IMRN International Mathematics Research Notices
2003, No. 7

A Ring Version of Mazur's Conjecture on Topology of Rational Points

Alexandra Shlapentokh

1 Introduction

The purpose of this paper is to explore a conjecture due to Barry Mazur and formulated for $\mathbb{Q}$, in a different setting. This conjecture, that is a part of a series of conjectures made by Mazur concerning topology of rational points, first appeared in [8], and consequently in [9, 10, 11]. It states the following.

Conjecture 1.1. Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components. (See [11, Conjecture 2, page 256].) □

Remark 1.2. Let W be an algebraic set defined over a number field. Then $W = V_1 \cup \cdots \cup V_k$, $k \in \mathbb{N}$, where V_i is a variety and $\bar{W} = \bar{V}_1 \cup \cdots \cup \bar{V}_k$, with $\bar{W}, \bar{V}_1, \ldots, \bar{V}_k$ denoting the topological closure of $W, V_1, \ldots, V_k$, respectively. Further, if $n_W, n_1, \ldots, n_k$ are the numbers of connected components of $\bar{W}, \bar{V}_1, \ldots, \bar{V}_k$, respectively and $n_i < \infty$ for all $i = 1, \ldots, k$, then $n_W \leq n_1 + \cdots + n_k$. Thus, without changing the scope of the conjecture we can apply Conjecture 1.1 to algebraic sets instead of varieties.

This conjecture has an important implication.

Conjecture 1.3. There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$. □

This implication has a great significance with respect to efforts to solve the analogue of Hilbert's tenth problem over $\mathbb{Q}$. The original Hilbert's tenth problem can be

Received 29 May 2002. Revision received 13 August 2002.
Communicated by Barry Mazur.

stated as follows: given an arbitrary polynomial equation in several variables over $\mathbb{Z}$, is there a uniform algorithm to determine whether such an equation has solutions in $\mathbb{Z}$? This question, known otherwise as Hilbert's tenth problem, has been answered negatively in the work of Davis, H. Putnam, Robinson, and Matijasevič (see [2, 3]). Since the time when this result was obtained, similar questions have been raised for other fields and rings. In other words, let R be a recursive ring. Then, given an arbitrary polynomial equation in several variables over R, is there a uniform algorithm to determine whether such an equation has solutions in R?

Arguably the two most interesting and difficult problems in the area concern $R = \mathbb{Q}$ and R equal to the ring of algebraic integers of an arbitrary number field.

One way to resolve the question of Diophantine decidability negatively over a ring of characteristic 0 is to construct a Diophantine definition of $\mathbb{Z}$ over such a ring. This notion is defined below.

Definition 1.4. Let R be a ring and let $A \subset R^k$, $k \in \mathbb{N}$. Then A has a Diophantine definition over R if there exists a polynomial $f(t_1, \dots, t_k, x_1, \dots, x_n) \in R[t_1, \dots, t_k, , x_1, \dots, x_n]$ such that for any $(t_1, \dots, t_k) \in R^k$,

$$\exists x_1, \dots, x_n \in R,\ f(t_1, \dots, t_k, x_1, \dots, x_n) = 0 \Longleftrightarrow (t_1, \dots, t_k) \in A. \tag{1.1}$$

In this case A is called a Diophantine subset of R^k. If the quotient field of R is not algebraically closed, we can allow a Diophantine definition to consist of several polynomials without changing the nature of the relation. (See [3] for more details.)

The usefulness of Diophantine definitions stems from the following easy lemma.

Lemma 1.5. Let $R_1 \subset R_2$ be two recursive rings such that the quotient field of R_2 is not algebraically closed. Assume that Hilbert's tenth problem (abbreviated as "HTP" in what follows) is undecidable over R_1, and R_1 has a Diophantine definition over R_2. Then HTP is undecidable over R_2. □

Diophantine definitions have been obtained for $\mathbb{Z}$ over the rings of algebraic integers of some number fields. Denef has constructed a Diophantine definition of $\mathbb{Z}$ for the finite-degree totally real extensions of $\mathbb{Q}$. Denef and Lipshitz extended Denef's results to the totally complex extensions of degree 2 of the finite-degree totally real fields. Pheidas and the author of this paper have independently constructed Diophantine definitions of $\mathbb{Z}$ for number fields with exactly one pair of nonreal conjugate embeddings. Finally, Shapiro and the author of this paper showed that the subfields of all the fields mentioned above "inherited" the Diophantine definitions of $\mathbb{Z}$. (These subfields include all the

abelian extensions.) The problem is still open for a general number field. The proofs of the results listed above can be found in [4, 5, 6, 12, 14, 15].

