4.23) $b \cong a \bmod x_m(a),$

where all these relations take place in O_K. From (4.4.20) and (4.4.22) we derive

(4.4.24) $b \cong 1 \bmod x_h(a).$

Additionally, from (4.4.9) we get

(4.4.25) $x_j(b) \cong_S x_e(a) \bmod x_m(a),$

and again by the same argument as above,

(4.4.26) $x_j(b) \cong x_e(a) \bmod x_m(a).$

From (4.4.11) we get

(4.4.27) $y_j(b) \cong_S \xi \bmod x_h(a).$

Next we derive the following equivalencies:

(4.4.28) $y_j(b) \cong j \bmod (b - 1)$ in O_K, by Lemma 2.10.
(4.4.29) $x_j(a) \cong x_j(b) \bmod x_m(a)$, by Lemma 2.10.
(4.4.30) $x_j(a) \cong x_e(a) \bmod x_m(a)$, by (4.4.26) and (4.4.29).
(4.4.31) $e \cong \pm j \bmod m$, by Lemma 2.12.

On the other hand, from the fact that $x_h(a) \mid b - 1$ in O_K, and (4.4.27) and (4.4.28) we obtain

(4.4.32) $\xi \cong_S \pm j \bmod x_h(a).$

Since, $x_h \mid m$ form (4.4.21), and given (4.4.31), we obtain

(4.4.33) $\xi \cong_S \pm e \bmod x_h(a).$

Next (4.4.33) can be rewritten as

$$U \equiv \pm Ve \bmod x_h(a). \tag{4.4.34}$$

Unless $U = \pm Ve$,

$$|N_{K/\mathbb{Q}}(U \pm Ve)| \geq |N_{K/\mathbb{Q}}(x_h(a))|, \tag{4.4.35}$$

$$\prod_{i=1}^{n} |\sigma_i(\xi) \pm e||\sigma_i(V)| \geq |N_{K/\mathbb{Q}}(x_h(a))|, \tag{4.4.36}$$

$$|N_{K/\mathbb{Q}}(V)| \prod_{i=1}^{n} |\sigma_i(\xi) \pm e| \geq |N_{K/\mathbb{Q}}(x_h(a))|. \tag{4.4.37}$$

From (4.4.13) and Lemma 3.5 we obtain

$$|\sigma_i(\xi^{n^3})| \geq |B_2 N_{K/\mathbb{Q}}(y_h(a))|^{-1}$$

so that

$$N_{K/\mathbb{Q}}(\xi^{n^3}) \geq |B_2 N_{K/\mathbb{Q}}(y_h(a))|^{-n}$$

and

$$|N_{K/\mathbb{Q}}(V^{n^2})| \leq |N_{K/\mathbb{Q}}(U^{n^2}) B_2 N_{K/\mathbb{Q}}(y_h(a))|. \tag{4.4.38}$$

On the other hand, since U is not divisible by any prime from S, some of the consequences of (4.4.12) are

$$U^{n^2} | y_h(a),$$

$$N_{K/\mathbb{Q}}(U^{n^2}) | N_{K/\mathbb{Q}}(y_h(a)),$$

and, finally,

$$|N_{K/\mathbb{Q}}(U^{n^2})| \leq |N_{K/\mathbb{Q}}(y_h(a))|,$$

since $y_h(a) \neq 0$, and therefore, from (4.4.38) we obtain

$$|N_{K/\mathbb{Q}}(V^{n^2})| \leq |B_2 N_{K/\mathbb{Q}}(y_h(a))^2|. \tag{4.4.39}$$

Since $((P^3 B_1 B_2)^n + 1, P) = 1$, $[y_h(a)/[(P^3 B_1 B_2)^n + 1]] \in O_K$, and therefore from (4.4.12) and Lemma 3.4, we obtain

$$\forall i = 1, \ldots, n, |\sigma_i(\xi)|^{n^2} < \left| B_1 N_{K/\mathbb{Q}}\left(\frac{y_h(a)}{(P^3 B_1 B_2)^n + 1} \right) \right|.$$

Similarly,

$$\forall i = 1, \ldots, n, |\sigma_i(x_e(a))|^{n^2} \leq \left| B_1 N_{K/\mathbb{Q}}\left(\frac{y_h(a)}{(P^3 B_1 B_2)^n + 1} \right) \right|.$$

Therefore,

$$\begin{aligned} |N_{K/\mathbb{Q}}(V)\| N_{K/\mathbb{Q}}(\xi \pm e)| &\leq \tfrac{1}{4} |N_{K/\mathbb{Q}}(y_h(a))^{2/n^2} N_{K/\mathbb{Q}}(y_h(a))^{1/n}| \\ &< |N_{K/\mathbb{Q}}(y_h(a))| < |N_{K/\mathbb{Q}}(x_h(a))|, \end{aligned}$$

and, hence, $\xi = \pm e$ and Pw^{2k} is integral. Next recall that $\forall p \in S$ ($\operatorname{ord}_p w < 0 \Rightarrow \operatorname{ord}_p Pw^{2k} < 0$). Hence, w is integral.

Next assume w, and consequently, ξ is an integer. Then let $(x, y) = (x_\xi, y_\xi)$, let h_0 be such that (4.4.12) and (4.4.13) are satisfied by $z = y_{h_0}$, and note that by Lemma 2.4, $\exists h \in \mathbb{Z}$, a multiple of h_0, such that $(\forall i > 2)\frac{1}{2} < |\sigma_i(x_h)| < C_2(\frac{1}{2}, a)$. Since $h_0 | h$ implies $y_{h_0} | y_h$ (4.4.12) and (4.4.13) are satisfied with $z = y_h(a)$.

Next, let $0 \neq m_0 \in \mathbb{N}$ be such that $2hx_h | m_0$, and using Lemma 2.4 again we can find m, a multiple of m_0 such that for $i > 2$ $|\sigma_i(x_m)| > \frac{1}{2}$. Let $u = x_m(a)$, $v = y_m(a)$, and by Lemma 2.3 we will have $x_h^2(a) | y_m(a)$. Define b using 4.4.7, and let $(f, t) = (x_\xi(b), y_\xi(b))$. Then $t \cong \xi \bmod (b-1)$ implies $t \cong \xi \bmod y_m(a)$, which in turn implies $t \cong \xi \bmod x_h$. So all the remaining equations will be satisfied.

To complete this Diophantine definition of O_K over $O_{K,S}$ let $w_1, \ldots, w_n$ be an integral basis of O_K over $\mathbb{Q}$. Then start with an equation $X = \sum_{i=1}^n a_i w_i$, and adjoin (4.4.1)–(4.4.12) for every a_i.

Corollary 4.5 *$\mathbb{Z}$ has a Diophantine definition over $O_{K,S}$.*

Proof: From [10] or [8] we know that for K with one pair of complex conjugate embeddings $\mathbb{Z}$ has a Diophantine definition over O_K. This fact together with the preceding lemma produces the desired result.

Lemma 4.6 *Let $K \subset M \subset L$ be number fields, S, W, V finite sets of finite primes of K, M, and L respectively, such that $O_{M,W}$ and $O_{L,V}$ are integral closures of $O_{K,S}$ in M and L respectively. Then*

$$\text{Dioph}(O_{L,V}/O_{K,S}) \Leftrightarrow (\text{Dioph}(O_{L,V}/O_{M,W}) \text{ and } \text{Dioph}(O_{M,W}/O_{K,S})).$$

Proof: The proof of the lemma can be obtained by a slight modification of the corresponding proof in [9].

Remark 4.7 Lemma 4.6 implies that in a totally real field K, $\mathbb{Z}$ has a Diophantine definition over a ring $O_{K,S}$. This follows from the fact that any totally real field has an extension of degree 2 which will have exactly two complex conjugate embeddings: select $d \in K$, such that $\sigma_1(d) < 0$, and for $i \geq 2$ $\sigma_i(d) > 0$, and $K(d^{1/2})$ will have the desired properties. (Existence of such a d follows from the Approximation Theorem.)

5 A Diophantine definition of $\mathbb{Z}$ for extensions of degree two of totally real number fields In this section we will show that the arguments used by Denef and Lipschitz in [4] to construct a Diophantine definition over the rings of algebraic integers of K can be extended to accommodate the rings $O_{K,S}$. (In this section we will also treat the case of a complex extension of degree 2 over $\mathbb{Q}$.)