A similar approach can, in theory, be applied to $\mathbb{Q}$. In other words, one could show that HTP is undecidable over $\mathbb{Q}$ by showing that $\mathbb{Z}$ has a Diophantine definition over $\mathbb{Q}$. However, if Conjecture 1.1 is true, this way of solving the analogue of HTP for $\mathbb{Q}$ is not going to work. Further, as has been demonstrated in [1], the truth of Conjecture 1.1 would have even more drastic consequences for proving the undecidability of the analogue of HTP over $\mathbb{Q}$. More precisely, Cornelissen and Zahidi have shown that Conjecture 1.1 implies the absence even of a Diophantine model of $\mathbb{Z}$ in $\mathbb{Q}$. The ring version of the notion of Diophantine model is presented below.

Definition 1.6. Let R_1 and R_2 be countable recursive rings. Then R_2 has a Diophantine model of R_1 if for some $k \in \mathbb{N}$ there exists a computable injection $\phi : R_1 \to R_2^k$ such that for every Diophantine subset $D \subseteq R_1$, $\phi(D)$ is a Diophantine subset of R_2^k.

It is clear that Diophantine definitions provide examples of Diophantine models. In other words, if $R_1 \subset R_2$, both rings are computable and R_1 has a Diophantine definition over R_2, then R_2 has a Diophantine model of R_1 with ϕ being the identity mapping. Further, it is equally clear that if R_1 has undecidable Diophantine sets and R_2 has a Diophantine model of R_1, then R_2 also has undecidable Diophantine sets. Thus if a computable ring R has a Diophantine model of $\mathbb{Z}$, some of its Diophantine sets are not computable and the analogue of HTP has no solution over it. Unfortunately, if Conjecture 1.1 is true, the result of Cornelissen and Zahidi discussed above shows that we cannot use a construction of a Diophantine model to prove that HTP is undecidable over $\mathbb{Q}$. On the other hand, Pheidas [13] has recently proposed an approach which, if successful, will yield a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ and will therefore falsify Conjecture 1.1.

Given the difficulty of establishing whether Conjectures 1.1 and 1.3 are true over $\mathbb{Q}$ (and number fields in general), one might adopt a gradual approach: consider the conjectures over the rings of W-integers of $\mathbb{Q}$ and number fields in general. These rings are defined as follows.

Definition 1.7. Let M be a number field and let W be a set of its primes. Then a ring

$$O_{M,W} = \{x \in M \mid \operatorname{ord}_{\mathfrak{p}} x \geq 0 \ \forall \mathfrak{p} \notin W\} \tag{1.2}$$

is called a ring of W-*integers*. (The term W-integers usually presupposes that W is finite, but we will use this term for infinite W also.) If $W = \varnothing$, then $O_{M,W} = O_M$—the ring of algebraic integers of M. If W contains all the primes of M, then $O_{M,W} = M$.

We have made some progress over such rings with respect to Diophantine definitions of $\mathbb{Z}$. In particular, we have shown the following theorem.

Theorem 1.8. Let $K \neq \mathbb{Q}$ be a totally real number field or a totally complex extension of degree 2 of a totally real number field. Then for any $\varepsilon > 0$, there exists a set W of primes of K whose Dirichlet density is bigger than $1-[K:\mathbb{Q}]^{-1}-\varepsilon$ and such that $\mathbb{Z}$ has a Diophantine definition over $O_{K,W}$. (Thus, HTP is undecidable over $O_{K,W}$.) □

The proof of this theorem can be found in [16, 17, 19].

We can try to apply the same approach to Conjecture 1.1. First we will need to restate this conjecture for the rings in question.

2 A ring version of Mazur's conjecture

Notations 2.1. (i) For a number field K, let $\mathcal{P}(K)$ denote the set of all finite primes of K.

(ii) Let $V \subset \mathbb{C}^n$ be an algebraic set defined over a field K. Let $A \subseteq K$. Then let $V(A) = \{\bar{x} = (x_1, \ldots, x_n) \in V \cap A^n\}$.

Question 2.2. Let K be a number field and let W_K be a set of primes of K. Let V be any affine algebraic set defined over K. Let $\overline{V(O_{K,W_K})}$ be the topological closure of $V(O_{K,W_K})$ in $\mathbb{R}$ if $K \subset \mathbb{R}$ or in $\mathbb{C}$, otherwise. Then how many connected components does $\overline{V(O_{K,W_K})}$ have?

First of all, we can make the following simple observations.