Lemma 5.1 *Let K be a number field of degree $n \geq 1$ over $\mathbb{Q}$, S a finite set of its finite primes, L a Galois extension of degree m of K, and W the set of all primes of L lying above primes of S. Let $\xi \in O_{L,W}$ be such that $\forall p \in W$ $\text{ord}_p \xi \leq 0$, let $w \in O_{K,S}$, and let $z \in O_K$ be such that $\forall p \in S$ $\text{ord}_p z = 0$, and*

$$(5.1.1) \quad w \cong_W \xi \bmod z,$$

$$(5.1.2) \quad (\xi^{m^4n^4} + P)((P+1)\xi^{m^4n^4} + P) \ldots (((n-1)P+1)\xi^{m^4n^4} + P) \,|_W T,$$

$$(5.1.3) \quad R_1 = (P^3 B_1 B_2)^{(mn)^3} + 1$$
$$R_2 = \xi^{m^3n^3}((\xi^{m^3n^3} + P) \ldots (\xi^{m^3n^3} + (mn-1)P),$$
$$R_1 R_2 \,|_W T,$$

where P is the product of all the rational primes lying below primes of S, and $|N_{L/\mathbb{Q}}(T)| \leq |N_{L/\mathbb{Q}}(z)|$. Assume additionally that $h = h(L)$ (see Lemma 3.2), $\xi = \omega^h$, $\omega \in O_{L,W}$. Then $\xi \in O_{K,S}$.

Proof: The proof of this lemma will be a modification of Lemma 1 proof on p. 386 of [4]. From (5.1.1), as in the above-mentioned lemma, one can obtain

$$\tau(\xi) \cong_W \xi \bmod z, \tag{5.1.4}$$

$\forall \tau \in \mathrm{Gal}(L/K)$. By Lemma 3.2, $\xi = j/t$, where $j, t \in O_{M,W}$, t is divisible by primes of W only, j is not divisible by any prime of W. Since z has no zeros at any valuation of S, (5.1.4) is actually equivalent to $z|(\tau(t)j - t\tau(j))$ and, assuming $\tau(\xi) \neq \xi$,

$$N_{L/\mathbb{Q}}(z) | N_{L/\mathbb{Q}}(\tau(t)j - t\tau(j)) \tag{5.1.5}$$

implying

$$\begin{aligned} |N_{L/\mathbb{Q}}(z)| &\leq \prod_{i=1}^{mn} |\sigma_i(\tau(t)j - t\tau(j)| \\ &= \prod_{i=1}^{mn} |\sigma_i(\xi) - \sigma_i(\tau(\xi))|\,|\sigma_i(\tau(t))\sigma_i(t)| \\ &= \prod_{i=1}^{mn} |\sigma_i(\xi) - \sigma_{k(i)}(\xi)|\,|N_{L/\mathbb{Q}}(t)|^2, \end{aligned} \tag{5.1.6}$$

since $\sigma_i \circ \tau = \sigma_{k(i)}$ is another embedding of L into $\mathbb{C}$, and as σ_i ranges through all the embeddings of L into $\mathbb{C}$, $\sigma_i \circ \tau = \sigma_{k(i)}$ ranges through all such embeddings also. Moreover, by Lemmata 3.4 and 3.5, from (5.1.2) and (5.1.3) we can derive $\forall \sigma$ – an embedding of L into $\mathbb{C}$

$$(B_2|N_{L/\mathbb{Q}}(T)|)^{-(mn)^{-4}} < |\sigma(\xi)| < B_1 \frac{|N_{L/\mathbb{Q}}(T)|^{(mn)^{-3}}}{((P^3 B_1 B_2)^{(mn)^3} + 1)^{(mn)^{-2}}}, \tag{5.1.7}$$

and using the same argument as in Lemma 4.4 obtain

$$|N_{L/\mathbb{Q}}(t)| \leq |B_2 N_{L/\mathbb{Q}}(T)|^{2(mn)^{-3}}. \tag{5.1.8}$$

Combining (5.1.7), (5.1.8), and (5.1.6) we obtain

$$|N_{L/\mathbb{Q}}(z)| \leq |N_{L/\mathbb{Q}}(T)|^{4(mn)^{-3}} \cdot \tfrac{1}{4} \cdot |N_{L/\mathbb{Q}}(T)|^{(mn)^{-2}}.$$

As this inequality cannot hold, we conclude for all $\tau \in \mathrm{Gal}(L/K)$ $\xi = \tau(\xi)$, i.e. $\xi \in K$.

Lemma 5.2 *Let $K \subset L$ be a Galois extension of number fields of degree 2, S, W finite sets of finite primes of K and L respectively such that $O_{L,W}$ is the integral closure of $O_{K,S}$ in L, and let $d \in O_L$, $d \neq 0$. Suppose the equalities*

$$x^2 - dy^2 = 1, \tag{5.2.1}$$

have infinitely many solutions in O_L and suppose there is an $e \in \mathbb{N}_0$ such that $\forall p \in W$, $\forall x, y \in O_{L,W}$ satisfying (5.2.1)

$$z = \frac{(x + yd^{1/2})^e + (x - yd^{1/2})^e}{2}, \tag{5.2.2}$$

$$T = \frac{(x + yd^{1/2})^e - (x - yd^{1/2})^e}{2d^{1/2}} \tag{5.2.3}$$

implies $z, T \in O_K$, *and* $\operatorname{ord}_p z = 0$. *Moreover, assume that for such a* z, T *the relationship*

$$N_{L/\mathbb{Q}}(z) \geq N_{L/\mathbb{Q}}(T) \tag{5.2.4}$$

is Diophantine over $O_{L,W}$, *and for every solution* $x - d^{1/2}y \in O_{L,W}$ *of* (5.2.1) *there exists a natural* m *such that for* $z - d^{1/2}T = (x - d^{1/2}y)^m$ (5.2.4) *is satisfied. Then* $O_{L,W}$ *is Diophantine over* $O_{K,S}$.

Proof: Let $\xi = (2P\omega^{2k} + 1)^h$, where P is the product of all the rational primes lying below S and W, $h = h(L)$, $k = \max_{p \in S}(\operatorname{ord}_p 2P)$, and consider equations (5.1.1)–(5.1.3), (5.2.1)–(5.2.4) together with

$$u^2 - dv^2 = 1, \tag{5.2.5}$$

$$zw = \frac{(u + vd^{1/2})^e + (u - vd^{1/2})^e}{2}. \tag{5.2.6}$$

Assume all the above listed equations are satisfied over $O_{L,W}$. Then, by our assumptions, $z, T, w \in K$, and we can apply Lemma 5.1 to conclude that $\xi \in O_{K,S}$.

On the other hand, if ω is a rational integer, and ξ is an odd rational integer, we can show that the above equations can be satisfied in $O_{L,W}$. Indeed, let $(x_0, y_0) \in O_L$ be such that $x_0 - d^{1/2}y_0$ is not a root of unity. Such a pair (x_0, y_0) exists by assumption that the set of solutions to (5.2.1) is infinite in O_L. Next, let $(x - d^{1/2}y) = (x_0 - d^{1/2}y_0)^r$, $r \in \mathbb{N}$, be such that $R_1 R_2$ as well as the left hand side of (5.1.2) divides y. This can be accomplished by Lemma 2.3. Next, let $(z - Td^{1/2}) = (x - d^{1/2}y)^{em}$, where m is selected so that (5.2.4) is satisfied. By Lemma 2.3, $y \mid_W T$, and consequently (5.1.2) and (5.1.3) will be satisfied. Finally, let

$$(u - vd^{1/2}) = (x - yd^{1/2})^{-\xi m} = (z - d^{1/2}T)^{-\xi/e}.$$

Then

$$\frac{(u + vd^{1/2})^e + (u - vd^{1/2})^e}{2z} = w \cong \xi \bmod z, \tag{5.2.7}$$

and we are done.

Finally, denote (5.1.1)–(5.1.3), (5.2.1)–(5.2.6) by $F(\xi, u, v, x, y, z, T, w)$. Next let $\xi_1 = (2P\omega^{2k} + 2P + 1)^h$, and note that $\forall p \in S \operatorname{ord}_p(2P\omega^{2k} + 2P + 1) = \min(\operatorname{ord}_p 2P\omega^{2k} + 1, \operatorname{ord}_p 2P) \leq 0$. Therefore, ξ_1 still satisfies conditions of Lemma 5.1. Next consider $F(\xi, u, v, x, y, z, w)$ together with $F(\xi_1, u_1, v_1, x_1, y_1, z_1, w_1)$. We now get $(2P\omega^{2k} + P + 1)^h$, $(2P\omega^{2k} + 1)^h \in O_{K,S}$. Since $K \subset L$ is an extension of degree 2, if $(2P\omega^{2k} + 1) \in L \setminus K$, then $(2P\omega^{2k} + 1) = ad^{1/2}$, where $a \in K$. But in this case $(2P\omega^{2k} + P + 1)^h$ cannot be in K, and we have a contradiction. Therefore, if $F(\xi, u, v, x, y, z, w)$ and $F(\xi_1, u_1, v_1, x_1, y_1, z_1, w_1)$ hold

at the same time, $\omega^{2^k} \in K$. Next write down the corresponding equations for $\omega + 1$. Then together with equations for ω they will assure that $\omega \in K$. On the other hand, if ω is a rational integer all the equations can be satisfied. Thus, if we use an integral basis of K over $\mathbb{Q}$ we can complete the Diophantine definition of $O_{K,S}$ over $O_{L,W}$.