Proposition 2.3. Let T_1 and T_2 be topological spaces. Consider $T = T_1 \times T_2$ under the product topology. Let $\pi : T \to T_1$ be a projection. Let $S \subset T$ be such that the topological closure $\overline{\pi(S)}$ of $\pi(S)$, has infinitely many components. Then the topological closure $\bar{S}$ of S has infinitely many components. □

Proof. First of all, observe that $\pi(\bar{S}) \subseteq \overline{\pi(S)}$, since a projection maps limit points to limit points. Thus, $\bar{S} \subseteq \pi^{-1}(\overline{\pi(S)})$. Therefore, if $\overline{\pi(S)} = \bigcup_{i\in I} C_i$, where I is infinite, C_i are closed, pairwise disjoint, and infinitely many C_i contain points of $\pi(S)$, then $\bar{S} = \bigcup_{i\in I}(\bar{S} \cap \pi^{-1}(C_i))$, that is $\bar{S}$, is a union of infinitely many nonempty pairwise disjoint closed sets. ■

Corollary 2.4. Suppose that for some ring R contained in a number field and for some affine variety V defined over the fraction field of R, $\overline{V(R)}$ has infinitely many connected components and R has a Diophantine definition over a ring $\tilde{R} \supset R$, where the fraction field of $\tilde{R}$ is a number field K. Then for some affine algebraic set W defined over K, $\overline{W(\tilde{R})}$ has infinitely many connected components. □

Proof. Let V be a variety as described in the statement of the proposition with infinitely many components of $\overline{V(R)}$. Let $g(t, \bar{y})$ be a Diophantine definition of R over $\tilde{R}$. Let $\{f_i(\bar{x}),\ \bar{x} = (x_1, \ldots, x_n),\ i = 1, \ldots, m\}$ be polynomials defining V. Then consider the following system:

$$\begin{aligned} &g(x_i, \bar{y}_i) = 0, \quad i = 1, \ldots, n, \\ &f_j(\bar{x}) = 0, \quad j = 1, \ldots, m. \end{aligned} \tag{2.1}$$

Let W be the algebraic set defined by this system. Note that projection of $W(\tilde{R})$ on $\bar{x}$-coordinates is precisely $V(R)$ and therefore the topological closure of $W(\tilde{R})$ in $\mathbb{R}$ or $\mathbb{C}$ will have infinitely many connected components. ■

Before we state the next corollary, we need the following proposition whose proof can be found in [18].

Proposition 2.5. Let K be a number field. Let $\mathfrak{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ be a finite set of non-archimedean primes of K. Then the set of elements of K integral at elements of $\mathfrak{P}$ has a Diophantine definition over K.

More generally, let W be any set of primes of K and let $S \subset W$, where S is finite. Then $O_{K,W\setminus S}$ has a Diophantine definition over $O_{K,W}$. □

Corollary 2.6. Let W and S be sets of finite primes of $\mathbb{Q}$, where $S = \mathcal{P}(\mathbb{Q}) \setminus W$ is finite. Suppose that Conjecture 1.1 holds over $\mathbb{Q}$. Let V be any variety defined over $\mathbb{Q}$. Then the real topological closure of $V(O_{\mathbb{Q},W})$ has finitely many connected components. □

Proof. By Proposition 2.5, $O_{\mathbb{Q},W}$ has a Diophantine definition over $\mathbb{Q}$. Therefore, we can apply Corollary 2.4 to reach the desired conclusion. ■

Proposition 2.7. Let R be a subring of a number field K such that for any variety V defined over K, the topological closure of $V(R)$ has finitely many connected components. Then no infinite discrete (in archimedean topology) subset of R has a Diophantine definition over R. In particular, no infinite subset of $\mathbb{Z}^n$, where n is a positive integer, has a Diophantine definition over R. □

Corollary 2.8. Let S be defined as in Corollary 2.6. Then there exists an affine variety U such that the real closure of $U(O_{\mathbb{Q},S})$ will have infinitely many components. □

Proof. By Proposition 2.5, $\mathbb{Z}$ has a Diophantine definition over $O_{\mathbb{Q},S}$. Therefore, we can apply Proposition 2.7 to reach the desired conclusion. ■

Thus if we allow finitely many primes in denominator, in the closure, we will have varieties over the resulting ring with infinitely many connected components. Similarly, if

Conjecture 1.1 is true and we remove a finite number of primes from the denominator, all the varieties over the resulting rings will have finitely many components only, in the closure. The natural question is then how many primes we can remove from the denominator before we see varieties with infinitely many components in the topological closure over the resulting rings. In this paper, we show that in case of totally real fields (including $\mathbb{Q}$), and their totally complex extensions of degree 2, we can remove sets of arbitrarily small positive density and get varieties with infinitely many connected components over the resulting rings. We have weaker results for complex fields with one pair of nonreal conjugate embeddings.

As has been mentioned above, Conjecture 1.1 implies that $\mathbb{Z}$ has no Diophantine definition over $\mathbb{Q}$. Also, as described in the introduction, we have been successful in constructing Diophantine definitions of $\mathbb{Z}$ over rings $O_{K,W}$, where K is a nontrivial totally real extension of $\mathbb{Q}$ or a totally complex extension of degree 2 of a totally real field and W is of density arbitrarily close to $1 - 1/[K : \mathbb{Q}]$. We do not have such a Diophantine definition over $\mathbb{Q}$ and over number fields with one pair of nonreal conjugate embeddings. However, by looking at a stronger conjecture, we are able to construct "counterexamples" over these fields also.

3 Equations with infinite discrete solution sets

Lemma 3.1. Let K be a number field. Let $W_K \subset \mathcal{P}(K)$ be such that for some finite extension M of K all the primes of W_K remain prime in the extension M/K. Let W_M be the set of all the M-primes above the primes of W_K. Then all the solutions $x \in O_{M,W_M}$ to the equation

$$\mathbf{N}_{M/K}(x) = 1 \tag{3.1}$$

are integral units. □

Proof. Let $\mathfrak{p}$ be a prime occurring in the numerator of the divisor of x in M. Then, since the divisor of the norm is trivial, a K-conjugate of $\mathfrak{p}$ must appear in the denominator of the divisor. Thus $\mathfrak{p}$ must lie above a prime of K splitting in the extension M/K. On the other hand, since $x \in O_{M,W_M}$, the only primes of M which can appear in the denominator of x are primes of W_M. But primes of W_M lie above primes of W_K which do not split in the extension M/K. Thus, the divisor of x has no primes in the numerator. A similar argument shows that the divisor of x has no primes in the denominator. Hence, x is an integral unit. ■

Lemma 3.2. Let M be any finite extension of $\mathbb{Q}$ of degree $n > 2$. Let $W_{\mathbb{Q}} \subset \mathcal{P}(\mathbb{Q})$ be a set of $\mathbb{Q}$-primes not splitting in the extension $M/\mathbb{Q}$. Let $\{\omega_1, \ldots, \omega_n\} \subset O_M$ be an integral basis

of M over $\mathbb{Q}$. Let $\{\omega_{i,j},\ j=1,\dots,n\}$, $\omega_{i,1}=\omega_i$, be all the conjugates of ω_i over $\mathbb{Q}$. Then all the solutions $(a_1,\dots,a_n)\in O_{\mathbb{Q},W_{\mathbb{Q}}}$ to

$$\prod_{j=1}^{n}\sum_{i=1}^{n}a_i\omega_{i,j}=1 \tag{3.2}$$

are actually in $\mathbb{Z}$. Furthermore, the set of these solutions is infinite. □

Proof. Let W_M contain all the M-primes lying above primes of $W_{\mathbb{Q}}$. Then $x=\sum_{i=1}^{n}a_i\omega_i\in O_{M,W_M}$. Further, the set $\{x_j=\sum_{i=0}^{n}a_i\omega_{i,j},\ j=1,\dots,n\}$ contains all the conjugates of $x=x_1$ over $\mathbb{Q}$. Thus, (3.2) is equivalent to (3.1), with $K=\mathbb{Q}$. Therefore, if $x=\sum_{i=1}^{n}a_i\omega_i$ is a solution to (3.2), then x is an integral unit of M. Since $\{\omega_1,\dots,\omega_n\}$ is an integral basis, we must conclude that $a_i\in\mathbb{Z}$. Conversely, if $x=\sum_{i=0}^{n}a_i\omega_i$ is a square of any integral unit of M, then $(a_1,\dots,a_n)$ are solutions to this equation. Since we assumed the degree of the extension to be greater than 2, we can conclude that by Dirichlet unit theorem (see [7, Theorem 11.19, page 61]), the unit group of M is of rank at least 1, and the solution set of (3.2) is infinite in $\mathbb{Z}^n$. ■

Proposition 3.3. For any $\varepsilon>0$, there exists a set of rational primes $W_{\mathbb{Q}}$ such that Dirichlet density of $W_{\mathbb{Q}}$ is greater than $1-\varepsilon$ and there exists a variety V defined over $\mathbb{Q}$ such that the topological closure of $V(O_{\mathbb{Q},W_{\mathbb{Q}}})$ in $\mathbb{R}$ has infinitely many connected components. □

Proof. It is enough to take M to be a cyclic extension of prime degree greater than ε^{-1}. Then by Chebotarev density theorem (see [7, Theorem 10.4, page 182]), the set of primes splitting in the extension $M/\mathbb{Q}$ has density less than ε and we can apply Lemma 3.2 and Proposition 2.7. ■

To prove our results concerning totally real number fields and their totally complex extensions of degree 2, we need the following results from [19].