Lemma 5.3 *If K is a totally real field, then $\exists d \in O_L$ such that the conditions of Lemma* 5.2 *are satisfied.*

Proof: Let $S = S_r \cup S_u$, where S_r consists of all the primes of S which ramify in L and S_u contains all the unramified primes. Let W_u and W_r be the primes of L above S_u and S_r respectively. Let $\sigma_1, \ldots, \sigma_z$ be all the embeddings of K into $\mathbb{C}$ not extending to real embeddings of L, and let $\sigma_{z+1}, \ldots, \sigma_n$ be the K-embeddings which extend to real embeddings of L. We can assume $z \geq 1$. Assume $d \in O_K$ has the following properties:

1. $\forall p \in S_u \ \mathrm{ord}_p d = 1$;
2. $\forall p \in S_r$ d is not a square mod p;
3. $\forall i = 1, \ldots, z \ \sigma_i(d) \geq 2^{2n}$;
4. $\forall i = z+1, \ldots, n \ \sigma_i(d) < -\frac{3}{4}$.

Let $L' = L(d^{1/2})$, $K' = K(d^{1/2})$ and let $\beta \in W_u$ lie above $p \in S_u$, then $\mathrm{ord}_\beta d = \mathrm{ord}_p d = 1$. On the other hand, let $\beta \in W_r$. Then $O_L/\beta \cong O_K/p$, where $p = \beta^2$. Therefore, if d is not a square mod p, it is not a square mod β. Therefore, in L' and K' the primes of W_u and S_u respectively will ramify, and primes of W_r and S_r respectively will remain prime. That is, primes of W and S will have only one prime each above them in L' and K' respectively. By Lemma 2.5, $H_{K,d,S}$ and $H_{L,d,W}$ will contain integral units only. (From the description of d, it follows that it is not a square of K or L.)

Moreover, by the same lemma, since for all the primes $p \in S_u$ and $\beta \in W_u$ $\mathrm{ord}_\beta d = \mathrm{ord}_p d = 1$, and it also follows that if $x - d^{1/2}y \in H_{L,d,W}$ then $\mathrm{ord}_\beta x \geq 0$, and $\mathrm{ord}_\beta y \geq 0$. On the other hand, taking into account the fact that primes from S_r, W_r do not divide d, consider $\{1, d^{1/2}\}$ as a basis for K' over K or L' over L. With the possible exception of the factors of 2, the discriminant of this basis is not divisible by any primes from S_r or W_r, and so it must be a local integral basis for these primes. Therefore x, y can fail to be integral at factors of 2 only if some factors of 2 ramify in the extension $K - L$.

To remedy the situation in this case, we consider a finite ring $O_{L'}/(2)$. Let r be the size of the multiplicative group of the ring. Since $x - d^{1/2}y$ is an integral unit, its equivalence class is invertible mod 2, and hence, if

$$z - d^{1/2}T = (x - d^{1/2}y)^r, \text{ where } x - d^{1/2}y \in H_{L,d,W},$$

then

$$z - d^{1/2}T \cong 1 \bmod 2,$$

$$z + d^{1/2}T \cong 1 \bmod 2,$$

$$2z \cong 0 \bmod 2,$$

$$\forall \gamma \mid 2 \text{ in } L' \ \mathrm{ord}_\gamma z \geq 0.$$

On the other hand, $2d^{1/2}T \cong 0 \bmod 2$ also and, as discussed above, the problem with a factor of 2 will occur only if it is ramified in the extension $K - L$ and by construction of d, it does not divide d. Therefore, T must be integral.

From the proof of the case (c) of the main theorem of [4] it follows that $H_{K,d,S}$ is of finite index i in $H_{L,d,W}$.

We also want to make sure that z is not divisible by any prime from W. Since primes of W_u divide d, z will not be divisible by them. To take care of the primes of W_r we can apply the same reasoning as was used to assure that z and T did not have negative orders at some factor of 2. Let ρ be the product of all the primes in W_r and consider $O_{L'}/2\rho$. Let k be the size of the multiplicative group of this ring and note that

$$(z + Td^{1/2}) = (x \pm d^{1/2}y)^k \cong 1 \bmod 2\rho.$$

Then $z \cong 1 \bmod \rho$. Finally, let $e = ikr$ and note

$$(z - d^{1/2}y) = (x - d^{1/2}y)^e,\ x - d^{1/2}y \in H_{L,d,W} \tag{5.3.1}$$

implies x, T are integral, $x, T \in K$, z is not divisible by any prime in W.