Proposition 3.4. Let L be any totally real field. Let M be the Galois closure of L over $\mathbb{Q}$. Let K be a cyclic extension of $\mathbb{Q}$ of prime degree p not dividing $[M:\mathbb{Q}]$. Let W_L^K be a set of primes of L remaining prime in the extension KL/L. Then there exists a set of L-primes $\bar{W}_L^K$ such that the set $(W_L^K\setminus\bar{W}_L^K)\cup(\bar{W}_L^K\setminus W_L^K)$ is finite and $O_{L,\bar{W}_L^K}\cap\mathbb{Q}$ has a Diophantine definition over $O_{L,\bar{W}_L^K}$. □

Proposition 3.5. Let L be a totally real field and let $d\in L$ be such that d and all of its conjugates over $\mathbb{Q}$ are negative. Let $K,F_1,\dots,F_{[L(\sqrt{d}):\mathbb{Q}]}$ be totally real cyclic extensions of $\mathbb{Q}$ of distinct odd prime degrees not dividing $[L:\mathbb{Q}]$. Let $W_{L(\sqrt{d})}$ be a set of primes of $L(\sqrt{d})$

not splitting in the extensions $F_u L(\sqrt{d})/L(\sqrt{d})$, $u = 1, \ldots, [L(\sqrt{d}) : \mathbb{Q}]$ and $KL(\sqrt{d})/L(\sqrt{d})$. Assume also that $p = [KL : L] = [KL(\sqrt{d}) : L(\sqrt{d})]$ does not divide the degree of the Galois closure of L over $\mathbb{Q}$. Then there exists a set of $L(\sqrt{d})$-primes $\bar{W}_{L(\sqrt{d})}$ such that $(W_{L(\sqrt{d})} \setminus \bar{W}_{L(\sqrt{d})}) \cup (\bar{W}_{L(\sqrt{d})} \setminus W_{L(\sqrt{d})})$ is finite and $O_{L(\sqrt{d}),\bar{W}_{L(\sqrt{d})}} \cap \mathbb{Q}$ has a Diophantine definition over $O_{L(\sqrt{d}),\bar{W}_{L(\sqrt{d})}}$. □

Theorem 3.6. Let L be a totally real field or a totally complex extension of degree 2 of a totally real field. Then for any $\varepsilon > 0$ there exists a set of primes $W_L \subset \mathcal{P}(L)$ such that Dirichlet density of W_L is greater than $1 - \varepsilon$ and there exists an affine algebraic set V defined over L such that $\overline{V(O_{L,W_L})}$ has infinitely many connected components. □

Proof. Since we have dealt with the case of $L = \mathbb{Q}$ already, we can assume that L is a nontrivial extension of $\mathbb{Q}$. We consider the case of totally real fields first. Let L, K, W_L^K, p be as described in Proposition 3.4 with the additional assumption that $p > \varepsilon^{-1}$ and W_L^K contains *all* the primes of L not splitting in the extension KL/L. Observe that under this assumption the density of the set of all L primes not splitting in the extension KL/L is greater than $1 - \varepsilon$. Removing and/or adding finitely many primes to W_L^K to form $\bar{W}_L^K$, as in Proposition 3.4, will not change the density. Let $W_{\mathbb{Q}}^K$ be the set of all the rational primes below the primes of W_L^K such that for every $q \in W_{\mathbb{Q}}^K$, W_L^K contains all the factors of q in L, and note that due to our assumption on p, primes of $W_{\mathbb{Q}}^K$ do not split in the extension $K/\mathbb{Q}$. Note also that $O_{L,W_L^K} \cap \mathbb{Q} = O_{\mathbb{Q},W_{\mathbb{Q}}^K}$. Let $\bar{W}_{\mathbb{Q}}^K$ be the set of all the rational primes below the primes of $\bar{W}_L^K$ such that for every $q \in \bar{W}_{\mathbb{Q}}^K$, $\bar{W}_L^K$ contains all the factors of q in L. Again we observe that $\mathbb{Q} \cap O_{L,\bar{W}_L^K} = O_{\mathbb{Q},\bar{W}_{\mathbb{Q}}^K}$. Finally let $\tilde{W}_{\mathbb{Q}}^K = \bar{W}_{\mathbb{Q}}^K \cap W_{\mathbb{Q}}^K$. By construction, $\tilde{W}_{\mathbb{Q}}^K$ can differ from $\bar{W}_{\mathbb{Q}}^K$ by finitely many primes only. Now note that by Propositions 3.4 and 2.5, $O_{\mathbb{Q},\tilde{W}_{\mathbb{Q}}^K}$ has a Diophantine definition over $O_{L,\bar{W}_L^K}$. Indeed, Proposition 3.4 tells us that $O_{\mathbb{Q},\bar{W}_{\mathbb{Q}}^K}$ has a Diophantine definition over $O_{L,\bar{W}_L^K}$ and Proposition 2.5 provides a Diophantine definition of $O_{\mathbb{Q},\tilde{W}_{\mathbb{Q}}^K}$ over $O_{\mathbb{Q},\bar{W}_{\mathbb{Q}}^K}$. On the other hand, by Lemma 3.2, there exists an infinite set of rational integers Diophantine over $O_{\mathbb{Q},\tilde{W}_{\mathbb{Q}}^K}$ and thus over $O_{L,\bar{W}_L^K}$. Now let $W_L = \bar{W}_L^K$ and the first part of the theorem follows from Proposition 2.7.

The case of L being a totally complex extension of degree 2 of a totally real field is handled in a similar manner using Proposition 3.5. The only observation that is needed here is that we should select K and $F_1, \ldots, F_{[L(\sqrt{d}):\mathbb{Q}]}$ so that $[K : \mathbb{Q}]^{-1} + \sum_u [F_u : \mathbb{Q}]^{-1} < \varepsilon$. ■

We now turn our attention to extensions with one pair of nonreal conjugate embeddings. There we do not have results analogous to Propositions 3.4 and 3.5, but we do know that rational integers have a Diophantine definition over the rings of integers of these fields. (See [12, 15].) We will use an approach utilized in the above cited result to prove the following theorem.

Theorem 3.7. Let K be a nonreal number field with exactly one pair of nonreal conjugate embeddings. Then there exists a set $W_K \subset \mathcal{P}(K)$ such that the Dirichlet density of W_K is $1/2$ and for some affine variety V defined over K, $\overline{V(O_{K,W_K})}$ has infinitely many connected components. □

Proof. Let $a \in O_K$ be such that all the real conjugates of a are less than 1. (Such an a exists by the strong approximation theorem.) Let $M = K(\sqrt{a^2-1})$ be a totally complex extension of degree 2 of K. Note that the density of the set of K-primes not splitting in the extension M/K is exactly $1/2$ by Chebotarev density theorem. So let $W_K \subset \mathcal{P}(K)$ be the set of primes not splitting in the extension M/K. Let W_M be the set of M-primes above the primes of W_K and observe that by Lemma 3.1 all the solutions to the norm equation $\mathbf{N}_{M/K}(z) = 1$ in O_{M,W_M} are algebraic integers. However in this case we can say a little bit more. A calculation of the ranks of the integral unit groups of M and K leads us to conclude that solutions to this norm equation form a multiplicative group of rank 1. If we select a to be such that $|a| > 2^{[K:\mathbb{Q}]}$, while all the real conjugates of a are less than one-half in absolute value, then all the solutions to the norm equation modulo roots of unity will be powers of $\mu = a - \sqrt{a^2-1}$. (See the references cited above for more details.) Note that either μ or μ^{-1} is of absolute value greater than 1. Otherwise μ will be a root of unity. Indeed, if $\sigma : K \to \mathbb{R}$ is a real embedding of K and $\sigma(x)^2 - (\sigma(a)^2 - 1)\sigma(y)^2 = 1$ for some $x, y \in K$, then $\sigma(x) - \sqrt{\sigma(a)^2-1}\sigma(y)$ is of absolute value equal to 1, given our assumption that $|\sigma(a)| < 1$. Further, if $|\mu| = |a - \sqrt{a^2-1}| = |\mu^{-1}| = |a + \sqrt{a^2-1}| = 1$, then $|\bar{\mu}| = |\bar{a} \pm \sqrt{\bar{a}^2-1}| = 1$, and therefore, indeed μ is an absolute unit—a root of unity.

Assume, without loss of generality, that $|\mu| > 1$ and let $\mu^{rk} = x_k - \sqrt{a^2-1}y_k$ for some sufficiently large r such that $|\mu^{rk}| > 2^k$. Then $|x_k| = |(\mu^{rk} + \mu^{-rk})/2| > (2^k - 1)/2$. Therefore, for any $l \in \mathbb{N}$, any neighborhood U of x_l, there exist only finitely many $m \in \mathbb{N}$ such that $x_m \in U$. In other words, the set

$$\begin{aligned}\{x \in O_{K,W_K} \mid &\exists x_0, y_0, y \in O_{K,W_K}, \\ &x - \sqrt{a^2-1}y = \left(x_0 - \sqrt{a^2-1}y_0\right)^r,\ x_0^2 - \left(a^2-1\right)y_0^2 = 1\}\end{aligned} \tag{3.3}$$

is discrete and the assertion of the theorem follows from Proposition 2.7. ■

4 Some questions

We would like to finish the paper with some obvious questions arising from the discussion above.