Next we would like to consider the issue of making (5.2.4) Diophantine. Assume (5.3.1) holds and let $\sigma_{i,j}$, $i = 1, \ldots, n$, $j = 1,2$ be all the embeddings of L into $\mathbb{C}$, with the old convention that σ_{ij} is an extension of K – embedding into $\mathbb{C}$ σ_i. Then

$$\sigma_{i1}(z) = \sigma_{i2}(z) = \sigma_i(z) \in \sigma_i(K) \subset \mathbb{R},$$

$$\sigma_{i1}(T) = \sigma_{i2}(T) = \sigma_i(T) \in \sigma_i(K) \subset \mathbb{R}.$$

By construction, $\forall i = 1, \ldots, z$ $\sigma_{i,j}(L)$ is not real, $\sigma_i(d) > 0$, and $\forall i = h + 1, \ldots, n$ $\sigma_{i,j}(L)$ is real, $\sigma_i(d) < 0$. In view of this, over $O_{L,W}$ consider (5.3.1) together with

$$\forall i = z + 1, \ldots, n\,|\sigma_{i,j}(z)| \geq \tfrac{1}{2}. \tag{5.3.2}$$

First of all, (5.3.2) can be made polynomial by Lemma 4.3. Secondly, by part 2 of Lemma 2.4, we can conclude that (5.3.1) and (5.3.2) imply that (5.2.4) holds. Conversely, by part 1 of Lemma 2.4, $\forall (x - d^{1/2}y) \in H_{K,d,S}\ \exists m \in \mathbb{N}_0$ such that if $z - Td^{1/2} = (x - d^{1/2}y)^m$, (5.3.2) holds. Therefore, assuming the above-described d exists we are done. The existence of the above described d follows from "The Very Strong Approximation Theorem" (see [7], p. 77).

Of all the number fields where Hilbert's Tenth Problem is known to be undecidable in the ring of algebraic integers, we have omitted only one case, that is, extensions of the form $\mathbb{Q} \overset{2}{-} K \overset{2}{-} L$, where K is not real. Unfortunately, in this case the methodology used in the previous cases does not yield the desired results.

REFERENCES

[1] Davis, M., "Hilbert's Tenth Problem is unsolvable," *American Mathematical Monthly*, vol. 80 (1973), pp. 233–269.

[2] Davis, M., Y. Matijasevich, and J. Robinson, "Positive aspects of a negative solution," pp. 323–378 in *Proceedings of the Symposium in Pure Mathematics*, American Mathematical Society, Providence, 1976.

[3] Denef, J., "Hilbert's Tenth Problem for quadratic rings," *Proceedings of the American Mathematical Society*, vol. 48 (1975), pp. 214–220.

[4] Denef, J. and L. Lipshitz, "Diophantine sets over some rings of algebraic integers," *Journal of the London Mathematical Society*, vol. 18 (1978), pp. 385–391.

[5] Denef, J., "Diophantine sets of algebraic integers, II," *Transactions of the American Mathematical Society*, vol. 257 (1980), pp. 227–236.

[6] Hardy, G. and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Clarendon Press, Oxford, 1960.

[7] O'Meara, O. T., *Introduction to Quadratic Forms*, second edition, Springer-Verlag, Berlin, 1971.

[8] Pheidas, T., "Hilbert's Tenth Problem for a class of rings of algebraic intergers," *Proceedings of the American Mathematical Society*, vol. 104 (1988), pp. 611–620.

[9] Shapiro, H. N. and A. Shlapentokh, "Diophantine relations between algebraic number fields," *Communications on Pure and Applied Mathematics*, vol. 42 (1989), pp. 1113–1122.

[10] Shlapentokh, A., "Extension of Hilbert's Tenth Problem to some algebraic number fields," *Communications on Pure and Applied Mathematics*, vol. 42 (1989), pp. 939–962.

[11] Shlapentokh, A., "Diophantine definitions for rings of rational numbers," forthcoming in *Communications on Pure and Applied Mathematics*.

Department of Mathematics
East Carolina University
Greenville, North Carolina 27858