Question 4.1. Is there a set $W_{\mathbb{Q}}$ of rational primes of Dirichlet density equal to one such that for some affine variety V defined over $\mathbb{Q}$, $\overline{V(O_{\mathbb{Q},W_{\mathbb{Q}}})}$ has infinitely many connected

components? Note that the answer to this question is not necessarily going to be the resolution of the status of Conjecture 1.1, if $\mathcal{P}(\mathbb{Q}) \setminus W_{\mathbb{Q}}$ is infinite.

Question 4.2. Let K be an arbitrary number field, let O_K be the ring of its integers. Then is there an affine variety V defined over K, such that $\overline{V(O_K)}$ has infinitely many connected components? (In particular, we are interested in number fields which are not totally complex extensions of degree 2 of totally real fields and have at least two pairs of nonreal embeddings into $\mathbb{C}$.)

Here we should note the following. If $\mathbb{Z}$ is to have a Diophantine definition over a ring of integers of an arbitrary number field, then the answer would have to be "yes." Thus, if the answer to this question is "no" for some number fields, then the situation with the respect to resolving HTP over the rings of algebraic integers of number fields is just as serious as it is over $\mathbb{Q}$. Indeed, we can modify slightly the argument of Cornelissen and Zahidi [1] to show the following.

Proposition 4.3. Let K be a number field and assume that for any affine variety V defined over K, $\overline{V(O_K)}$ has finitely many connected components. Then O_K does not have a Diophantine model of $\mathbb{Z}$. (Since discussion of a Diophantine model entails a discussion of a computable map from $\mathbb{Z}$ to $(O_K)^k$, $k \in \mathbb{N}$, one must specify a computable presentation of O_K. This is done below.) □

Proof. We start with specifying a computable presentation of K. Let α be an integral generator of K over $\mathbb{Q}$. Let $f(T)$ be its monic irreducible polynomial over $\mathbb{Q}$. If α is real, then let $a_1 < b_1 \in \mathbb{Q}$ be such that $\alpha \in (a_1, b_1)$ and $[a, b]$ contains no other real root of f. If α is not real, let $a_1 < b_1, a_2 < b_2 \in \mathbb{Q}$ be such that $\alpha \in \{z \in \mathbb{C} \mid \Re z \in (a_1, b_1),\ \Im z \in (a_2, b_2)\}$ and $\{z \in \mathbb{C} \mid \Re z \in [a_1, b_1],\ \Im z \in [a_2, b_2]\}$ contains no other root of f. We represent every element of K as a linear combination of the elements of the power basis of α with rational coefficients. It is not hard to see that under this presentation, K and O_K are recursive as sets and all the field operations are represented by total computable functions. Further, from these data one can compute effectively the decimal expansion of α if it is real, and the decimal expansions of its real and imaginary parts if α is not real. Finally, given decimal expansions for α, we can effectively produce the corresponding decimal expansion for any element of the field presented by its coordinates with respect to the power basis of α.

Assume now that O_K has a Diophantine model of $\mathbb{Z}$. This means that for some $k \in \mathbb{N}$, there exists an injective and computable function $\phi : \mathbb{Z} \hookrightarrow D \subset (O_K)^k$ under the presentation described above, such that D is a Diophantine subset of $(O_K)^k$ and ϕ-image of every Diophantine subset of $\mathbb{Z}$ is Diophantine over $(O_K)^k$. Let $P(x_1, \ldots, x_k, t_1, \ldots, t_m)$

be a Diophantine definition of D over $(O_K)^k$. Let $V = \{(x_1, \ldots, x_k, t_1, \ldots, t_m) \in (O_K^k) \mid P(x_1, \ldots, x_k, t_1, \ldots, t_m) = 0\}$ and consider the map

$$f : V(O_K) \longrightarrow (O_K)^k \tag{4.1}$$

implemented by projection on the first k coordinates. Note that $f(V) = D$. By assumption and by Proposition 2.3, $\bar{D}$ will have finitely many connected components. Since D has infinitely many points, for at least one connected component C of $\bar{D}$, $C \cap D$ must have more than one point, and projection of C onto one of the coordinates if K is real, or on the imaginary or real part of one of the coordinates, if K is not real, will contain an interval whose endpoints are rational numbers. Let a be the left endpoint of this interval and let l be its length. Let $d_n = s \circ \phi(n)$, where s is either projection on the coordinate described above, or the real part or the imaginary part of the projection, as necessary, and let

$$\tilde{Z} = \left\{ n \in \mathbb{Z} \mid a + \frac{l}{2j+1} \leq d_n \leq a + \frac{l}{2j},\ j \in \mathbb{Z}^+ \right\}. \tag{4.2}$$

Since ϕ is computable and we can compute effectively decimal expansions for real and (if necessary) imaginary parts of all the elements of O_K, $\tilde{Z}$ is recursively enumerable and therefore $\tilde{Z}$ is a Diophantine subset of $\mathbb{Z}$ by the result of Matijasevič, Robinson, Davis, and Putnam. Further, $s(D) \cap [a, a+l]$ is dense in $[a, a+l]$. Indeed, $[a, a+l] \subseteq s(C) \subset s(\bar{D})$. Since D is dense in $\bar{D}$ and projection maps dense subsets into dense subsets, our claim is true. Thus, any interval $[a + l/(2j+1), a + l/2j]$ will have infinitely many points from $s(D)$ and therefore elements d_n, $n \in \tilde{Z}$ by definition of $\tilde{Z}$. Let $\tilde{D} = \{\phi(n) \mid n \in \tilde{Z}\}$. Then $\tilde{D}$ has a Diophantine definition over $(O_K)^k$ as the ϕ-image of a Diophantine subset of $\mathbb{Z}$. Let $\tilde{P}(x_1, \ldots, x_k, t_1, \ldots, t_m)$ be a Diophantine definition of $\tilde{D} = \phi(\tilde{Z})$, and let $\tilde{V}$ be the algebraic set defined by $\tilde{P}(x_1, \ldots, x_k, t_1, \ldots, t_m) = 0$. Then $s \circ f$, the projection from $\tilde{V}$ on the first k coordinates combined with projection onto a real or imaginary part of a coordinate chosen as above will produce a projection of $\tilde{V}$ onto set whose closure has infinitely many components. Thus, $\tilde{V}$ must have infinitely many components giving an affirmative answer to Question 4.2 in contradiction of our assumptions for this proposition. ■

Acknowledgments

The research for this paper has been partially supported by National Science Foundation (NSF) grant DMS-9988620 and East Carolina University Faculty Senate Research grant. The author would also like to thank Michael Fried and Aharon Razon for helpful comments.

References

[1] G. Cornelissen and K. Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (J. Denef, L. Lipshitz, T. Pheidas, and J. Van Geel, eds.), Contemp. Math., vol. 270, American Mathematical Society, Rhode Island, 2000, pp. 253–260.

[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*, Mathematical Developments Arising from Hilbert Problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), American Mathematical Society, Rhode Island, 1976, pp. 323–378.

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

[5] ———, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236.

[6] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391.

[7] G. J. Janusz, *Algebraic Number Fields*, Pure and Applied Mathematics, vol. 55, Academic Press, New York, 1973.

[8] B. Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45.

[9] ———, *Questions of decidability and undecidability in number theory*, J. Symbolic Logic **59** (1994), no. 2, 353–371.

[10] ———, *Speculations about the topology of rational points: an update*, Astérisque (1995), no. 228, 165–182.

[11] ———, *Open problems regarding rational points on curves and varieties*, Galois Representations in Arithmetic Algebraic Geometry (Durham, 1996) (A. J. Scholl and R. L. Taylor, eds.), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge University Press, Cambridge, 1998, pp. 239–265.

[12] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620.

[13] ———, *An effort to prove that the existential theory of* $\mathbf{Q}$ *is undecidable*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (J. Denef, L. Lipshitz, T. Pheidas, and J. Van Geel, eds.), Contemp. Math., vol. 270, American Mathematical Society, Rhode Island, 2000, pp. 237–252.

[14] H. N. Shapiro and A. Shlapentokh, *Diophantine relationships between algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 8, 1113–1122.

[15] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939–962.

[16] ———, *Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator*, Invent. Math. **129** (1997), no. 3, 489–507.

[17] ———, *Defining integrality at prime sets of high density in number fields*, Duke Math. J. **101** (2000), no. 1, 117–134.

[18] ———, *Hilbert's tenth problem over number fields, a survey*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (J. Denef, L. Lipshitz, T. Pheidas, and J. Van Geel, eds.), Contemp. Math., vol. 270, American Mathematical Society, Rhode Island, 2000, pp. 107–137.

[19] ———, *On Diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree* 2, to appear.

Alexandra Shlapentokh: Department of Mathematics, East Carolina University, Greenville, NC 27858, USA

E-mail address: shlapentokha@mail.ecu.edu